Robustel

Application Note

OpenVPN Client with Pre-shared key for R3000

Document Name:	**Application Note**
Version:	**v1.0.0**
Date:	**2014-05-30**
Status:	**Confidential**
DocID:	**RT_AN003_R3000 S_OpenVPN Client with Pre-shared key for R3000**

Contents

Chapter 1. Introduction

1.1 Overview

OpenVPN is an open source project with the GPL license agreement, complete solution characteristics of SSL VPN, can provide solutions which contain the VPN between site-to-site, WIFI security and enterprise remote access. OpenVPN permit to establish VPN that use the pre-shared key, the third party certificate or username/password to authenticate.

This application note is written for customer who has good understanding Robustel products and experienced with OpenVPN. It shows customer how to configure and test the OpenVPN between the R3000 and Windows OpenVPN server through the cellular network.

1.2 Assumptions

OpenVPN feature has been fully test and this Application Note is written by technically competent engineer who is familiar with Robustel products and the application requirement.
This Application Note is basing on:

- Product Model: Robustel GoRugged R3000 industrial cellular VPN router.
- Firmware Version: R3000_S_V1.01.01.fs.
- Software required: OpenVPN 2.2.2
- Configuration: This Application Note assumes the Robustel products are set to factory default. Most configure steps are only shown if they are different from the factory default settings. The Internet is connecting and there is no firewall feature enable.

  R3000's cellular WAN could be dynamic or static, public or "private with NAT" IP address. OpenVPN is certificate based, but we using pre-shared key for authentication at this time. A PC will be install the OpenVPN Easy-RSA certificate authority and create & sign the certificates. Any Easy-RSA is free and simple to use.

1.3 Rectifications

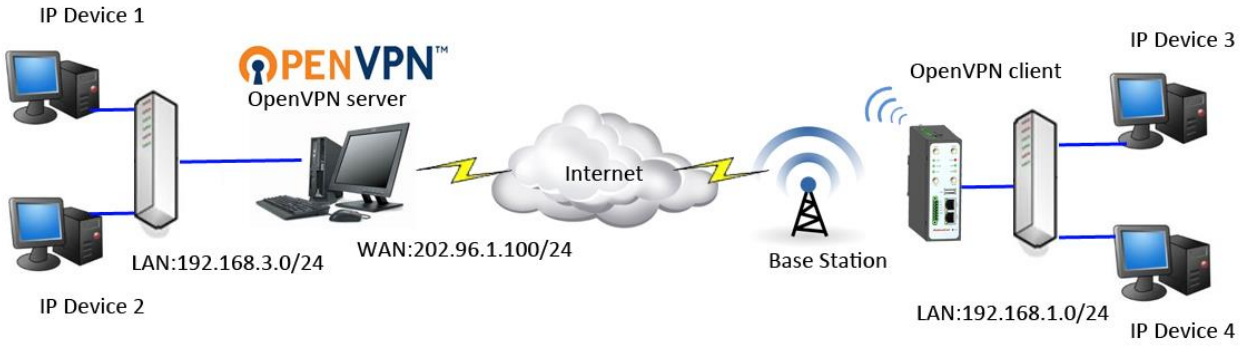
Appreciate for the corrections and Rectifications to this Application Note, and if there are requests for new Application Notes please also send to email address: support@robustel.com .

1.4 File Version

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

Release Date	Firmware Version	Details
2014-05-26	V1.01.01	First Release

Chapter 2. Application Topology



1. The PC run as OpenVPN server should have a fixed public IP address and open the specify port of OpenVPN.
2. Another R3000 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 established between server and client. It is a typical application for Point-to-Point connection.

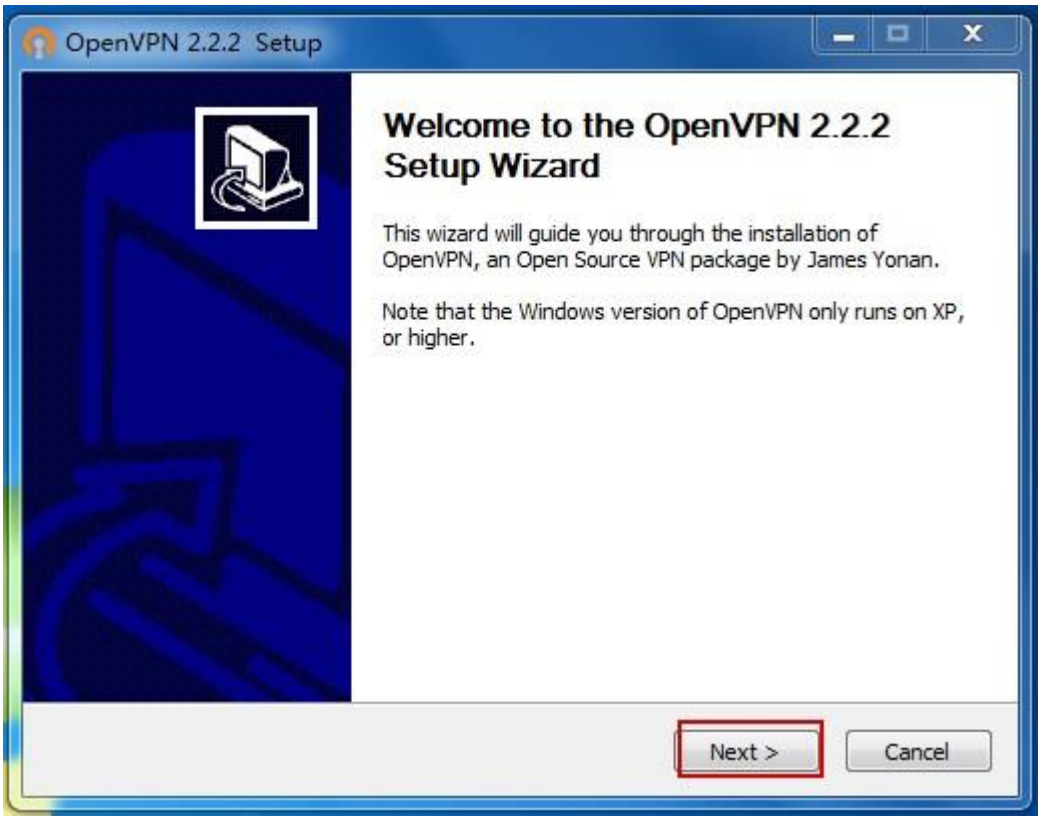
Note: *if the server behind a Gateway Router, the Router must open the port of 1194 and do port forwarding to the internal server.*

Chapter 3. Configuration

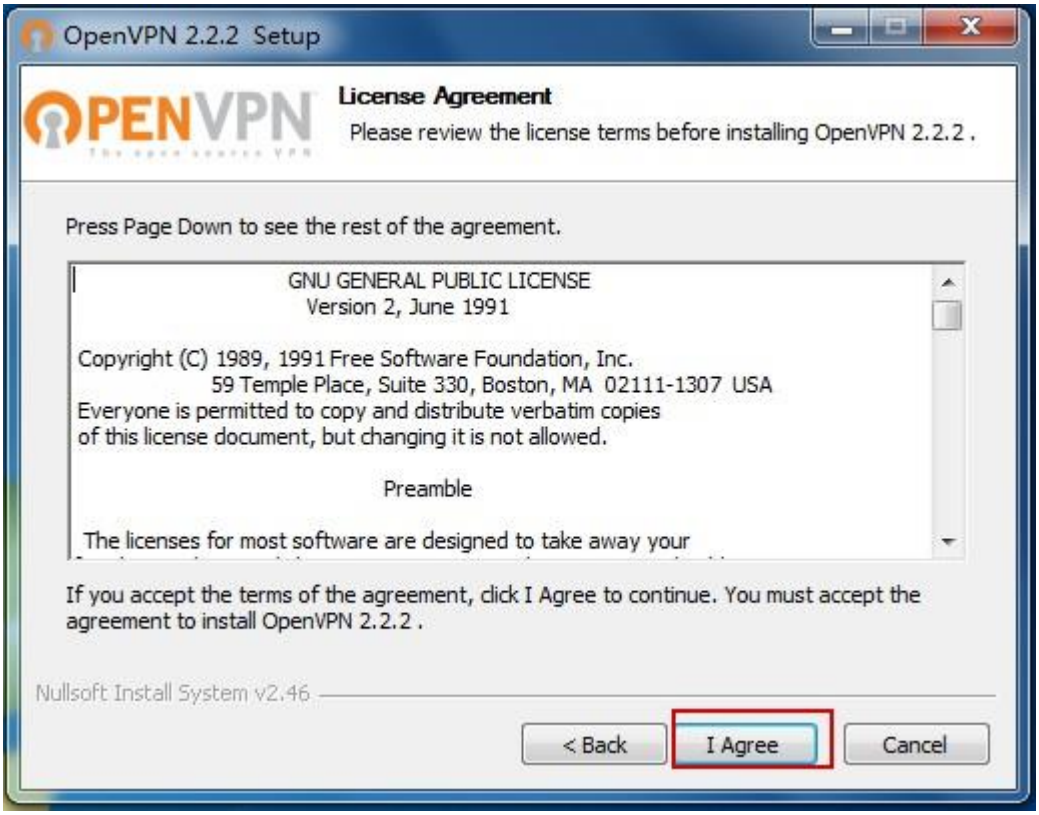
3.1 OpenVPN Installation on Windows

This step should be done on a PC that will be used to create certificates, this can be the OpenVPN server. The download is available from: **http://openvpn.net/index.php**

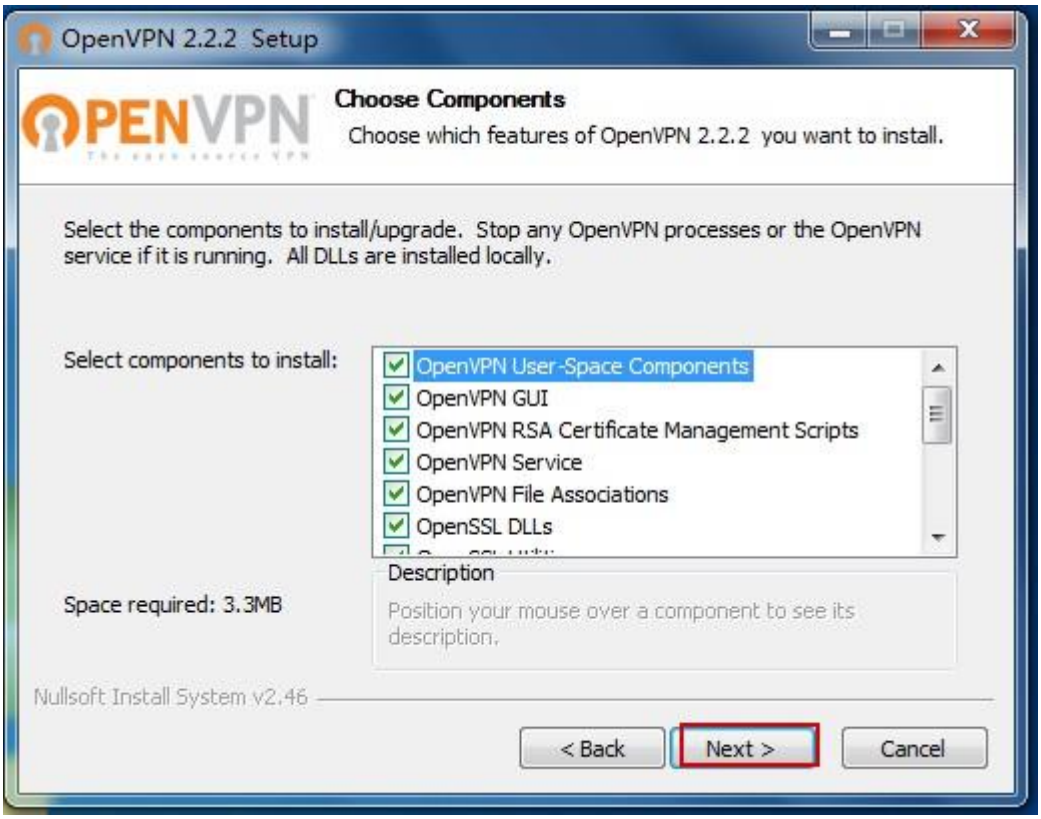
1. Download the release of the Windows installer. Run the installation program.



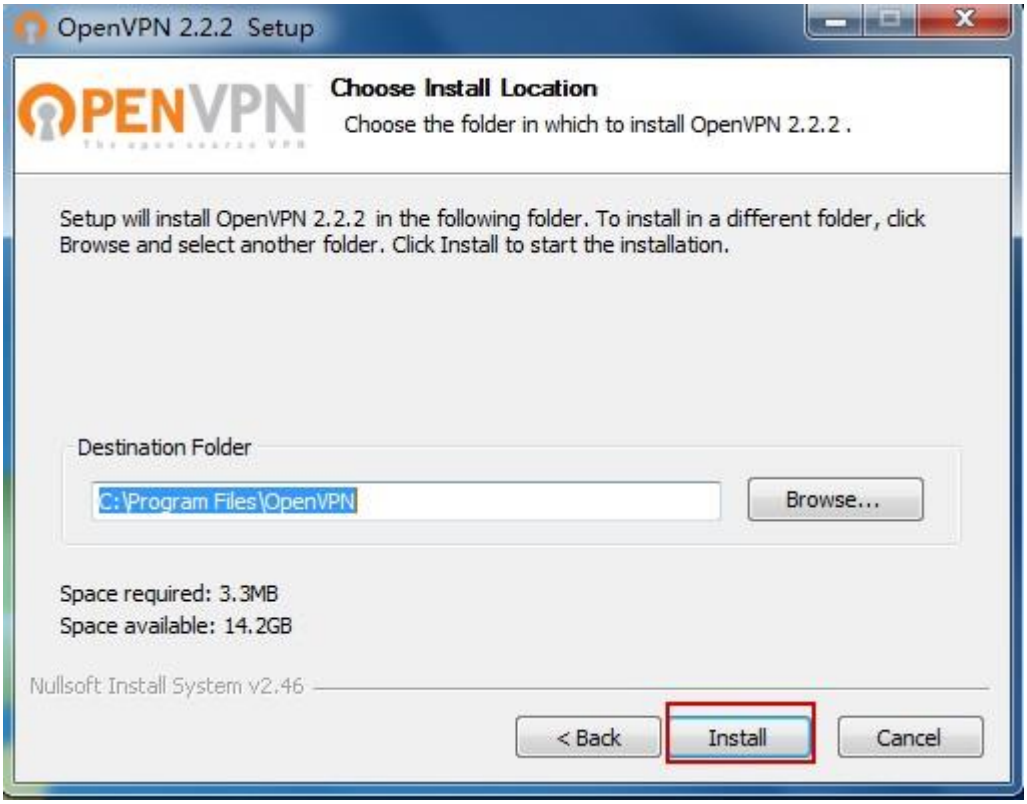
2. License Agreement.



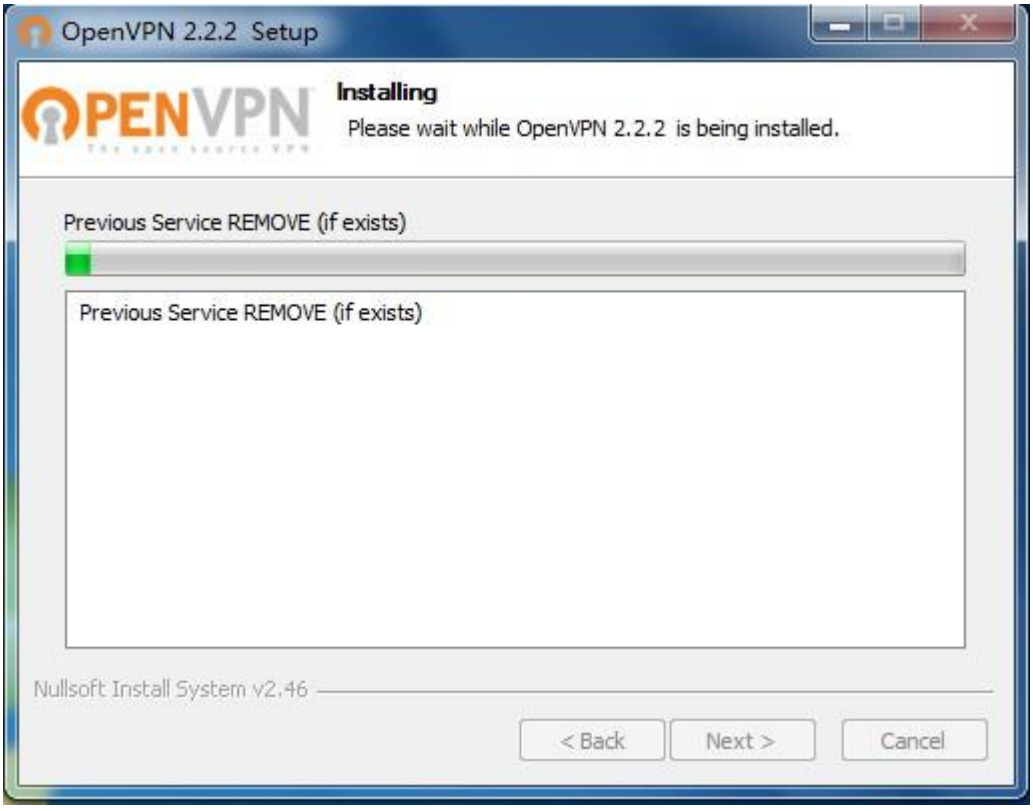
3. Select all the options by default.



4. Select the installation path. Save in default Destination Folder.

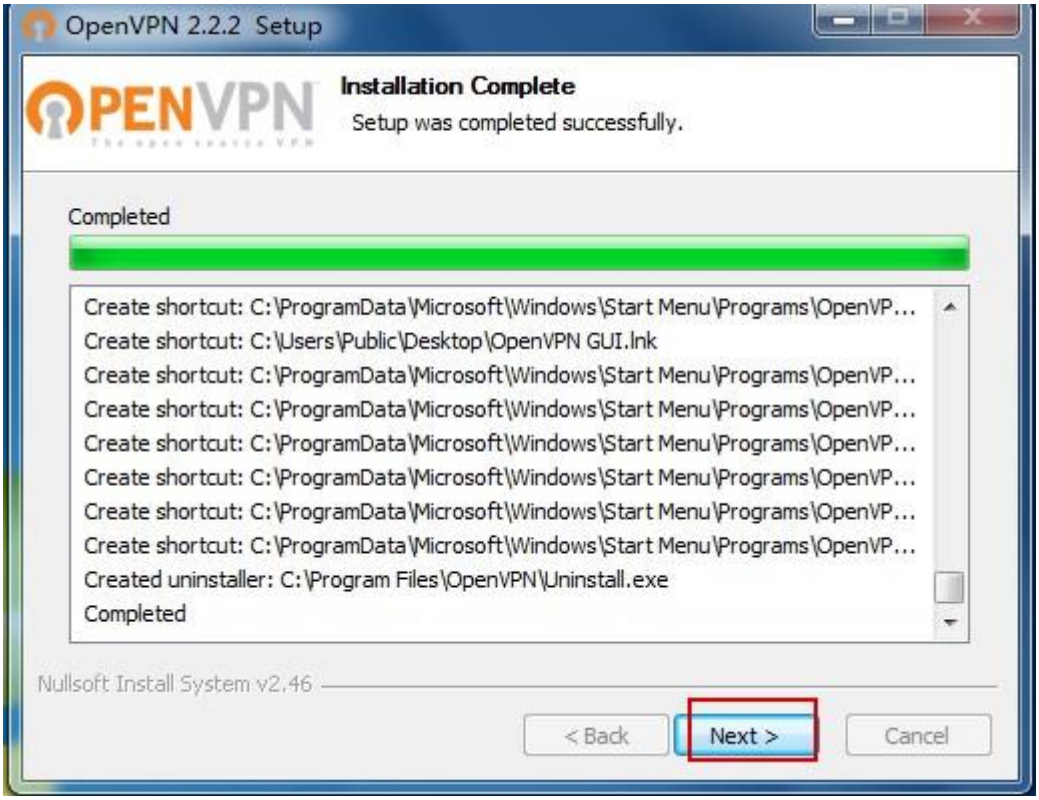


5. The installation schedule.



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

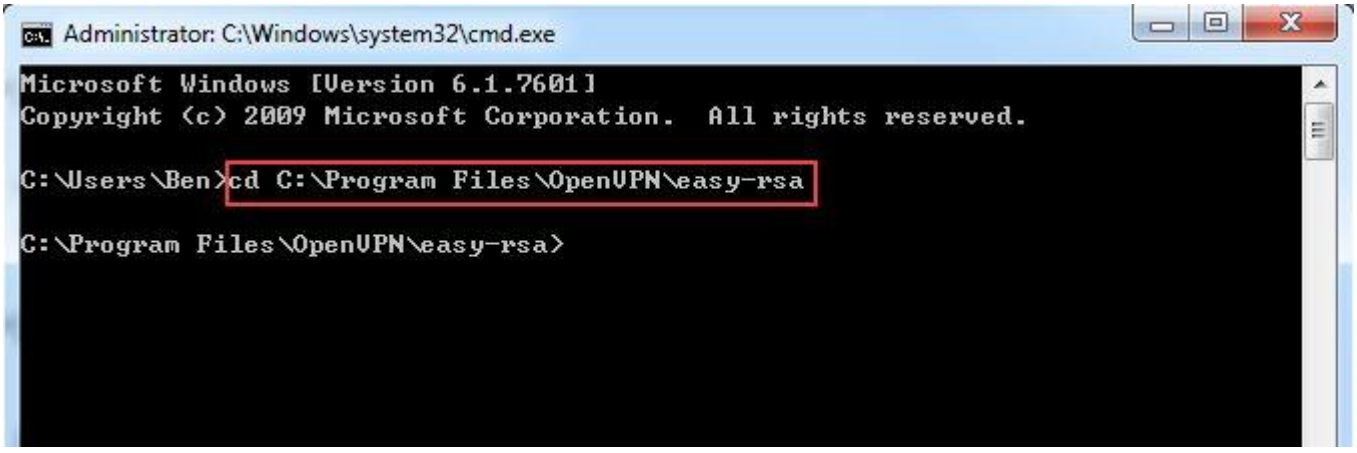
7. The installation will be completed.



8. Click “Finish” button and complete the installation.

3.2 Initialize environment for OpenVPN

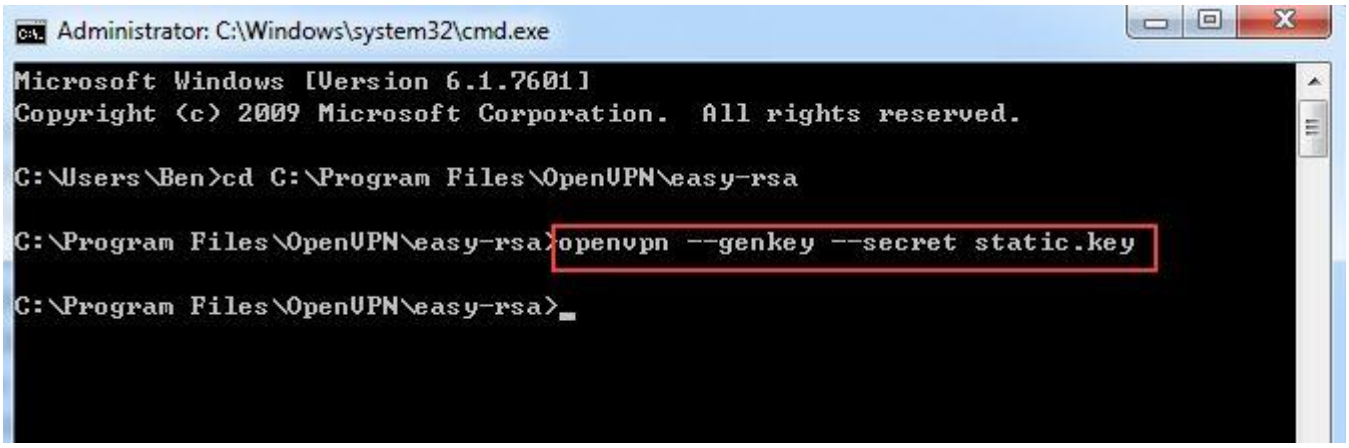
On Windows, open up a Command line interface and cd to **C:\Program Files\OpenVPN\easy-rsa**.



3.2.1 Generate the pre-shared key for OpenVPN

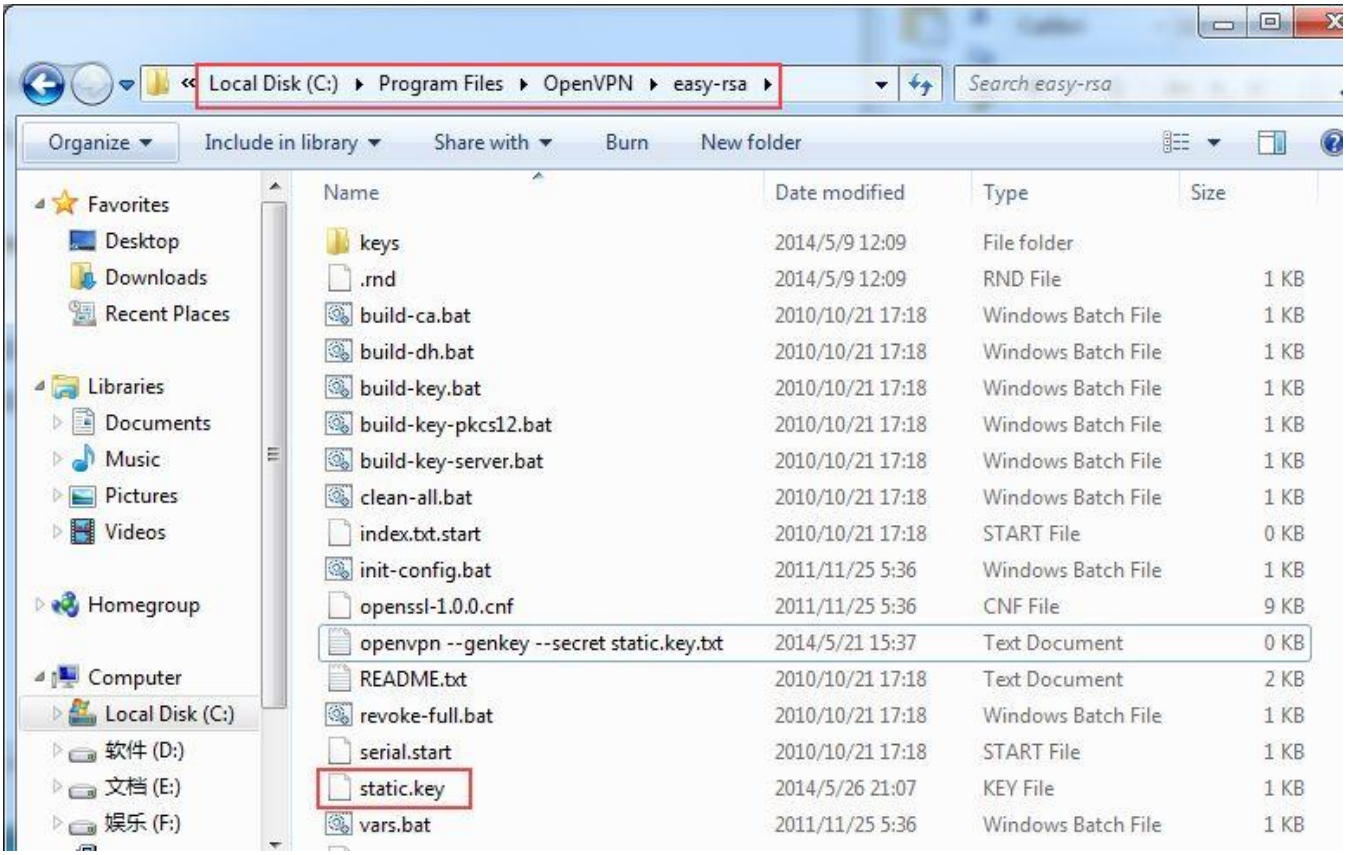
1. Generate the static pre-shared key on Windows.

>openvpn --genkey --secret static.key



2. Check the status of static.key.

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



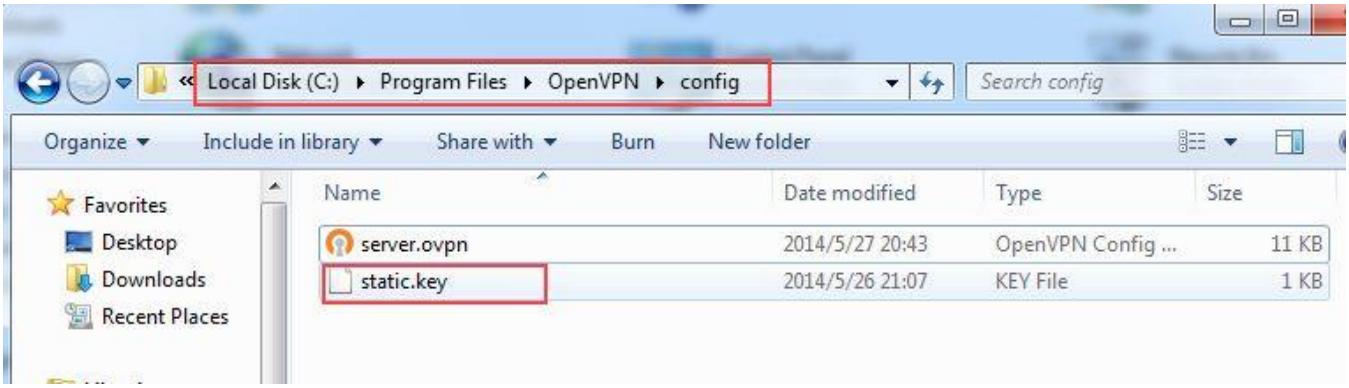
3.3 Windows OpenVPN Server Configuration

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

3.3.1 Open and Edit the server.ovpn file

1. Place the static.key in the OpenVPN\config directory.

Path: C:\Program Files\OpenVPN\config\server.ovpn



2. The configuration of the server.

Note: These red following 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
```

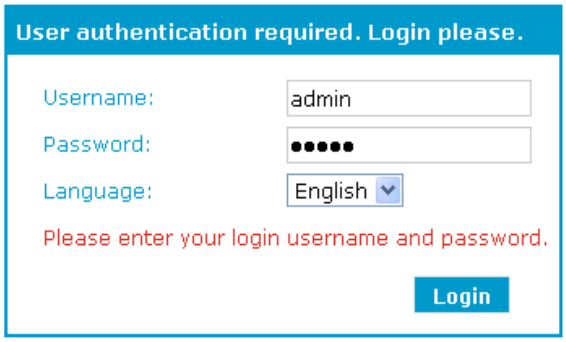
```
# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#       openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on 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 R3000 Configuration

3.4.1 Configure Link Management

1. Install antenna, insert SIM card to R3000 -> power on R3000 and login R3000's Web GUI page.



Note: Factory Settings when login Web GUI

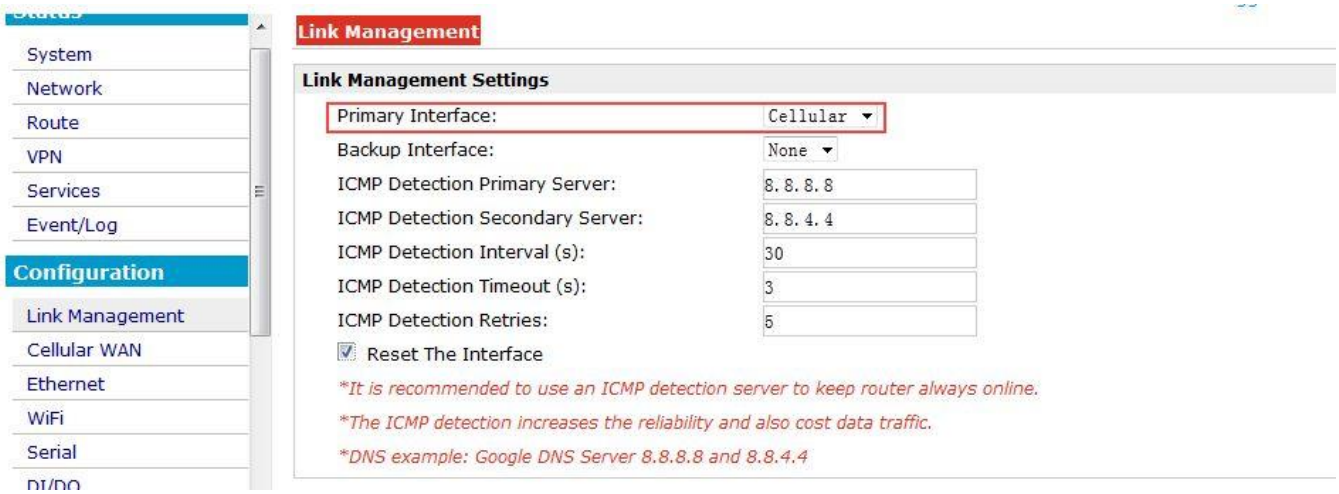
Item	Description
Username	admin
Password	admin
Eth0	192.168.0.1/255.255.255.0, LAN mode

Eth1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled.

2. Browse to “Configuration”-> “Link Management”.

- Click the drop-down box of “Primary Interface” and select “Cellular”.
- Click “Apply”.

Item	Description	Setting
Primary Interface	Select “Cellular”, “Eth0”, “WiFi” as the primary connection interface.	Cellular



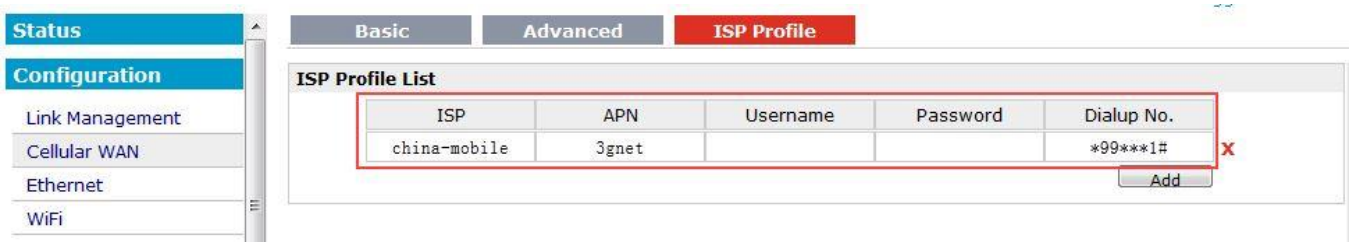
3.4.2 Configure Cellular WAN

1. Browse to “Configuration”-> “Cellular WAN”-> “ISP Profile”.

- Click “Add” to enter the APN (Access Point Name) and Dialup No. for each ISP.
- If required please enter Username and Password in the appropriate fields.
- Click “Apply”.

Note: Usually APN, Username, Password and Dialup No. are provided by ISP accordingly.

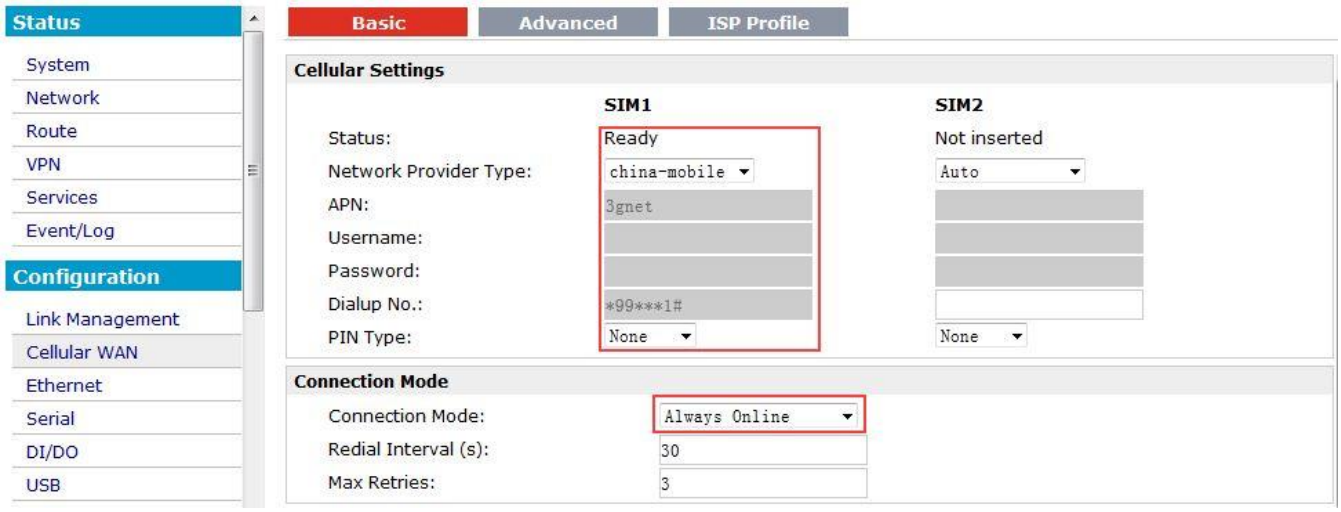
Item	Description	Setting
ISP	Enter relevant ISP network name	Enter accordingly
APN	Enter correct APN for the network	Enter accordingly
Username	Enter correct Username for the network	Enter accordingly
Password	Enter correct Password for the network	Enter accordingly
Dialup No.	Enter correct Dialup No. for the network	Enter accordingly



2. Browse to “Configuration”-> “Cellular WAN”-> “Basic”.

- In region “**Cellular Settings**”. Click the drop-down box of “Network Provider Type” of both SIM cards and select the correct “ISP” that you configure in “Configuration”-> “Cellular WAN”-> “ISP Profile”.
- If required please enter PIN number for SIM1 and SIM 2 in “PIN Type”.
- In region “**Connection Mode**”. Click the drop-down box of “Connection Mode” to select the connection mode accordingly. “Always Online” mode is selected in this Application Note.
- Click “Apply”.

Item	Description	Setting
Network Provider Type	Select from “Auto”, “Custom” or the ISP name you preset in *“Configuration”->”Cellular WAN”->”ISP Profile”*.	Enter accordingly
Connection Mode	Select the connection mode when R3000 dial up to get access to Internet.	Always Online



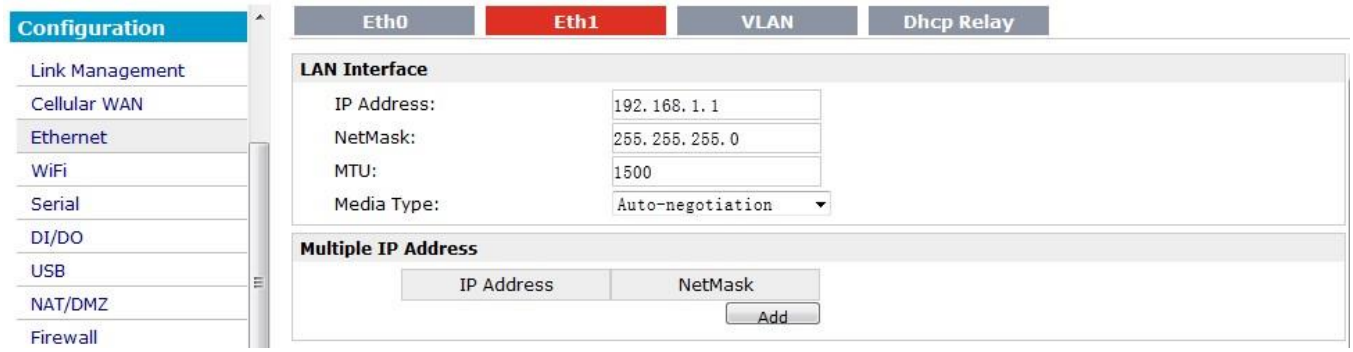
3.4.3 Configure LAN IP address

1. Browse to “Configuration”-> “Ethernet”-> “Eth1”.

- Set IP address and netmask of Eth1 accordingly.
- Click “Apply”.

  Note: Eth0 works under bridge mode with Eth1 by default settings. Eth0 and Eth1 will share the Eth1’s IP address under bridge mode.

Item	Description	Setting
IP Address	Set the IP address of Eth1	Enter accordingly
NetMask	Set the Netmask of Eth1	Enter accordingly
MTU	Set the MTU of Eth1	1500
Media Type	Set the Media Type of Eth1	Auto-negotiation



3.4.4 OpenVPN client Configuration

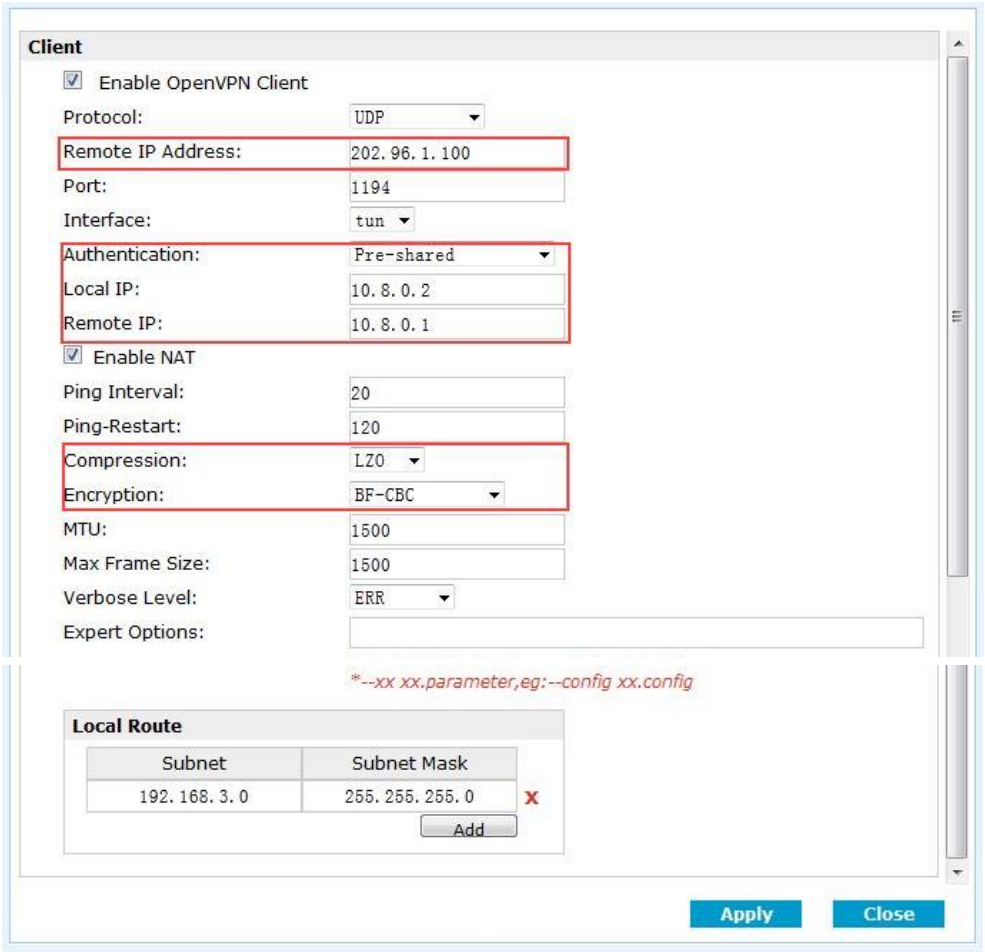
The following sections relate to the Open VPN parameters.

1. Browse to “Configuration”-> “OpenVPN”-> “Client”. Click “Add”.

2. Client Panel, configure the parameters that match OpenVPN server side.

Item	Description	Setting
Enable	Enable OpenVPN Client, the max tunnel account is 3	Enable
Protocol	Select from “UDP” and “TCP Client” which depends on the application.	Select accordingly
Remote IP Address	Enter the remote IP address or domain name of remote side OpenVPN server.	Enter accordingly
Port	Enter the listening port of remote side OpenVPN server.	Enter accordingly
Interface	Select from “tun” and “tap” which are two different kinds of device interface for OpenVPN.	Select accordingly
Authentication	Select from four different kinds of authentication ways: “Pre-shared”, “Username/Password”, “X.509 cert” and “X.509 cert+user”.	Select accordingly
Local IP	Define the local IP address of OpenVPN tunnel.	Enter accordingly
Remote IP	Define the remote IP address of OpenVPN tunnel.	Enter accordingly
Enable NAT	Tick to enable SNAT for OpenVPN.	Enable
Ping Interval	Set ping interval to check if the tunnel is active.	Enter accordingly
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	Enter accordingly
Compression	Select “LZO” to use the LZO compression library to compress the data stream.	Select accordingly

Encryption	Select from “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC” and “AES256-CBC”.	Select accordingly
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	Enter accordingly
Max Frame Size	Set the Max Frame Size for transmission.	Enter accordingly
Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. The higher level will output more log information.	Select accordingly
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null
Subnet&Subnet Mask@Local Route	Set the subnet and subnet Mask of local route.	Enter accordingly



3. Import the certificate for OpenVPN.

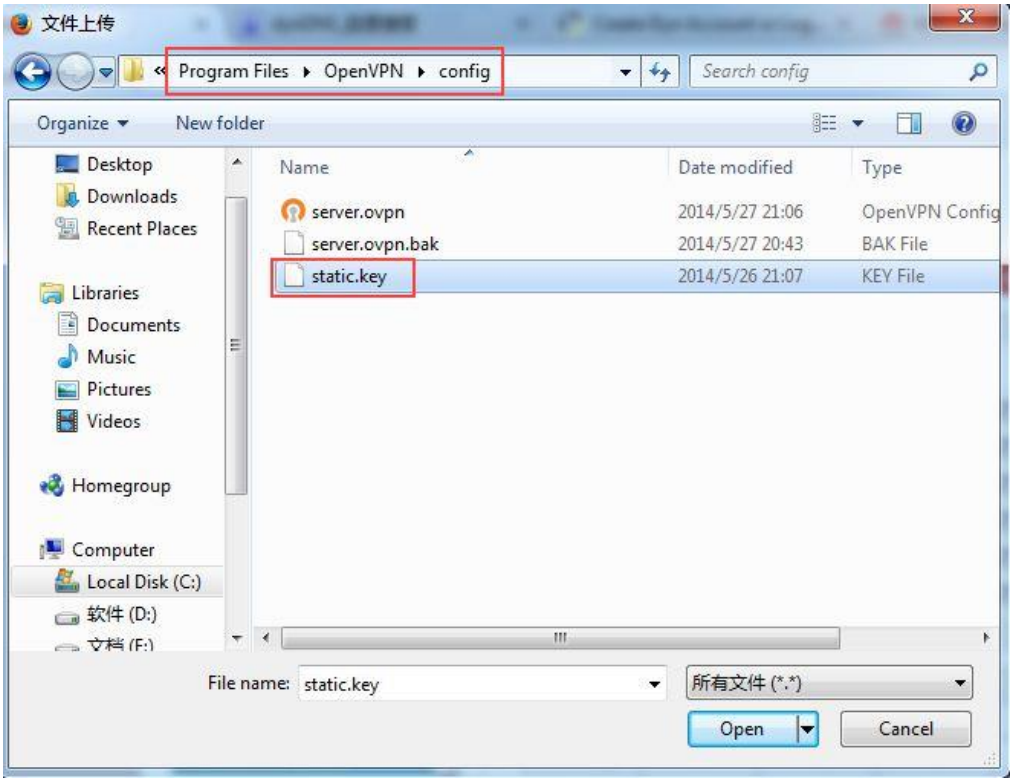
- Browse to “Configuration”-> “OpenVPN”-> “X.509”.

Item	Description	Setting
Select Cert Type	Select the OpenVPN client or server which the certification used for.	Select accordingly
CA	Click “Browse” to select the correct CA file from	Null

	your PC, and then click “Import” to import it to the router. Click “Export” you can export the CA file from router to your PC.	
Public Key	Click “Browse” to select the correct Public Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Public Key A file from router to your PC.	Null
Private Key	Click “Browse” to select the correct Private Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Private Key file from router to your PC.	Null
DH	Click “Browse” to select the correct DH A file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the DH file from router to your PC.	Null
TA	Click “Browse” to select the correct TA file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the TA file from router to your PC.	Null
CRL	Click “Browse” to select the correct CRL file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the CRL file from router to your PC.	Null
Pre-Share Static Key	Click “Browse” to select the correct Pre-Share Static Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Pre-Share Static Key file from router to your PC.	Select accordingly

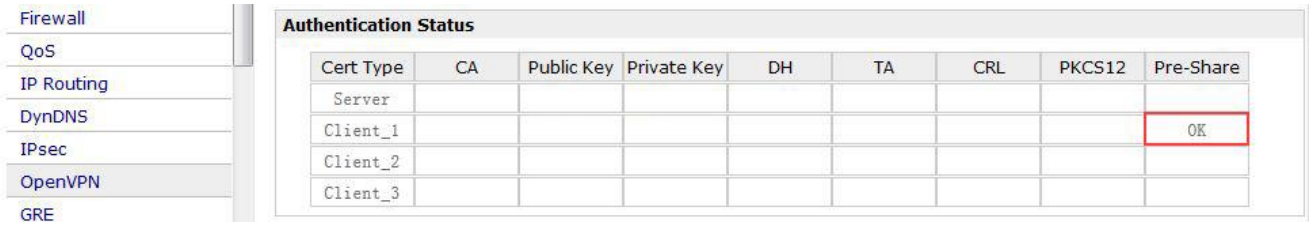
4. Import the certificate, select Cert Type for **Client_1** and click the “browse”

5. Select the static.key with path C:\Program Files\OpenVPN\config



6. Click the “Import” button and you could check the status of pre-shared key.

7. “OK” means that the certificates have been imported successfully. Then click “Save”->”Reboot”.



Chapter 4. Testing

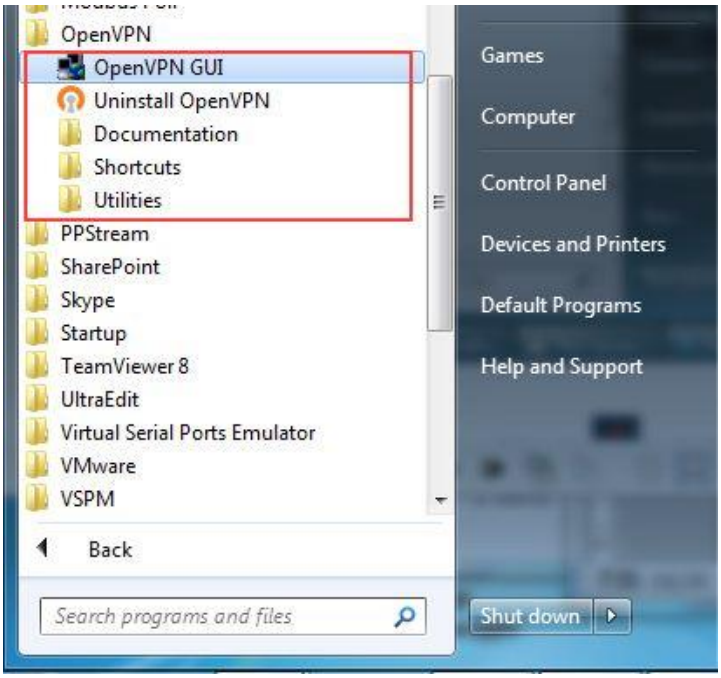
4.1 Cellular Status

1. Browse to “Status”-> “System”->“Current WAN Link” and “Cellular Information”.

- Check that R3000 has 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. You could check the OpenVPN icon in the system tray.

3. Double click the icon, when the OpenVPN server has successfully started, the icon will turn green and prompt a notification with the assigned IP address.

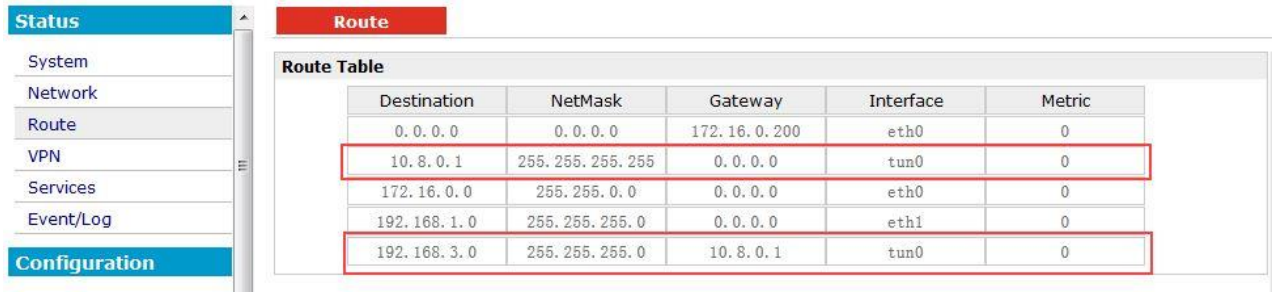
This server will now wait for OpenVPN clients connection.

4.3 VPN Status and Communication

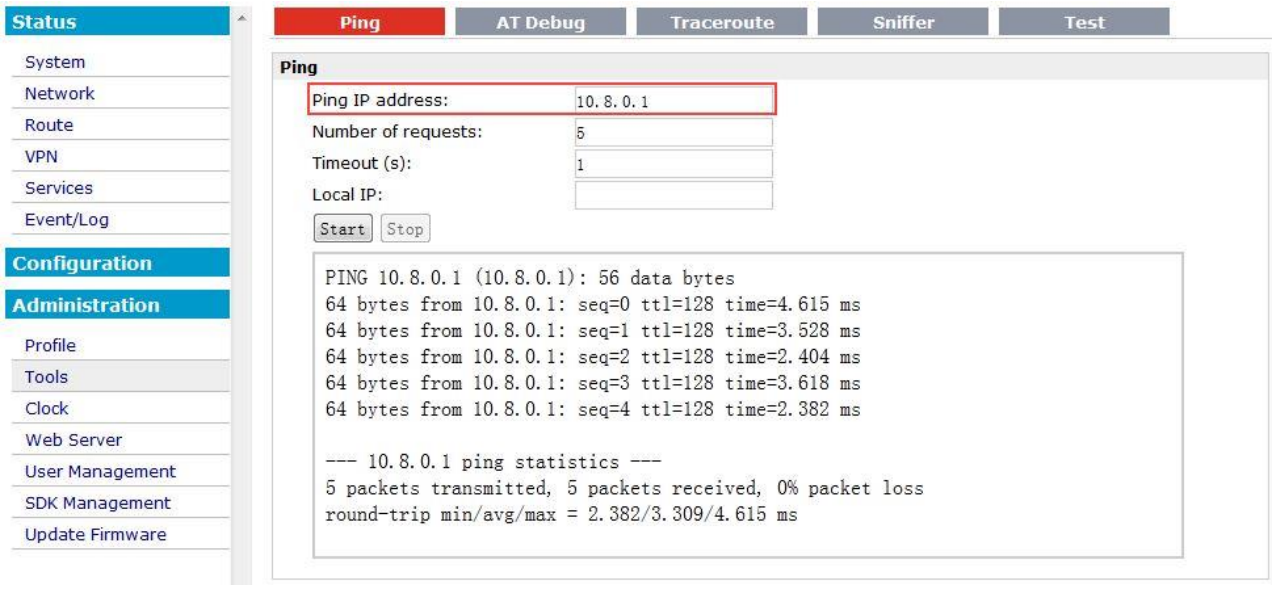
1. Browse to “Status”-> “VPN” ->“OpenVPN”.

- Check that R3000 has established OpenVPN tunnel with Server side.

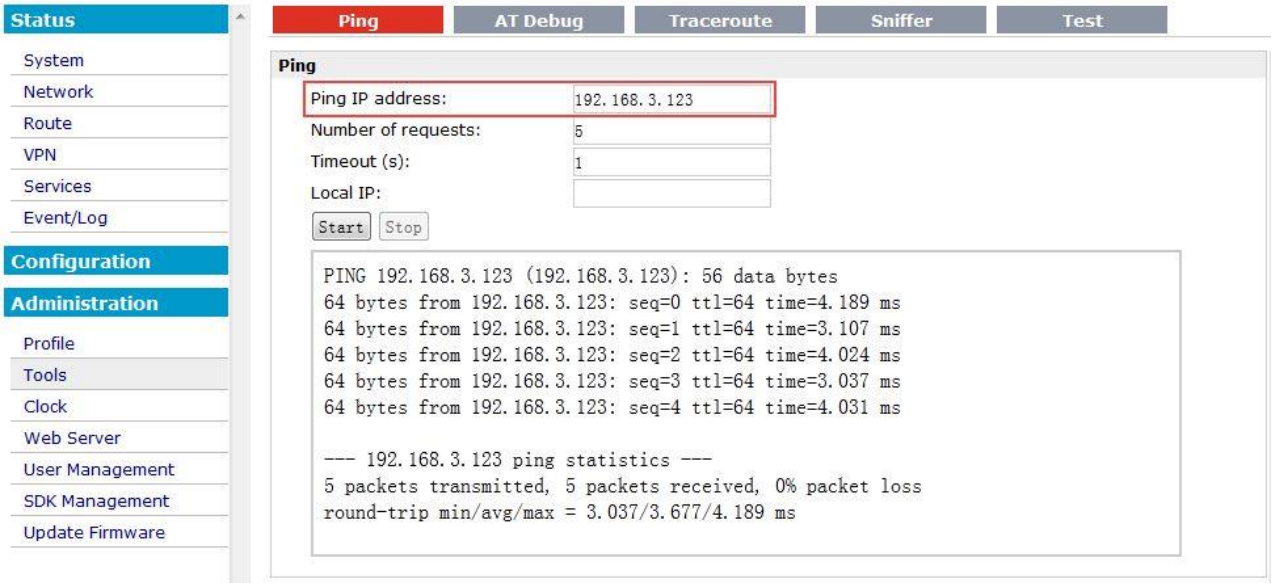
- Check the virtual tunnel on Route table. Browse to “Status”-> “Route”.



- Browse to “Administration”-> “Tools” and “Ping”.
  Ping virtual IP of OpenVPN tunnel and got ICMP reply from OpenVPN server.

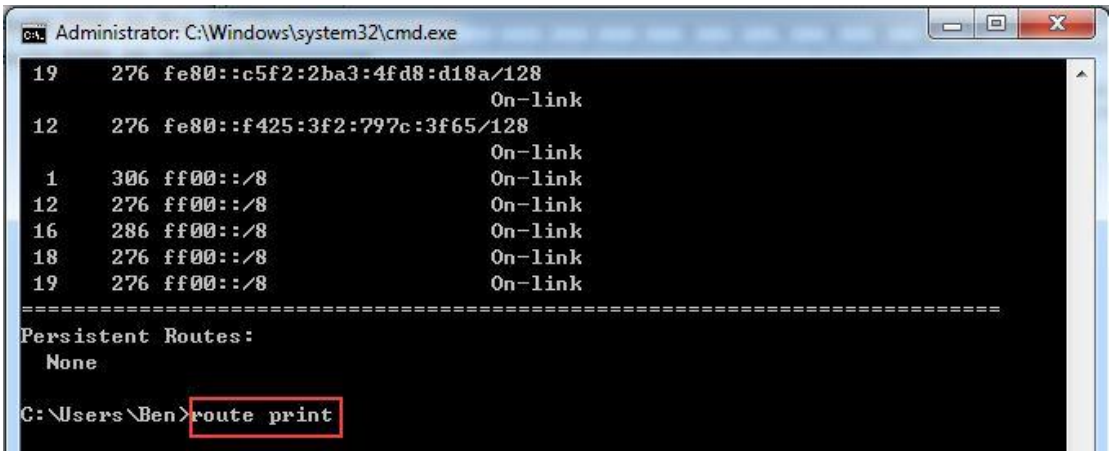


- Browse to “Administration”-> “Tools” and “Ping”.
  Ping LAN IP address behind OpenVPN server and got ICMP reply from remote subnet.

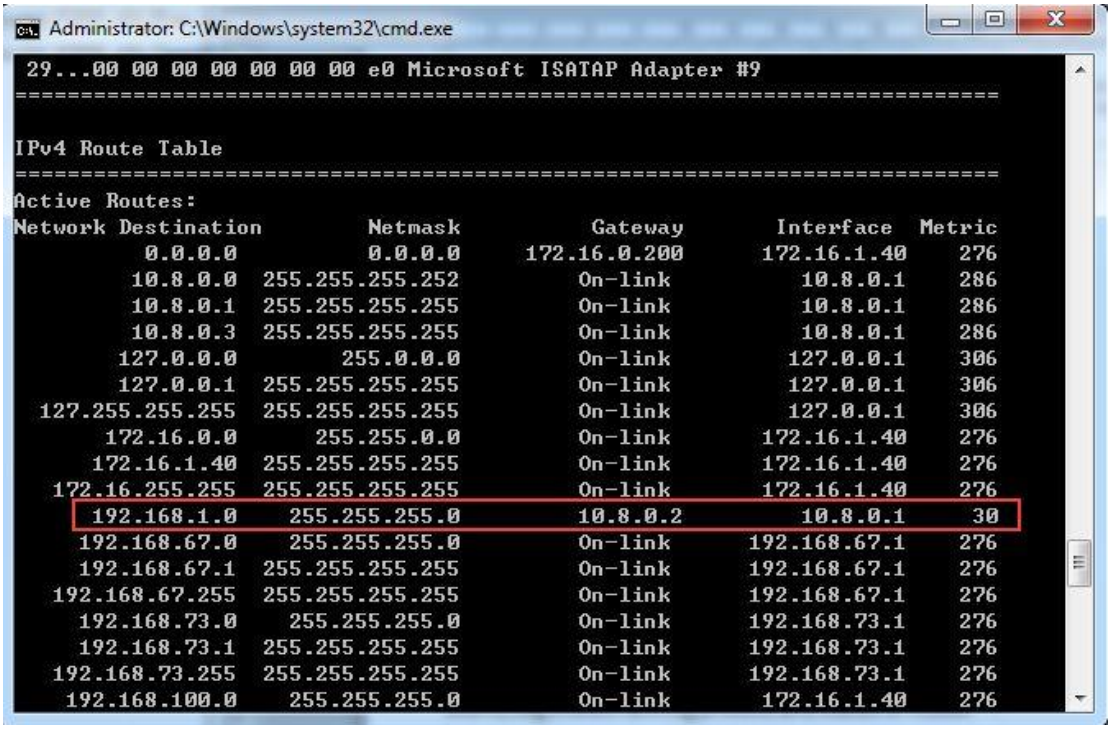


4.4 Testing at OpenVPN server

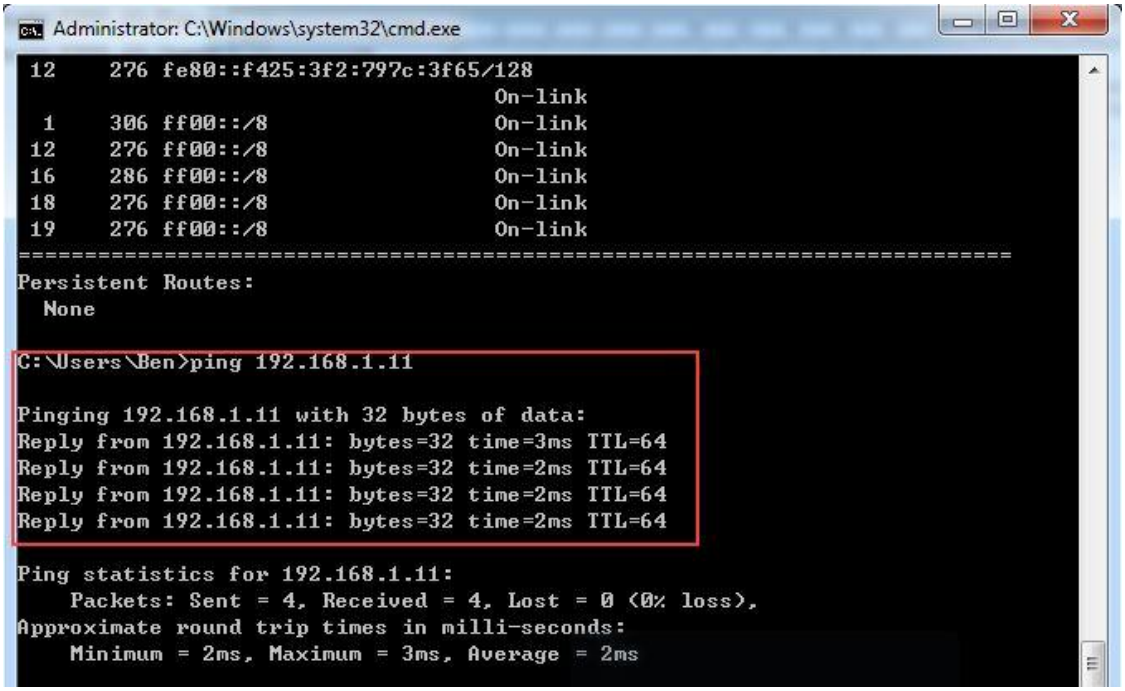
1. Running the CLI and type “route print” command to check the route-table in Windows 7.



2. There is remote subnet 192.168.1.0/24 via OpenVPN tunnel.



3. Ping LAN IP address behind R3000 and got ICMP reply from remote subnet.



4.5 Event/log

Event/Log shows running process and status of R3000.

Note: Usually you can check the Event/Log file in "Status"-> "Event/Log".

.....

14-05-27 21:49:36 <0> router: openvpn client 0 start up.

14-05-27 21:49:36 <1> OpenVPN: OpenVPN 2.2.2 arm-linux [SSL] [LZO2] [EPOLL] [eurephia] built on Apr 3 2014

14-05-27 21:49:36 <3> OpenVPN: NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or executables

14-05-27 21:49:36 <3> OpenVPN: WARNING: file '/cfg/x509/openvpn/client_0/pre-share.key' is group or others accessible

14-05-27 21:49:36 <1> OpenVPN: LZO compression initialized

14-05-27 21:49:36 <1> OpenVPN: NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-delay

14-05-27 21:49:36 <1> OpenVPN: UDPv4 link local: [undef]

14-05-27 21:49:36 <1> OpenVPN: UDPv4 link remote: 202.96.1.100:1194

14-05-27 21:49:38 <1> OpenVPN: Peer Connection Initiated with 202.96.1.100:1194

14-05-27 21:49:38 <1> OpenVPN: TUN/TAP device tun0 opened

14-05-27 21:49:38 <1> OpenVPN: /sbin/ifconfig tun0 10.8.0.2 pointopoint 10.8.0.1 mtu 1500

14-05-27 21:49:38 <1> OpenVPN: GID set to root

14-05-27 21:49:38 <1> OpenVPN: UID set to root

14-05-27 21:49:38 <1> OpenVPN: Initialization Sequence Completed

14-05-27 21:49:52 <0> router: snmpd start up. Starting to process data.

14-05-27 21:50:02 <0> router: sent:AT+COPS?

14-05-27 21:50:02 <0> router: rcvd:

+COPS: 0

OK

Chapter 5. Appendix

5.1 Firmware Version

The configuration above was tested on R3000 with firmware version *R3000_S_V1.01.01.fs.*

Router Information	
Device Model:	R3000
Serial Number:	robustel sn
Device Name:	Cellular Router
Firmware Version:	1.01.01
Hardware Version:	1.02.01
Kernel Version:	2.6.39-7
Radio Module Type:	BGS2
Radio Firmware Version:	REVISION 01.301

5.2 OpenVPN software Version

The software version of OpenVPN is version 2.2.2.

```
C:\Program Files\OpenVPN\bin>openvpn --version
OpenVPN 2.2.2 Win32-MSVC++ [SSL] [LZO2] [PKCS11] built on Dec 15 2011
Originally developed by James Yonan
Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>
```