

Application Note

OpenVPN Server with x.509 certificates

Document Name: **Application Note**
Version: **v.1.0.0**
Date: **2014-06-11**
Status: **Confidential**
DocID: **RT_AN006_OpenVPN Server with x.509 certificates**

Contents

Chapter 1.	Introduction.....	2
1.1	Overview.....	2
1.2	Assumptions	2
1.3	Rectifications	2
1.4	File Version	2
Chapter 2.	Application Topology	4
Chapter 3.	Configuration	5
3.1	OpenVPN Installation on Windows.....	5
3.2	Certificates Management for OpenVPN.....	9
3.2.1	Certificate about OpenVPN.....	9
3.2.2	Generate certificates for OpenVPN server and multiple clients.....	10
3.3	Windows OpenVPN client Configuration	16
3.3.1	Open and Edit the client01.ovpn file	16
3.3.2	Open and Edit the client02.ovpn file	19
3.4	R3000 Configuration	23
3.4.1	Configure Link Management.....	23
3.4.2	Configure Cellular WAN	24
3.4.3	Configure LAN IP address.....	25
3.4.4	OpenVPN server Configuration	25
Chapter 4.	Testing.....	31
4.1	Cellular Status	31
4.2	Running the OpenVPN software in Windows OS	31
4.3	VPN Status and Communication	32
4.4	Testing at Windows OS	34
4.4.1	Testing at OpenVPN Client01	34
4.4.2	Testing at OpenVPN Client02	35
4.4.3	Testing between two OpenVPN Clients.....	36
4.5	Event/log	37
Chapter 5.	Appendix.....	39
5.1	Firmware Version	39
5.2	OpenVPN software Version.....	39

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 works as OpenVPN server in this solution. And R3000's cellular WAN should be dynamic public IP address with DDNS or static public IP address. OpenVPN is certificate based, we using x.509 certificate for authentication at this application. 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

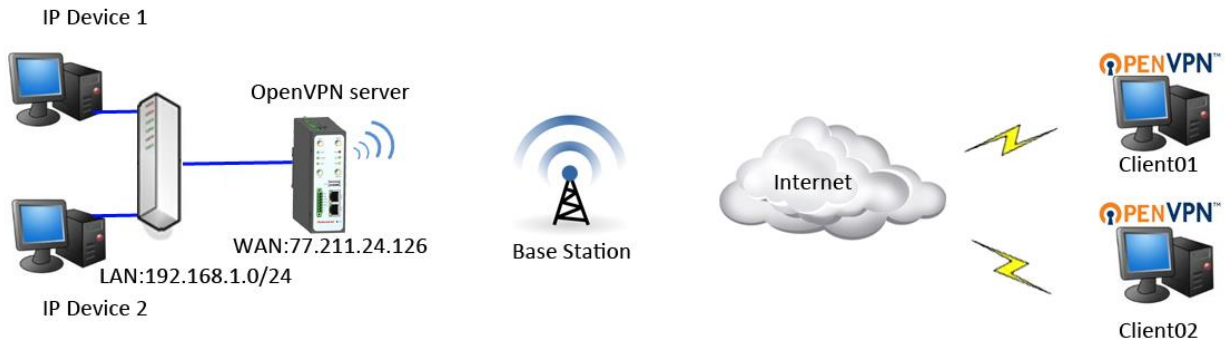
Updates between document versions are cumulative. Therefore, the latest document version contains all updates

OpenVPN Client with x.509 certificates

made to previous versions.

Release Date	Firmware Version	Details
2014-06-11	V1.01.01	First Release

Chapter 2. Application Topology



1. R3000 works as OpenVPN server.
2. R3000 should have static public IP address or dynamic public IP address with DDNS. It opens the specify port of OpenVPN.
3. Two PCs works as OpenVPN clients with any kind of IP addresses which can access internet and one of them is used for creating and signing certificates.
4. OpenVPN tunnel established between server and clients.
5. Client01 and Client02 could communicate with each other, as long as server enable client-to-client feature.

Chapter 3. Configuration

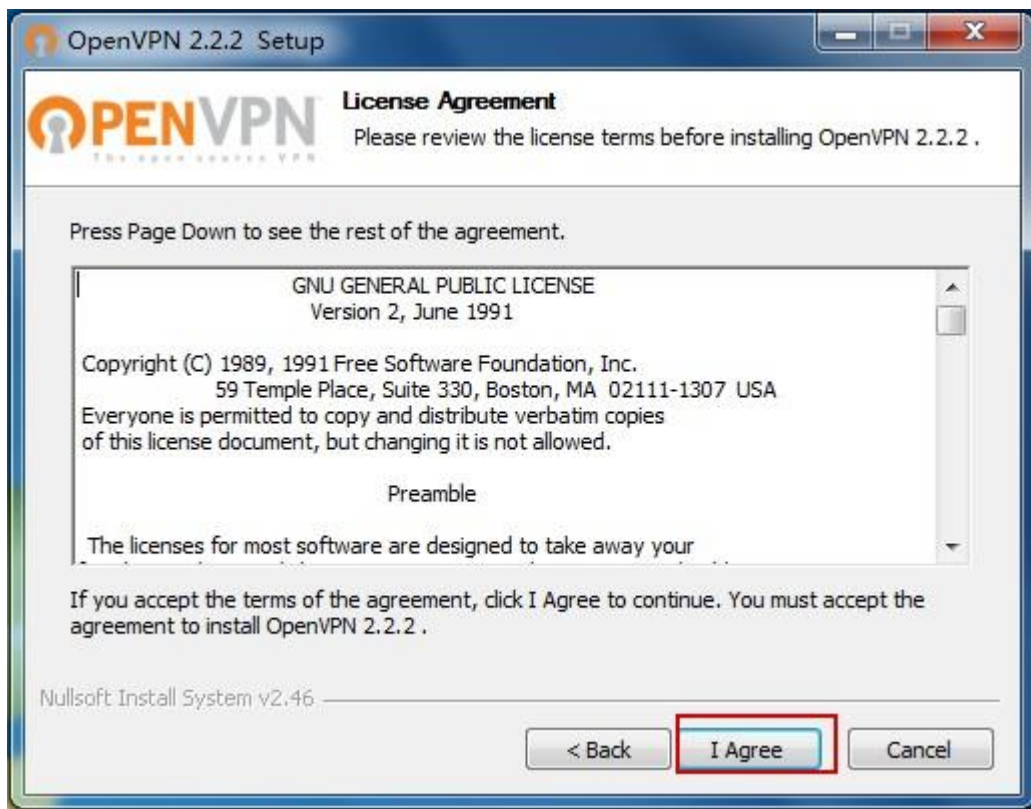
3.1 OpenVPN Installation on Windows

This step should be done on a PC that will be used to create certificates, this can be one of OpenVPN clients. 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.



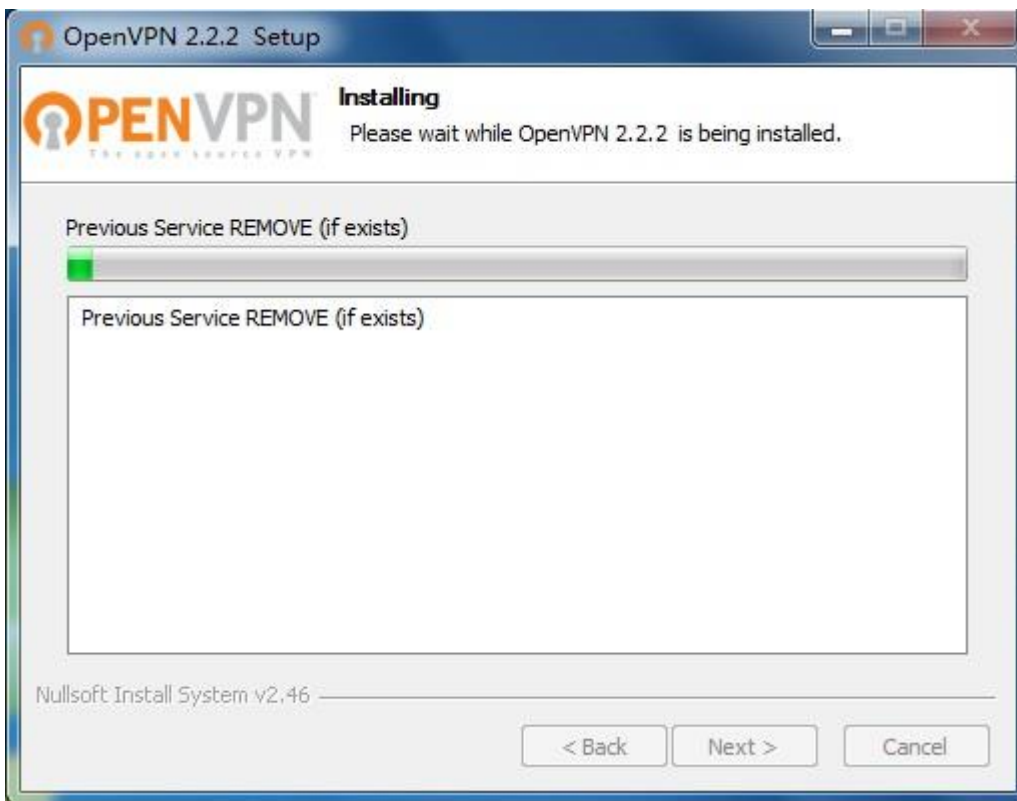
3. Select all the options by default.



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



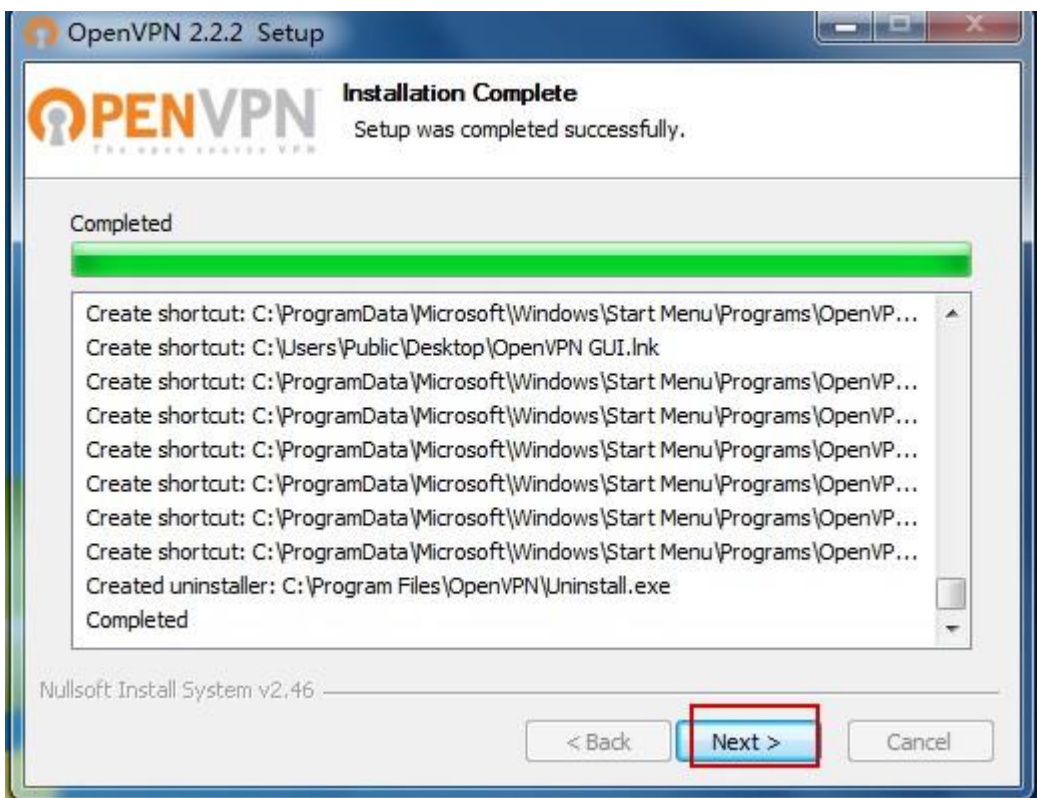
5. The installation schedule.



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 Certificates Management for OpenVPN

3.2.1 Certificate about OpenVPN

The first step in building an OpenVPN is to establish a PKI (public key infrastructure). The PKI consists of:

- a separate certificate (also known as a public key) and private key for the server and each client.
- a master Certificate Authority (CA) and private key which is used to sign certificates for each server and client.

OpenVPN supports bidirectional authentication based on certificates, it means that client must authenticate the server's certificate and the server must authenticate client's certificate before tunnel is established.

Both server and client will authenticate the presented certificate firstly, which was signed by the master certificate authority (CA), and then by testing information in the now-authenticated certificate header, such as the certificate common name or certificate type (client or server).

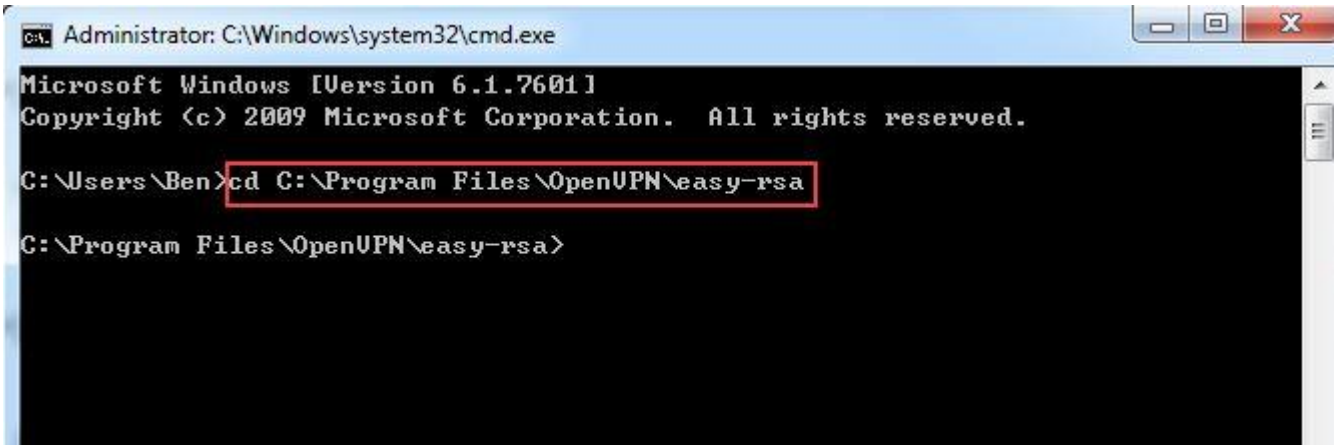
The features of OpenVPN:

- The server only concern its own certificate/key -- it has no need to know the individual certificates of each client.
- The server will only accept clients whose certificates were signed by the master CA certificate. Because the server can perform this signature verification without needing access to the CA private key itself. We could place the CA key (the most sensitive key in the entire PKI) to a completely different machine without Internet access.
- If a private key is compromised and not security any more, the private key could be disqualified by using CRL (certificate revocation list). The CRL disable the compromised certificates and no need to rebuilt the entire PKI.
- The server can enforce client-specific access rights based on client's certificates, such as the Common Name.

3.2.2 Generate certificates for OpenVPN server and multiple clients

In this section we will generate a master CA certificate/key, one server certificate/key and one client certificate/key.

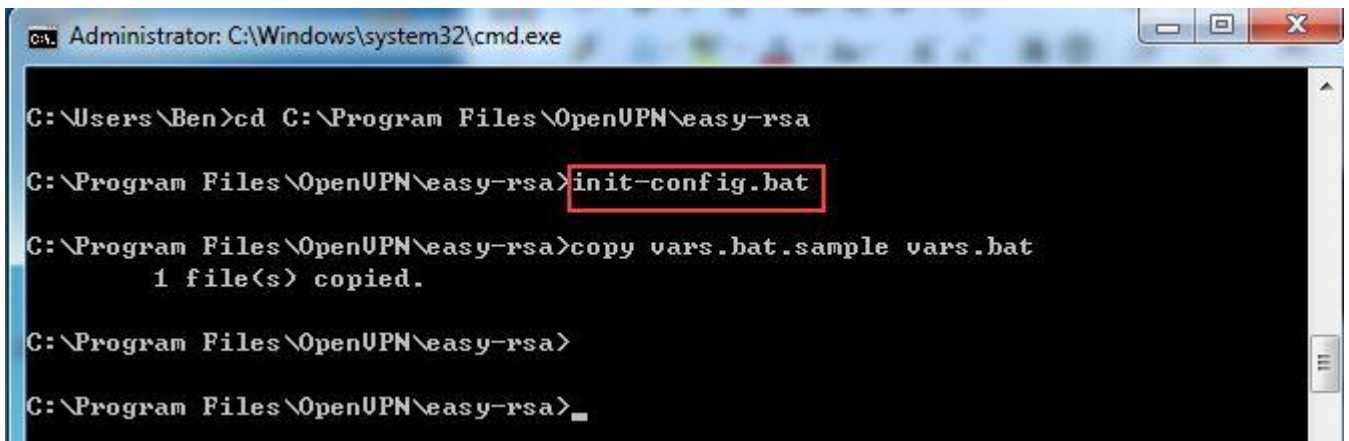
1. For PKI management, we could pre-set the scripts bundled with OpenVPN. On Windows, open up a Command line interface and cd to **C:\Program Files\OpenVPN\easy-rsa**.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Ben>cd C:\Program Files\OpenUPN\easy-rsa
C:\Program Files\OpenUPN\easy-rsa>
```

2. Run the **init-config.bat** to copy configuration files into place (this command would overwrite the previous vars.bat and openssl.cnf files).



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Ben>cd C:\Program Files\OpenUPN\easy-rsa
C:\Program Files\OpenUPN\easy-rsa>init-config.bat
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
1 file(s) copied.
C:\Program Files\OpenUPN\easy-rsa>
C:\Program Files\OpenUPN\easy-rsa>
```

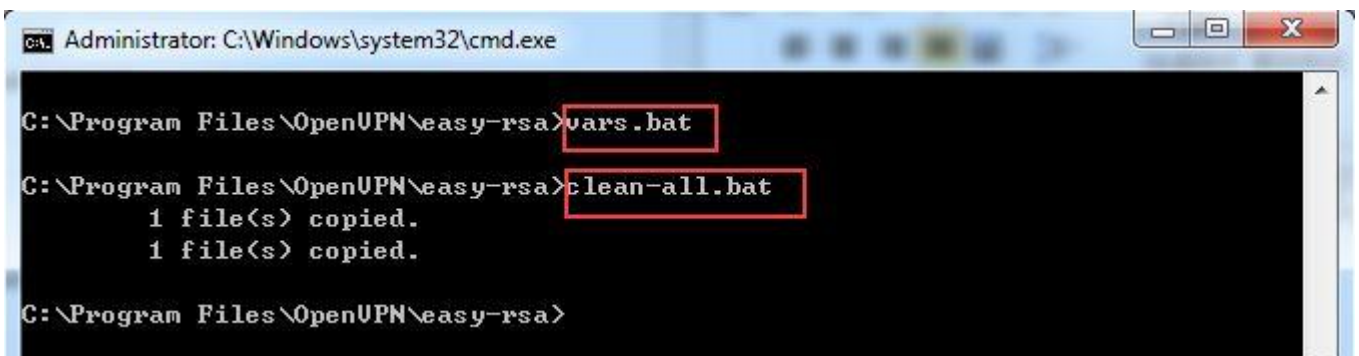
3. Edit the **vars.bat** and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL parameters and so on. Don't leave any blank in this part.

```

0 10 20 30 40 50 60 70 80
1 @echo off
2 rem Edit this variable to point to
3 rem the openssl.cnf file included
4 rem with easy-rsa.
5
6 set HOME=%ProgramFiles%\OpenVPN\easy-rsa
7 set KEY_CONFIG=openssl-1.0.0.cnf
8
9 rem Edit this variable to point to
10 rem your soon-to-be-created key
11 rem directory.
12 rem
13 rem WARNING: clean-all will do
14 rem a rm -rf on this directory
15 rem so make sure you define
16 rem it correctly!
17 set KEY_DIR=keys
18
19 rem Increase this to 2048 if you
20 rem are paranoid. This will slow
21 rem down TLS negotiation performance
22 rem as well as the one-time DH parms
23 rem generation process.
24 set KEY_SIZE=1024
25
26 rem These are the default values for fields
27 rem which will be placed in the certificate.
28 rem Change these to reflect your site.
29 rem Don't leave any of these parms blank.
30
31 set KEY_COUNTRY=CN
32 set KEY_PROVINCE=GD
33 set KEY_CITY=Guangzhou
34 set KEY_ORG=OpenVPN
35 set KEY_EMAIL=mail@robustel.domain
36 set KEY_CN=OpenVPN
37 set KEY_NAME=OpenVPN
38 set KEY_OU=OpenVPN
39 set PKCS11_MODULE_PATH=changeme
40 set PKCS11_PIN=1234
41

```

4. Run the following commands to initialize the environment.



```

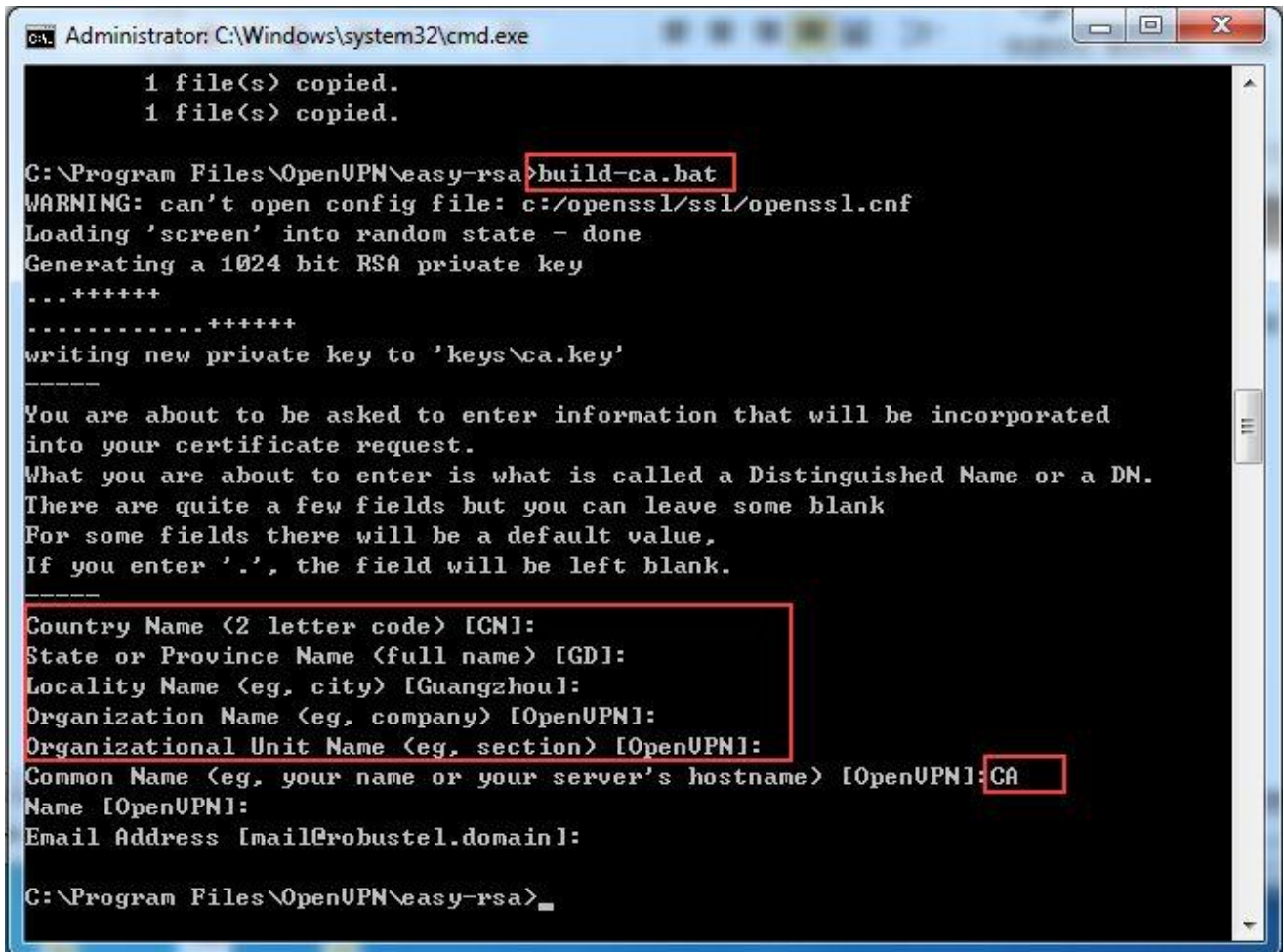
Administrator: C:\Windows\system32\cmd.exe

C:\Program Files\OpenVPN\easy-rsa>vars.bat
C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
1 file(s) copied.
1 file(s) copied.

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

```

5. The command(build-ca.bat) will build the certificate authority(CA) certificate and key by invoking the interactive openssl command.



```
Administrator: C:\Windows\system32\cmd.exe

  1 file(s) copied.
  1 file(s) copied.

C:\Program Files\OpenUPN\easy-rsa>build-ca.bat
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
...+++++
.....+++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenUPN]:
Organizational Unit Name (eg, section) [OpenUPN]:
Common Name (eg, your name or your server's hostname) [OpenUPN]:CA
Name [OpenUPN]:
Email Address [mail@robustel.domain]:

C:\Program Files\OpenUPN\easy-rsa>
```

Note: in the above sequence, most queried parameters were defaulted to the values set in the vars.bat file. The only parameter which must be explicitly entered is the Common Name.

6. Generate a certificate and private key for server, using **build-key-server.bat Server01**. When the Common Name is queried, please enter "Server01".

```

Administrator: C:\Windows\system32\cmd.exe

C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat Server01
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
..+++++
writing new private key to 'keys\Server01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:Server01
Name [OpenVPN]:
Email Address [mail@robustel.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CN'
stateOrProvinceName  :PRINTABLE:'GD'
localityName         :PRINTABLE:'Guangzhou'
organizationName     :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName           :PRINTABLE:'Server01'
name                 :PRINTABLE:'OpenVPN'

emailAddress          :IA5STRING:'mail@robustel.domain'
Certificate is to be certified until May 26 13:06:36 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

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

```

Note: Server01 in "build-key-server.bat Server01" is the file name of certificate(the name of public key and private key).

7. Generate a certificate and private key for client.

```
>build-key.bat Client01
```

```
>build-key.bat Client02
```

```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\OpenVPN\easy-rsa>build-key.bat Client01
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
...+++++
writing new private key to 'keys\Client01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:Client01
Name [OpenVPN]:
Email Address [mail@robustel.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName           :PRINTABLE:'Guangzhou'
organizationName       :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName             :PRINTABLE:'Client01'
name                   :PRINTABLE:'OpenVPN'

emailAddress           :IA5STRING:'mail@robustel.domain'
Certificate is to be certified until May 26 13:27:14 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

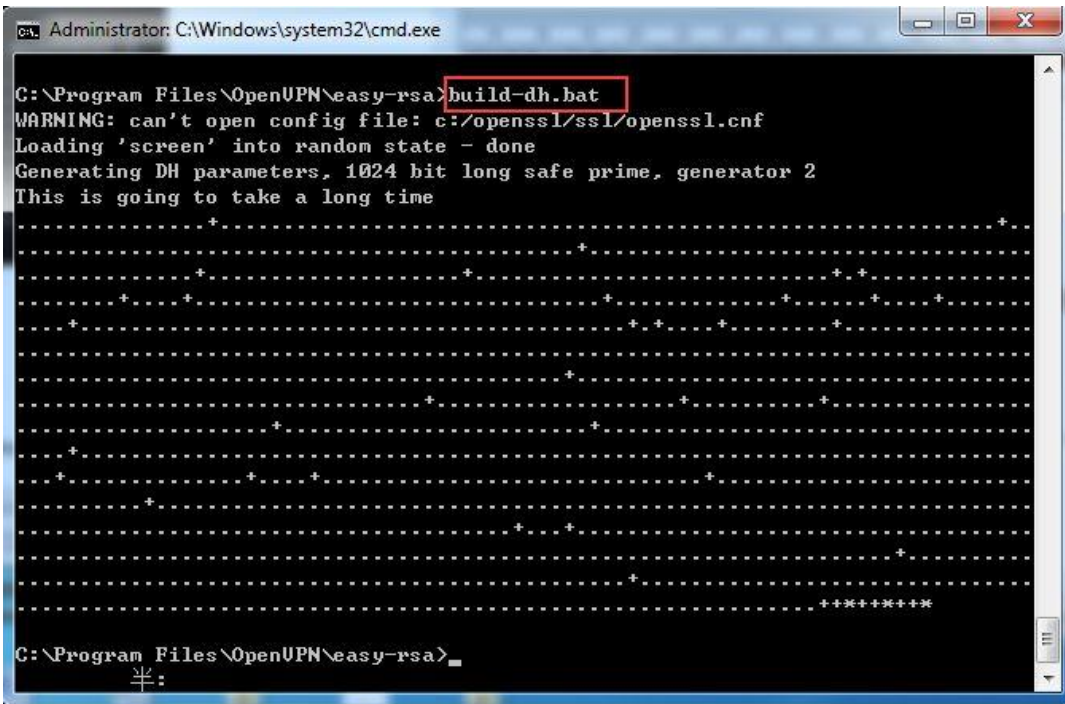
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>_
```

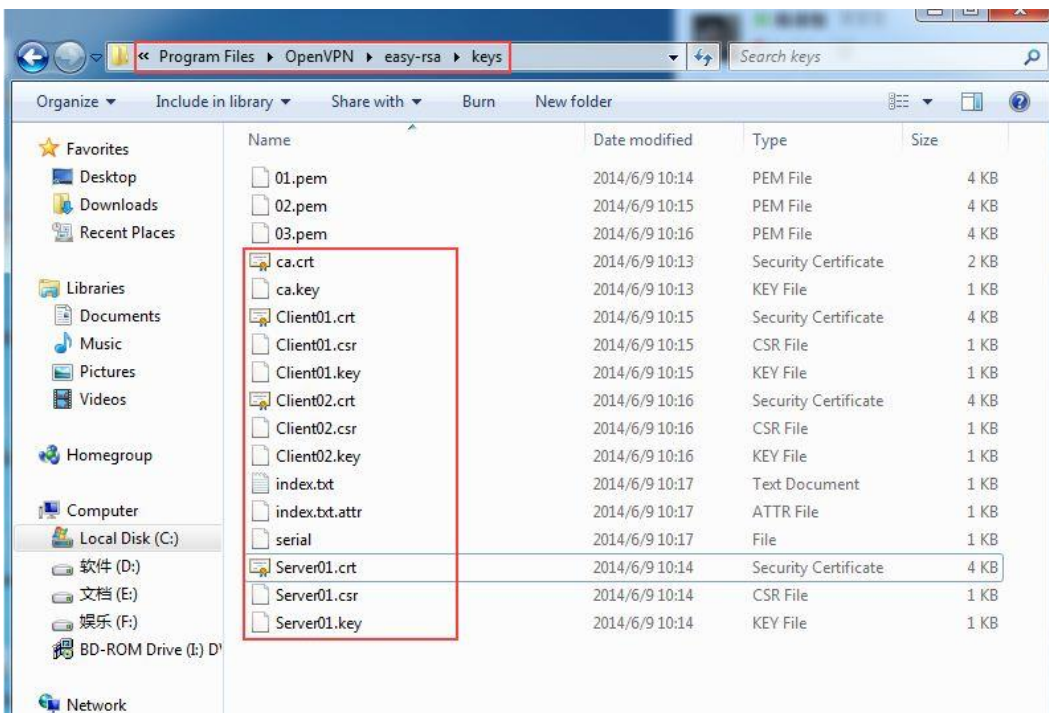
Note: Client01 in "build-key-server.bat Client01" is the file name of certificate(the name of public key and private

key). Please refer to the above steps to generate the certificates for **Client02**. *Always use a unique common name for each client.*

8. Generate Diffie Hellman parameters.



9. Now, find the newly-generated keys and certificates in the easy-rsa\keys subdirectory.



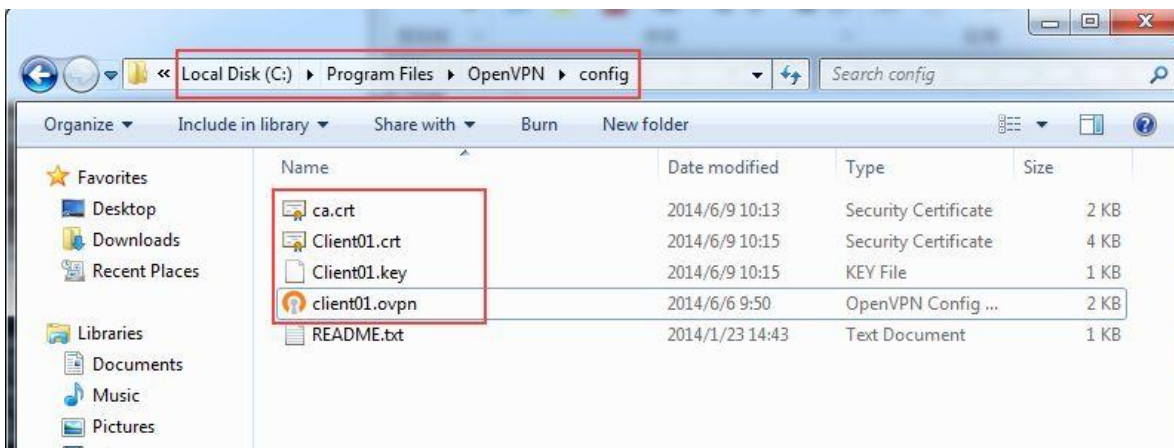
3.3 Windows OpenVPN client Configuration

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

3.3.1 Open and Edit the client01.ovpn file

1. Copy the required files to the OpenVPN client configuration directory.

Path: C:\Program Files\OpenVPN\config



2. The configuration of the client01.ovpn.

Note: These red following have been changed from the sample configure defaults. And the extra comments are in blue.

```
#####
# Sample client-side OpenVPN 2.0 config file      #
# for connecting to multi-client server.         #
#                                                 #
# This configuration can be used by multiple     #
# clients, however each client should have      #
# its own cert and key files.                   #
#                                                 #
# On Windows, you might want to rename this    #
# file so it has a .ovpn extension              #
#####

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# 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

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 77.211.24.126 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun
```

```
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert Client01.crt
key Client01.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
```

cipher BF-CBC

Enable compression on the VPN link.
Don't enable this unless it is also
enabled in the server config file.

comp-lzo

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

If you have fragmentation issues or misconfigured
routers in the path which block Path MTU discovery,
lower the TCP MSS and internally fragment non-TCP
protocols.

fragment 1500

Set log file verbosity.

verb 3

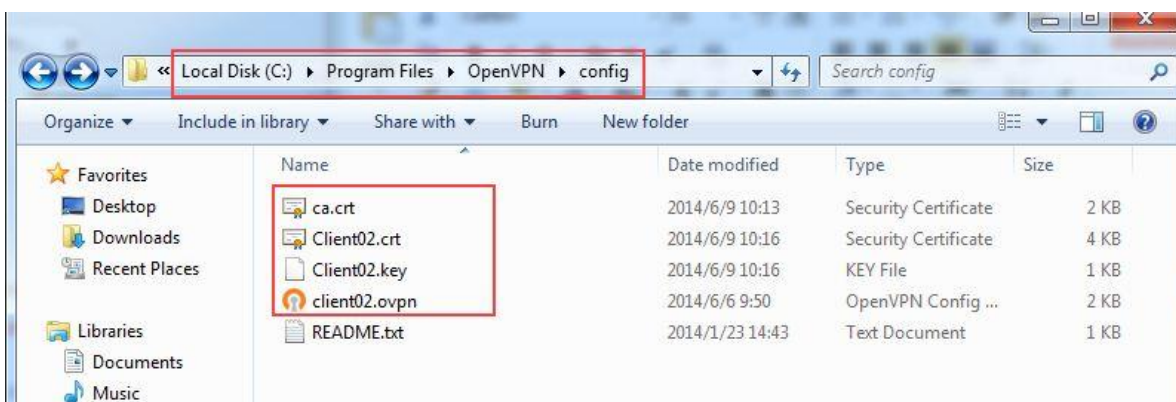
Silence repeating messages

;mute 20

3.3.2 Open and Edit the client02.ovpn file

2. Copy the required files to the OpenVPN client configuration directory.

Path: C:\Program Files\OpenVPN\config



3. The configuration of the client02.ovpn.

Note: These red following have been changed from the sample configure defaults. And the extra comments are in blue.

```
#####  
# Sample client-side OpenVPN 2.0 config file      #  
# for connecting to multi-client server.         #
```

```
# #
# This configuration can be used by multiple #
# clients, however each client should have #
# its own cert and key files. #
# #
# On Windows, you might want to rename this #
# file so it has a .ovpn extension #
#####

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# 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

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one. On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server? Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 77.211.24.126 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random
```

```
# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert Client02.crt
key Client02.key

# Verify server certificate by checking
# that the certificate has the nsCertType
```

```
# field set to "server". This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
cipher BF-CBC

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# 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

# If you have fragmentation issues or misconfigured
# routers in the path which block Path MTU discovery,
# lower the TCP MSS and internally fragment non-TCP
# protocols.
fragment 1500

# Set log file verbosity.
verb 3

# Silence repeating messages
;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.

User authentication required. Login please.

Username:

Password:

Language: ▼

Please enter your login username and password.

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

Link Management

Link Management Settings

Primary Interface: Cellular ▼

Backup Interface: None ▼

ICMP Detection Primary Server: 8.8.8.8

ICMP Detection Secondary Server: 8.8.4.4

ICMP Detection Interval (s): 30

ICMP Detection Timeout (s): 3

ICMP Detection Retries: 5

Reset The Interface

*It is recommended to use an ICMP detection server to keep router always online.

*The ICMP detection increases the reliability and also cost data traffic.

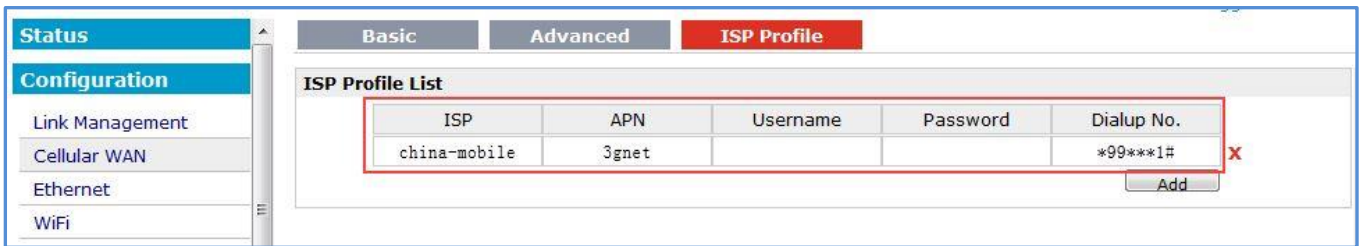
*DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4

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”.

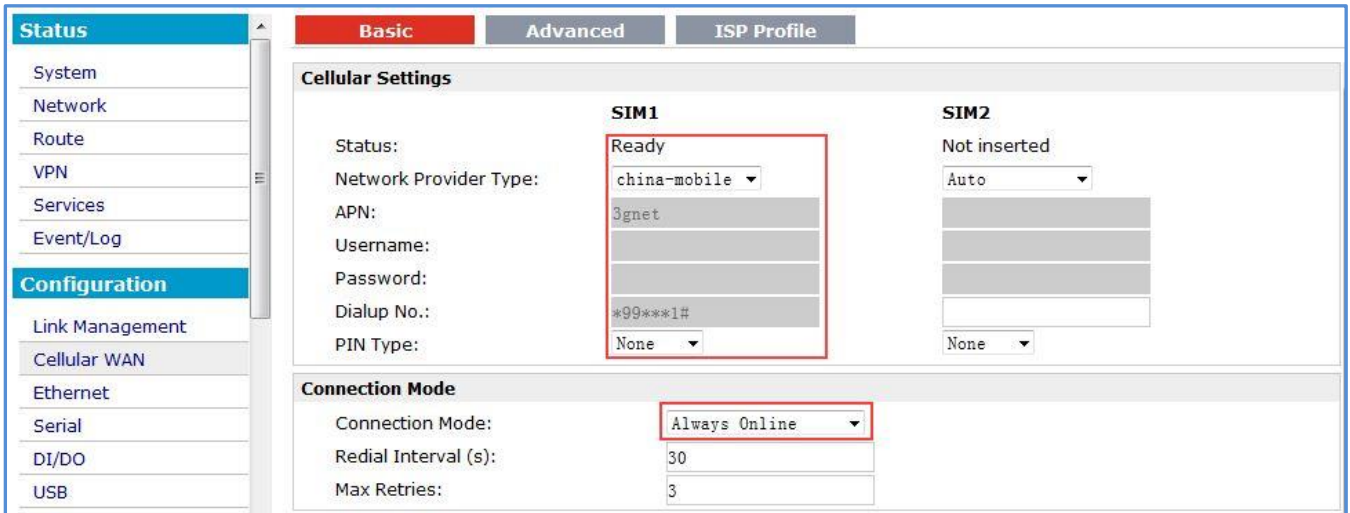
Note: Usually APN, Username, Password and Dialup No. are provided by ISP accordingly.

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 SIM card and select the correct “ISP” that you configure in “Configuration”-> “Cellular WAN”-> “ISP Profile”.
 - If required please enter PIN number for the SIM 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

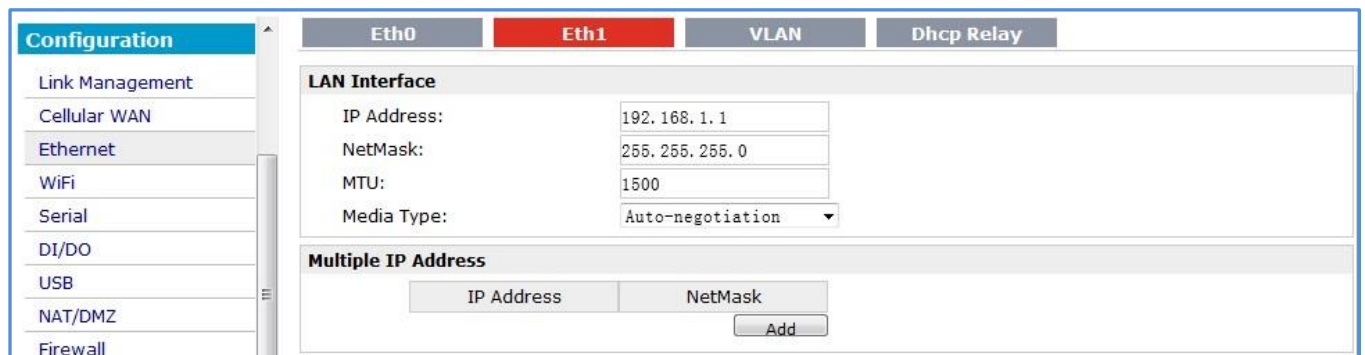


3.4.3 Configure LAN IP address

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



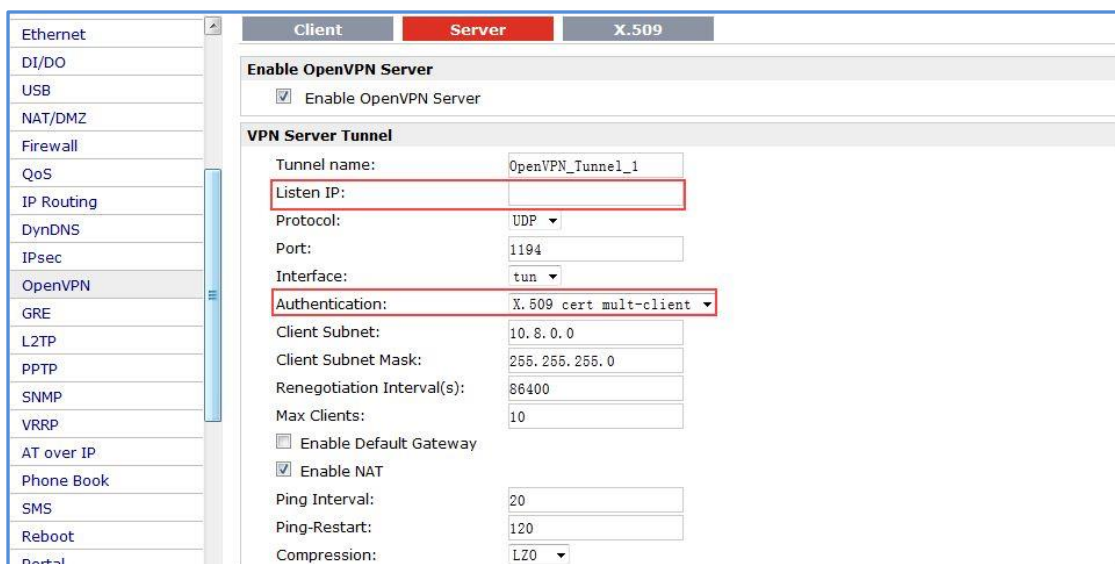
3.4.4 OpenVPN server Configuration

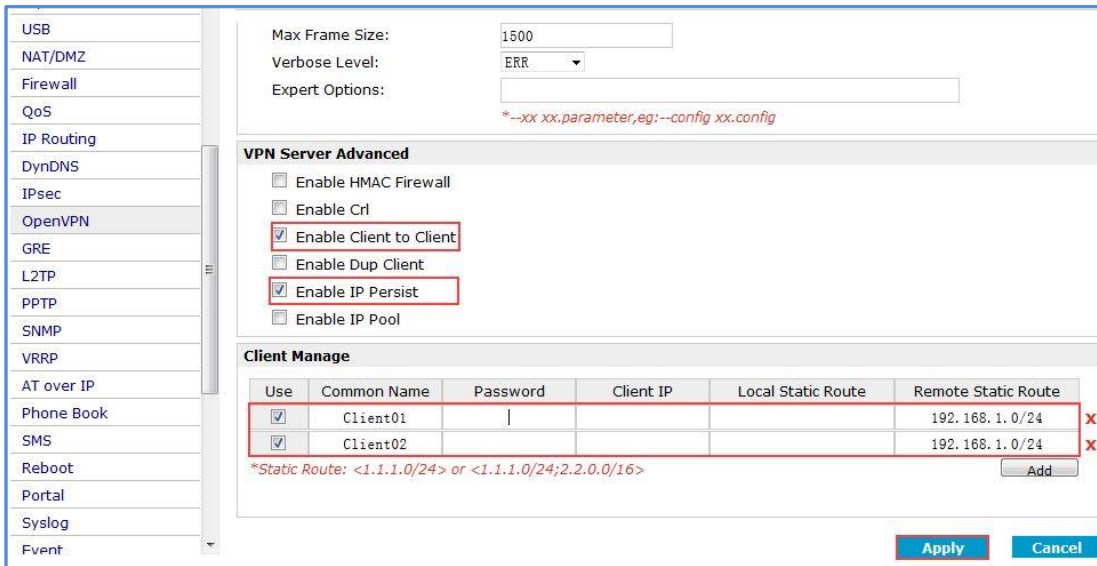
The following sections relate to the Open VPN parameters.

1. Browse to “Configuration”-> “OpenVPN”-> “Server”. Tick “Enable OpenVPN Server”.

Item	Description	Setting
Enable OpenVPN Server	Tick to enable OpenVPN server tunnel.	Enable
Tunnel name	Name the OpenVPN server tunnel.	Enter accordingly
Listen IP	You can enter the IP address of cellular WAN, Ethernet WAN or Ethernet LAN. Null or 0.0.0.0 stands for using the active WAN link currently-cellular WAN or Ethernet WAN.	Enter accordingly
Protocol	Select from "UDP" and "TCP Client" which depends on the application.	Select accordingly
Port	Set the local listening port	Select 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
Client Subnet	Define the Client IP address of OpenVPN tunnel.	Enter accordingly
Client Subnet Mask	Define the Client's subnet mask of OpenVPN tunnel.	Enter accordingly
Renegotiation Interval(s)	Keep alive mechanism for OpenVPN tunnel	Enter accordingly
Max Clients	The max connection of OpenVPN clients	Enter accordingly
Enable Default Gateway	all clients to redirect their default network gateway through the VPN	Null
Enable NAT	Tick to enable SNAT for OpenVPN. The source IP address of host Behind R3000 will be disguised before accessing the remote OpenVPN client.	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.	Select accordingly
Compression	Select from "None" and "LZO", 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.	Null
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Enter accordingly

Enable HMAC Firewall @ VPN Server Advanced	In order to prevent malicious attacks, such as DOS, UDP port flooding, we generate a "HMAC is firewall "	Disable
Enable Crl @ VPN Server Advanced	Generate a certificate revoked chain file, to prevent someone lost certificate in the future, users access VPN by illegal. You could find the certificate tab of R3000, there is one option for Crl.	Disable
Enable Client to Client @ VPN Server Advanced	Uncomment this directive to allow different clients to be able to "see" each other. By default, clients will only see the server. To force clients to only see the server, you will also need to appropriately firewall the server's TUN/TAP interface.	Enable
Enable Dup Client @ VPN Server Advanced	While establish OpenVPN with keys, must open this option, otherwise only allows one VPN connection with the same certificate.	Disable
Enable IP Persist @ VPN Server Advanced	Maintain a record of client <-> virtual IP address associations in this file. If OpenVPN goes down or is restarted, reconnecting clients can be assigned the same virtual IP address from the pool that was previously assigned.	Enable
Enable IP pool @ VPN Server Advanced	Define the range of virtual IP address.	Disable
Client Manage	Click "Add" to add a OpenVPN client info which include "Common Name", "Password", "Client IP", "Local Static Route" and "Remote Static Route". This field only can be configured when you select "Username/Password" in "Authentication".	Enter accordingly





2. Import the certificate for OpenVPN.
- Browse to "Configuration"-> "OpenVPN"-> "X.509".

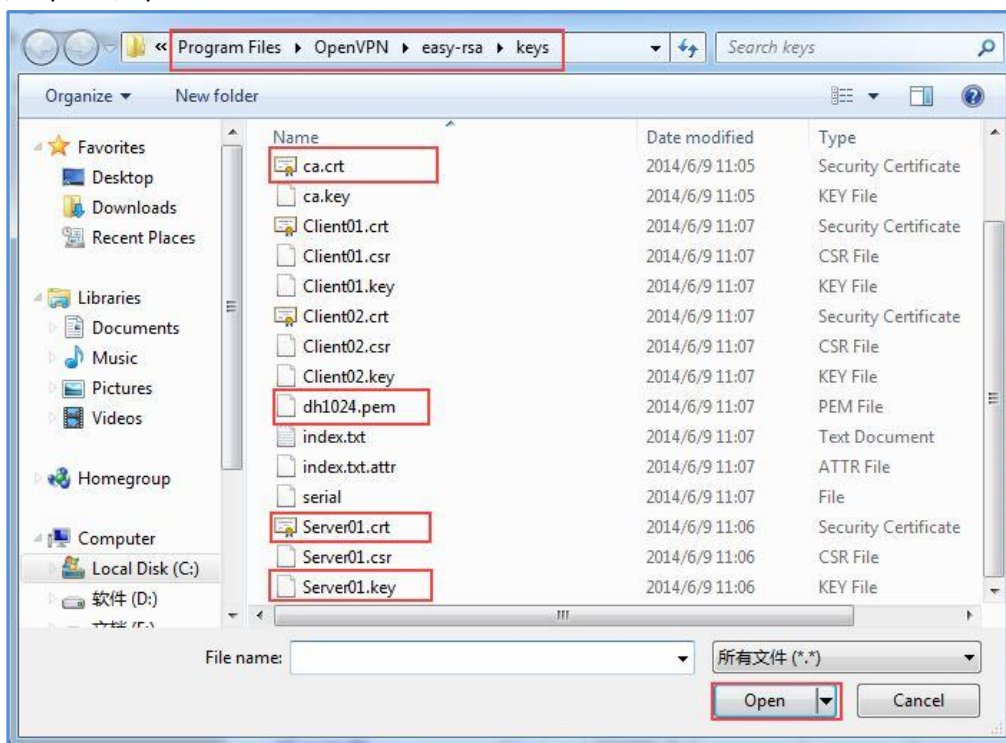
Item	Description	Setting
Select Cert Type	Select the OpenVPN client or server which the certificate used for.	Select accordingly
CA	Click "Browse" to select the correct CA file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CA file from router to your PC.	Select accordingly
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.	Select accordingly
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.	Select accordingly
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.	Select accordingly
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.	Null

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

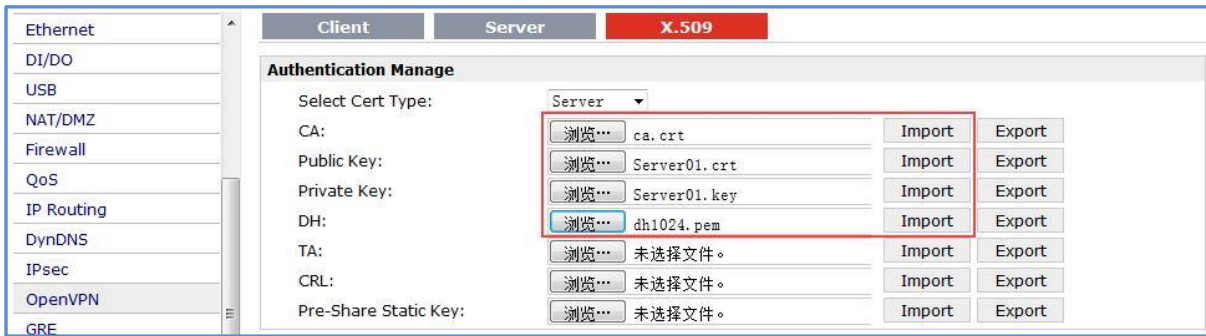


5. Select the **ca.crt**, **Server01.crt**, **Server01.key** and **dh1024.pem** with path C:\Program Files\OpenVPN\easy-rsa\keys

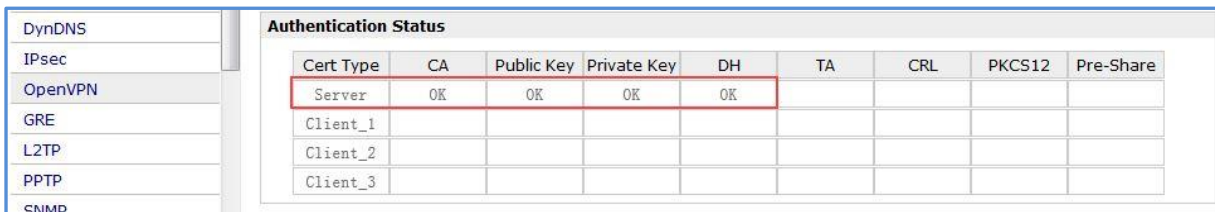


Note: While we using x.509 certificate for authentication, CA, public key, private key and dh1024.pem for server is required.

6. Click the “Import” button and you could check the status of CA.



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.

The screenshot shows the OpenVPN client interface. On the left is a navigation menu with sections for 'Status' and 'Configuration'. The 'Status' section includes System, Network, Route, VPN, Services, and Event/Log. The 'Configuration' section includes Link Management, Cellular WAN, Ethernet, Serial, DI/DO, USB, NAT/DMZ, Firewall, QoS, and IP Routing. The main content area is titled 'System' and contains the following information:

System Time:	2014-06-09 04:45:15
Current WAN Link	
Current WAN Link:	Cellular
IP Address:	77.211.24.126
Gateway:	192.168.254.254
NetMask:	255.255.255.255
DNS Server:	212.166.132.102, 212.73.32.3
Keepalive PING IP Address:	8.8.8.8, 8.8.4.4
Keepalive PING Interval:	30
Cellular Information	
Current SIM:	SIM1
Phone No.:	
SMS Service Center:	34607003110
Modem Status:	Ready
Network Status:	Registered to home network
Signal Level (RSSI):	📶 (31,-51DB)

4.2 Running the OpenVPN software in Windows OS

1. Run the OpenVPN software.

The screenshot shows the Windows Start menu. The 'OpenVPN' folder is expanded, and the 'OpenVPN GUI' application is highlighted with a red box. Other items in the folder include 'Uninstall OpenVPN', 'Documentation', 'Shortcuts', and 'Utilities'. The Start menu also shows other system options like Games, Computer, Control Panel, Devices and Printers, Default Programs, and Help and Support. A search bar at the bottom says 'Search programs and files' and a 'Shut down' button is visible.

2. You could check the OpenVPN icon in the system tray.



3. Double click the icon, when the OpenVPN Client01 has successfully started, the icon will turn green and prompt a notification with the assigned IP address.

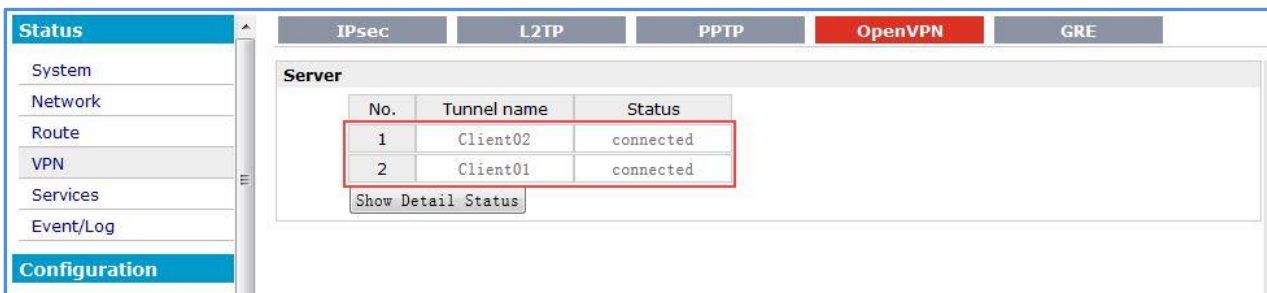


4. Double click the icon, when the OpenVPN Client02 has successfully started, the icon will turn green and prompt a notification with the assigned IP address.

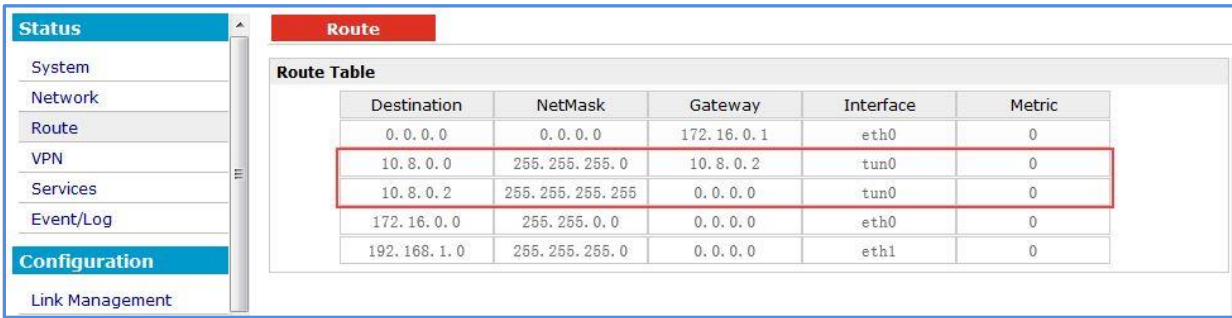


4.3 VPN Status and Communication

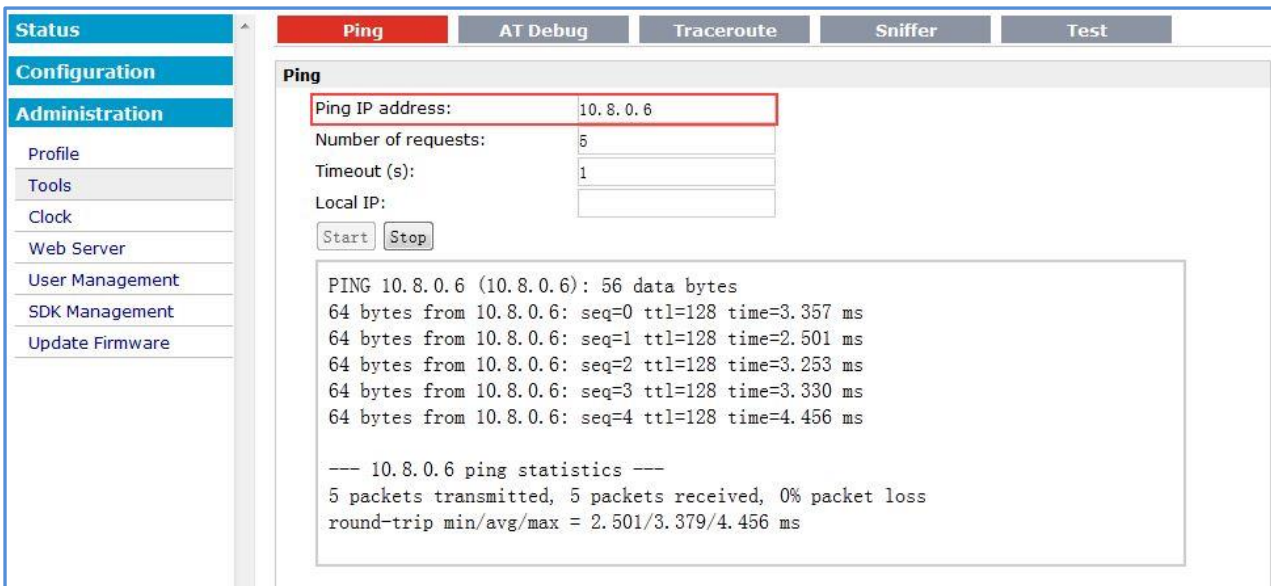
1. Browse to "Status" -> "VPN" -> "OpenVPN".
 - Check that R3000 has established OpenVPN tunnel with Server side.



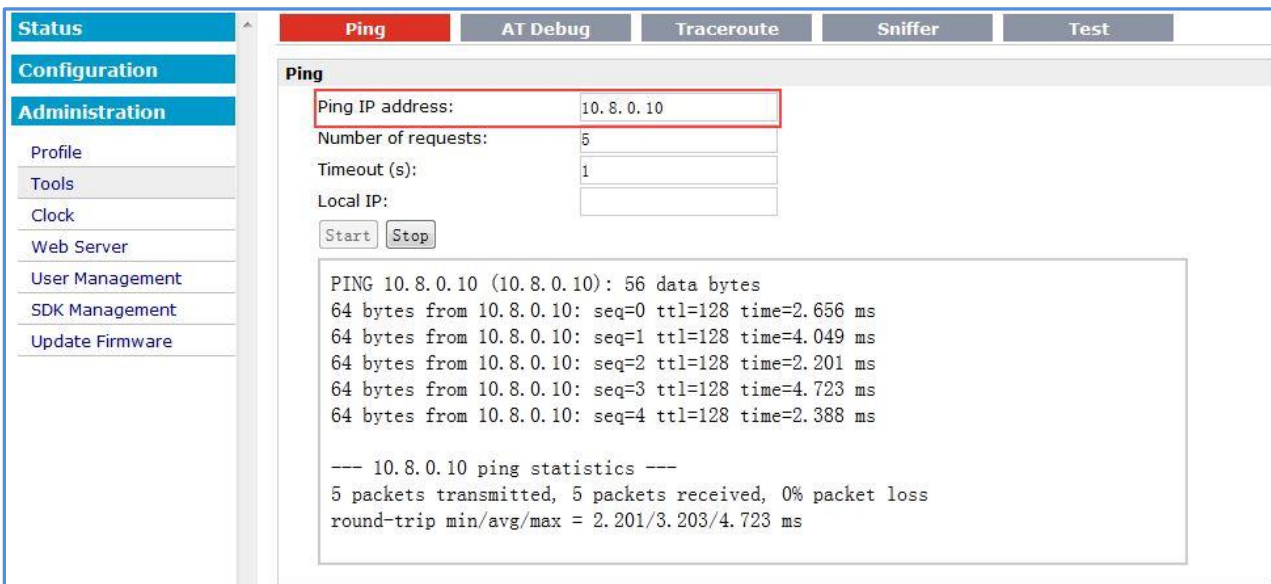
- Check the virtual tunnel on Route table. Browse to "Status" -> "Route".



- Browse to "Administration" -> "Tools" and "Ping".
Ping virtual IP of OpenVPN tunnel and got ICMP reply from OpenVPN Client01.



- Browse to "Administration" -> "Tools" and "Ping".
Ping LAN IP address behind OpenVPN server and got ICMP reply from OpenVPN Client02.



4.4 Testing at Windows OS

4.4.1 Testing at OpenVPN Client01

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

```

Administrator: C:\Windows\system32\cmd.exe
19 276 fe80::c5f2:2ba3:4fd8:d18a/128
    On-link
12 276 fe80::f425:3f2:797c:3f65/128
    On-link
1 306 ff00::/8
    On-link
12 276 ff00::/8
    On-link
16 286 ff00::/8
    On-link
18 276 ff00::/8
    On-link
19 276 ff00::/8
    On-link
=====
Persistent Routes:
None
C:\Users\Ben>route print
  
```

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

```

Administrator: C:\Windows\system32\cmd.exe
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          172.16.0.1      172.16.1.40     276
10.8.0.0               255.255.255.0   10.8.0.5        10.8.0.6        30
10.8.0.4               255.255.255.252 On-link         10.8.0.6        286
10.8.0.6               255.255.255.255 On-link         10.8.0.6        286
10.8.0.7               255.255.255.255 On-link         10.8.0.6        286
127.0.0.0              255.0.0.0       On-link         127.0.0.1       306
127.0.0.1              255.255.255.255 On-link         127.0.0.1       306
127.255.255.255       255.255.255.255 On-link         127.0.0.1       306
172.16.0.0             255.255.0.0     On-link         172.16.1.40     276
172.16.1.40           255.255.255.255 On-link         172.16.1.40     276
172.16.255.255        255.255.255.255 On-link         172.16.1.40     276
192.168.1.0           255.255.255.0   10.8.0.5        10.8.0.6        30
192.168.2.0           255.255.255.0   On-link         172.16.1.40     276
192.168.2.123         255.255.255.255 On-link         172.16.1.40     276
192.168.2.255         255.255.255.255 On-link         172.16.1.40     276
192.168.3.0           255.255.255.0   On-link         172.16.1.40     276
192.168.3.44         255.255.255.255 On-link         172.16.1.40     276
192.168.3.255         255.255.255.255 On-link         172.16.1.40     276
224.0.0.0             240.0.0.0       On-link         127.0.0.1       306
224.0.0.0             240.0.0.0       On-link         172.16.1.40     276
224.0.0.0             240.0.0.0       On-link         10.8.0.6        286
255.255.255.255       255.255.255.255 On-link         127.0.0.1       306
  
```

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

```
Administrator: C:\Windows\system32\cmd.exe
12  276 fe80::f425:3f2:797c:3f65/128
    On-link
1   306 ff00::/8
    On-link
12  276 ff00::/8
    On-link
16  286 ff00::/8
    On-link
18  276 ff00::/8
    On-link
19  276 ff00::/8
    On-link
-----
Persistent Routes:
None

C:\Users\Ben>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=3ms TTL=64
Reply from 192.168.1.11: bytes=32 time=2ms TTL=64
Reply from 192.168.1.11: bytes=32 time=2ms TTL=64
Reply from 192.168.1.11: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

4.4.2 Testing at OpenVPN Client02

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

```
Administrator: C:\Windows\system32\cmd.exe
19  276 fe80::c5f2:2ba3:4fd8:d18a/128
    On-link
12  276 fe80::f425:3f2:797c:3f65/128
    On-link
1   306 ff00::/8
    On-link
12  276 ff00::/8
    On-link
16  286 ff00::/8
    On-link
18  276 ff00::/8
    On-link
19  276 ff00::/8
    On-link
-----
Persistent Routes:
None

C:\Users\Ben>route print
```

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

```

Administrator: C:\Windows\system32\cmd.exe
=====
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.16.0.1       172.16.1.40      276
10.8.0.0                    255.255.255.0    10.8.0.9         10.8.0.10        30
10.8.0.8                    255.255.255.252  On-link          10.8.0.10        286
10.8.0.10                   255.255.255.255  On-link          10.8.0.10        286
10.8.0.11                   255.255.255.255  On-link          10.8.0.10        286
127.0.0.0                   255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                   255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
172.16.0.0                  255.255.0.0      On-link          172.16.1.40      276
172.16.1.40                 255.255.255.255  On-link          172.16.1.40      276
172.16.255.255             255.255.255.255  On-link          172.16.1.40      276
192.168.1.0                 255.255.255.0    10.8.0.9         10.8.0.10        30
192.168.2.0                 255.255.255.0    On-link          172.16.1.40      276
192.168.2.123               255.255.255.255  On-link          172.16.1.40      276
192.168.2.255               255.255.255.255  On-link          172.16.1.40      276
192.168.3.0                 255.255.255.0    On-link          172.16.1.40      276
192.168.3.44                255.255.255.255  On-link          172.16.1.40      276
192.168.3.255               255.255.255.255  On-link          172.16.1.40      276
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
    
```

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

```

Persistent Routes:
None

C:\Users\Ben>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=5ms TTL=64
Reply from 192.168.1.11: bytes=32 time=2ms TTL=64
Reply from 192.168.1.11: bytes=32 time=4ms TTL=64
Reply from 192.168.1.11: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 3ms

C:\Users\Ben>
    
```

4.4.3 Testing between two OpenVPN Clients

1. **Client01:** Ping virtual IP address of Client02 and got ICMP reply from Client02.

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.8.0.10

Pinging 10.8.0.10 with 32 bytes of data:
Reply from 10.8.0.10: bytes=32 time=3ms TTL=128
Reply from 10.8.0.10: bytes=32 time=5ms TTL=128
Reply from 10.8.0.10: bytes=32 time=4ms TTL=128
Reply from 10.8.0.10: bytes=32 time=5ms TTL=128

Ping statistics for 10.8.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Users\Administrator>
    
```

2. **Client02:** Ping virtual IP address of Client01 and got ICMP reply from Client01.

```

C:\Users\Ben>ping 10.8.0.6

Pinging 10.8.0.6 with 32 bytes of data:
Reply from 10.8.0.6: bytes=32 time=6ms TTL=64
Reply from 10.8.0.6: bytes=32 time=3ms TTL=64
Reply from 10.8.0.6: bytes=32 time=6ms TTL=64
Reply from 10.8.0.6: bytes=32 time=3ms TTL=64

Ping statistics for 10.8.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 6ms, Average = 4ms

C:\Users\Ben>
    
```

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".

```

.....
14-06-09 17:04:42 <0> router: sdk-server startup.
14-06-09 17:04:47 <2> router: change network (Null)->(Ethernet - up)
14-06-09 17:04:47 <0> router: system service starting...
14-06-09 17:04:51 <0> router: openvpn server 0 start up.
14-06-09 17:04:51 <1> OpenVPN: OpenVPN 2.2.2 arm-linux [SSL] [LZO2] [EPOLL] [eurephia] built on Nov 19 2013
14-06-09 17:04:51 <3> OpenVPN: NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined
scripts or executables
14-06-09 17:04:51 <3> OpenVPN: WARNING: file '/cfg/x509/openvpn/server_0/server.key' is group or others
accessible
14-06-09 17:04:51 <1> OpenVPN: TUN/TAP device tun0 opened
14-06-09 17:04:51 <1> OpenVPN: /sbin/ifconfig tun0 10.8.0.1 pointopoint 10.8.0.2 mtu 1500
14-06-09 17:04:51 <1> OpenVPN: GID set to root
    
```

```
14-06-09 17:04:51 <1> OpenVPN: UID set to root
14-06-09 17:04:51 <1> OpenVPN: UDPv4 link local (bound): [undef]:1194
14-06-09 17:04:51 <1> OpenVPN: UDPv4 link remote: [undef]
14-06-09 17:04:51 <1> OpenVPN: Initialization Sequence Completed
14-06-09 17:05:45 <0> router: sent:AT+COPS?
14-06-09 17:05:45 <0> router: rcvd:
ERROR
14-06-09 17:07:07 <1> OpenVPN: Re-using SSL/TLS context
14-06-09 17:07:07 <1> OpenVPN: LZO compression initialized
14-06-09 17:07:07 <1> OpenVPN: [Client01] Peer Connection Initiated with 10.168.1.2:53865
14-06-09 17:07:10 <3> OpenVPN: IPv6 in tun mode is not supported in OpenVPN 2.2
14-06-09 17:07:27 <1> OpenVPN: Re-using SSL/TLS context
14-06-09 17:07:27 <1> OpenVPN: LZO compression initialized
14-06-09 17:07:27 <1> OpenVPN: [Client02] Peer Connection Initiated with 10.196.123.40:63021
.....
```

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-MSUC++ [SSL] [LZO2] [PKCS11] built on Dec 15 2011
Originally developed by James Yonan
Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>
```