Application Note

OpenVPN Client with Username&Password for R3000

Document Name:	**Application Note**
Version:	**v.1.0.0**
Date:	**2014-06-04**
Status:	**Confidential**
DocID:	**RT_AN004_R3000 S_OpenVPN Client with Username&Password for R3000**

www.robustel.com

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, we using certificate and username/password for authentication at this time. A PC need to install the OpenVPN Easy-RSA certificate authority and create & sign the certificates. Any Easy-RSA is free and simple to use.

1.3 Rectifications

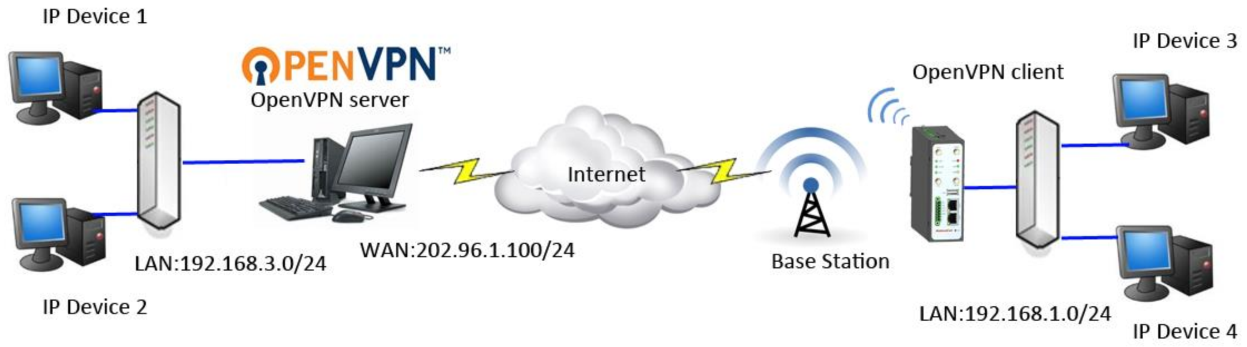
Appreciate for the corrections and Rectifications to this Application Note, and if there are requests for new Application Notes please also send to email address: support@robustel.com .

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
2014-06-04	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. Multiple OpenVPN clients can connect to the same OpenVPN server.

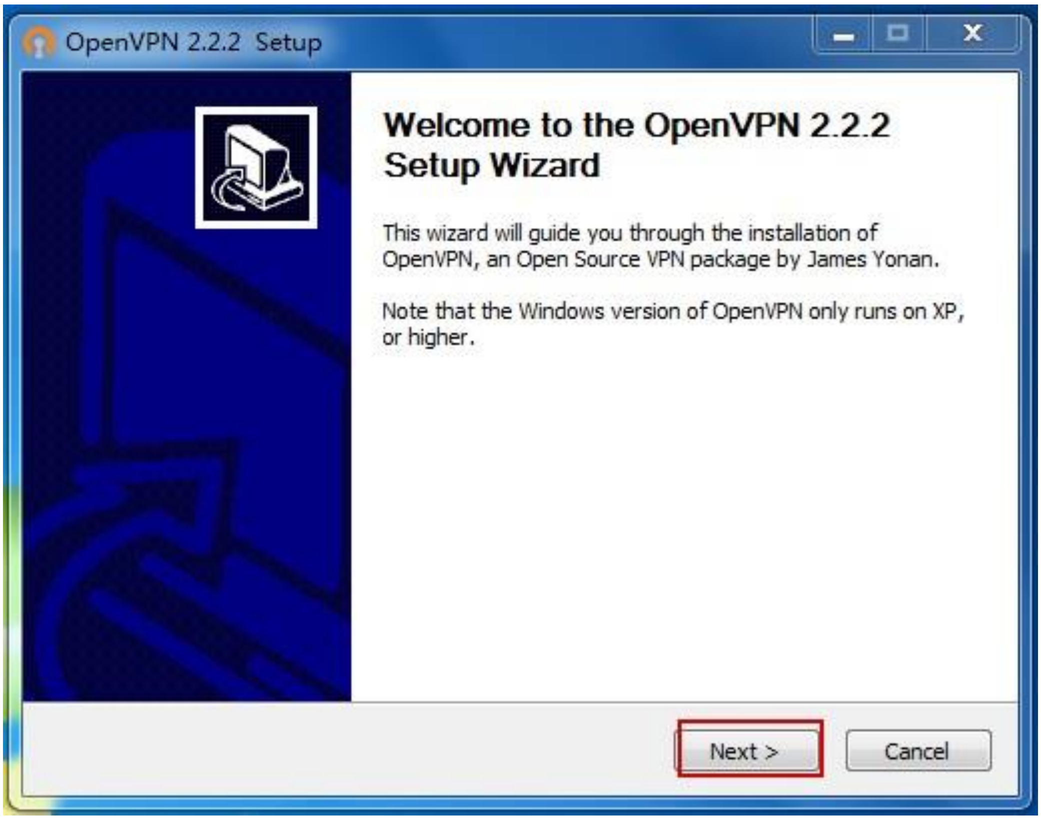
Note: *if OpenVPN server behind a Gateway Router, the Router must open the port of 1194 and port forwarding to the internal server. 1194 is the default port number for OpenVPN negotiation.*

Chapter 3. Configuration

3.1 OpenVPN Installation on Windows

This step should be done on 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.



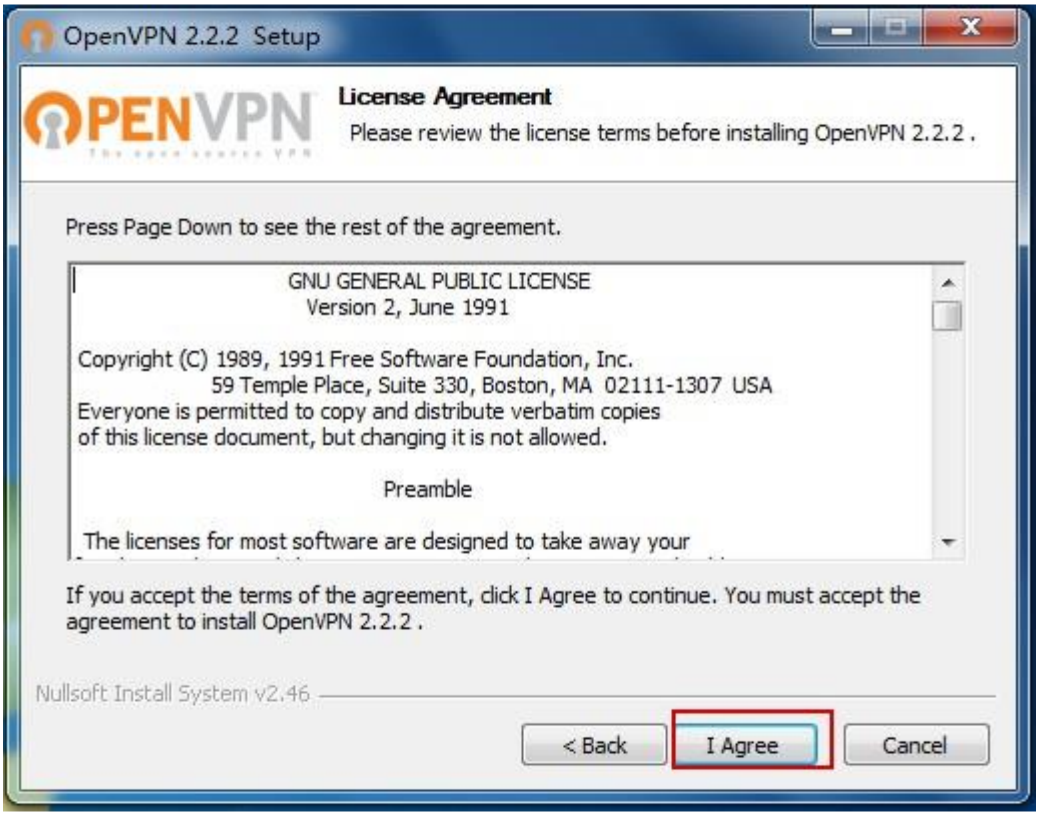
OpenVPN 2.2.2 Setup

Welcome to the OpenVPN 2.2.2 Setup Wizard

This wizard will guide you through the installation of OpenVPN, an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN only runs on XP, or higher.

2. License Agreement.



OpenVPN 2.2.2 Setup

License Agreement

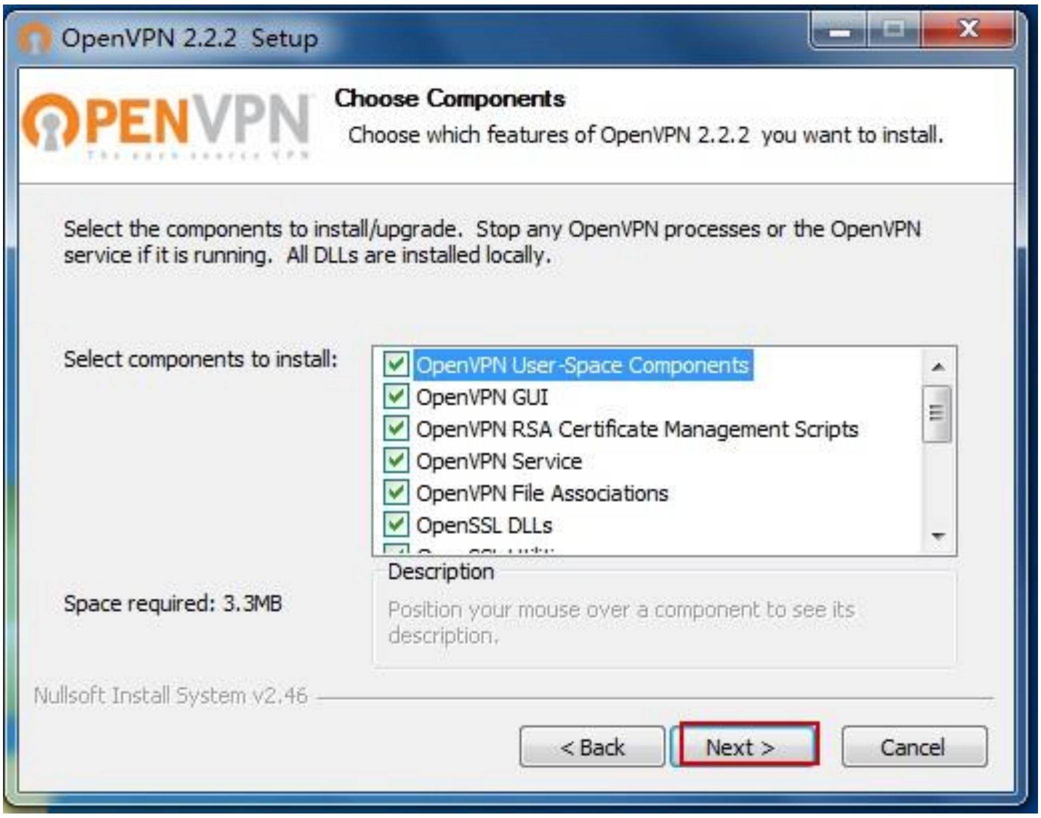
Please review the license terms before installing OpenVPN 2.2.2 .

Press Page Down to see the rest of the agreement.

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
              59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                            Preamble

 The licenses for most software are designed to take away your
```

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.2.2 .

3. Select all the options by default.



OpenVPN 2.2.2 Setup

Choose Components

Choose which features of OpenVPN 2.2.2 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

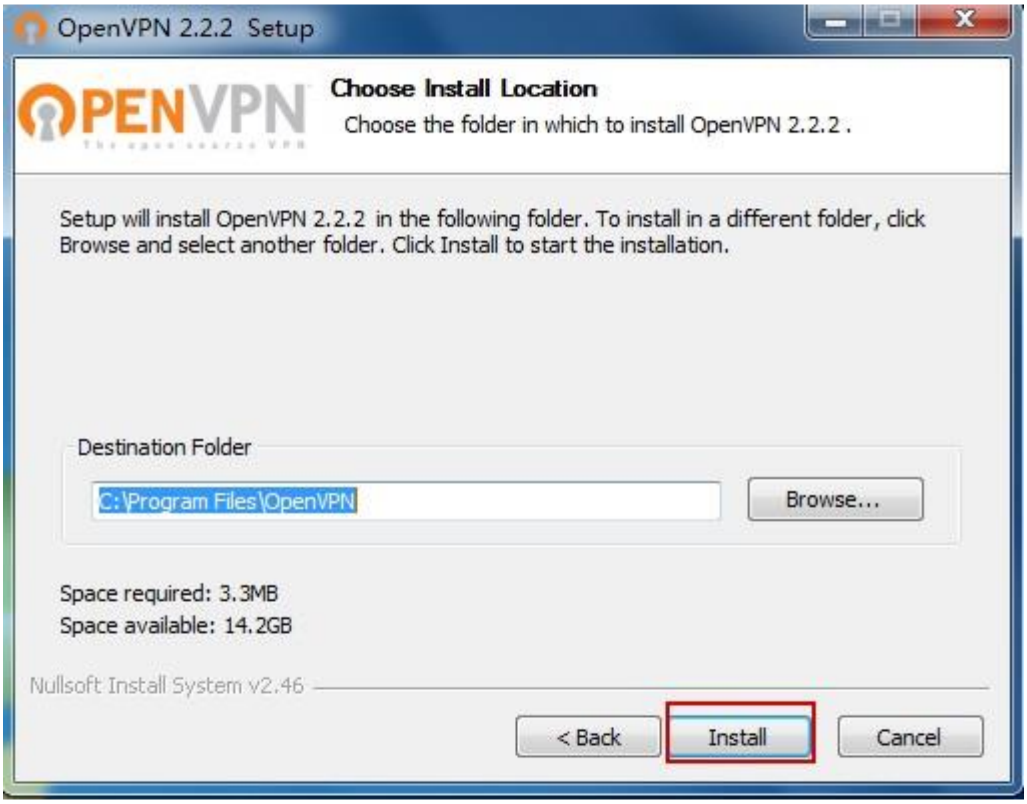
- ☑ OpenVPN User-Space Components
- ☑ OpenVPN GUI
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ OpenVPN Service
- ☑ OpenVPN File Associations
- ☑ OpenSSL DLLs

Space required: 3.3MB

Description

Position your mouse over a component to see its description.

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



OpenVPN 2.2.2 Setup

Choose Install Location

Choose the folder in which to install OpenVPN 2.2.2 .

Setup will install OpenVPN 2.2.2 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

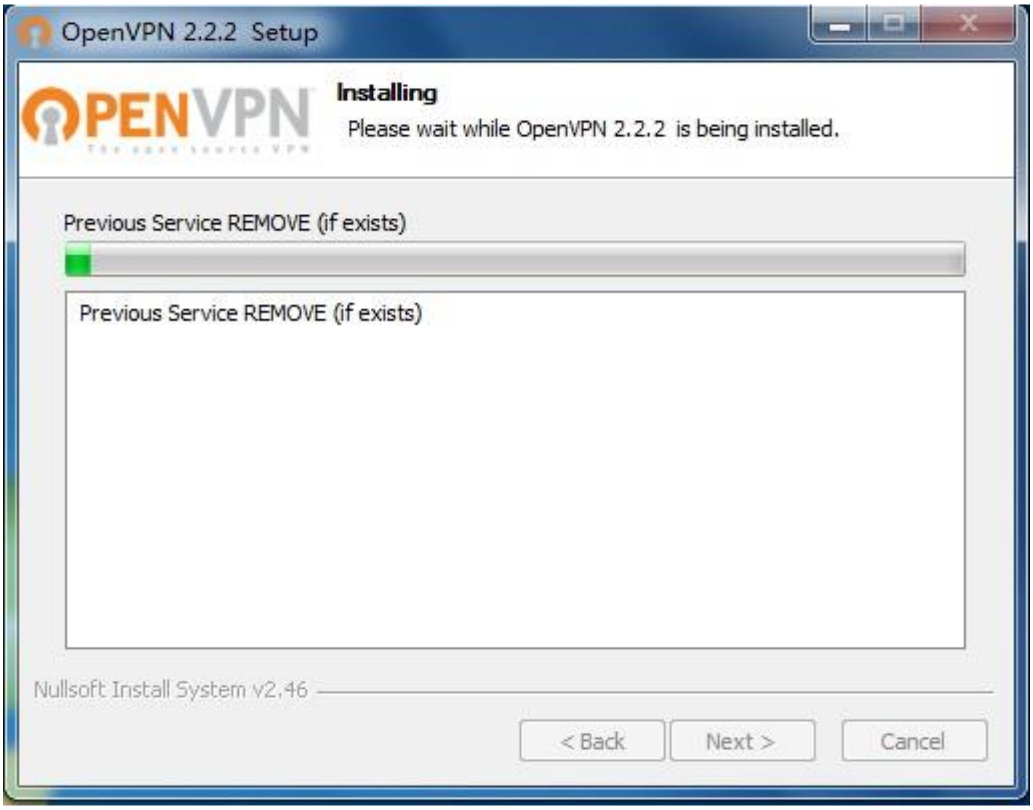
Destination Folder

C:\Program Files\OpenVPN

Space required: 3.3MB

Space available: 14.2GB

5. The installation schedule.



OpenVPN 2.2.2 Setup

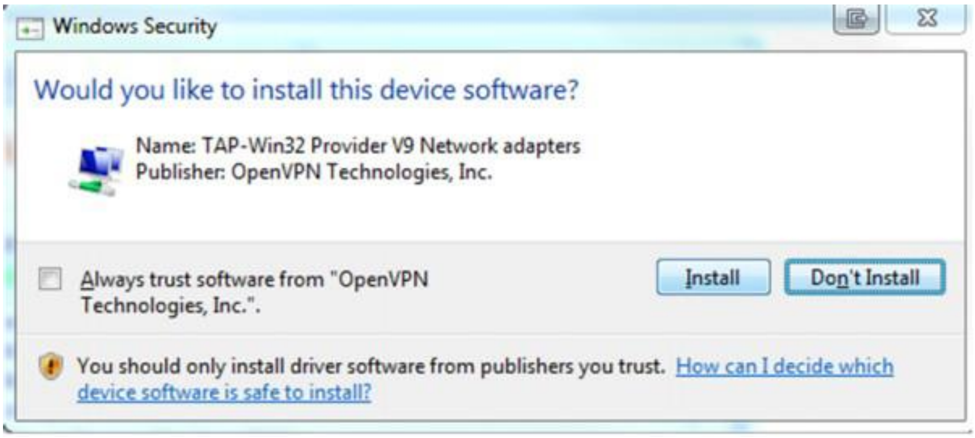
Installing

Please wait while OpenVPN 2.2.2 is being installed.

Previous Service REMOVE (if exists)

Previous Service REMOVE (if exists)

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



Windows Security

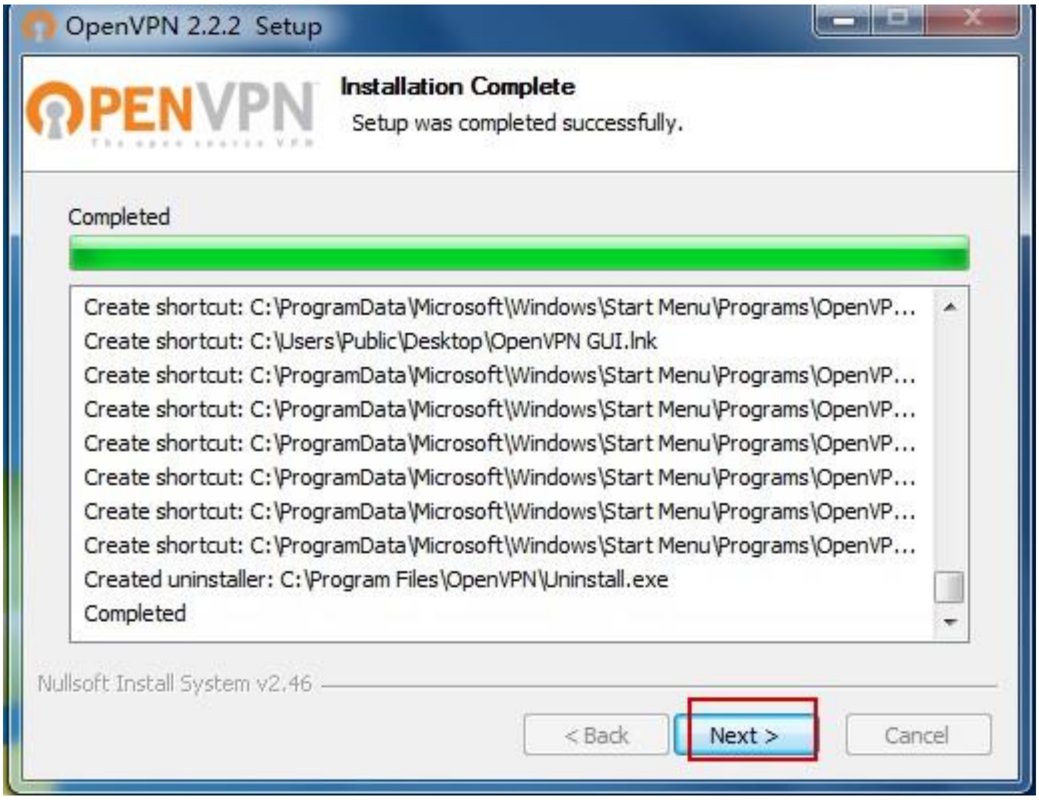
Would you like to install this device software?

Name: TAP-Win32 Provider V9 Network adapters
Publisher: OpenVPN Technologies, Inc.

□ Always trust software from "OpenVPN Technologies, Inc.".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

7. The installation will be completed.



OpenVPN 2.2.2 Setup

Installation Complete

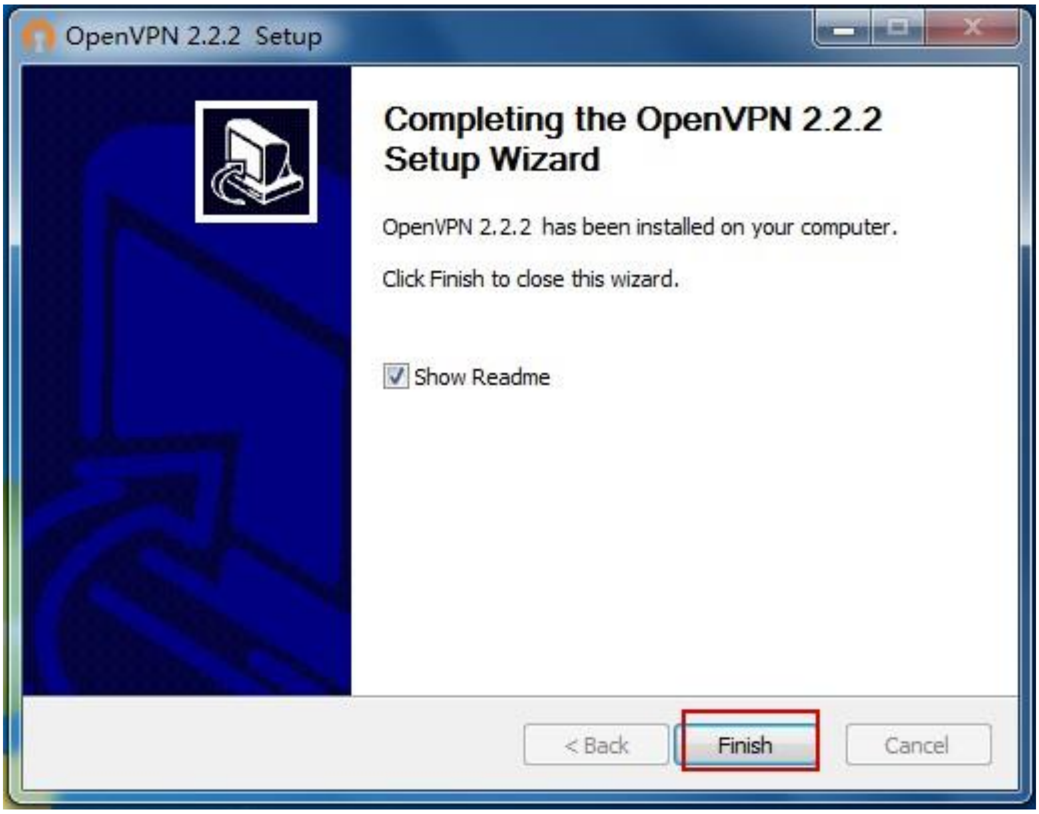
Setup was completed successfully.

Completed

```
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\Users\Public\Desktop\OpenVPN GUI.lnk
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Completed
```

Nullsoft Install System v2.46

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



OpenVPN 2.2.2 Setup

Completing the OpenVPN 2.2.2 Setup Wizard

OpenVPN 2.2.2 has been installed on your computer.

Click Finish to close this wizard.

☑ Show Readme

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).

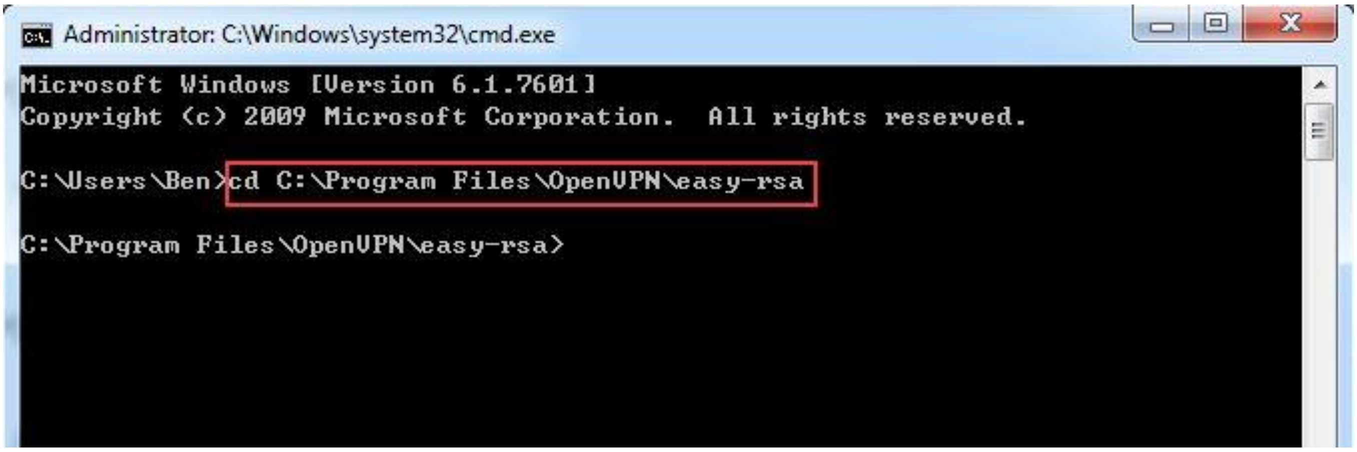
The features of OpenVPN:

- 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

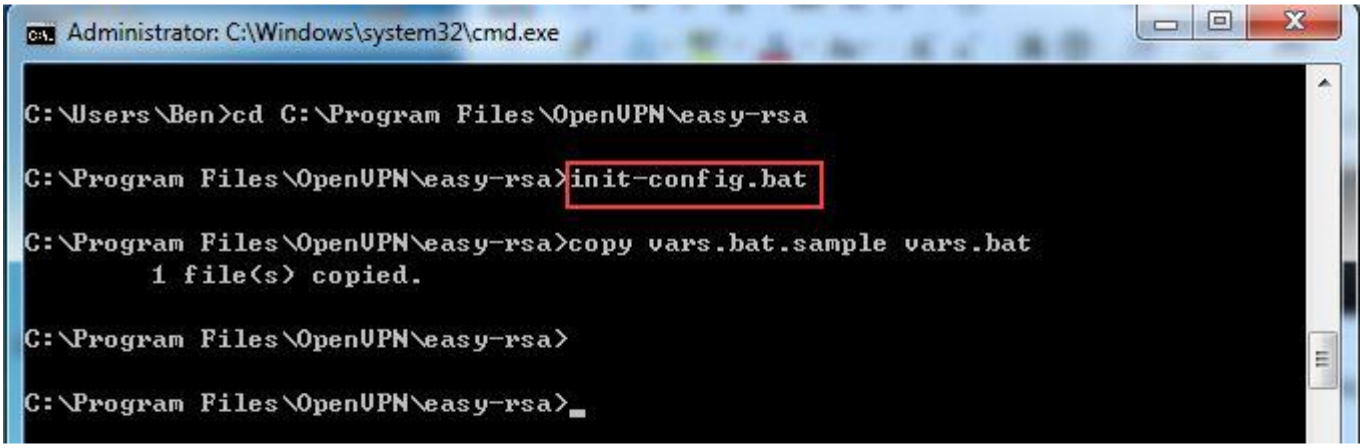
In this section we will generate a master CA certificate/key, one server certificate/key and one client certificate/key.

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**.



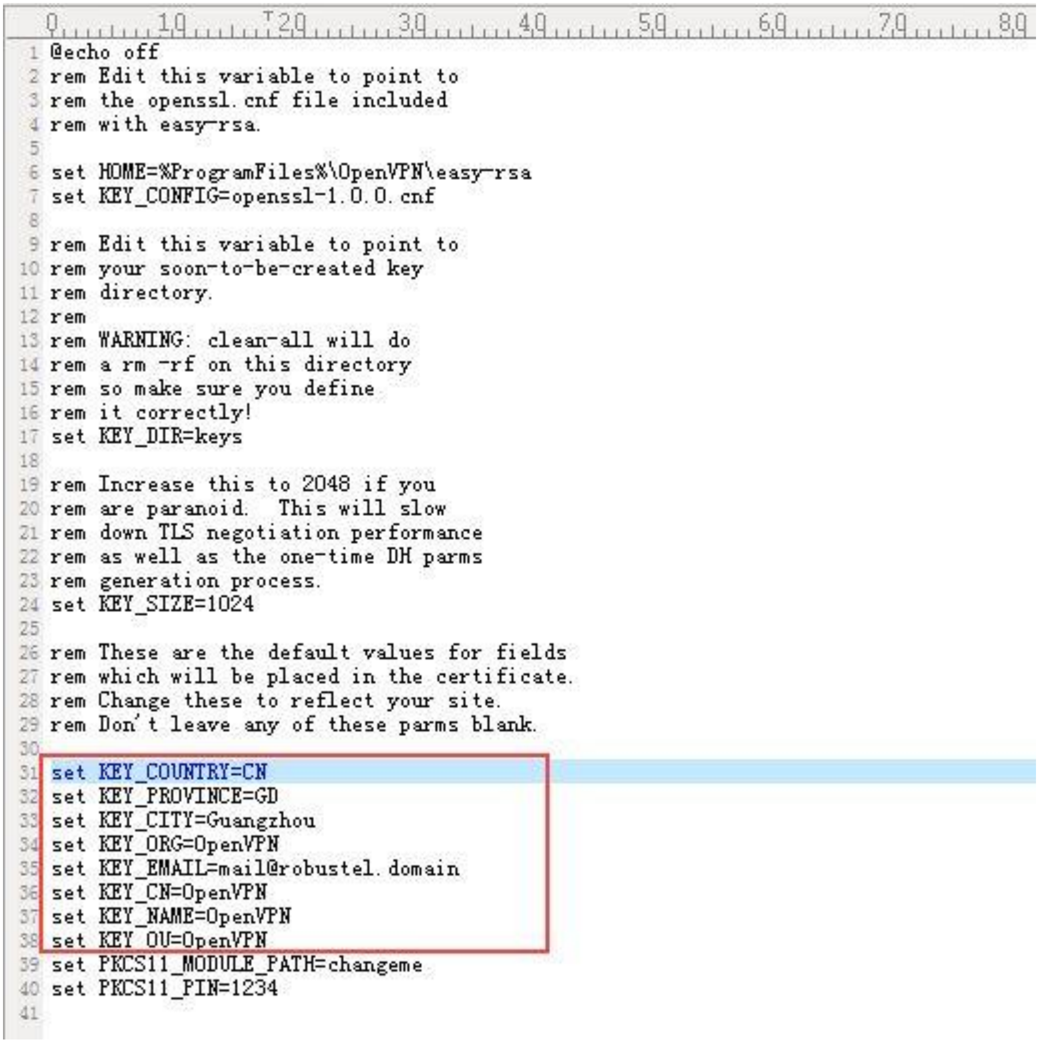
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Program Files\OpenVPN\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).



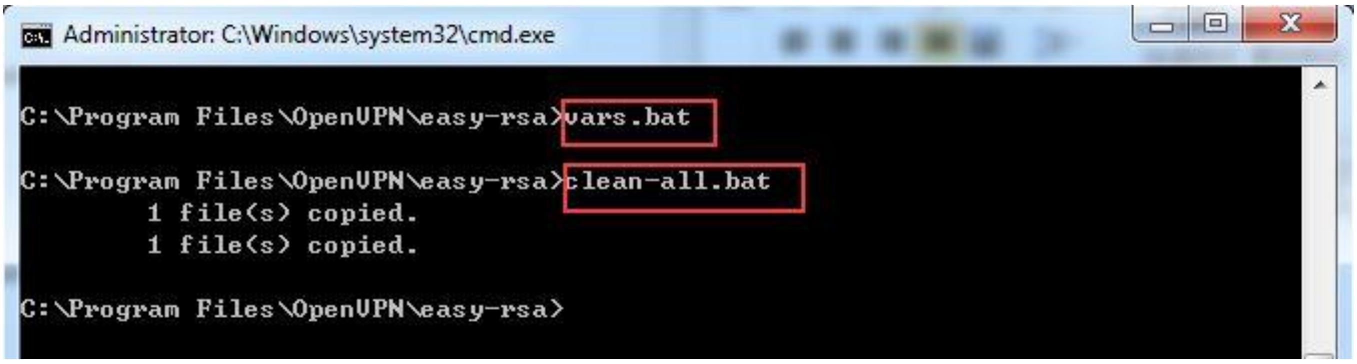
```
C:\Users\Ben>cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>init-config.bat

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

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

C:\Program Files\OpenVPN\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.



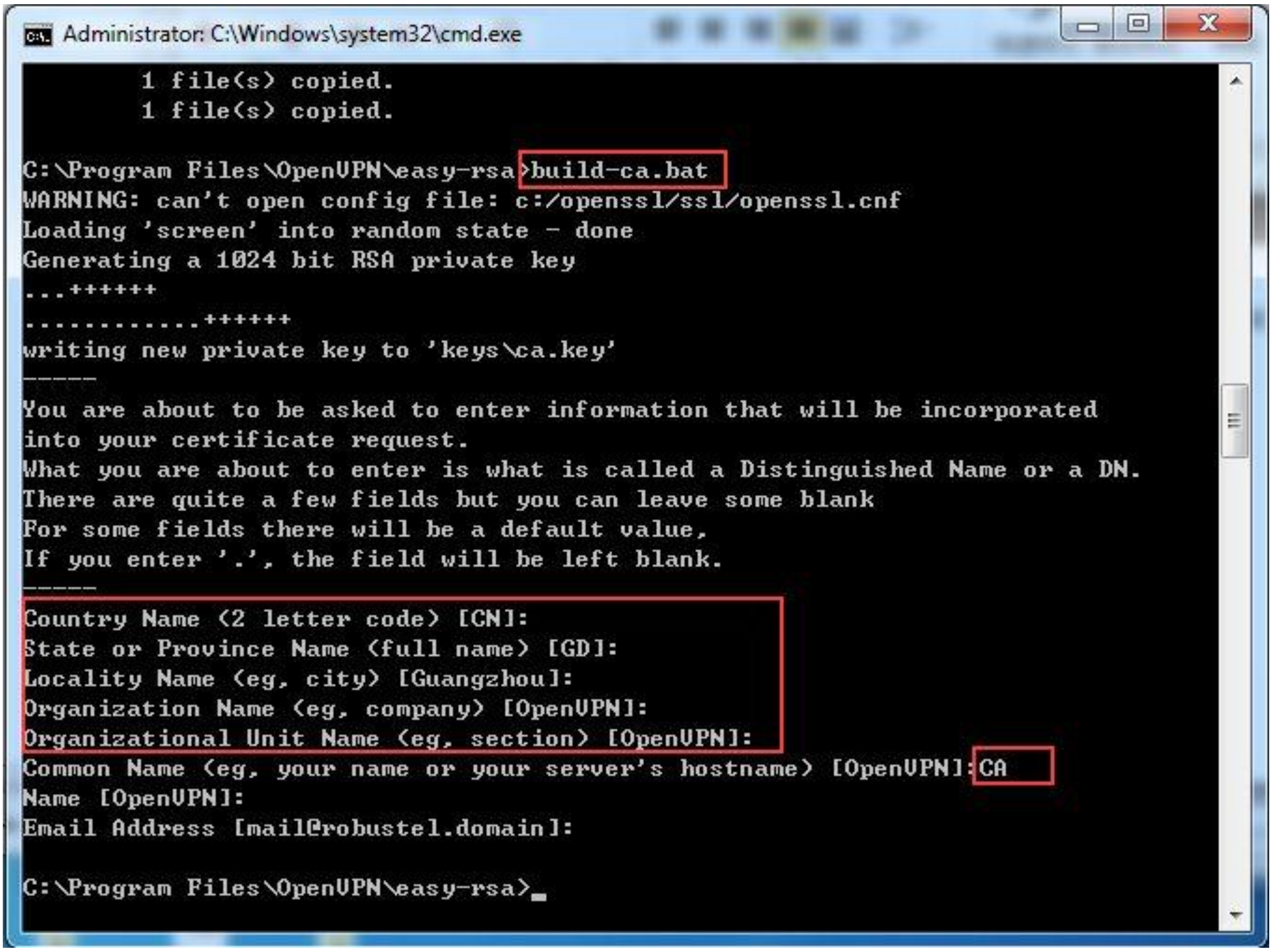
```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=Guangzhou
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@robustel.domain
set KEY_CN=OpenVPN
set KEY_NAME=OpenVPN
set KEY_OU=OpenVPN
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

4. Run the following commands to initialize the environment.



```
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>
```

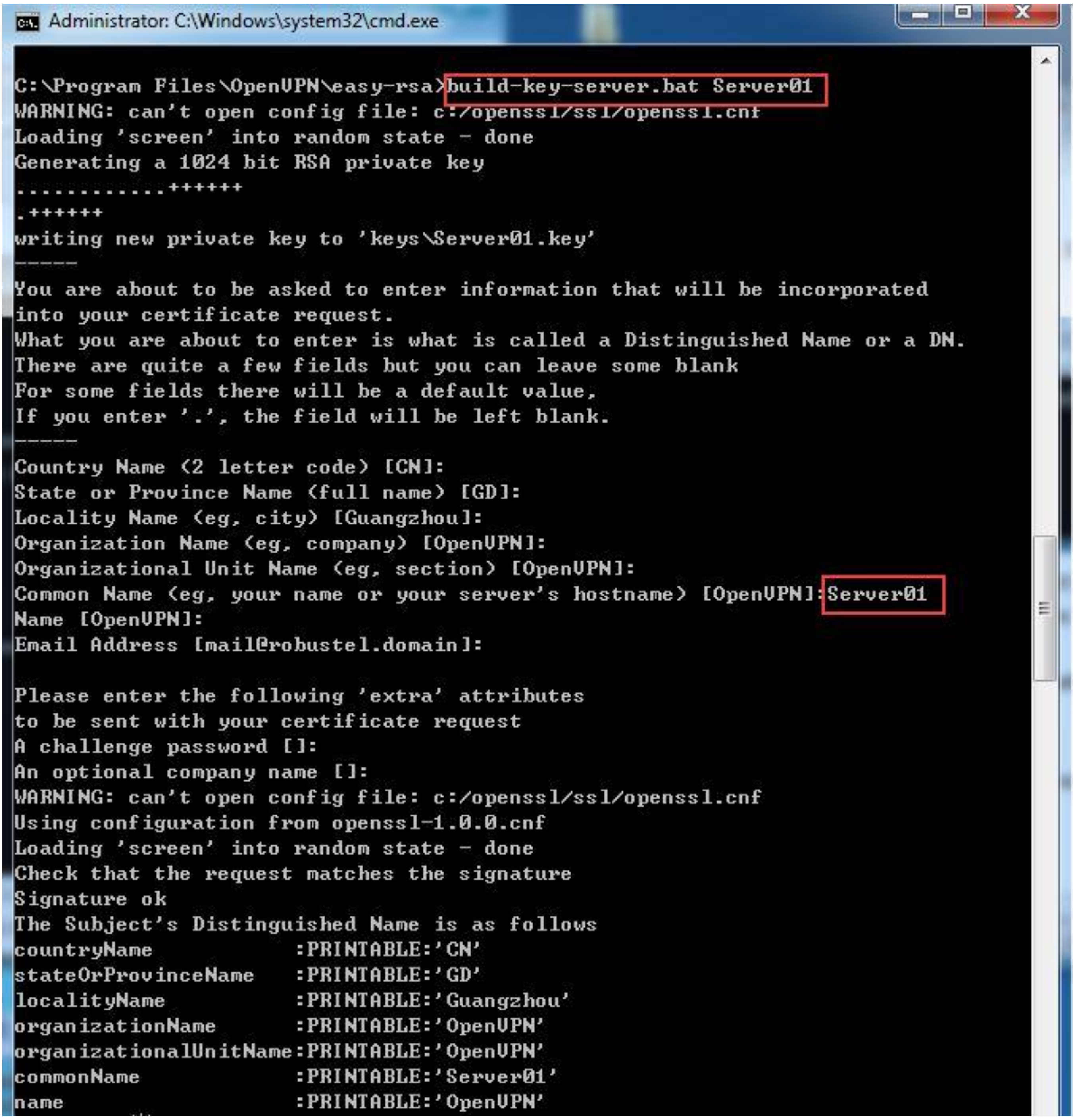
5. The command(build-ca.bat) will build the certificate authority(CA) certificate and key by invoking the interactive openssl command.



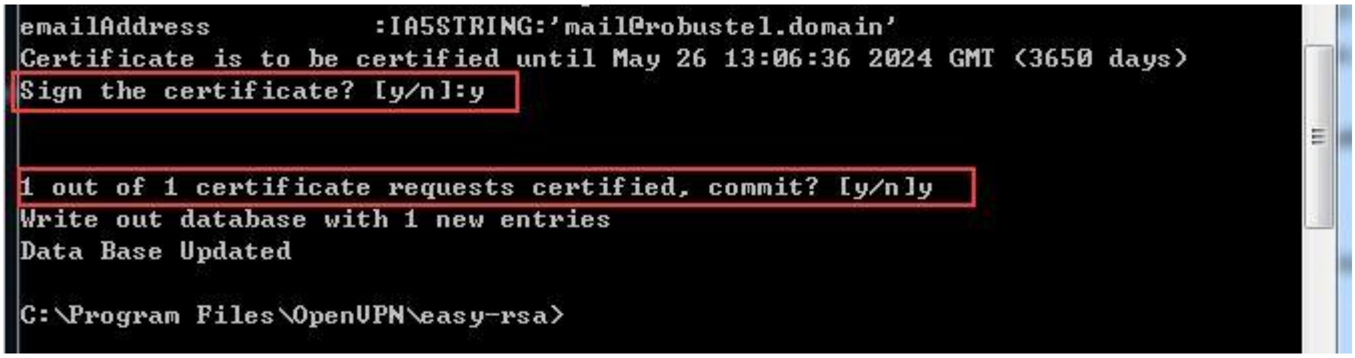
```
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\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) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:CA
Name [OpenVPN]:
Email Address [mail@robustel.domain]:

C:\Program Files\OpenVPN\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**".



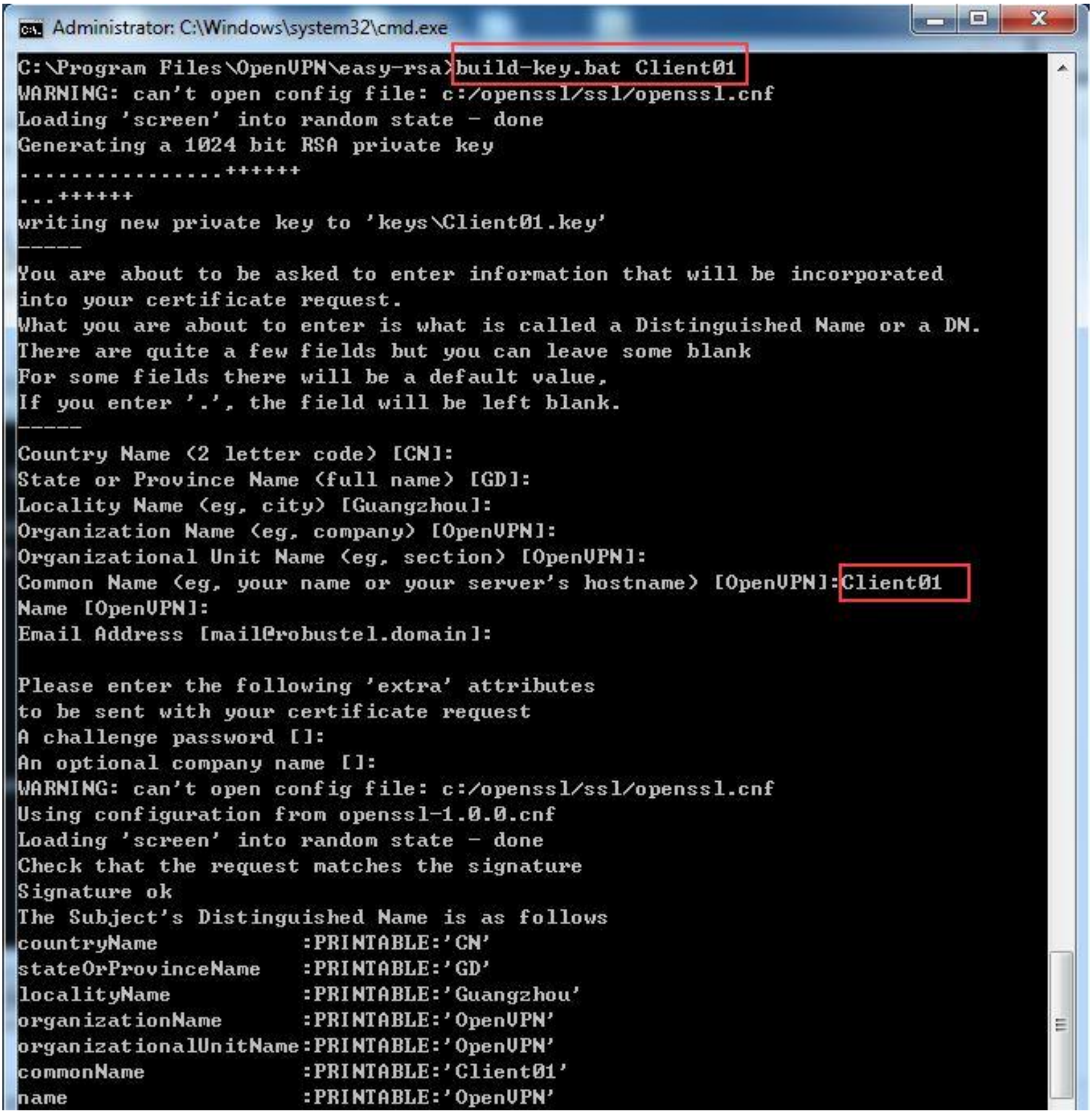
```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat Server01
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
............++++++
.++++++
writing new private key to 'keys\Server01.key'
-----
You are about 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'
```



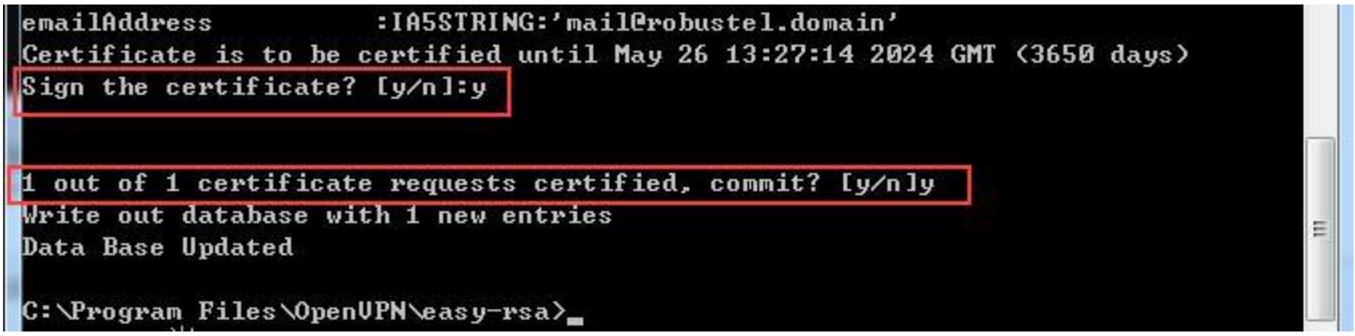
```
emailAddress          :IA5STRING:'mail@robustel.domain'
Certificate is to be certified until May 26 13:06:36 2024 GMT (3650 days)
Sign the certificate? [y/n]:y


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.



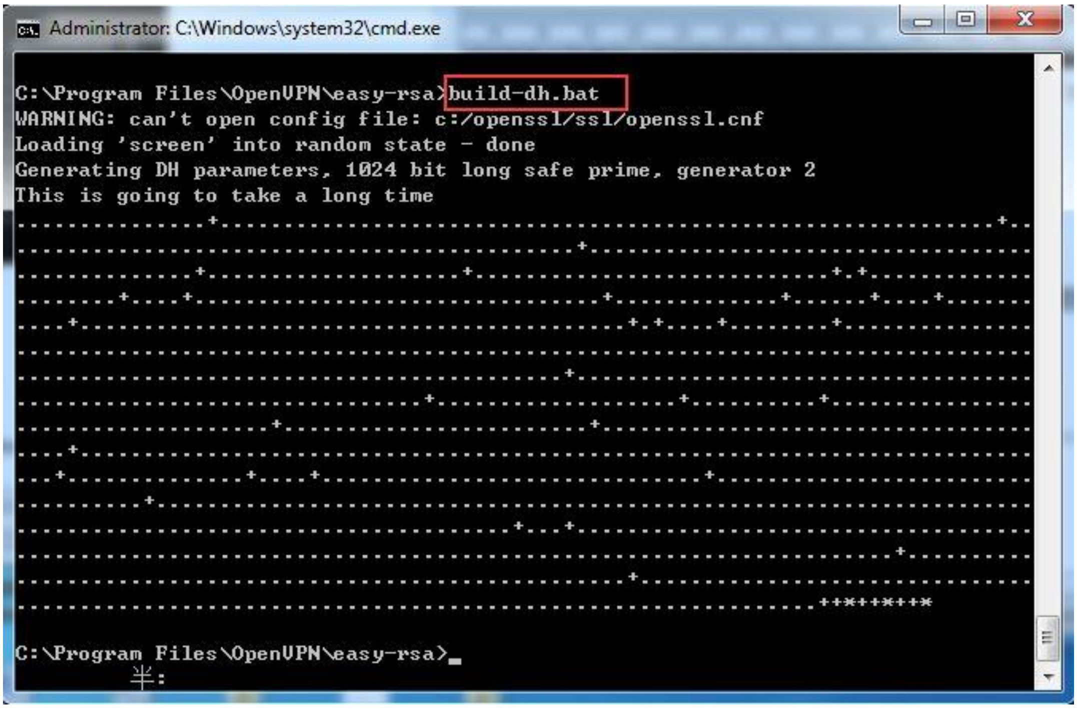
```
C:\Program Files\OpenVPN\easy-rsa>build-key.bat Client01
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
................++++++
...++++++
writing new private key to 'keys\Client01.key'
-----
You are about 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>_
```

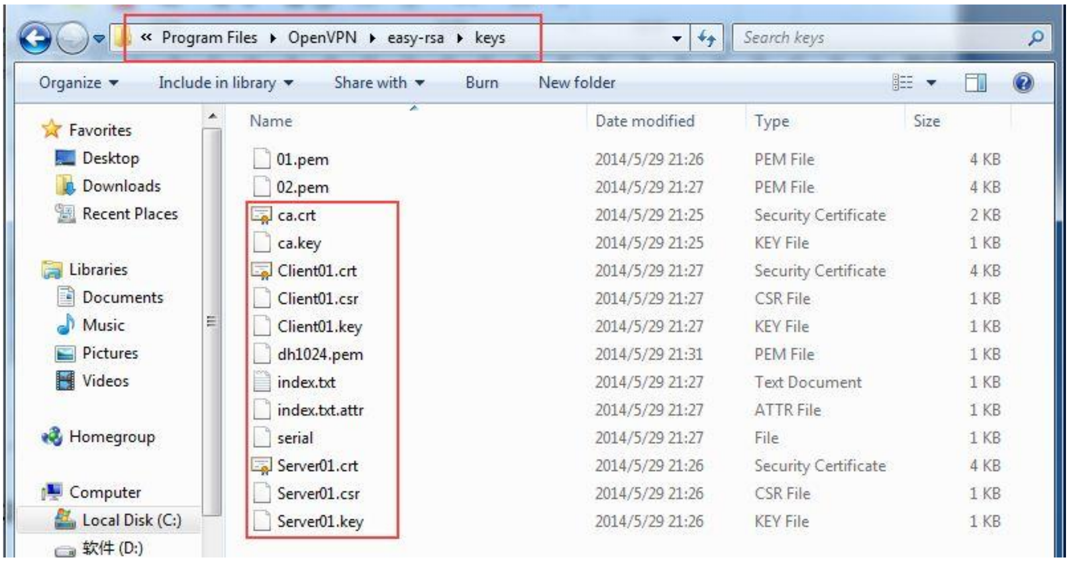
Note: ***<u>Client01</u>*** *in “**build-key-server.bat Client01**” is the file name of certificate(the name of public key and private key). **Always use a unique common name for each client**.*

8. Generate Diffie Hellman parameters.



```
C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
WARNING: can't open config file: c:/openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
...............+.............................................................+..
............................................+...................................
..............+....................+............................+.+.............
........+....+................................+.............+......+....+.......
....+...........................................+.+....+........+...............
................................................................................
...........................................+....................................
................................+...................+..........+................
....................+........................+..................................
....+...........................................................................
...+..............+....+..............................+.........................
..........+.....................................................................
.......................................+...+....................................
.....................................................................+..........
................................................+...............................
...............................................................++*++*++*

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

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

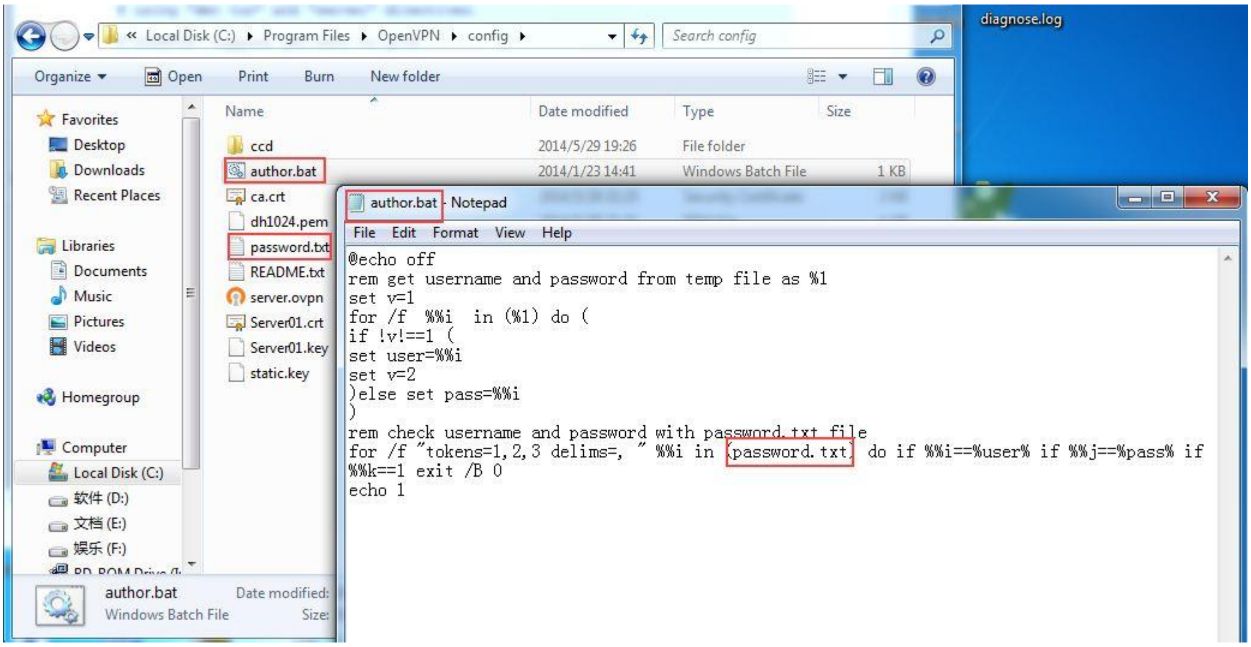


Name	Date modified	Type	Size
01.pem	2014/5/29 21:26	PEM File	4 KB
02.pem	2014/5/29 21:27	PEM File	4 KB
ca.crt	2014/5/29 21:25	Security Certificate	2 KB
ca.key	2014/5/29 21:25	KEY File	1 KB
Client01.crt	2014/5/29 21:27	Security Certificate	4 KB
Client01.csr	2014/5/29 21:27	CSR File	1 KB
Client01.key	2014/5/29 21:27	KEY File	1 KB
dh1024.pem	2014/5/29 21:31	PEM File	1 KB
index.txt	2014/5/29 21:27	Text Document	1 KB
index.txt.attr	2014/5/29 21:27	ATTR File	1 KB
serial	2014/5/29 21:27	File	1 KB
Server01.crt	2014/5/29 21:26	Security Certificate	4 KB
Server01.csr	2014/5/29 21:26	CSR File	1 KB
Server01.key	2014/5/29 21:26	KEY File	1 KB

3.2.3 Manage the username/password script for OpenVPN

1. Generate one Notepad file and rename it as "**author.bat**".
   Path: C:\Program Files\OpenVPN\config

```
@echo off
rem get username and password from temp file as %1
set v=1
for /f    %%i    in (%1) do (
if !v!==1 (
set user=%%i
set v=2
)else set pass=%%i
)
rem check username and password with password.txt file
for /f "tokens=1,2,3 delims=, " %%i in (password.txt) do if %%i==%user% if %%j==%pass% if %%k==1 exit /B 0
echo 1
```



Name	Date modified	Type	Size
ccd	2014/5/29 19:26	File folder	
author.bat	2014/1/23 14:41	Windows Batch File	1 KB
ca.crt			
dh1024.pem			
password.txt			
README.txt			
server.ovpn			
Server01.crt			
Server01.key			
static.key			

```
@echo off
rem get username and password from temp file as %1
set v=1
for /f  %%i  in (%1) do (
if !v!==1 (
set user=%%i
set v=2
)else set pass=%%i
)
rem check username and password with password.txt file
for /f "tokens=1,2,3 delims=, " %%i in (password.txt) do if %%i==%user% if %%j==%pass% if
%%k==1 exit /B 0
echo 1
```

Note: *keep the default code of scripts, and password.txt is the file which registerd the multiple clients' username and password.*

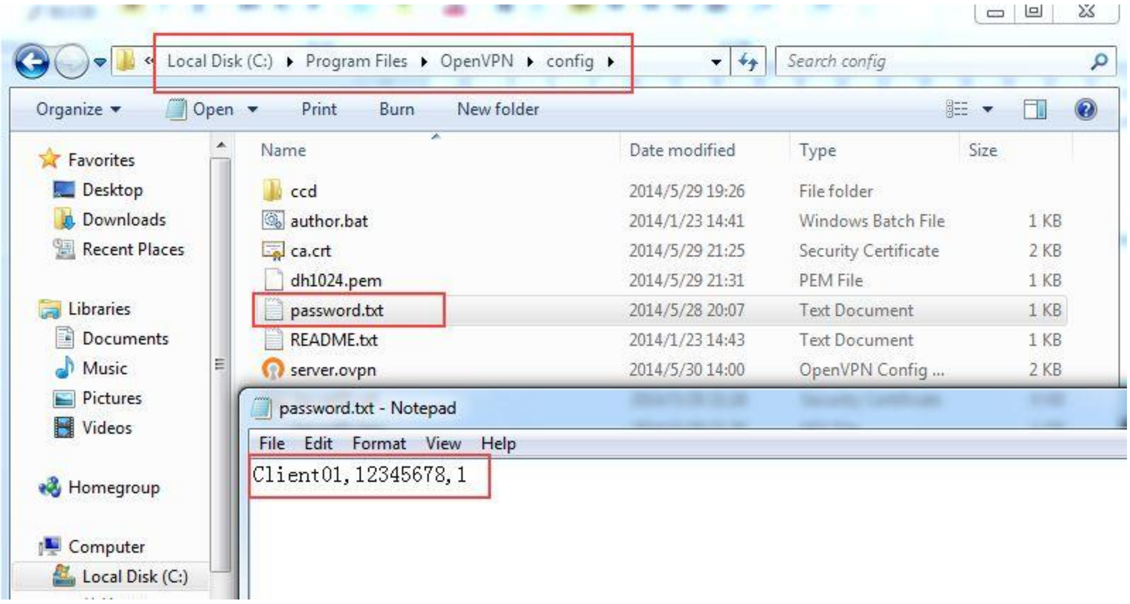
2. Edit file for username and password.

- In the configuration file and directory to create a new password.txt file. Add the content in the following format. Use ", "as a delimiter, format:

  The Common name, password, whether to enable (1, enable, 0, disabled)

  User1, passowrd1, 1

  User2, password2, 0



Name	Date modified	Type	Size
ccd	2014/5/29 19:26	File folder	
author.bat	2014/1/23 14:41	Windows Batch File	1 KB
ca.crt	2014/5/29 21:25	Security Certificate	2 KB
dh1024.pem	2014/5/29 21:31	PEM File	1 KB
password.txt	2014/5/28 20:07	Text Document	1 KB
README.txt	2014/1/23 14:43	Text Document	1 KB
server.ovpn	2014/5/30 14:00	OpenVPN Config ...	2 KB

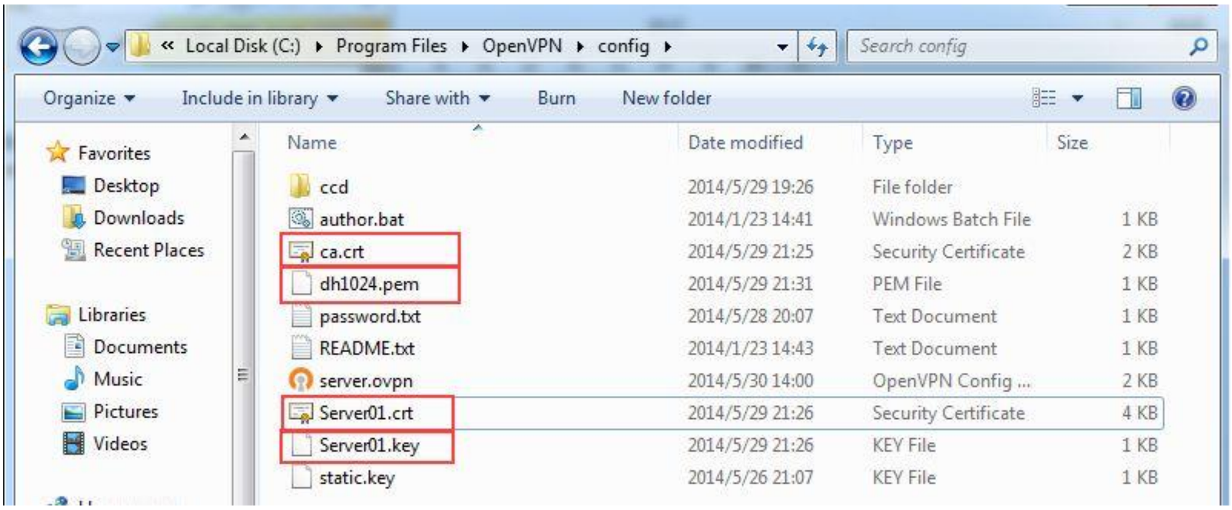
```
Client01,12345678,1
```

3.3 Windows OpenVPN Server Configuration

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

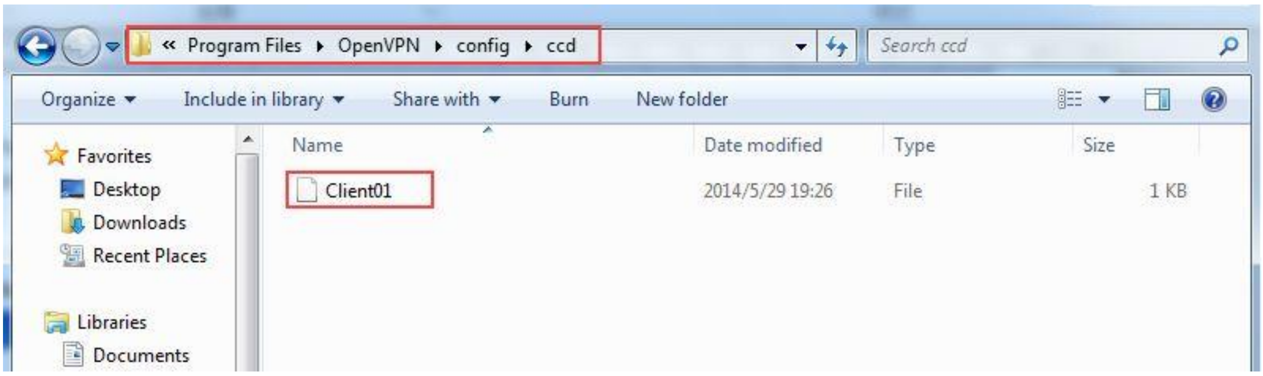
3.3.1 Open and Edit the server.ovpn file

1. Copy the required files to the OpenVPN server configuration directory.
   Path: C:\Program Files\OpenVPN\config



Name	Date modified	Type	Size
ccd	2014/5/29 19:26	File folder	
author.bat	2014/1/23 14:41	Windows Batch File	1 KB
ca.crt	2014/5/29 21:25	Security Certificate	2 KB
dh1024.pem	2014/5/29 21:31	PEM File	1 KB
password.txt	2014/5/28 20:07	Text Document	1 KB
README.txt	2014/1/23 14:43	Text Document	1 KB
server.ovpn	2014/5/30 14:00	OpenVPN Config ...	2 KB
Server01.crt	2014/5/29 21:26	Security Certificate	4 KB
Server01.key	2014/5/29 21:26	KEY File	1 KB
static.key	2014/5/26 21:07	KEY File	1 KB

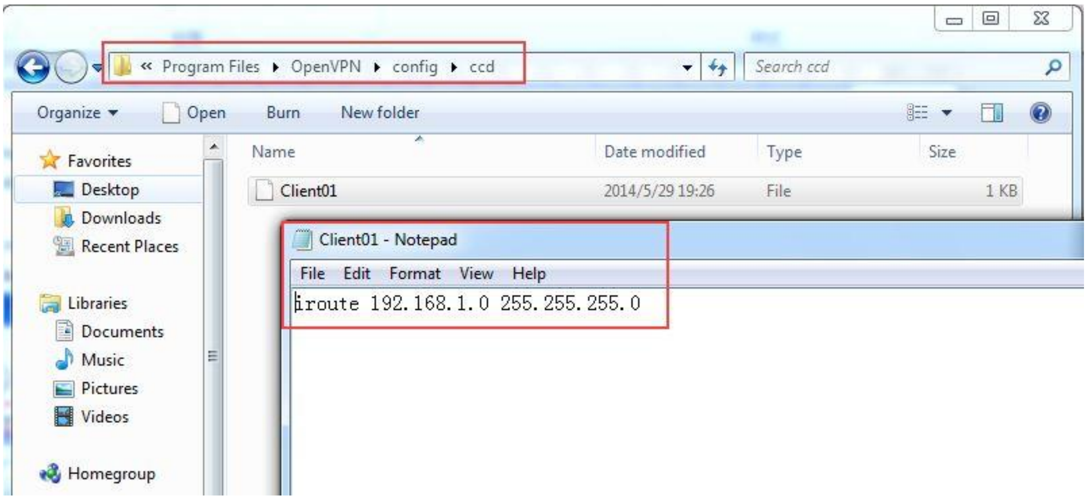
2. To assign specific IP addresses to specific clients or if a connecting client has a private subnet behind it that should also have VPN access, use the subdirectory "ccd" for client-specific configuration files Add a new folder name “ccd”, then create a new notepad and rename it without suffix.



Name	Date modified	Type	Size
Client01	2014/5/29 19:26	File	1 KB

Note: *”Client01”is the Common Name predefined in the certificate but not the file name.*

3. Edit this notepad and save it.



```
iroute 192.168.1.0 255.255.255.0
```

Note: *192.168.1.0/24 is the subnet behind R3000.*

4. The configuration of the server.ovpn.

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

# OpenVPN working in Server mode,
# can support multiple client dynamic access at the same time.
```

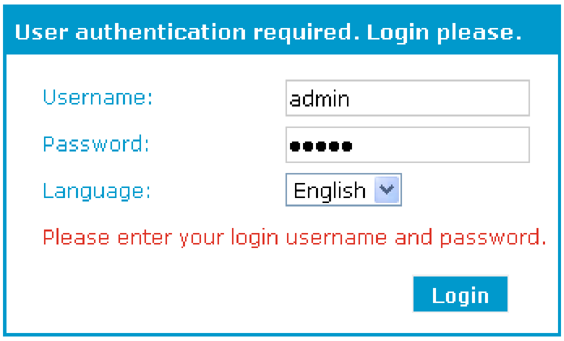
```
mode server

# OpenVPN client could not provide the certificate
client-cert-not-required

# Login Name is the Common Name
username-as-common-name

# Activate login authentication, asks for the username and password
auth-user-pass-verify author.bat via-env

# 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

# 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

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).   Each client
# and the server must have their own cert and
# key file.   The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.   Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert Server01.crt
key Server01.key   # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#     openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh1024.pem

# 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

# 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.
```

```
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# 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 192.168.3.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# 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

# 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

# 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

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.   Use one
# or the other (but not both).
;log              openvpn.log
;log-append   openvpn.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.



User authentication required. Login please.

Username: admin

Password: ●●●●●

Language: English

Please enter your login username and password.

Note: Factory Settings when login Web GUI

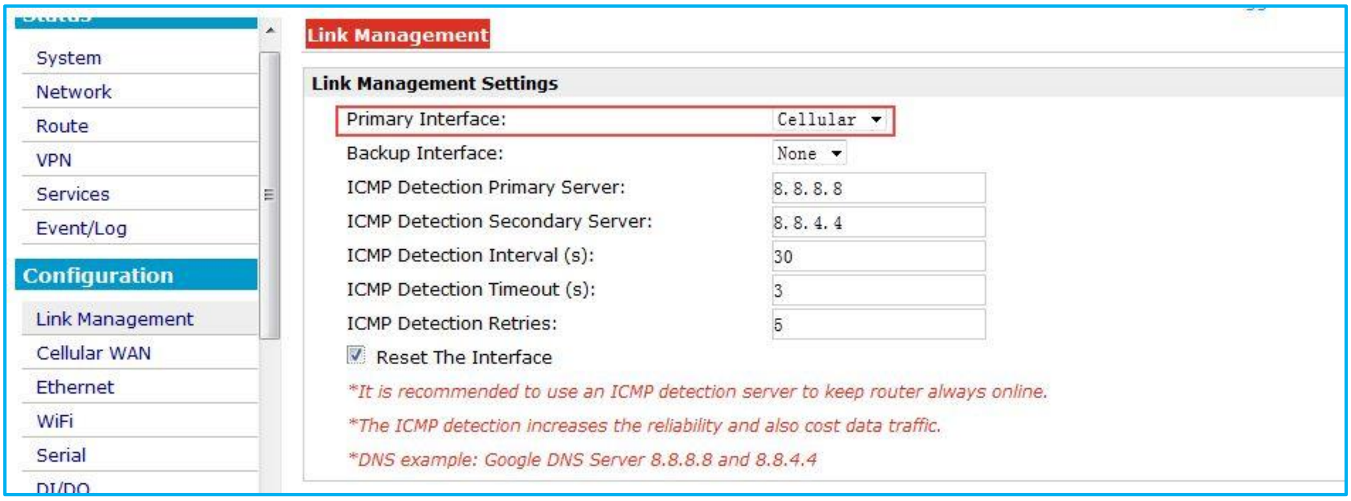
Item	Description
Username	admin
Password	admin
Eth0	192.168.0.1/255.255.255.0, LAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled.

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

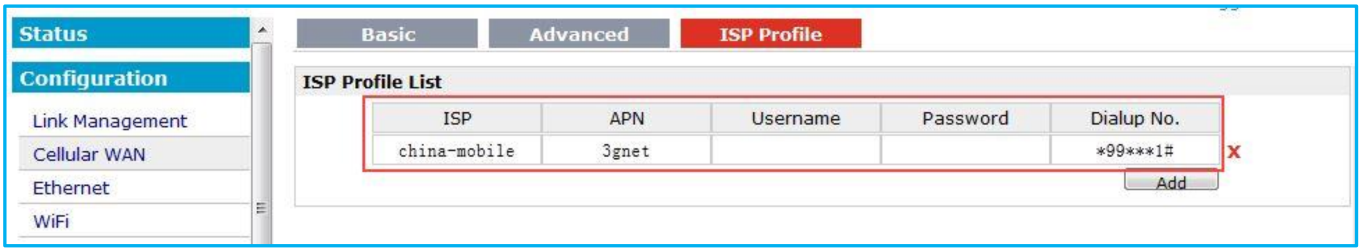
3.4.2 Configure Cellular WAN

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



ISP Profile List

ISP	APN	Username	Password	Dialup No.
china-mobile	3gnet			*99***1#

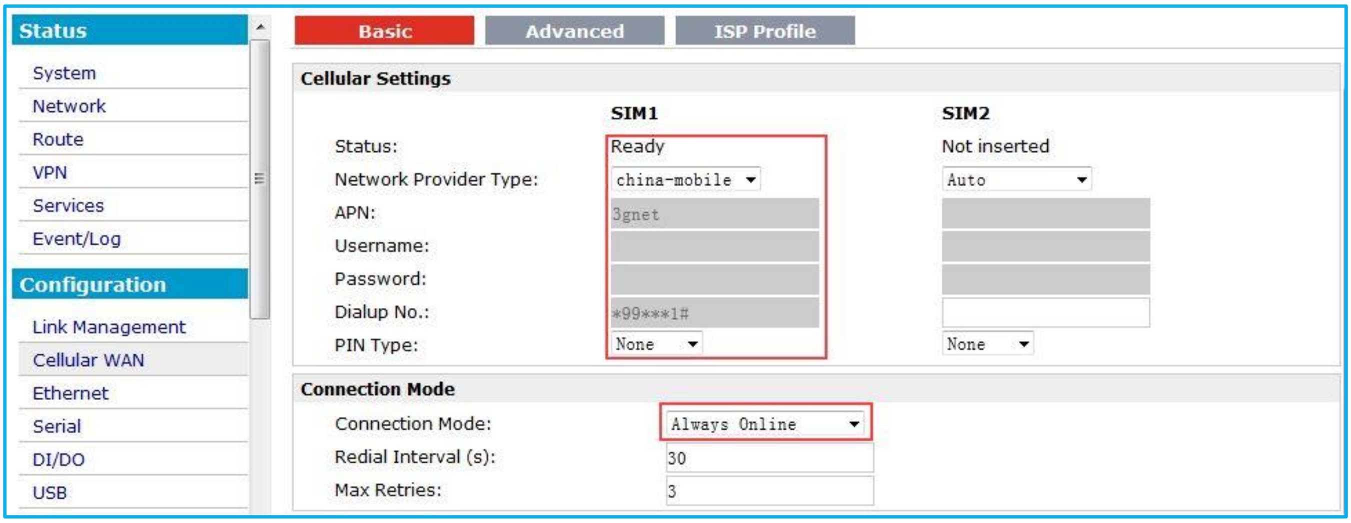
2. Browse to “Configuration”-> “Cellular WAN”-> “Basic”.

- 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 SIM1 or 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



Cellular Settings

	SIM1	SIM2
Status:	Ready	Not inserted
Network Provider Type:	china-mobile	Auto
APN:	3gnet	
Username:		
Password:		
Dialup No.:	*99***1#	
PIN Type:	None	None

Connection Mode

Connection Mode:	Always Online
Redial Interval (s):	30
Max Retries:	3

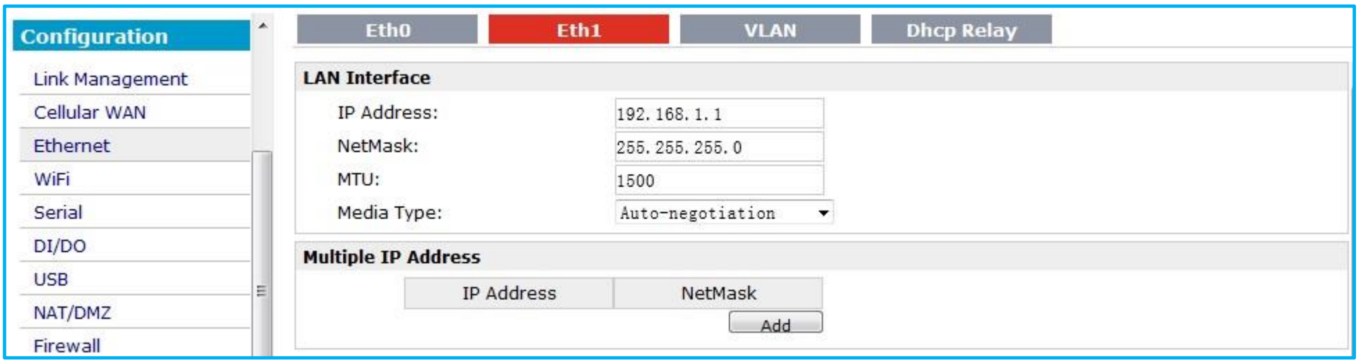
3.4.3 Configure LAN IP address

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



LAN Interface

IP Address: 192. 168. 1. 1

NetMask: 255. 255. 255. 0

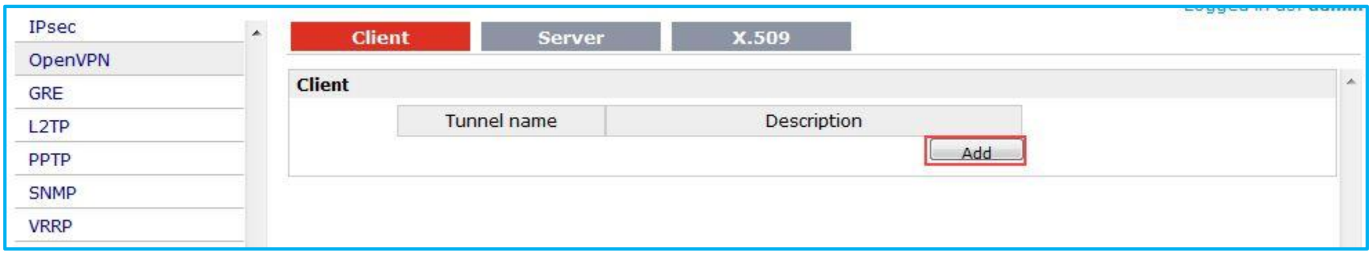
MTU: 1500

Media Type: Auto-negotiation

3.4.4 OpenVPN client Configuration

The following sections relate to the Open VPN parameters.

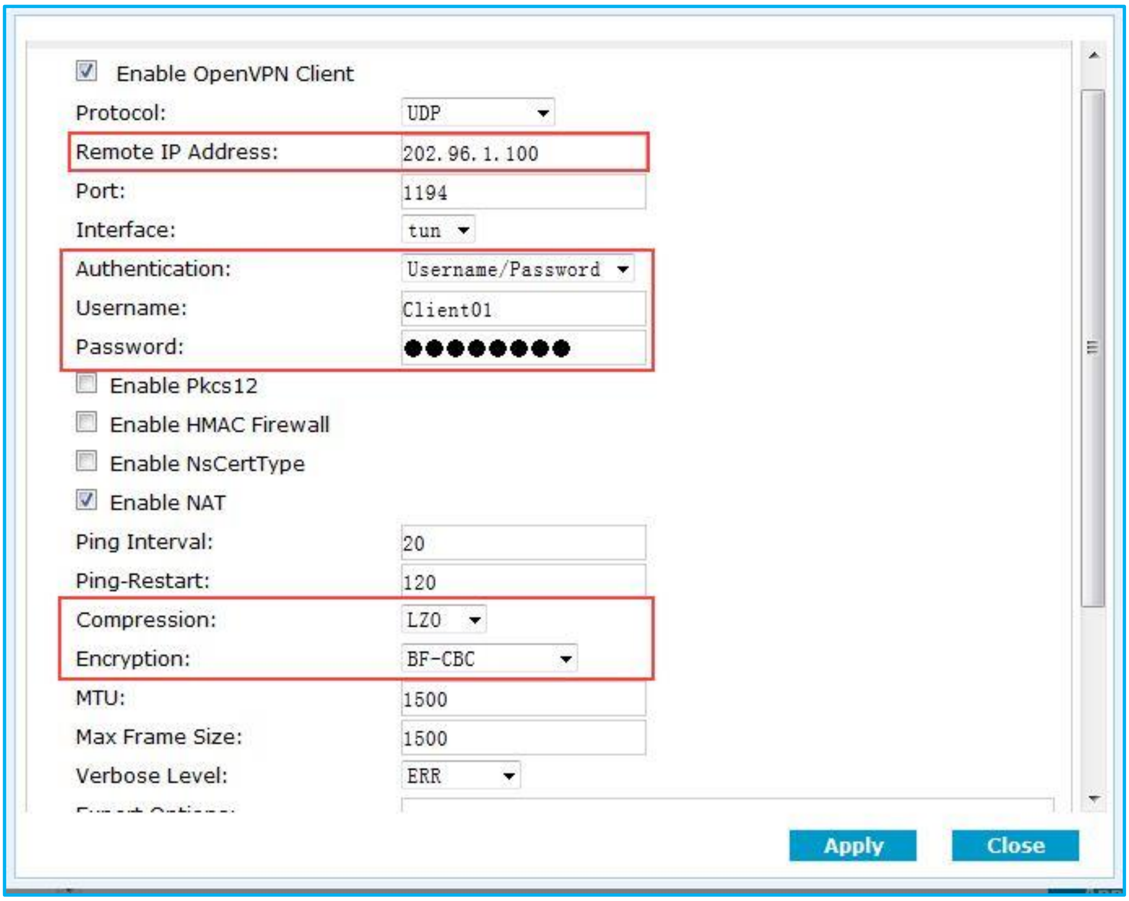
1. Browse to "Configuration"-> "OpenVPN"-> "Client". Click "Add".



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



☑ Enable OpenVPN Client

Protocol: UDP

Remote IP Address: 202.96.1.100

Port: 1194

Interface: tun

Authentication: Username/Password

Username: Client01

Password: ●●●●●●●●

☐ Enable Pkcs12

☐ Enable HMAC Firewall

☐ Enable NsCertType

☑ Enable NAT

Ping Interval: 20

Ping-Restart: 120

Compression: LZO

Encryption: BF-CBC

MTU: 1500

Max Frame Size: 1500

Verbose Level: ERR

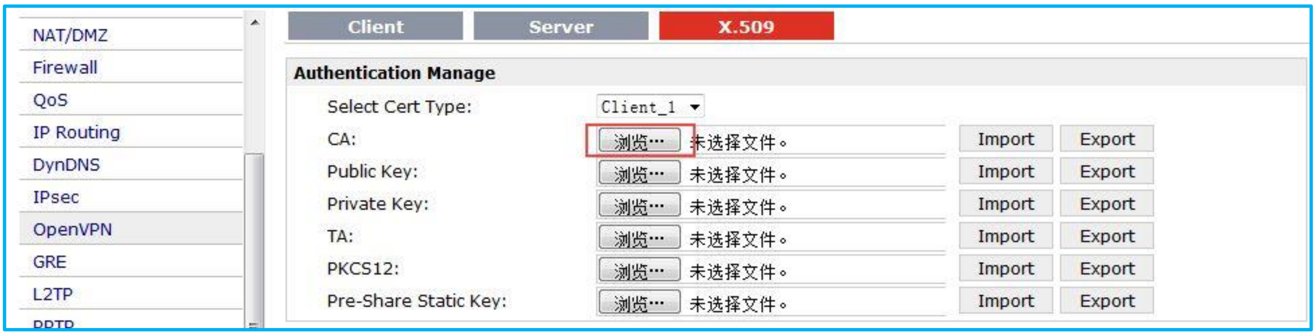
3. Import the certificate for OpenVPN.

- 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 your PC, and then click "Import" to import it to the	Null

	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

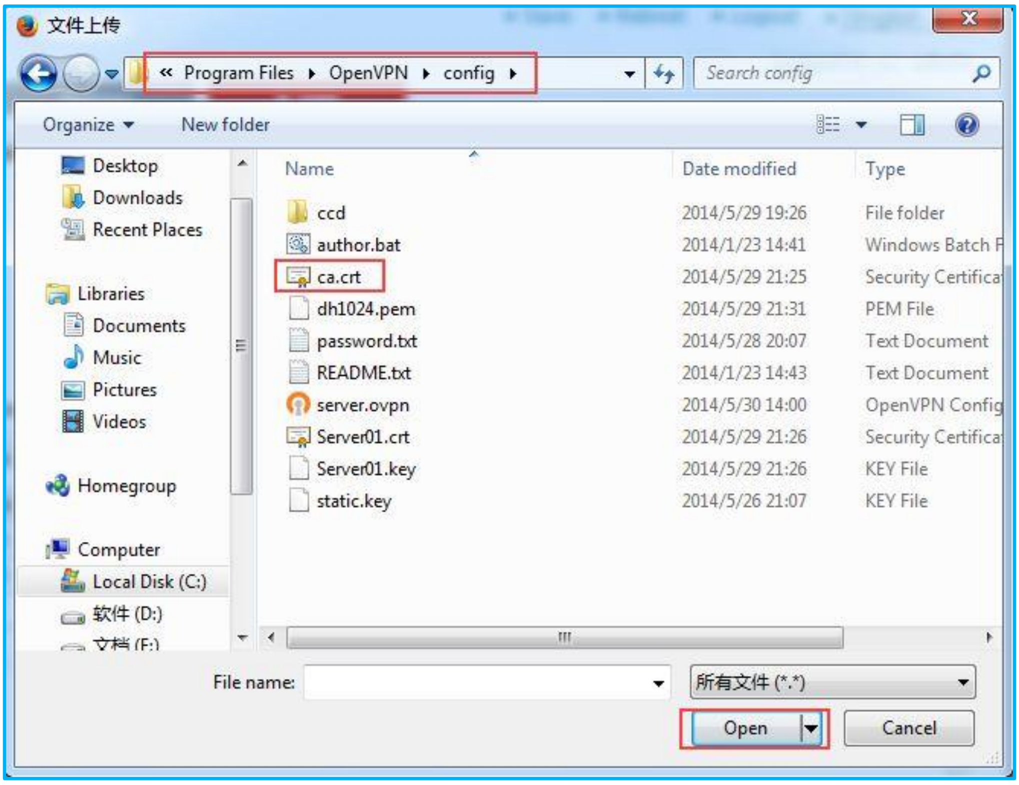
4. Import the certificate, select Cert Type for **Client_1** and click the “browse”



Authentication Manage

Select Cert Type:	Client_1		
CA:	浏览… 未选择文件。	Import	Export
Public Key:	浏览… 未选择文件。	Import	Export
Private Key:	浏览… 未选择文件。	Import	Export
TA:	浏览… 未选择文件。	Import	Export
PKCS12:	浏览… 未选择文件。	Import	Export
Pre-Share Static Key:	浏览… 未选择文件。	Import	Export

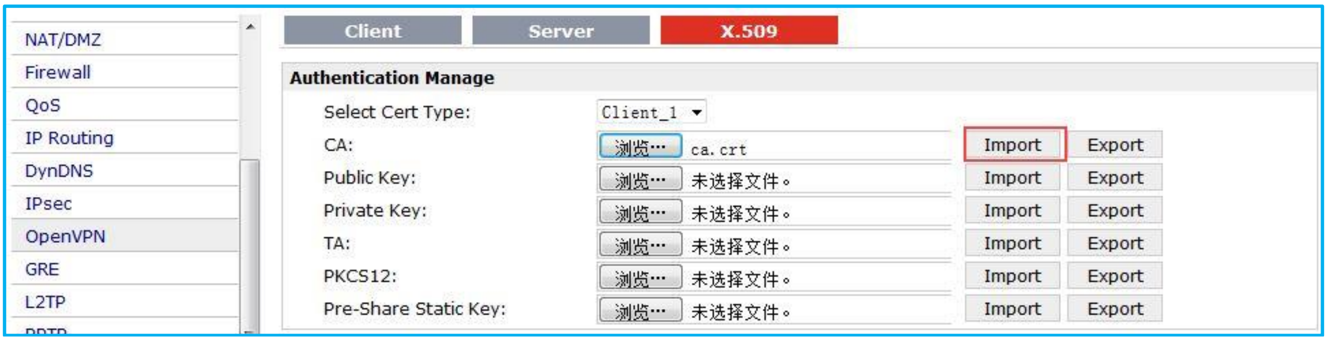
5. Select the **ca.crt** with path C:\Program Files\OpenVPN\config



Name	Date modified	Type
ccd	2014/5/29 19:26	File folder
author.bat	2014/1/23 14:41	Windows Batch F
ca.crt	2014/5/29 21:25	Security Certifica
dh1024.pem	2014/5/29 21:31	PEM File
password.txt	2014/5/28 20:07	Text Document
README.txt	2014/1/23 14:43	Text Document
server.ovpn	2014/5/30 14:00	OpenVPN Config
Server01.crt	2014/5/29 21:26	Security Certifica
Server01.key	2014/5/29 21:26	KEY File
static.key	2014/5/26 21:07	KEY File

Note: *While we using Username/Password for authentication, CA is still required for OpenVPN client, but public key and private key for client is not required.*

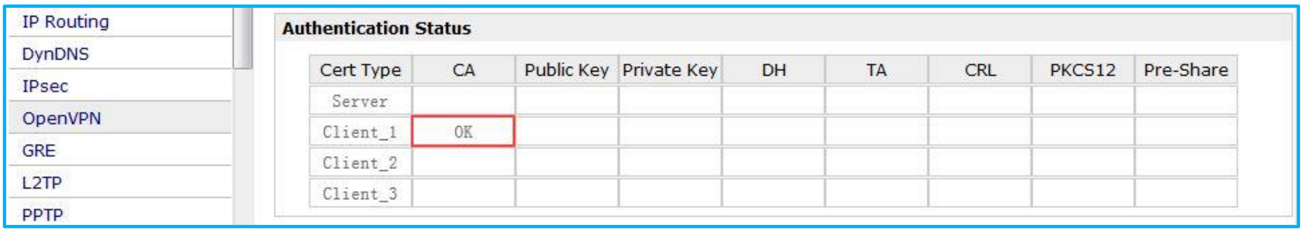
6. Click the “Import” button and you could check the status of CA.



Authentication Manage

Select Cert Type:	Client_1 ▾		
CA:	浏览… ca.crt	Import	Export
Public Key:	浏览… 未选择文件。	Import	Export
Private Key:	浏览… 未选择文件。	Import	Export
TA:	浏览… 未选择文件。	Import	Export
PKCS12:	浏览… 未选择文件。	Import	Export
Pre-Share Static Key:	浏览… 未选择文件。	Import	Export

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



Authentication Status

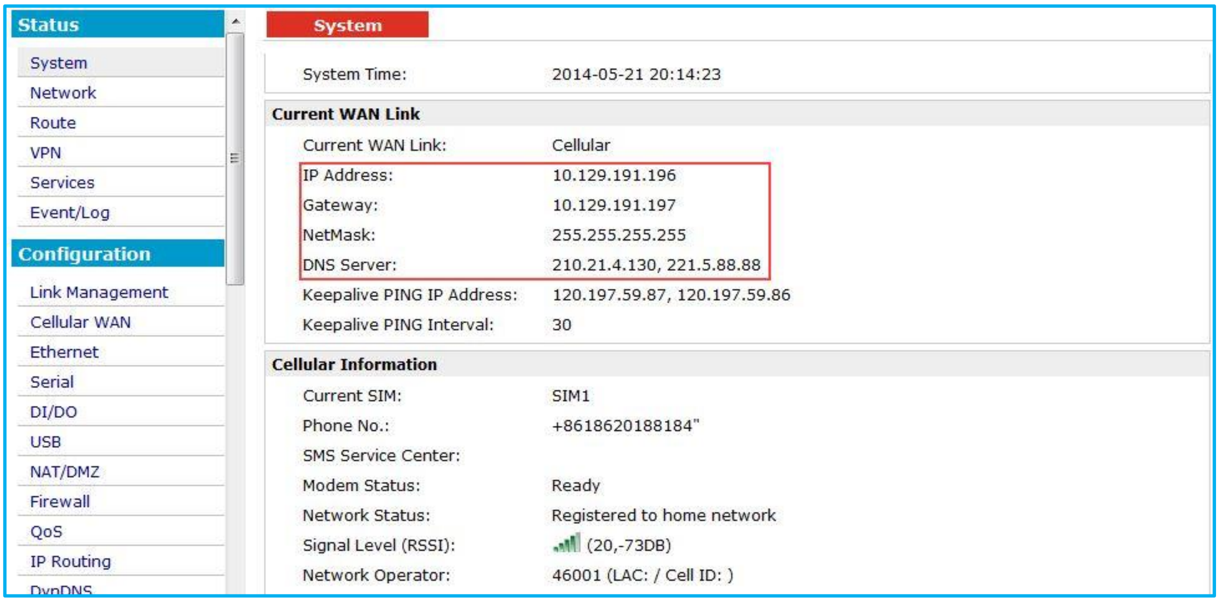
Cert Type	CA	Public Key	Private Key	DH	TA	CRL	PKCS12	Pre-Share
Server								
Client_1	OK							
Client_2								
Client_3								

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.



System

System Time: 2014-05-21 20:14:23

Current WAN Link

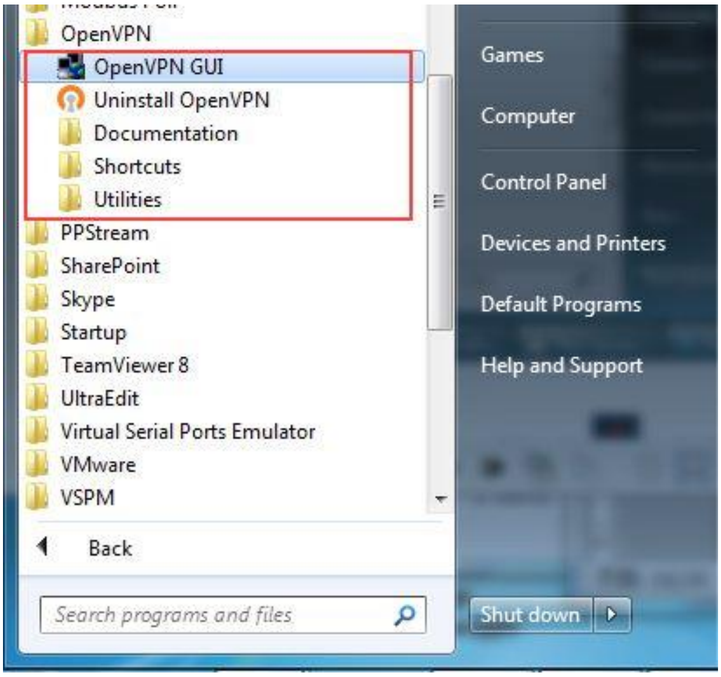
Current WAN Link: Cellular
IP Address: 10.129.191.196
Gateway: 10.129.191.197
NetMask: 255.255.255.255
DNS Server: 210.21.4.130, 221.5.88.88
Keepalive PING IP Address: 120.197.59.87, 120.197.59.86
Keepalive PING Interval: 30

Cellular Information

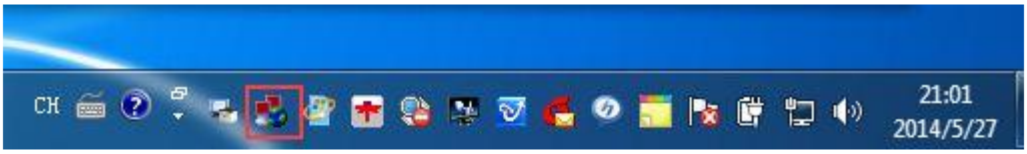
Current SIM: SIM1
Phone No.: +8618620188184"
SMS Service Center:
Modem Status: Ready
Network Status: Registered to home network
Signal Level (RSSI): (20,-73DB)
Network Operator: 46001 (LAC: / Cell ID:)

4.2 Running the OpenVPN software in Windows OS

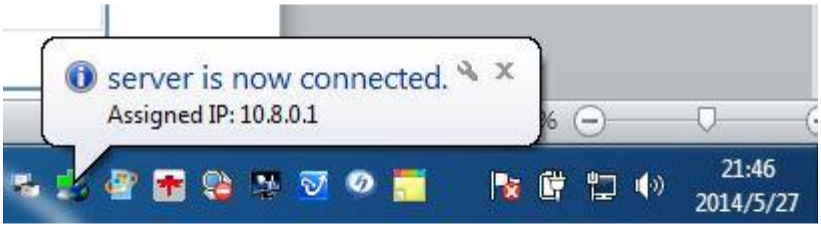
1. Run the OpenVPN software.



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.



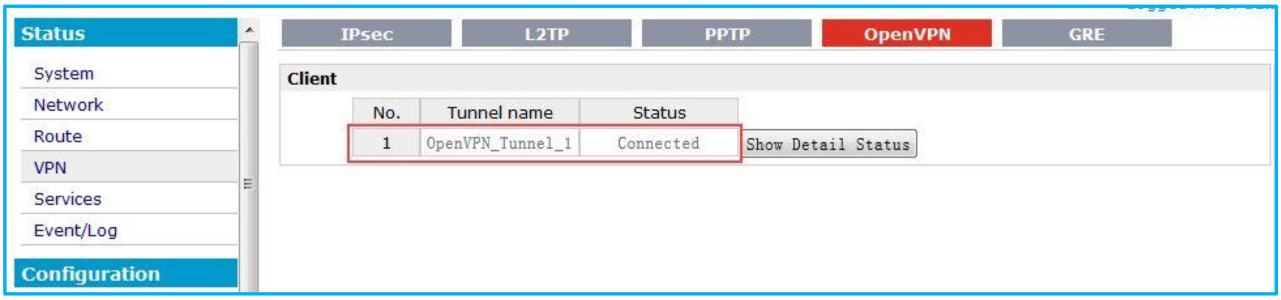
server is now connected.
Assigned IP: 10.8.0.1

This server will now wait for OpenVPN clients connection.

4.3 VPN Status and Communication

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

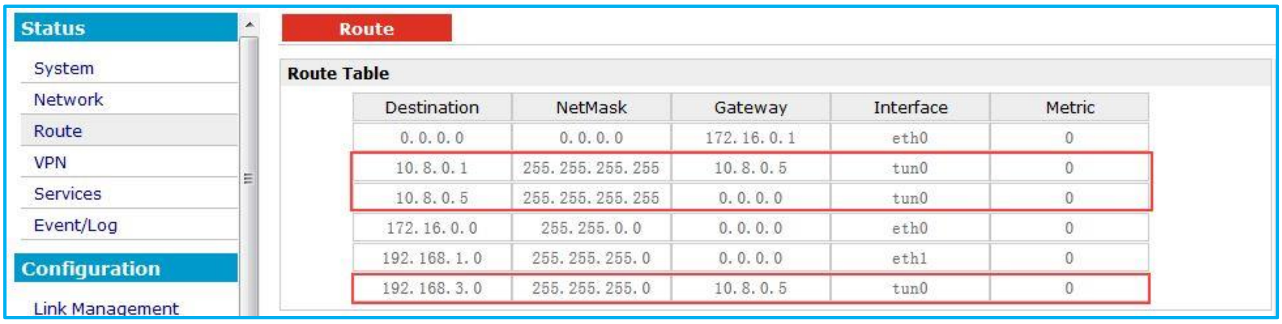
- Check that R3000 has established OpenVPN tunnel with Server side.



Client

No.	Tunnel name	Status
1	OpenVPN_Tunnel_1	Connected

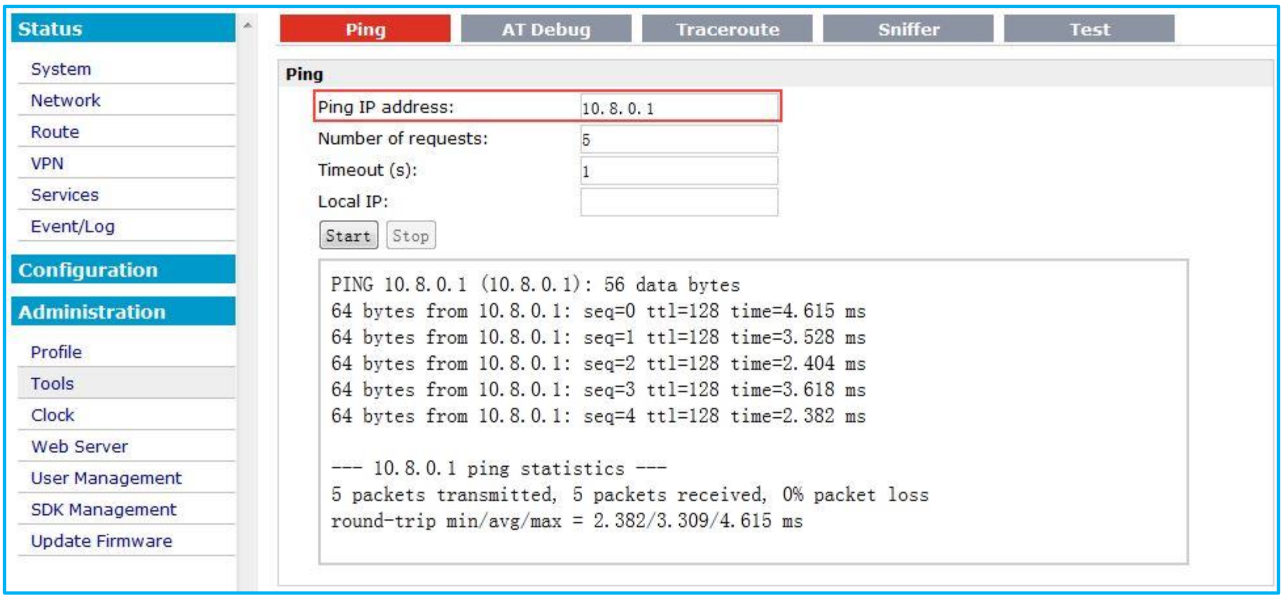
- Check the virtual tunnel on Route table. Browse to “Status”-> “Route”.



Route Table

Destination	NetMask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.16.0.1	eth0	0
10.8.0.1	255.255.255.255	10.8.0.5	tun0	0
10.8.0.5	255.255.255.255	0.0.0.0	tun0	0
172.16.0.0	255.255.0.0	0.0.0.0	eth0	0
192.168.1.0	255.255.255.0	0.0.0.0	eth1	0
192.168.3.0	255.255.255.0	10.8.0.5	tun0	0

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



Ping IP address: 10.8.0.1

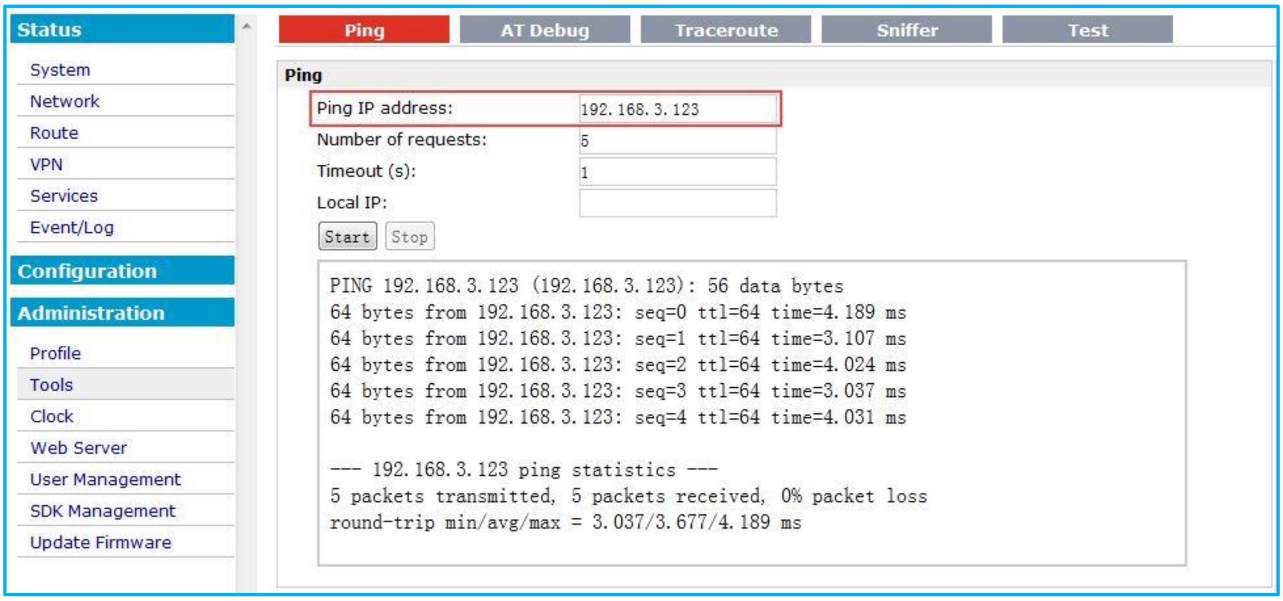
Number of requests: 5

Timeout (s): 1

Local IP:

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=4.615 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.528 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=2.404 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=3.618 ms
64 bytes from 10.8.0.1: seq=4 ttl=128 time=2.382 ms

--- 10.8.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.382/3.309/4.615 ms
```

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



Ping IP address: 192.168.3.123

Number of requests: 5

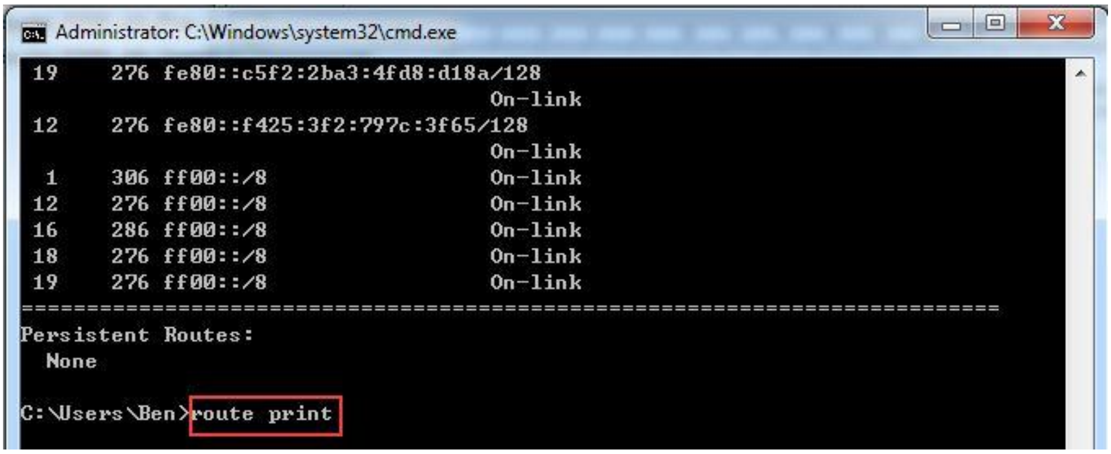
Timeout (s): 1

Local IP:

```
PING 192.168.3.123 (192.168.3.123): 56 data bytes
64 bytes from 192.168.3.123: seq=0 ttl=64 time=4.189 ms
64 bytes from 192.168.3.123: seq=1 ttl=64 time=3.107 ms
64 bytes from 192.168.3.123: seq=2 ttl=64 time=4.024 ms
64 bytes from 192.168.3.123: seq=3 ttl=64 time=3.037 ms
64 bytes from 192.168.3.123: seq=4 ttl=64 time=4.031 ms

--- 192.168.3.123 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.037/3.677/4.189 ms
```

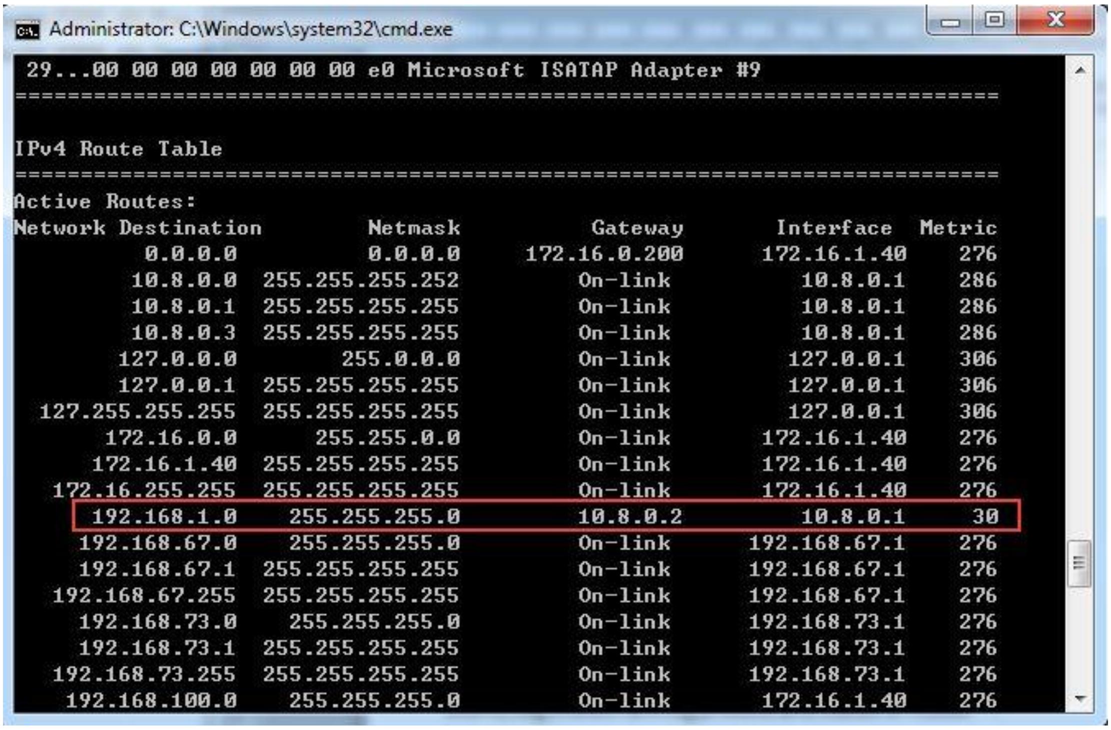
4.4 Testing at OpenVPN server

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



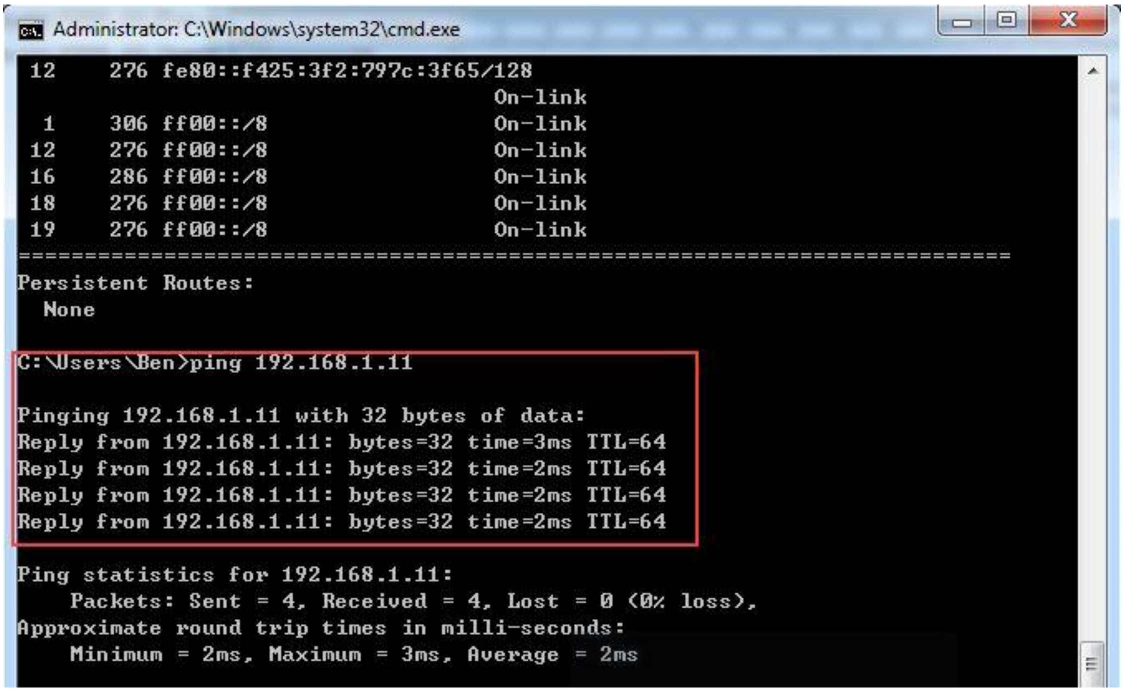
```
 19    276 fe80::c5f2:2ba3:4fd8:d18a/128
                                    On-link
 12    276 fe80::f425:3f2:797c:3f65/128
                                    On-link
  1    306 ff00::/8                 On-link
 12    276 ff00::/8                 On-link
 16    286 ff00::/8                 On-link
 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.



```
 29...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #9
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.16.0.200     172.16.1.40    276
         10.8.0.0  255.255.255.252         On-link         10.8.0.1    286
         10.8.0.1  255.255.255.255         On-link         10.8.0.1    286
         10.8.0.3  255.255.255.255         On-link         10.8.0.1    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         10.8.0.2        10.8.0.1     30
     192.168.67.0    255.255.255.0         On-link     192.168.67.1    276
     192.168.67.1  255.255.255.255         On-link     192.168.67.1    276
   192.168.67.255  255.255.255.255         On-link     192.168.67.1    276
     192.168.73.0    255.255.255.0         On-link     192.168.73.1    276
     192.168.73.1  255.255.255.255         On-link     192.168.73.1    276
   192.168.73.255  255.255.255.255         On-link     192.168.73.1    276
    192.168.100.0    255.255.255.0         On-link      172.16.1.40    276
```

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



```
 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
```

4.5 Event/log

Event/Log shows running process and status of R3000.

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

……

14-06-03 11:51:17 <0> router: system service starting...

14-06-03 11:51:21 <0> router: openvpn client 0 start up.

14-06-03 11:51:21 <1> OpenVPN: OpenVPN 2.2.2 arm-linux [SSL] [LZO2] [EPOLL] [eurephia] built on Nov 19 2013

14-06-03 11:51:21 <3> OpenVPN: WARNING: file '/etc/openvpn/client_0/USER' is group or others accessible

14-06-03 11:51:21 <3> OpenVPN: WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.

14-06-03 11:51:21 <3> OpenVPN: NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or executables

14-06-03 11:51:21 <1> OpenVPN: LZO compression initialized

14-06-03 11:51:21 <1> OpenVPN: NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-delay

14-06-03 11:51:21 <1> OpenVPN: UDPv4 link local: [undef]

14-06-03 11:51:21 <1> OpenVPN: UDPv4 link remote: 202.96.1.100:1194

14-06-03 11:51:21 <3> OpenVPN: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this

14-06-03 11:51:21 <1> OpenVPN: [Server01] Peer Connection Initiated with 202.96.1.100:1194

14-06-03 11:51:22 <0> router: start dhcpd

14-06-03 11:51:24 <1> OpenVPN: TUN/TAP device tun0 opened

14-06-03 11:51:24 <1> OpenVPN: /sbin/ifconfig tun0 10.8.0.6 pointopoint 10.8.0.5 mtu 1500

14-06-03 11:51:24 <1> OpenVPN: GID set to root

14-06-03 11:51:24 <1> OpenVPN: UID set to root

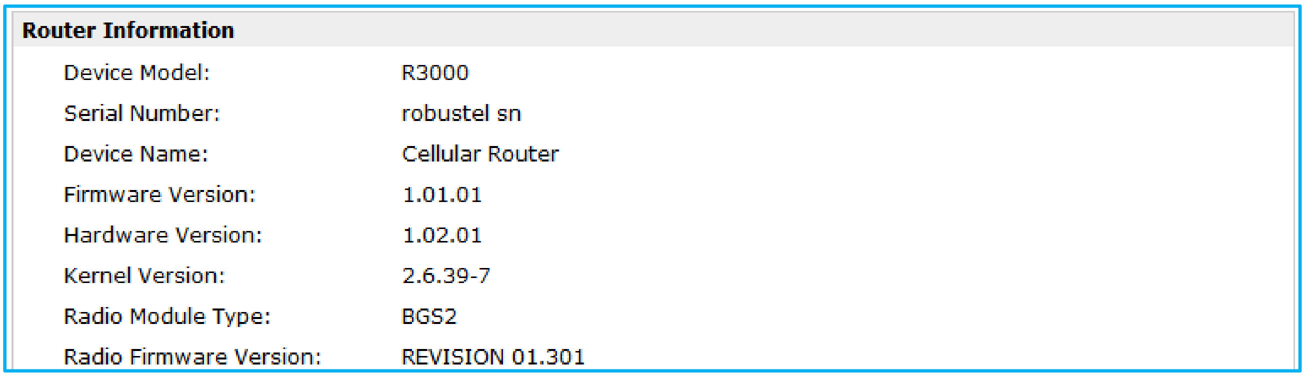
14-06-03 11:51:24 <1> OpenVPN: Initialization Sequence Completed

……

Chapter 5. Appendix

5.1 Firmware Version

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

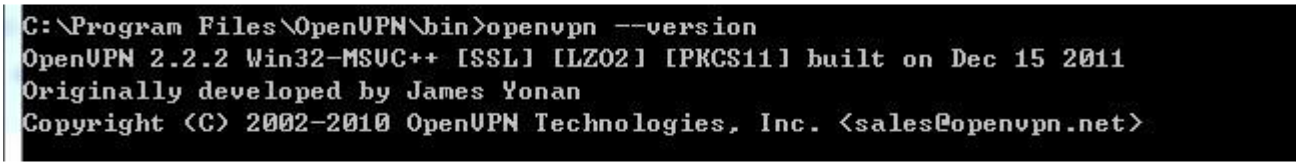


Router Information

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>
```