

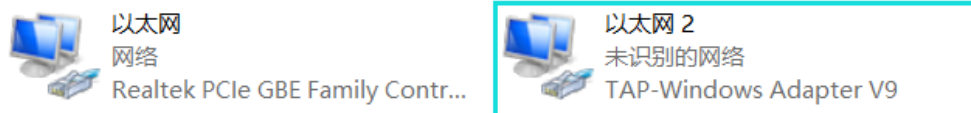
## Assignment5

Construct a VPN by making use of OpenVPN :

### 1. OpenVPN 安装

Win10 系统，安装版本为：openvpn-install-2.3.4-I001-i686.exe（安装时必须手动勾选 OpenSSL 和 RSA 两项）。

OpenVPN 会使用 TAP 虚拟网卡，安装 openvpn 后会自动创建一个 TAP 设备。



上图以太网 2 即为安装 OpenVPN 后自动添加的，初始状态为“网络电缆被拔出”。

### 2. OpenVPN 配置

#### 2.1 创建加密证书和私钥

1) 在服务器端修改 var.bat.sample

(1) 修改 HOME 值为本机具体安装路径

```
vars.bat.sample
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=D:\software\OpenVPN\easy-rsa
7 set KEY_CONFIG=openssl-1.0.0.cnf
```

(2) 设置注册信息相关变量的默认值，避免在后续步骤中重复设置。

稍后生成证书时，如果对应项不输入，就会采用此处的默认值。

```
31 set KEY_COUNTRY=CN
32 set KEY_PROVINCE=GD
33 set KEY_CITY=GuangZhou
34 set KEY_ORG=sysu
35 set KEY_EMAIL=807174205@qq.com
36 set KEY_CN=hanxu
37 set KEY_NAME=hanxuVPN
38 set KEY_OU=changeme
39 set PKCS11_MODULE_PATH=changeme
40 set PKCS11_PIN=1234
```

2) 初始化执行环境

在服务器端以**管理员方式**运行命令行：

- (1) 进入 easy-rsa 目录下
- (2) init-config（初始化设置，把 vars.bat.sample 复制到 vars.bat）
- (3) vars（设置环境变量，使在 vars.bat.sample 中修改的内容生效）
- (4) clean-all（清理）

```
管理员: 命令提示符
Microsoft Windows [版本 10.0.15063]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Windows\system32>D:

D:\>cd D:\software\OpenVPN\easy-rsa

D:\software\OpenVPN\easy-rsa>init-config

D:\software\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
已复制          1 个文件。

D:\software\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
覆盖 vars.bat 吗? (Yes/No/All): y
已复制          1 个文件。

D:\software\OpenVPN\easy-rsa>vars

D:\software\OpenVPN\easy-rsa>clean-all
系统找不到指定的文件。
已复制          1 个文件。
已复制          1 个文件。
```

### 3) 创建 CA 根证书

>build-ca

```
D:\software\OpenVPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/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) [sysu]:
Organizational Unit Name (eg, section) [changeme] admin
Common Name (eg, your name or your server's hostname) [hanxu] CA
Name [hanxuVPN]:
Email Address [807174205@qq.com]:
```

设证书的通用名称为 CA。

在 keys 下生成 ca.crt, ca.key 两个文件。

#### 4) 创建服务器端 (server) 证书

>build-key-server server

此处 server 指生成证书文件的名称。

注意：common name 处设置的名称必须要和此处声明的一致。

```
D:\software\OpenVPN\easy-rsa>build-key-server server
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\server.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) [sysu]:
Organizational Unit Name (eg, section) [changeme]:admin
Common Name (eg, your name or your server's hostname) [hanxu]:server
Name [hanxuVPN]:
Email Address [807174205@qq.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:secret
An optional company name []:hanxuVPN
WARNING: can't open config file: /etc/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:'sysu'
organizationalUnitName  :PRINTABLE:'admin'
commonName              :PRINTABLE:'server'
name                   :PRINTABLE:'hanxuVPN'
emailAddress            :IA5STRING:'807174205@qq.com'
Certificate is to be certified until Nov 23 13:43:53 2027 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

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

信息补充完毕后有两次确定的机会，两次都输入 y 即可注册并提交证书。

在 keys 下生成 server.crt, server.csr, server.key 三个文件。

#### 5) 创建密钥

>build-dh

为服务器生成加密交换时的 Diffie-Hellman 文件，(Diff-Hellman key exchange, “D-H”) 是一种安全协议，可以让双方在没有任何预先信息的条件下通过不安全信道创建一个密钥，创建成功后在 keys 下生成文件 dh1024.pem。



```

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:'sysu'
organizationalUnitName:PRINTABLE:'guest'
commonName        :PRINTABLE:'client'
name              :PRINTABLE:'hanxuVPN'
emailAddress       :IA5STRING:'807174205@qq.com'
Certificate is to be certified until Nov 23 13:45:06 2027 GMT (3650 days)
Sign the certificate? [y/n]:y







1 out of 1 certificate requests certified, commit? [y/n]y

```

## 7) 文件复制

- (1) 把 keys 文件夹中相应的文件复制到服务器端和客户端的 config 目录中。
- (2) 把 OpenVPN/ ample-config 文件夹中的 server.ovpn 和 client.ovpn 文件分别复制到服务器端和客户端对应的 config 目录中。

server :

	ca.key	2017/11/25 21:40	KEY 文件
	server.key	2017/11/25 21:43	KEY 文件
	server.ovpn	2017/11/25 22:17	OpenVPN Confi...
	dh1024.pem	2017/11/25 21:44	PEM 文件
	ca.crt	2017/11/25 21:40	安全证书
	server.crt	2017/11/25 21:43	安全证书

client :

	ca.crt	2017/11/25 21:40	安全证书
	client.crt	2017/11/25 21:45	安全证书
	client.key	2017/11/25 21:45	KEY 文件
	client.ovpn	2017/11/25 22:10	OpenVPN Config Fi...

## 3. 配置文件修改

### 3.1 服务器端配置文件

进入命令行：

>ipconfig

```

以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . . : sysu.edu.cn
    IPv6 地址 . . . . . : 2001:250:3002:4630:54b6:c339:e8df:8e0c
    临时 IPv6 地址. . . . . : 2001:250:3002:4630:20dc:55dd:a09c:5983
    本地链接 IPv6 地址. . . . . : fe80::54b6:c339:e8df:8e0c%10
    IPv4 地址 . . . . . : 172.18.136.220
    子网掩码 . . . . . : 255.255.252.0
    默认网关. . . . . : fe80::7625:8aff:fe69:f115%10
                        172.18.139.254

```

```

23 # Which local IP address should OpenVPN
24 # listen on? (optional)
25 local 172.18.136.220

```

把监听的本机 IP 设置为已连接的以太网 IP 地址。

### 3.2 客户端配置文件

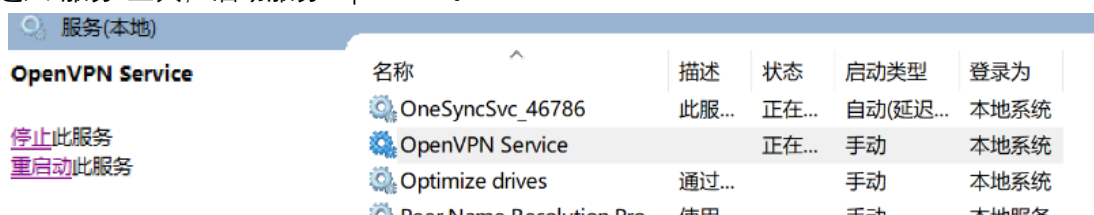
```
39 # The hostname/IP and port of the server.
40 # You can have multiple remote entries
41 # to load balance between the servers.
42 remote 172.18.136.220 1194
43 ;remote my-server-2 1194
```

指定连接的远程服务器端的实际 IP 地址和端口号。

## 4. 连接测试

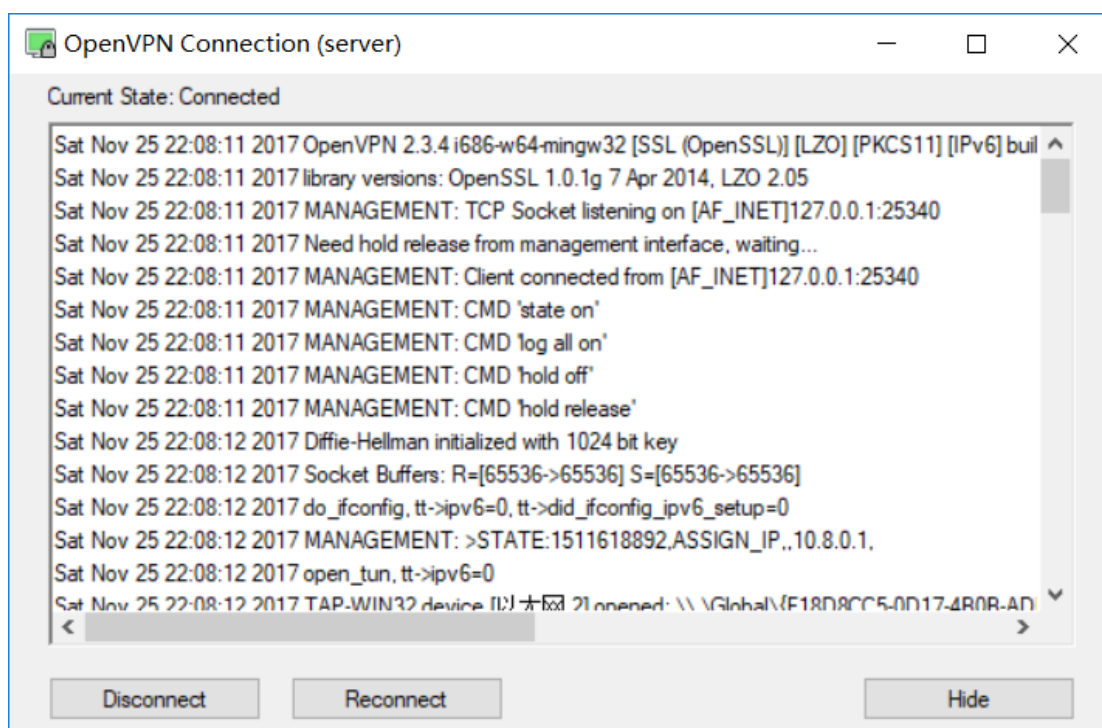
### 4.1 服务器端

- 1) 进入“服务”工具，启动服务 OpenVPN。

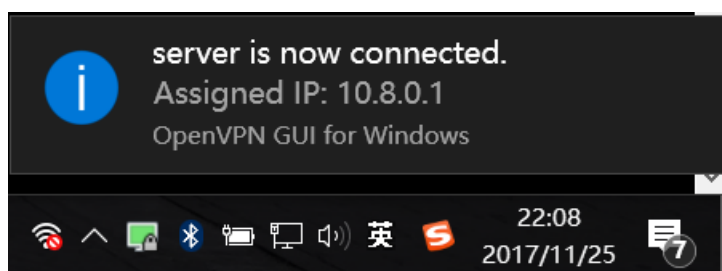
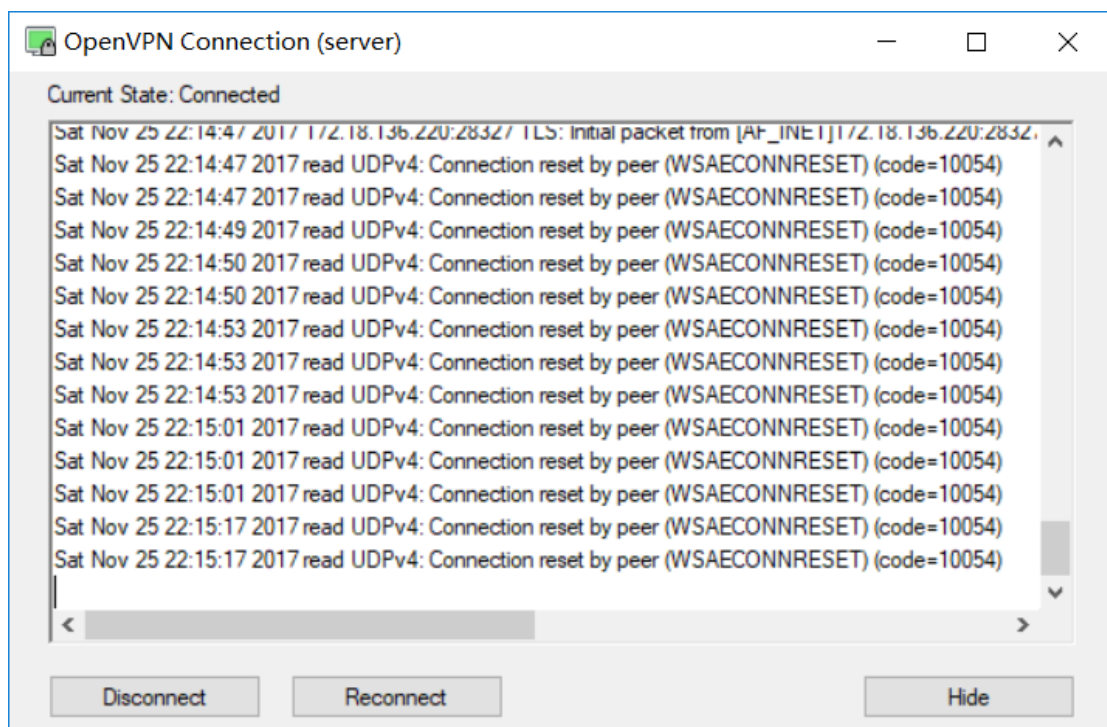


- 2) 测试服务器端连通性

以管理员身份运行 OpenVPN GUI，在任务栏出现 GUI 图标，右键连接，观察结果。、



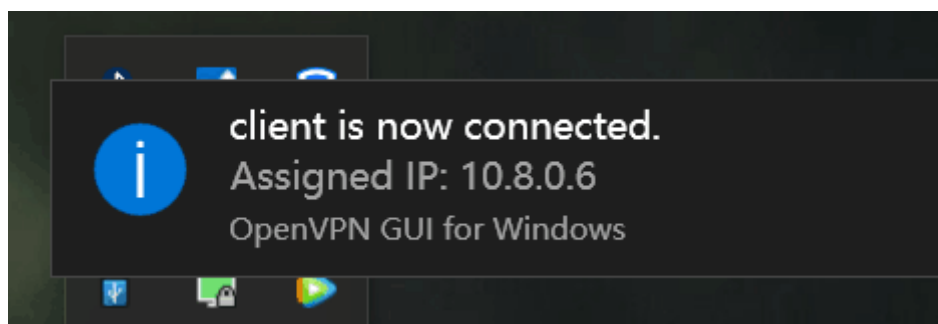




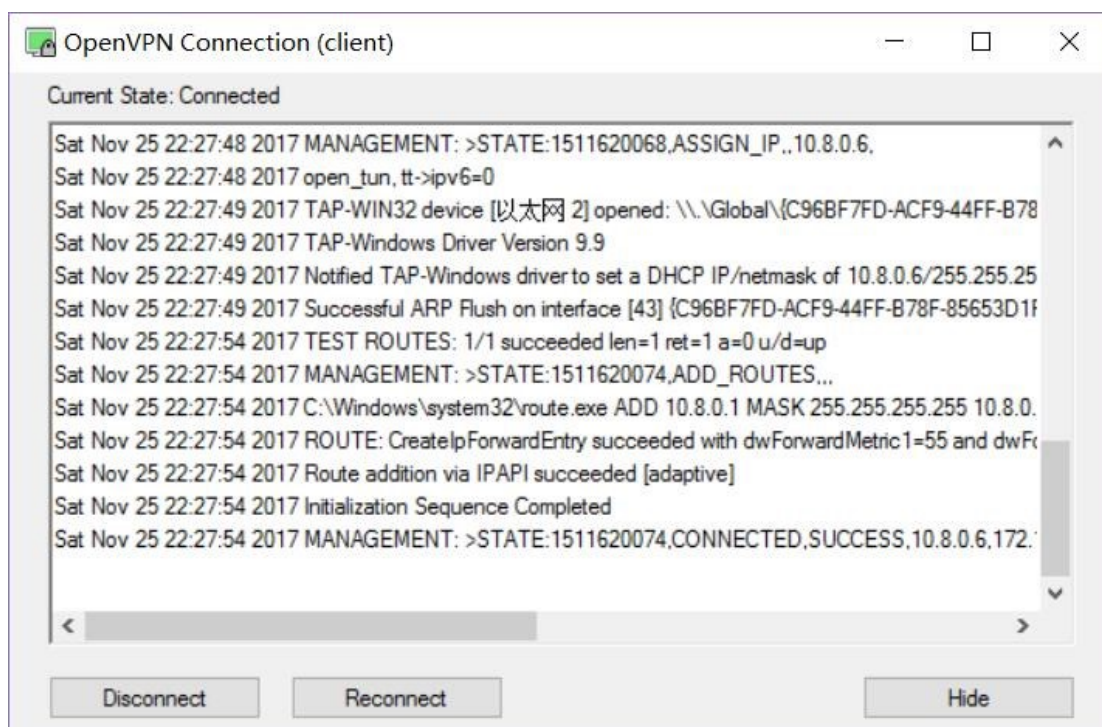
显示连接成功，图标变为绿色。

## 4.2 客户端

测试客户端连通性：



显示连接成功，图标变为绿色。（因需要两台设备，此处借用其他同学的电脑测试连接）



## 5. 结论

成功使用 OpenVPN 创建了一个可用的 VPN。

## 6. 实验心得总结

### 6.1 安装 OpenVPN

- 1) 要选择合适的版本，如 OpenVPN2.3.4，如选择不合适会导致安装部分失败，不能正常连接。
- 2) 运行安装 exe 文件时必须以管理员身份运行。
- 3) 安装中提示是否允许创建虚拟网络时一定要选择同意。
- 4) 卸载之后再重新安装时一定要安装在和上次安装相同的目录下，否则会使注册表出现问题，不能正常运行 OpenVPN GUI，解决方法是再次卸载，重新安装至上次安装的路径。

### 6.2 配置 OpenVPN

common name 处设置的名称必须要和命令中声明的一致。

### 6.3 修改配置文件

配置中 IP 地址信息可以由 ipconfig 命令结果获得。

### 6.4 连接测试

- 1) 最好关闭 window 防火墙
- 2) 客户端电脑不要使用 WIFI 连接（校园网下的 WIFI 可能对连接有影响，直接造成连接失败）可以选择校园网下不同主机。