

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÀI THỰC HÀNH 7

THỰC TẬP CƠ SỞ

Họ và tên: Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

Hà Nội – 2022

Bài thực hành số 7 - Cài đặt cấu hình VPN server

1. Mục đích

- Tìm hiểu về mạng riêng ảo (VPN-Virtual Private Network), kiến trúc và hoạt động của mạng riêng ảo.
- Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ mạng riêng ảo (VPN server)

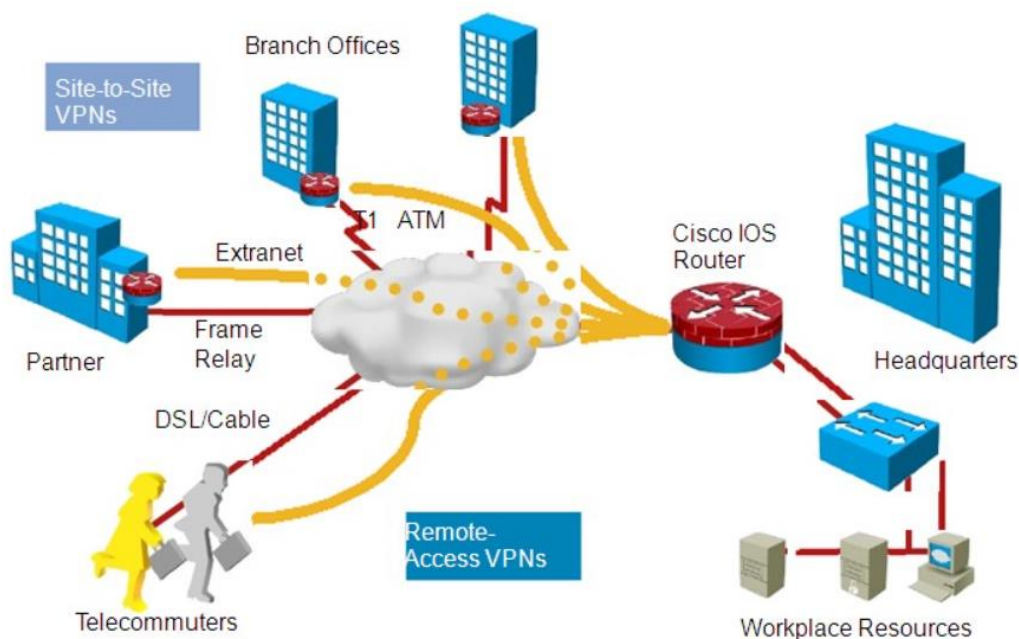
2. Nội dung thực hành

2.1. Tìm hiểu lý thuyết

- **Khái quát về VPN:**

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

- **Mô hình VPN**



- **Ứng dụng của VPN**

- ✓ **Truy cập mạng**

- Truy cập vào mạng doanh nghiệp khi ở xa: VPN thường được sử dụng cho những người làm kinh doanh. Họ có thể truy cập vào tài nguyên trên mạng cục bộ khi đang có mặt ở khắp mọi nơi. Các nguồn lực

mạng nội bộ không nhất thiết phải tiếp xúc với internet nên độ bảo mật được tăng lên.

- Truy cập mạng gia đình, dù không ở nhà: Bạn có thể thiết lập VPN riêng để truy cập vào mạng khi không ở nhà. Thao tác này sẽ cho phép truy cập Windows từ xa thông qua Internet. Có thể sử dụng tập tin được chia sẻ trong mạng nội bộ.

✓ Liên quan đến trang web

- Duyệt web ẩn danh: Sử dụng VPN sẽ giúp bạn bảo vệ được dữ liệu của mình khi duyệt web ẩn danh. Mọi thông tin truyền qua mạng lúc này sẽ được mã hóa.
- Truy cập đến những website bị chặn giới hạn địa lý.

• Tìm hiểu về các giao thức tạo đường hầm cho VPN

○ Point-To-Point Tunneling Protocol (PPTP)

PPTP không chỉ định giao thức mã hóa nhưng có thể sử dụng một số giao thức như MPPE-128 mạnh mẽ. Việc thiếu sự tiêu chuẩn hóa về giao thức mạng là một rủi ro, vì nó chỉ có thể sử dụng tiêu chuẩn mã hóa mạnh nhất mà cả 2 phía cùng hỗ trợ. Nếu một phía chỉ hỗ trợ tiêu chuẩn yếu hơn thì kết nối phải sử dụng mã hóa yếu hơn người dùng mong đợi

○ L2TP

Giao thức L2TP thường hoạt động với thuật toán mã hóa IPsec. Nó mạnh hơn đáng kể so với PPTP nhưng vẫn khiến người dùng lo ngại. Lỗi hồng chính trong L2TP/IPsec là phương thức trao đổi khóa công khai (public key). Trao đổi khóa công khai Diffie-Hellman là cách để hai bên thỏa thuận về khóa mã hóa tiếp theo và không ai được biết về khóa này. Có một phương pháp có thể “bẻ khóa” quá trình này, đòi hỏi sức mạnh điện toán khá lớn, nhưng sau đó nó cho phép truy cập vào tất cả các giao tiếp trên một VPN nhất định

• Tìm hiểu về SoftEther VPN

Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và BẢO MẬT cao hơn.

Hiện tại, SoftEther VPN hỗ trợ **Windows, Linux, Mac, Solaris, FreeBSD** và thường là một lựa chọn tốt để thay thế cho OpenVPN vì nhanh hơn. SoftEther VPN cũng hỗ trợ Microsoft SSTP VPN cho Windows Vista/7/8.

Bên cạnh ưu điểm nhanh, SoftEther VPN còn sử dụng **key certificate AES 256 bit**, 1 cấp độ bảo mật và mã hóa cao. Thêm một điểm cộng lớn cho phần mềm

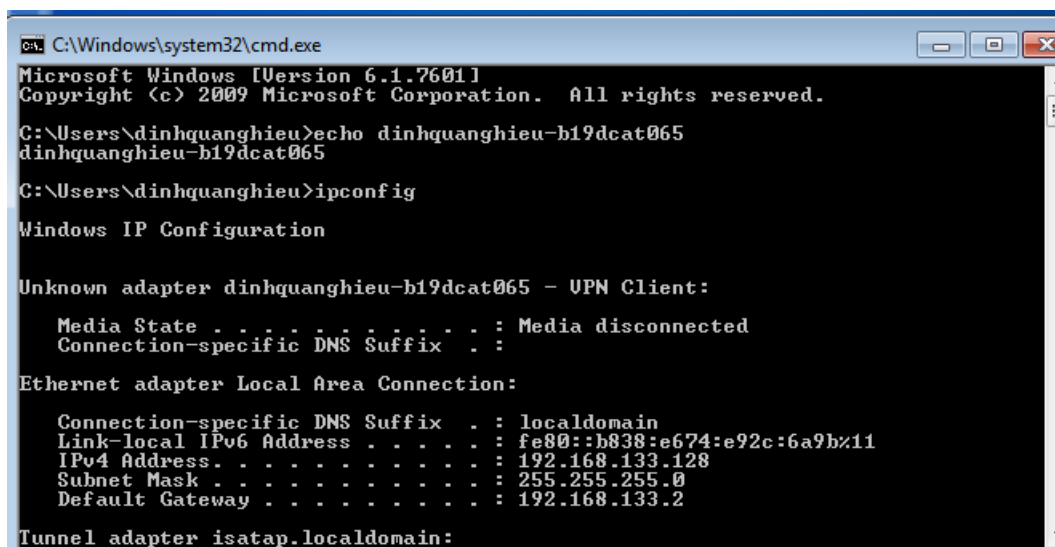
này là nó tích hợp tất cả các tính năng của các giao thức VPN khác nhau như PPTP, L2TP, OpenVPN và SSTP, trong khi loại bỏ nhược điểm của chúng

2.2 Chuẩn bị môi trường, công cụ

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet) để cài đặt VPN server.
- 01 máy tính (máy thật hoặc máy ảo) chạy MS Windows để cài đặt VPN client

2.3. Các bước thực hiện

Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.2. Máy Windows được đổi tên thành -VPNClient và máy cài VPN server thành -VPNServer. Các máy có địa chỉ IP và kết nối mạng LAN



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

C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065

C:\Users\dinhquanghieu>ipconfig

Windows IP Configuration

Unknown adapter dinhquanghieu-b19dcat065 - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Local Area Connection:

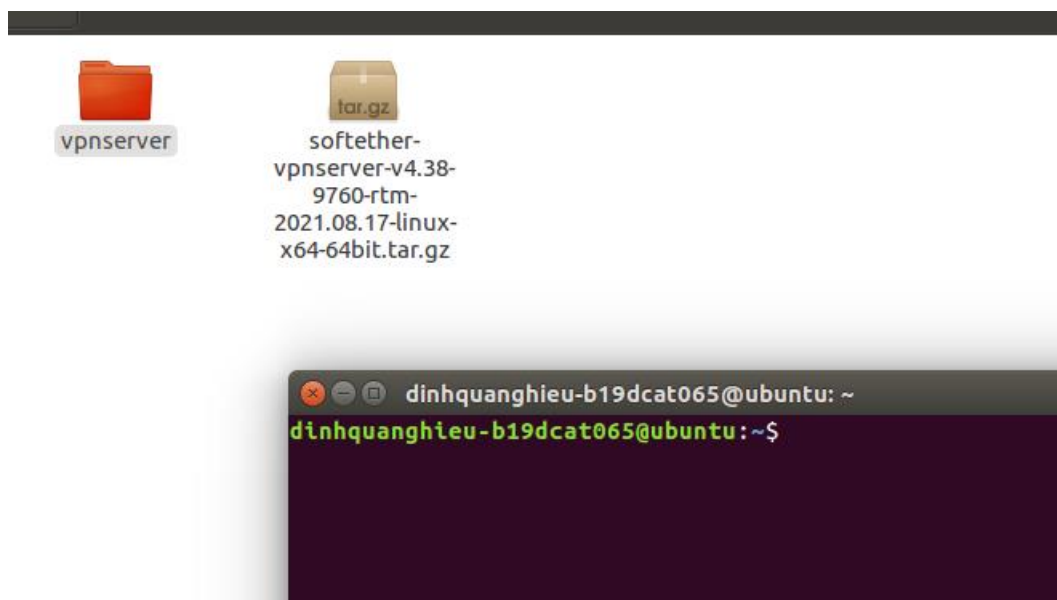
    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::b838:e674:e92c:6a9b%11
    IPv4 Address. . . . . : 192.168.133.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.133.2

Tunnel adapter isatap.localdomain:
```

```
dinhquanghieu-b19dcat065@ubuntu: ~  
dinhquanghieu-b19dcat065@ubuntu:~$ ifconfig  
ens33    Link encap:Ethernet  HWaddr 00:0c:29:63:34:21  
          inet addr:192.168.133.129  Bcast:192.168.133.255  Mask:255.255.255.0  
          inet6 addr: fe80::b659:2eb5:f31a:4705/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1007 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:585 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:1234278 (1.2 MB)  TX bytes:43779 (43.7 KB)  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:264 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:264 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:20903 (20.9 KB)  TX bytes:20903 (20.9 KB)  
  
dinhquanghieu-b19dcat065@ubuntu:~$
```

Bước 2: Tải SoftEther VPN server tại <https://www.softether.org/5-download>.
Cài đặt và cấu hình VPN server theo hướng dẫn sau:

- ✓ Giải nén file cài đặt bằng lệnh `tar -vxzf`



- ✓ Chuyển vào thư mục VPN server: `cd vpnserver`

```
dinhquanghieu-b19dcat065@ubuntu: ~/vpnservice
dinhquanghieu-b19dcat065@ubuntu:~$ cd vpnservice/
dinhquanghieu-b19dcat065@ubuntu:~/vpnservice$
```

- ✓ Biên dịch và cài đặt: make (lưu ý hệ thống phải có sẵn trình biên dịch gcc)

```
dinhquanghieu-b19dcat065@ubuntu:~/vpnservice$ sudo make
[sudo] password for dinhquanghieu-b19dcat065:
-----

SoftEther VPN Server (Ver 4.38, Build 9760, Intel x64 / AMD64) for Linux Build U
tility
Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Rese
rved.

-----

Copyright (c) all contributors on SoftEther VPN project in GitHub.
Copyright (c) Daiyuu Nobori, SoftEther Project at University of Tsukuba, and Sof
tEther Corporation.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed
```

- ✓ Khởi động máy chủ VPN: sudo ./vpnservice start

```
dinhquanghieu-b19dcat065@ubuntu:~/vpnservice$ sudo ./vpnservice start
The SoftEther VPN Server service has been started.

Let's get started by accessing to the following URL from your PC:

https://192.168.133.129:5555/
or
https://192.168.133.129/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certif
icate by default. That is natural. Continue with ignoring the TLS warning.

dinhquanghieu-b19dcat065@ubuntu:~/vpnservice$
```

- ✓ Chạy tiện ích quản trị VPN Server: ./vpncmd (chọn chức năng số 1 và gõ Enter 2 lần để vào giao diện quản trị). Tạo Virtual Hub và tài khoản người dùng VPN trong giao diện quản trị:

```
dinhquanghieu-b19dcat065@ubuntu:~/vpnserver$ sudo ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Server or VPN Bridge is operating on.
By specifying according to the format 'host name:port number', you can also specify the port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the port number 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name: 
```

- Tạo 1 Virtual Hub mới:

```
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Server or VPN Bridge is operating on.
By specifying according to the format 'host name:port number', you can also specify the port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the port number 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>HubCreate b19dcat065
```



```
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver
If nothing is input and the Enter key is pressed, the connection will be made to
the port number 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual
Hub name.
If connecting by server admin mode, please press Enter without inputting anythin
g.
Specify Virtual Hub Name:
Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>HubCreate b19dcat065
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server>
```

- Chọn Virtual Hub đã tạo: Hub <tên Virtual Hub>
- Tạo 1 người dùng VPN mới: UserCreate /GROUP:none /REALNAME:Tên sinh viên /NOTE:none ▪ Đặt mật khẩu cho người dùng: UserPasswordSet

```
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver
The command completed successfully.

VPN Server>Hub b19dcat065
Hub command - Select Virtual Hub to Manage
The Virtual Hub "b19dcat065" has been selected.
The command completed successfully.

VPN Server/b19dcat065>UserCreate b19dcat065-hieu /GROUP:none /REALNAME:dinhquang
hieu/NOTE:none
UserCreate command - Create User
User Description:

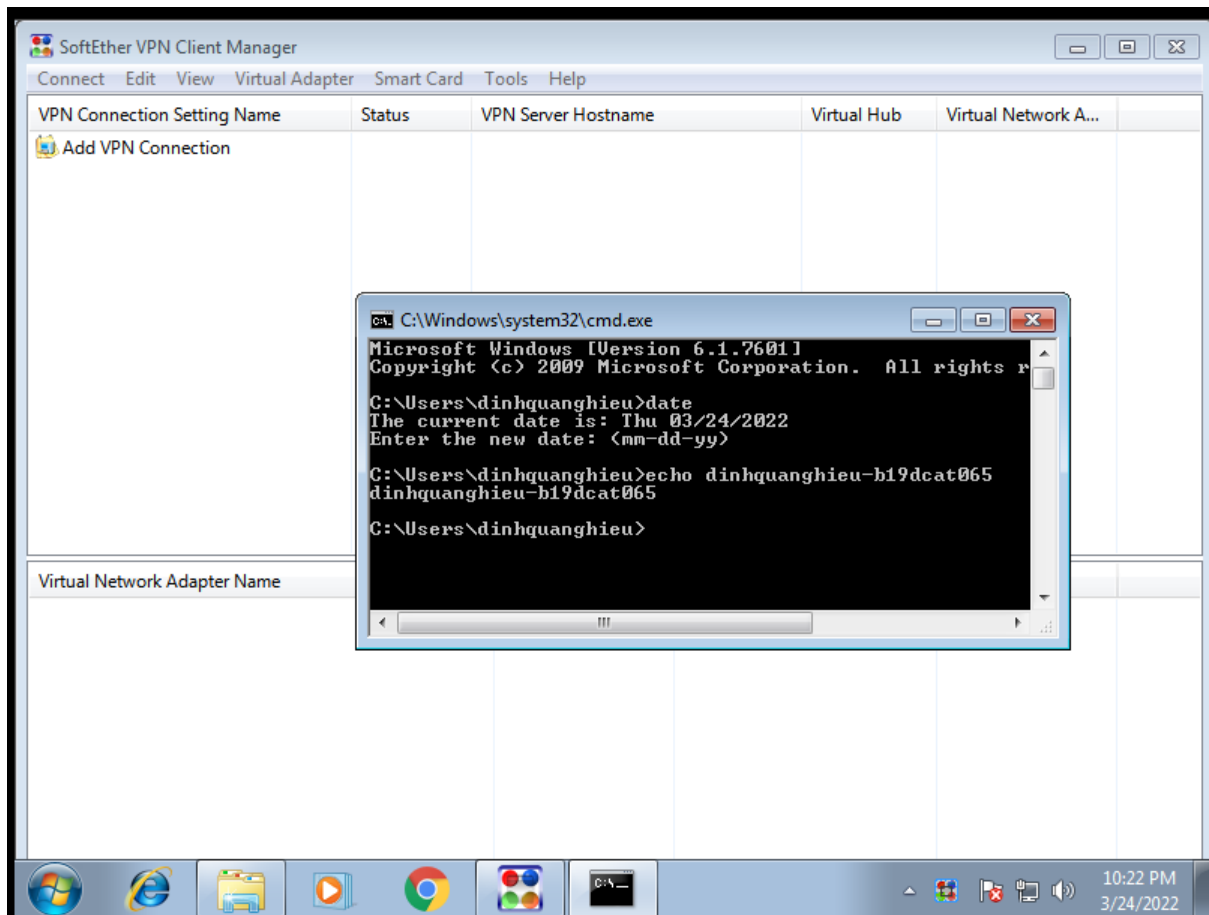
The command completed successfully.

VPN Server/b19dcat065>UserPasswordSet b19dcat065-hieu
UserPasswordSet command - Set Password Authentication for User Auth Type and Set
Password
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

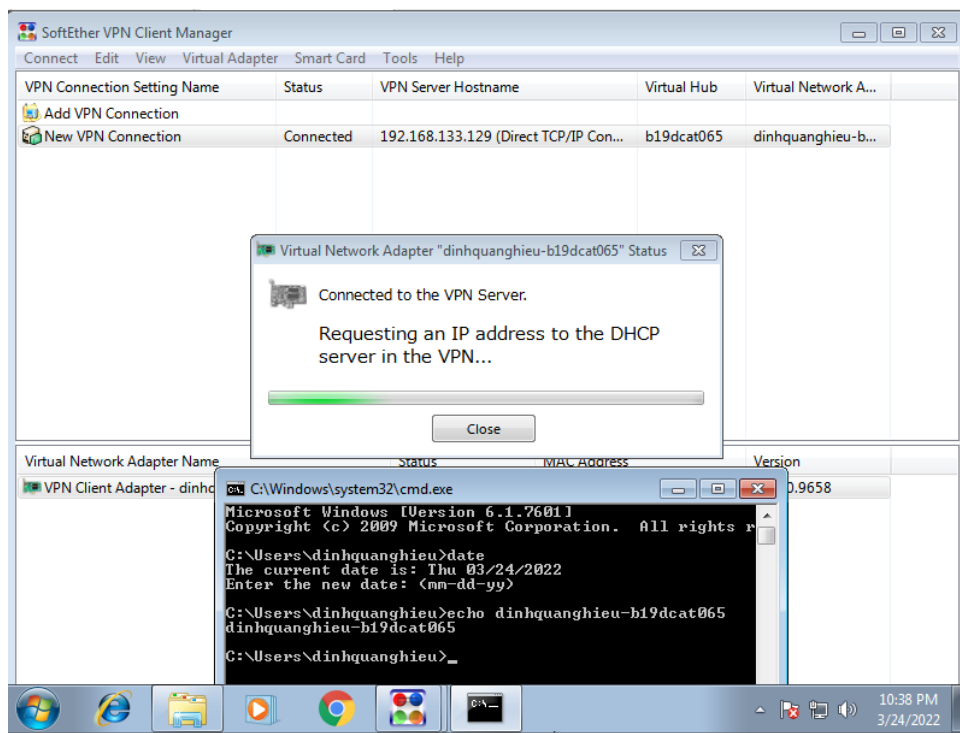
The command completed successfully.
```

Bước3: Tải SoftEther VPN client cho Windows tại <https://www.softether.org/5-download>. Cài đặt VPN client.



Bước 4: Tạo và kiểm tra kết nối VPN.

- ✓ Từ giao diện SoftEther VPN Client Manager, tạo 1 kết nối mới (Add New Connection) với địa chỉ IP của máy chủ VPN, tên Virtual Hub, tên và mật khẩu người dùng. Đặt tên kết nối là <Mã sinh viên>-<họ tên>
- ✓ Thử kết nối: Nếu thành công sẽ báo connected.



- ✓ Kiểm tra kết nối bên máy chủ: Chuyển sang máy chủ VPN, mở 1 terminal mới chuyển đến thư mục vpnserver/server_log để kiểm tra log trên VPN server: `sudo grep vpnserver/server_log/*.log`

```
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver/server_log
bash: cd: server_log/: Permission denied
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver$ sudo chmod 777 server_log/
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver$ cd server_log/
dinhquanghieu-b19dcat065@ubuntu: /usr/local/vpnserver/server_log$ sudo grep b19dcat065 vpn_20220324.log
2022-03-24 07:22:36.854 Monitoring the directory "/home/dinhquanghieu-b19dcat065/vpnserver". If the amount of available free disk space becomes less than 100.00 MBytes, the backup files for log files and configurations that are saved on the sub-directories of this directory will be automatically deleted in the order of oldest first. The amount of free disk space that determines when to start deletion can be modified by changing the "AutoDeleteCheckDiskFreeSpaceMin" item in the configuration file.
2022-03-24 07:26:10.222 Connection "CID-1" connected using Virtual Hub Admin Mode. The name of the Virtual Hub is "b19dcat065".
2022-03-24 07:27:15.144 Connection "CID-2" connected using Virtual Hub Admin Mode. The name of the Virtual Hub is "HubCreate b19dcat065".
2022-03-24 07:28:06.417 Connection "CID-3" connected using Virtual Hub Admin Mode. The name of the Virtual Hub is "HubCreate b19dcat065 kaisa0903".
2022-03-24 08:07:41.404 Administration mode [RPC-42]: A new Virtual Hub "b19dcat065" has been created.
2022-03-24 08:07:41.404 Virtual Hub "b19dcat065" has been started.
2022-03-24 08:07:41.404 The MAC address of Virtual Hub "b19dcat065" is "00-AE-79-C6-69-C5".
```

2.4 Kết quả cần đạt

- ✓ Cài đặt thành công VPN server và VPN client
- ✓ Tạo Virtual Hub, tài khoản người dùng VPN trên máy chủ VPN

- ✓ Tạo kết nối và kết nối thành công đến máy chủ (có ảnh chụp màn hình minh chứng bên máy khách và log bên máy chủ).