

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI THỰC HÀNH
THỰC TẬP CƠ SỞ
Bài 07 - Cài đặt cấu hình VPN server

Họ và tên: Nguyễn Huy Quang

Mã sinh viên: B20DCAT144

Giảng viên: Nguyễn Hoa Cường

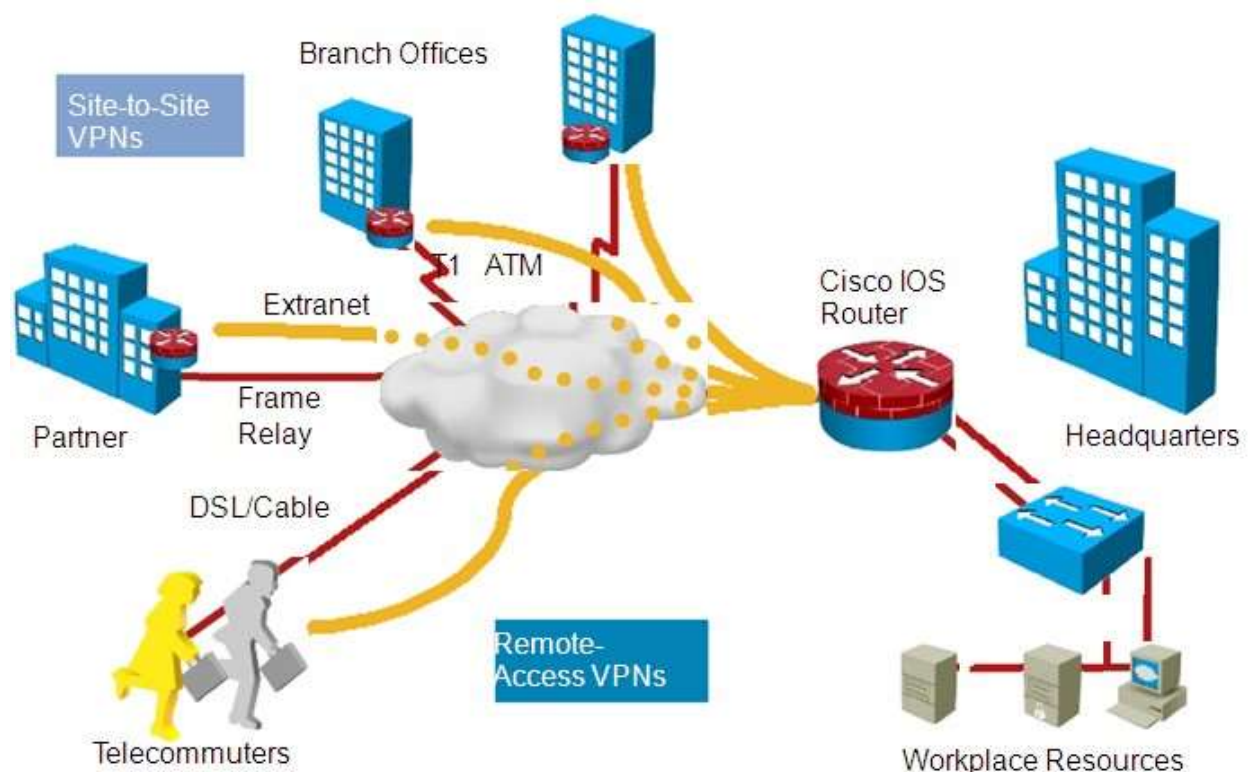
Hà Nội – 2023

I. 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.

- Các mô hình VPN:

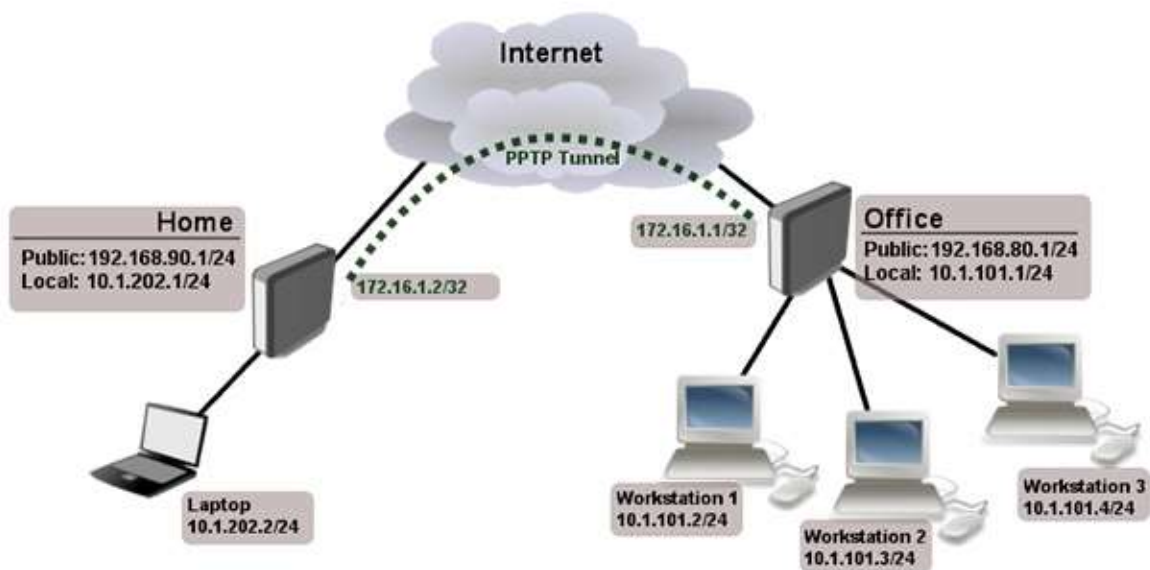


- Một số ứng dụng của VPN:

- + **Truy cập vào mạng doanh nghiệp khi ở xa:** VPN thường được sử dụng bởi những người kinh doanh để truy cập vào mạng lưới kinh doanh của họ, bao gồm tất cả tài nguyên trên mạng cục bộ, trong khi đang đi trên đường, đi du lịch,... Các nguồn lực trong mạng nội bộ không cần phải tiếp xúc trực tiếp với Internet, nhờ đó làm tăng tính bảo mật.
- + **Truy cập mạng gia đình, dù không ở nhà:** Bạn có thể thiết lập VPN riêng để truy cập khi không ở nhà. Thao tác này sẽ cho phép truy cập

Windows từ xa thông qua Internet, sử dụng tập tin được chia sẻ trong mạng nội bộ, chơi game trên máy tính qua Internet giống như đang ở trong cùng mạng LAN.

- + **Duyệt web ẩn danh:** Nếu đang sử dụng WiFi công cộng, duyệt web trên những trang web không phải https, thì tính an toàn của dữ liệu trao đổi trong mạng sẽ dễ bị lộ. Nếu muốn ẩn hoạt động duyệt web của mình để dữ liệu được bảo mật hơn thì bạn nên kết nối VPN. Mọi thông tin truyền qua mạng lúc này sẽ được mã hóa.
- + **Truy cập đến những website bị chặn giới hạn địa lý,** bỏ qua kiểm duyệt Internet, vượt tường lửa,...
- + **Tải tập tin:** Tải BitTorrent trên VPN sẽ giúp tăng tốc độ tải file. Điều này cũng có ích với các traffic mà ISP của bạn có thể gây trở ngại.
- Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS,...
- **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 hổng 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.

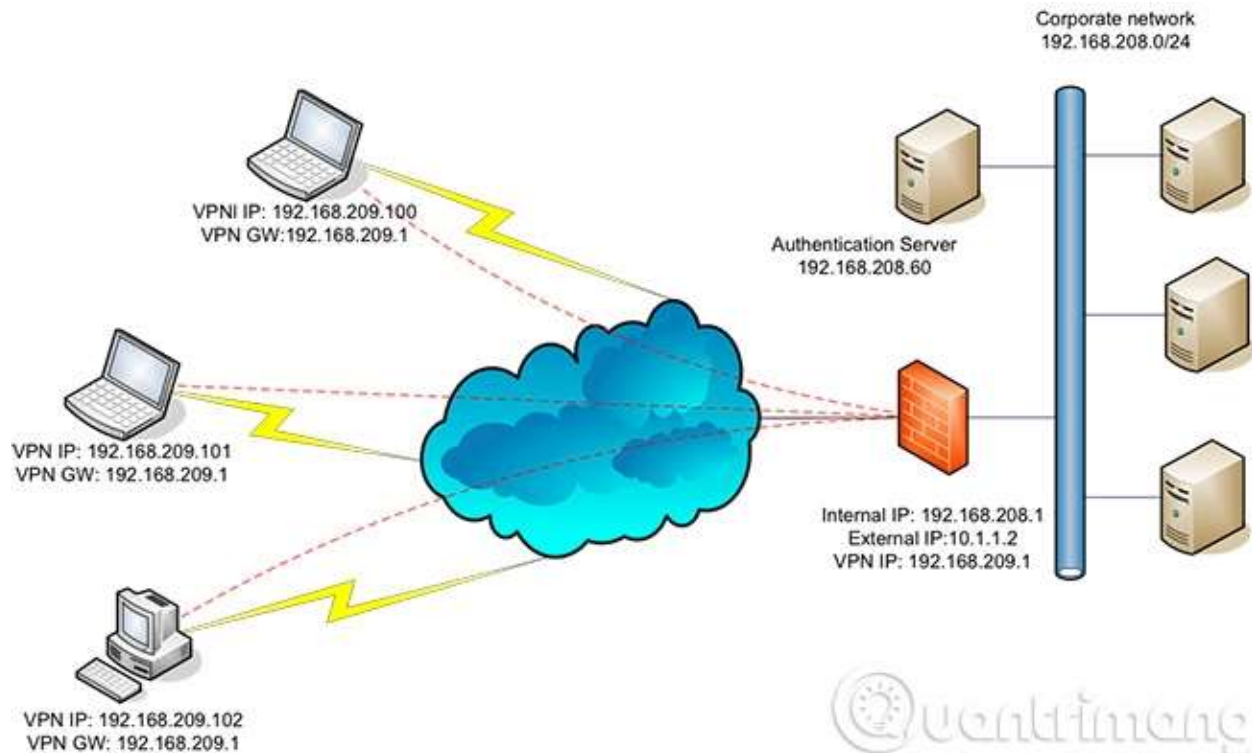
- Các giao thức bảo mật cho VPN: IPSec, SSL/TLS

- **IP security (IPSec)**

Được dùng để bảo mật các giao tiếp, các luồng dữ liệu trong môi trường **Internet** (môi trường bên ngoài VPN). Đây là điểm mấu chốt, lượng traffic qua IPSec được dùng chủ yếu bởi các **Transport mode**, hoặc các **tunnel** (hay gọi là hầm - khái niệm này hay dùng trong Proxy, SOCKS) để **MÃ HÓA** dữ liệu trong VPN.

- **Secure Sockets Layer (SSL) và Transport Layer Security (TLS)**

Có 1 phần tương tự như IPSec, 2 giao thức trên cũng dùng mật khẩu để đảm bảo an toàn giữa các kết nối trong môi trường Internet.



Bên cạnh đó, 2 giao thức trên còn sử dụng chế độ **Handshake** - có liên quan đến quá trình xác thực tài khoản giữa client và server. Để 1 kết nối được coi là thành

công, quá trình xác thực này sẽ dùng đến các **Certificate** - chính là các khóa xác thực tài khoản được lưu trữ trên cả server và client.

- **Tìm hiểu về SoftEther VPN**

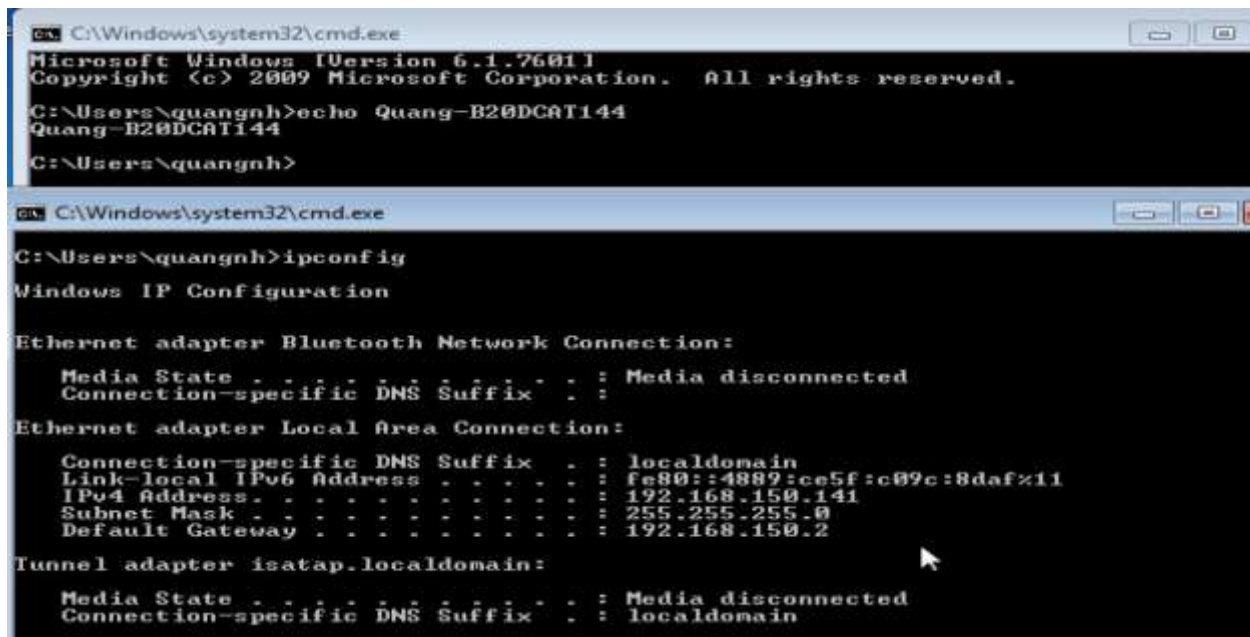
Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và **BẢO MẬT** cao hơn.

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.

II. BÁO CÁO THỰC HÀNH

1. Đổi tên máy và kiểm tra IP (máy thật win , máy ảo linux)



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

C:\Users\quangnh>echo Quang-B20DCAT144
Quang-B20DCAT144
C:\Users\quangnh>

C:\Windows\system32\cmd.exe
C:\Users\quangnh>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::4882:ce5f:c09c:8daf%11
    IPv4 Address. . . . . : 192.168.150.141
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.150.2

Tunnel adapter isatap.localdomain:

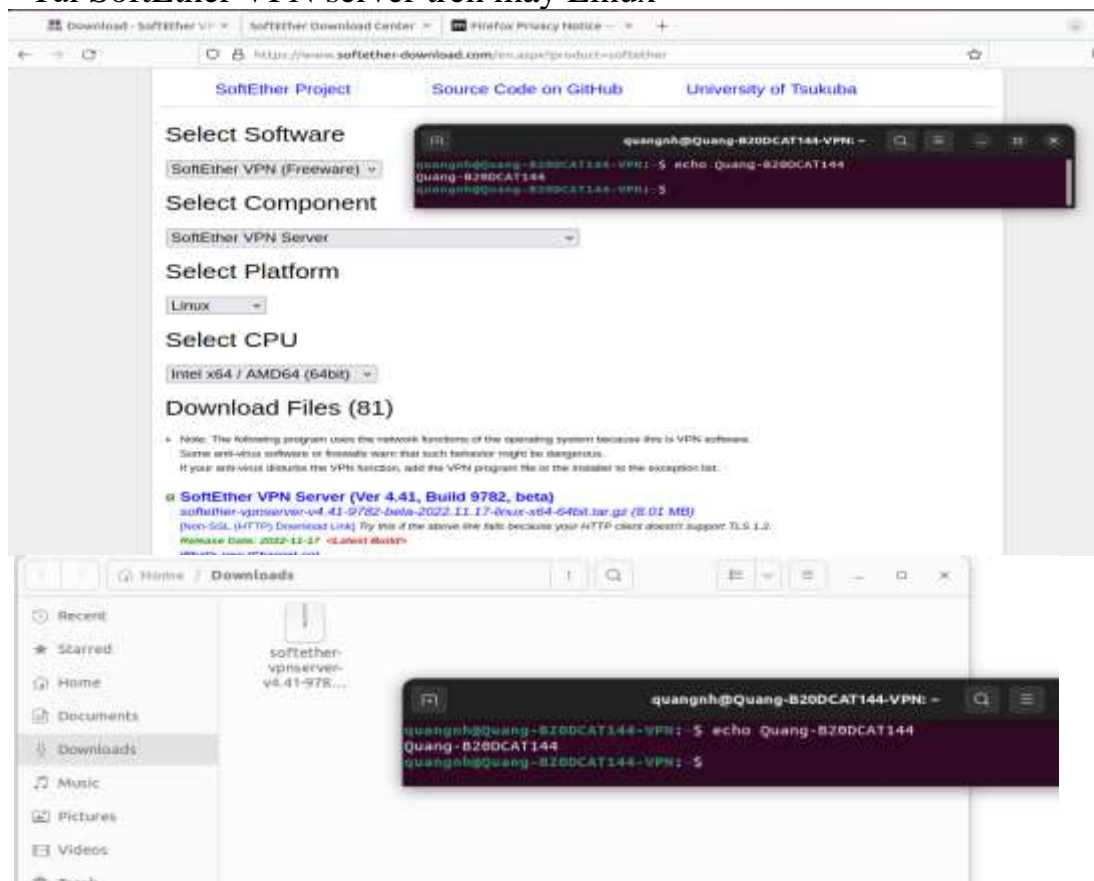
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : localdomain
```

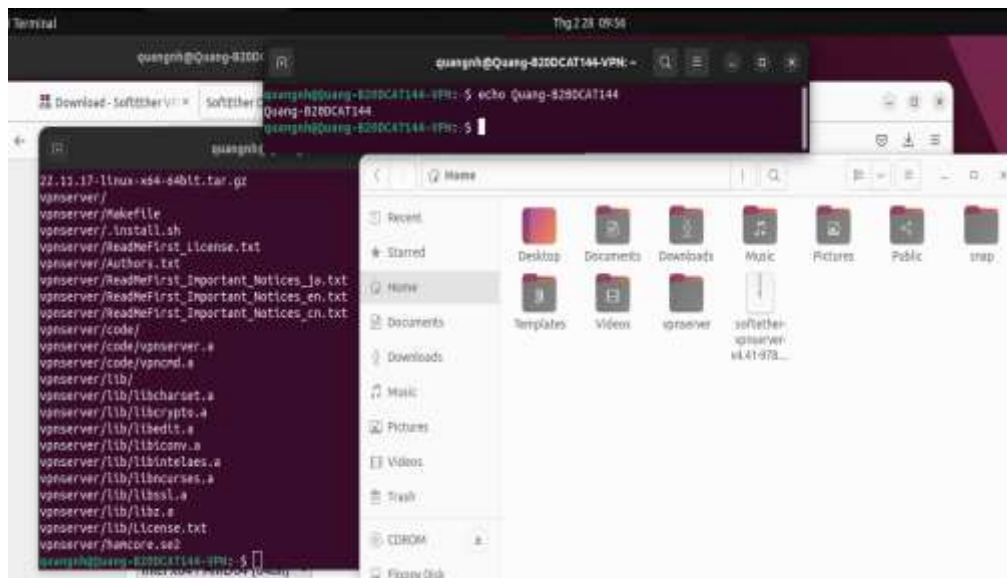


```
quangnh@Quang-B20DCAT144-VPN: ~  
quangnh@Quang-B20DCAT144-VPN:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.150.140 netmask 255.255.255.0 broadcast 192.168.150.255  
    inet6 fe80::b8c7:6d02:6ca2:902 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:47:9f:77 txqueuelen 1000 (Ethernet)  
    RX packets 1303 bytes 1110302 (1.1 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 419 bytes 46624 (46.6 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 131 bytes 11372 (11.3 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 131 bytes 11372 (11.3 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
quangnh@Quang-B20DCAT144-VPN:~$
```

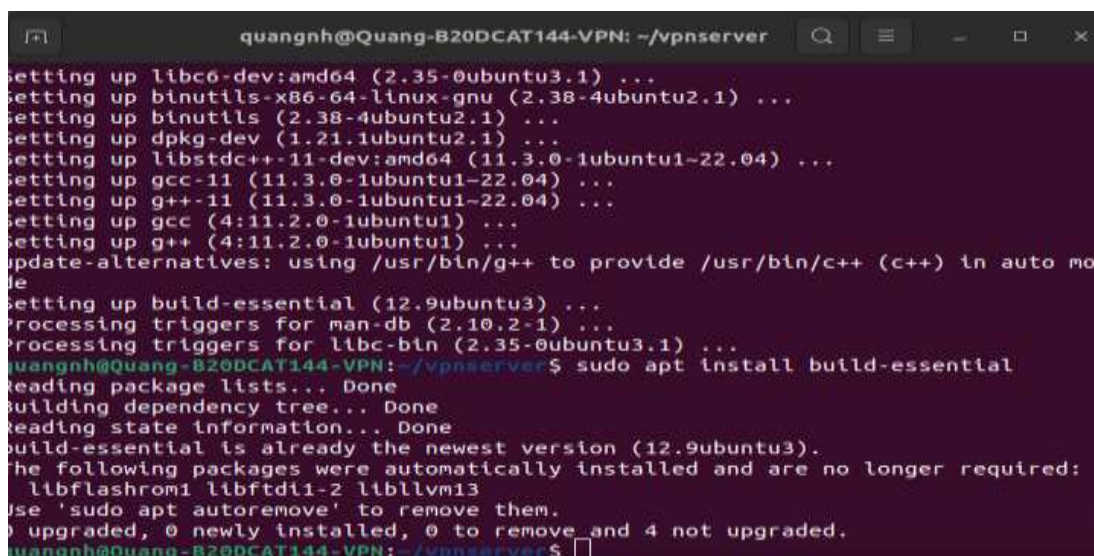
2.Tải SoftEther VPN server , cài đặt và cấu hình VPN server

- Tải SoftEther VPN server trên máy Linux

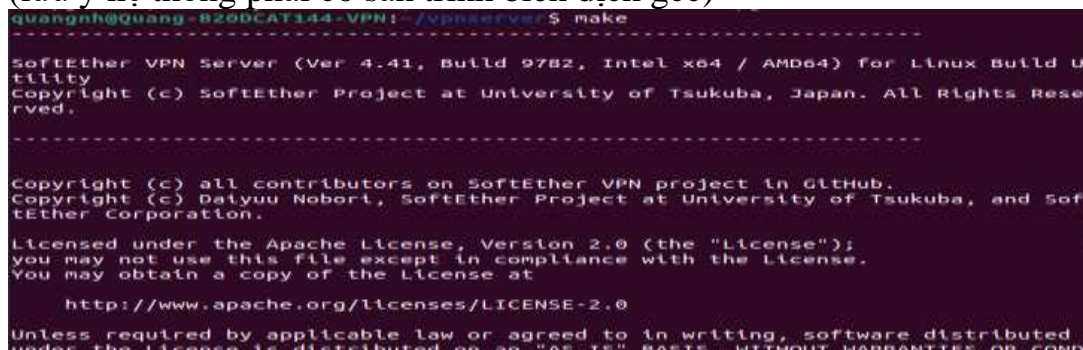




- Cài đặt GCC



- Chuyển vào thư mục VPN server: cd vpnsrvr. Biên dịch và cài đặt: make (lưu ý hệ thống phải có sẵn trình biên dịch gcc)



- Khởi động máy chủ VPN: `sudo ./vpnservice star`

```
quangnh@Quang-B20DCAT144-VPN:~/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://192.168.150.140:5555/
or
https://192.168.150.140/

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

quangnh@Quang-B20DCAT144-VPN:~/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:
- Tạo 1 Virtual Hub mới: `HubCreate` (là tên Virtual Hub - dùng mã sinh viên làm tên Virtual Hub)
- Chọn Virtual Hub đã tạo: `Hub` - Tạo 1 người dùng VPN mới: `UserCreate` /GROUP:none /REALNAME:Tên sinh viên /NOTE:none

```
quangnh@Quang-B20DCAT144-VPN:~/vpnservice$ ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.41 Build 9782 (English)
Compiled 2022/11/17 16:36:25 by buildsan at crosswin with OpenSSL 3.0.7
Copyright (c) 2012-2022 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

quangnh@Quang-B20DCAT144-VPN: ~/vpnservice
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).
Host name or 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 B20DCAT144 /PASSWORD: Quang112
HubCreate command - Create New Virtual Hub
The command completed successfully.
```

```
VPN Server>Hub B20DCAT144
Hub command - Select Virtual Hub to Manage
The Virtual Hub "B20DCAT144" has been selected.
The command completed successfully.
```

```
VPN Server/B20DCAT144>
```

- Đặt mật khẩu cho người dùng: UserPasswordSet

```
VPN Server/B20DCAT144>UserCreat B20DCAT144-nguyenhuyquang /GROUP:none /REALNAME:
NguyenHuyQuang /NOTE:none
UserCreate command - Create User
The command completed successfully.
```

```
quangnh@Quang-B20DCAT144-VPN:~/vpnservers$ make
```

```
-----
SoftEther VPN Server (Ver 4.41, Build 9782, 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
under the license is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR COND
```

3.Tải SoftEther VPN client cho Windows

The screenshot shows a web browser window displaying the 'Download - SoftEther VPN Project' page. The page includes a sidebar with links to Documents, Download, Version History (ChangeLog), Source Code, Support & Forum, About SoftEther VPN Project, and Japanese (日本語). The main content area states that SoftEther VPN is open-source free software and provides instructions for downloading. It lists the Primary Download Server (hosted by Windows Azure) and offers a link to 'Download SoftEther VPN'. It also mentions downloading from CNET Download.com. Below the browser window, a Windows command prompt is open, showing the command 'C:\Users\quangnh>echo Quang-B20DCAT144' and its output 'Quang-B20DCAT144'.

Download - SoftEther VPN Project

SoftEther VPN is [open-source free software](#). You may use, copy, modify, merge, publish, distribute, and make copies of SoftEther VPN.

Primary Download Server (hosted by Windows Azure):

- [Download SoftEther VPN](#)

Language: English, Japanese and Simplified Chinese.
OS: Windows, Linux, Mac OS X, FreeBSD and Solaris.

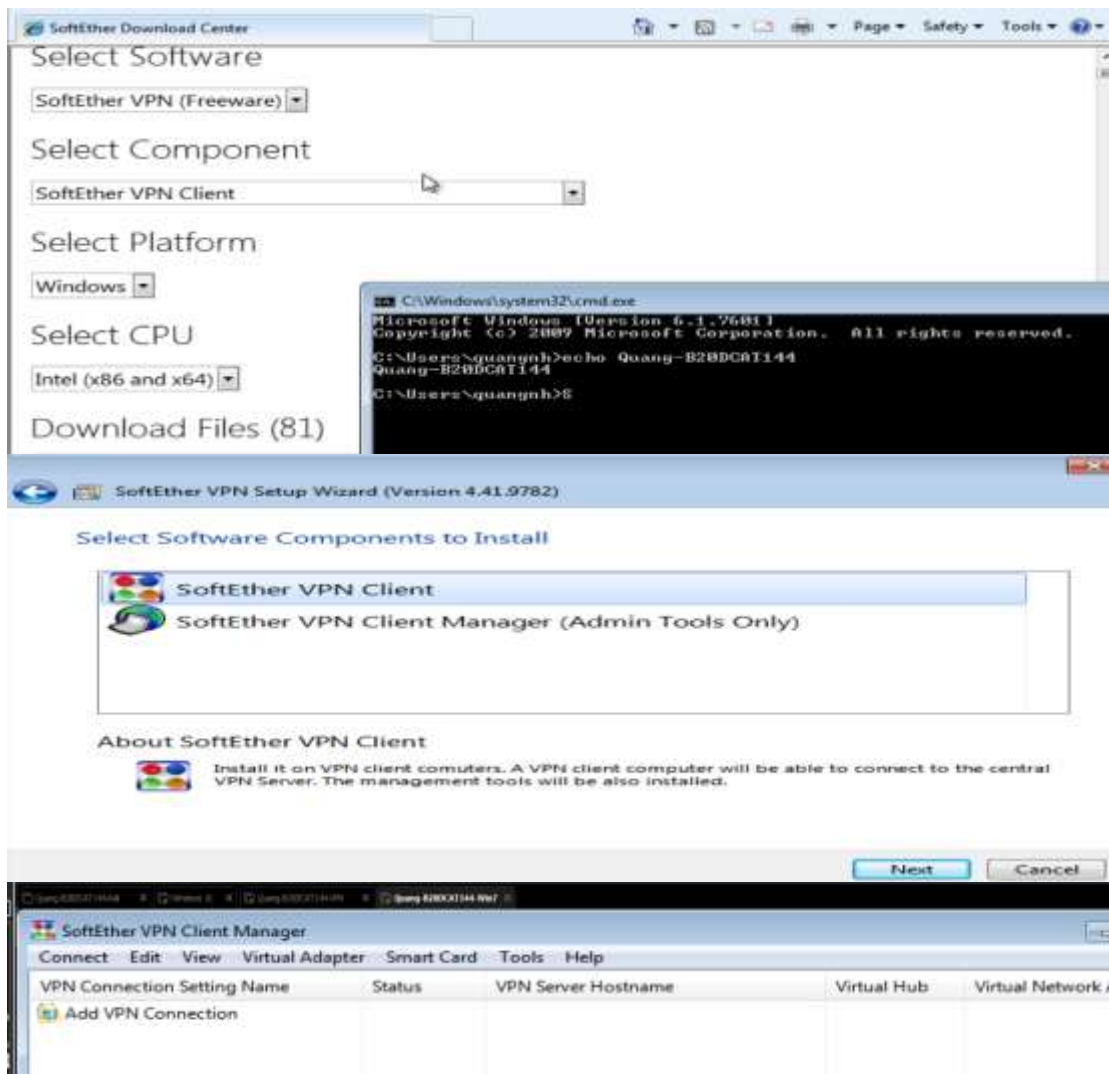
Download from CNET Download.com:

- [Download SoftEther VPN from CNET Download.com](#)

Table of contents

Primary Download Server (hosted by Windows Azure):
[Download from CNET Download.com](#):
[Download from Softpedia.com](#):
See also:

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\quangnh>echo Quang-B20DCAT144
Quang-B20DCAT144

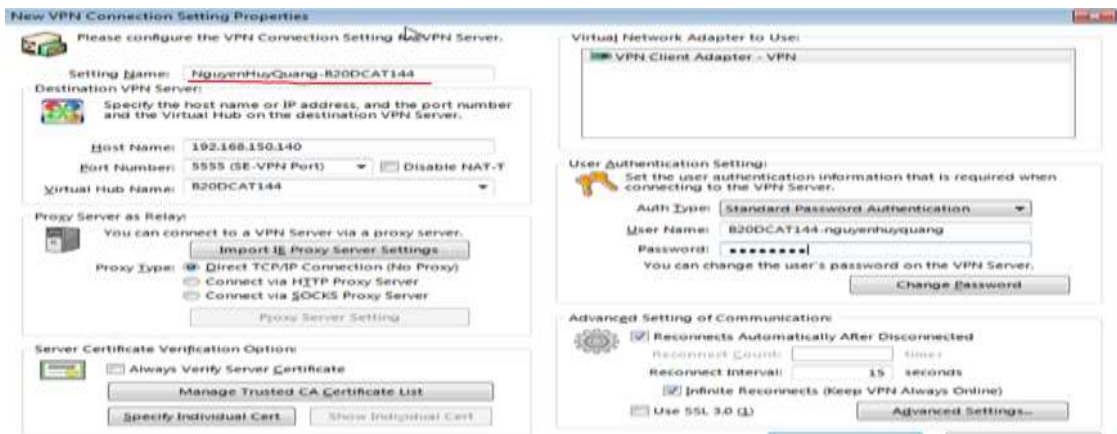


1. Tạo và kiểm tra kết nối VPN

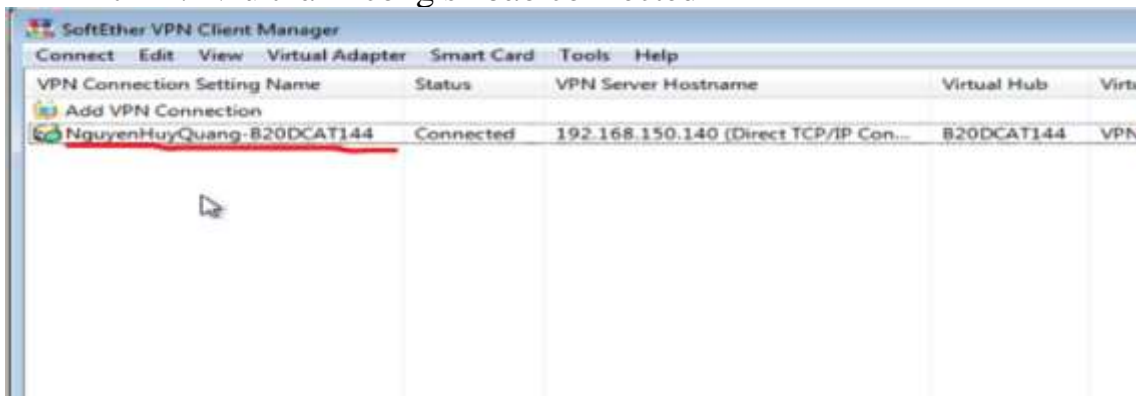
Từ giao diện SoftEther VPN Client Manager tạo 1 kết nối mới (Add New Connection)

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>



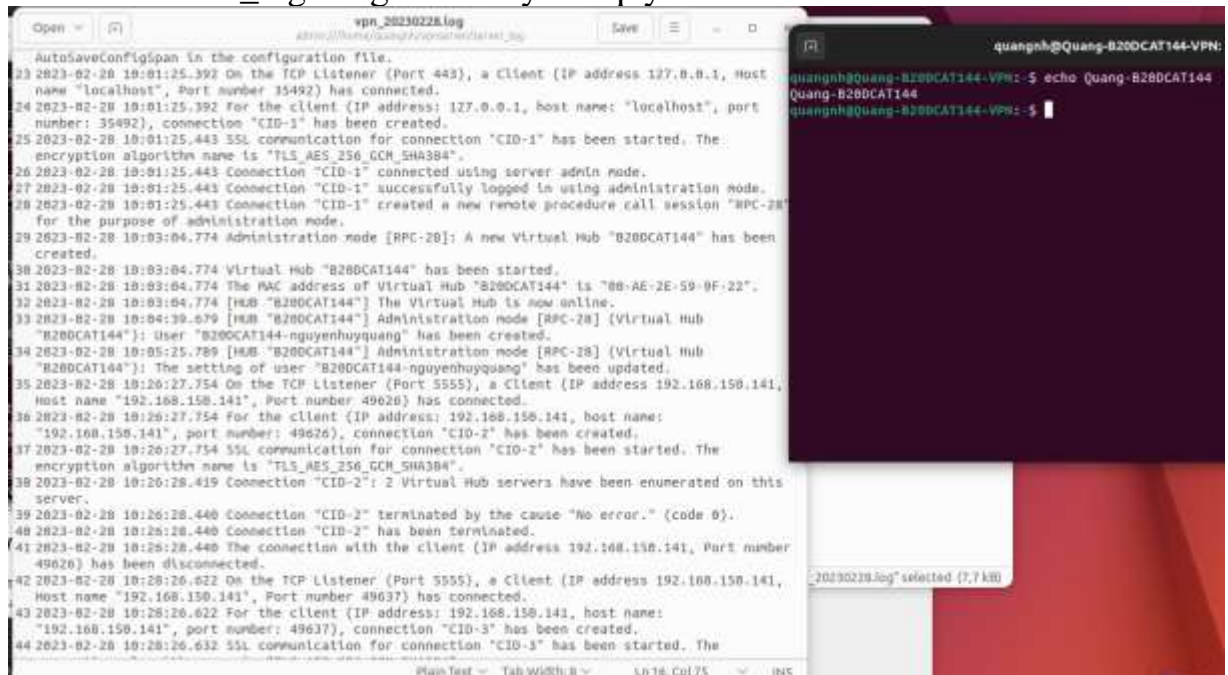
- Thử kết nối: Nếu thành công sẽ báo connected



- 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 <Mã sinh viên> vpnserver/server_log/*.log`
==> Hiện thị các dòng log có liên quan đến <Mã sinh viên>

```
quangnh@Quang-B20DCAT144-VPN:~$ sudo -s
[sudo] password for quangnh:
root@Quang-B20DCAT144-VPN:/home/quangnh# grep B20DCAT144 vpnserver/server_log/*.log
2023-02-28 10:03:04.774 Administration mode [RPC-28]: A new Virtual Hub "B20DCAT144" has been created.
2023-02-28 10:03:04.774 Virtual Hub "B20DCAT144" has been started.
2023-02-28 10:03:04.774 The MAC address of Virtual Hub "B20DCAT144" is "00-AE-2E-59-9F-22".
2023-02-28 10:03:04.774 [HUB "B20DCAT144"] The Virtual Hub is now online.
2023-02-28 10:04:39.679 [HUB "B20DCAT144"] Administration mode [RPC-28] (Virtual Hub "B20DCAT144"): User "B20DCAT144-nguyenhuyquang" has been created.
2023-02-28 10:05:25.789 [HUB "B20DCAT144"] Administration mode [RPC-28] (Virtual Hub "B20DCAT144"): The setting of user "B20DCAT144-nguyenhuyquang" has been updated.
2023-02-28 10:28:27.301 [HUB "B20DCAT144"] The connection "CID-3" (IP address: 192.168.150.141, Host name: 192.168.150.141, Port number: 49637, Client name: "SoftEther VPN Client", Version: 4.41, Build: 9782) is attempting to connect to the Virtual Hub. The auth type provided is "Password authentication" and the user name is "B20DCAT144-nguyenhuyquang".
2023-02-28 10:28:27.301 [HUB "B20DCAT144"] Connection "CID-3": Successfully authenticated as user "B20DCAT144-nguyenhuyquang".
2023-02-28 10:28:27.301 [HUB "B20DCAT144"] Connection "CID-3": The new session "SID-B20DCAT144-NGUYENHUYQUANG-1" has been created. (IP address: 192.168.150.141,
```

- Xem file server_log bằng cách thay đổi quyền



The image shows a Notepad++ window with the file `vpn_20230228.log` open. The log contains the following text:

```
AutosaveConfigSpan in the configuration file.
23 2023-02-28 18:01:25.392 On the TCP listener (Port 443), a client (IP address 127.0.0.1, host
name "localhost", port number 35492) has connected.
24 2023-02-28 18:01:25.392 For the client (IP address: 127.0.0.1, host name: "localhost", port
number: 35492), connection "CID-1" has been created.
25 2023-02-28 18:01:25.443 SSL communication for connection "CID-1" has been started. The
encryption algorithm name is "TLS_AES_256_GCM_SHA384".
26 2023-02-28 18:01:25.443 Connection "CID-1" connected using server admin mode.
27 2023-02-28 18:01:25.443 Connection "CID-1" successfully logged in using administration mode.
28 2023-02-28 18:01:25.443 Connection "CID-1" created a new remote procedure call session "RPC-28"
for the purpose of administration mode.
29 2023-02-28 18:03:04.774 Administration mode [RPC-28]: A new Virtual Hub "B28DCAT144" has been
created.
30 2023-02-28 18:03:04.774 Virtual Hub "B28DCAT144" has been started.
31 2023-02-28 18:03:04.774 The MAC address of Virtual Hub "B28DCAT144" is "08-AE-2E-59-0F-22".
32 2023-02-28 18:03:04.774 [HUB "B28DCAT144"] The Virtual Hub is now online.
33 2023-02-28 18:04:39.679 [HUB "B28DCAT144"] Administration mode [RPC-28] [Virtual Hub
"B28DCAT144"]: User "B28DCAT144-nguyenhuyquang" has been created.
34 2023-02-28 18:05:25.789 [HUB "B28DCAT144"] Administration mode [RPC-28] [Virtual Hub
"B28DCAT144"]: The setting of user "B28DCAT144-nguyenhuyquang" has been updated.
35 2023-02-28 18:20:27.754 On the TCP listener (Port 5555), a client (IP address 192.168.150.141,
Host name "192.168.150.141", Port number 49626) has connected.
36 2023-02-28 18:20:27.754 For the client (IP address: 192.168.150.141, host name:
"192.168.150.141", port number: 49626), connection "CID-2" has been created.
37 2023-02-28 18:20:27.754 SSL communication for connection "CID-2" has been started. The
encryption algorithm name is "TLS_AES_256_GCM_SHA384".
38 2023-02-28 18:20:28.419 Connection "CID-2": 2 Virtual Hub servers have been enumerated on this
server.
39 2023-02-28 18:20:28.440 Connection "CID-2" terminated by the cause "No error." (code 0).
40 2023-02-28 18:20:28.440 Connection "CID-2" has been terminated.
41 2023-02-28 18:20:28.440 The connection with the client (IP address 192.168.150.141, Port number
49626) has been disconnected.
42 2023-02-28 18:20:20.622 On the TCP listener (Port 5555), a client (IP address 192.168.150.141,
Host name "192.168.150.141", Port number 49637) has connected.
43 2023-02-28 18:20:20.622 For the client (IP address: 192.168.150.141, host name:
"192.168.150.141", port number: 49637), connection "CID-3" has been created.
44 2023-02-28 18:20:20.632 SSL communication for connection "CID-3" has been started. The
```

Overlaid on the right is a terminal window with the prompt `quangnh@Quang-B28DCAT144-VPN: $`. It shows the command `echo Quang-B28DCAT144` being executed, resulting in the output `Quang-B28DCAT144`.