

# DỊCH VỤ VPN

**Tô Vũ Song Phương**  
Cao Đẳng Kỹ Thuật Cao Thắng

# Nội dung

1. Tại sao cần có VPN?
2. VPN là gì?
3. Hoạt động của VPN
4. Các dịch vụ phần mềm VPN
5. Phân loại VPN
6. Các giao thức đường ống trong VPN
7. Các giao thức xác thực trong VPN
8. VPN Reconnect
9. Câu hỏi ôn tập

# 1. Tại sao cần có VPN?

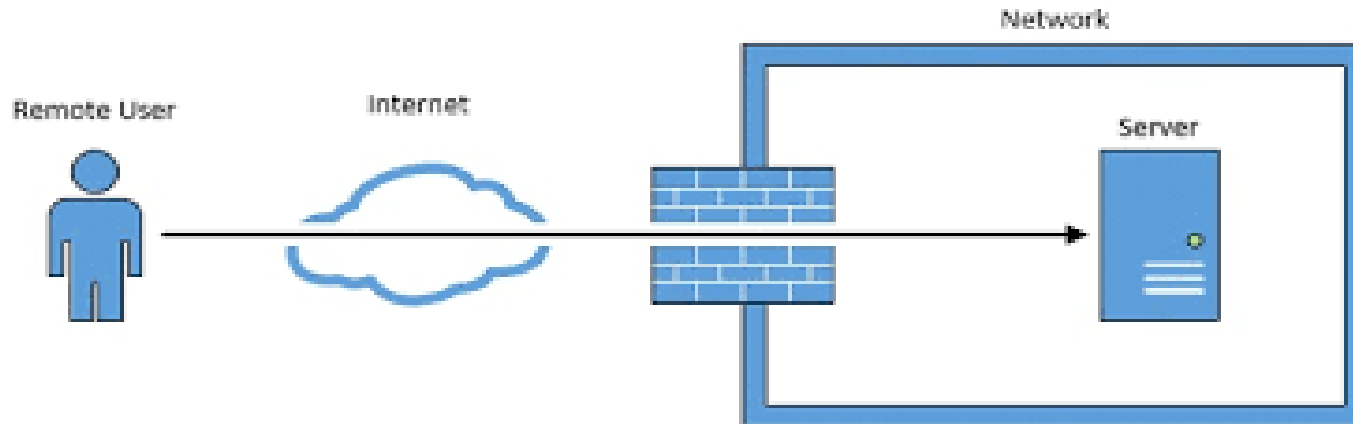


## Tình huống 1:

- Ông P (người quản trị) đi xa, Server công ty gặp trục trặc cần khôi phục ngay lập tức → ông P không thể bỏ công việc mà quay về công ty để tùy chỉnh.

## Giải pháp:

- Ông P có thể Remote Access (1 dạng của VPN) máy Server từ Internet, đồng thời truy cập tài liệu giữa các máy trong mạng WORKGROUP của mình.



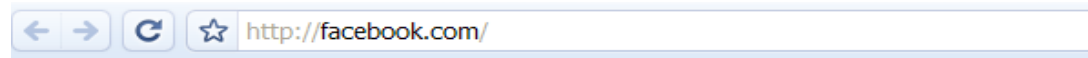
# 1. Tại sao cần có VPN?

## Tình huống 2:

- Ông P đang ở Việt Nam muốn truy cập Facebook để xem thông tin bạn bè nhưng bị chặn bởi các nhà mạng.

## Giải pháp:

- Ông P ứng dụng công nghệ VPN để truy cập nội dung bị chặn trên internet tại địa điểm hay quốc gia không cho phép hoạt động.



**This webpage is not available.**

The webpage at <http://facebook.com/> might be temporarily down or it may have moved permanently to a new web address.

Here are some suggestions:

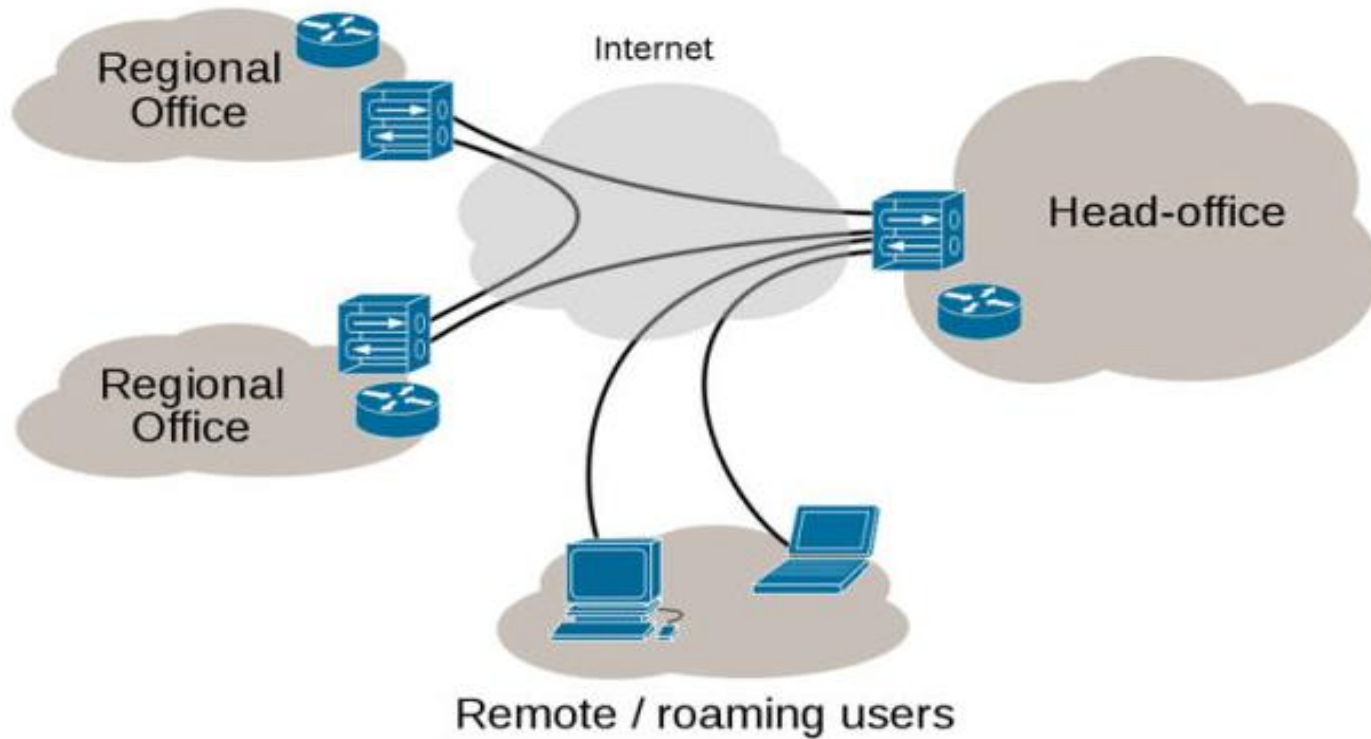
- [Reload](#) this web page later.

[+ More information on this error](#)

## 2. VPN là gì?

- **VPN (Virtual Private Network, mạng riêng ảo)** dịch vụ mạng ảo được triển khai trên hệ thống mạng công cộng (internet) để kết nối các văn phòng chi nhánh, người dùng di động từ xa kết nối về văn phòng chính

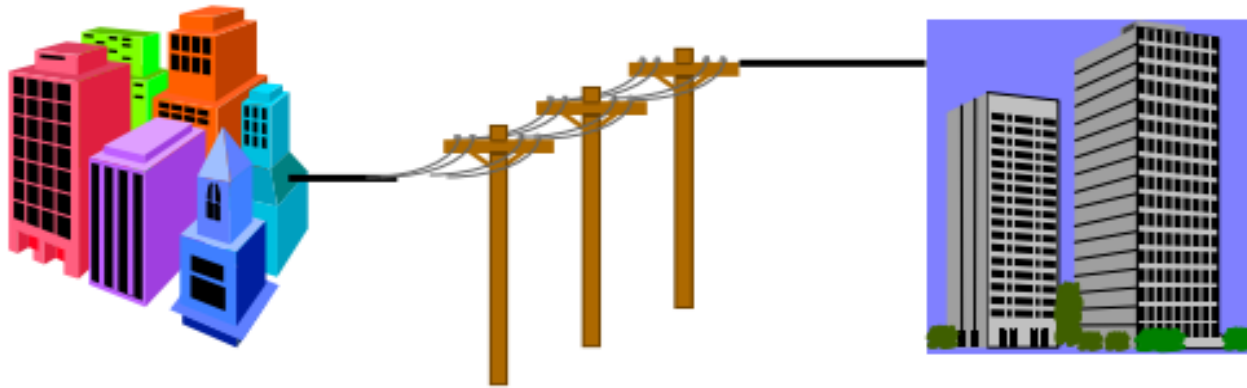
## 2. VPN là gì?



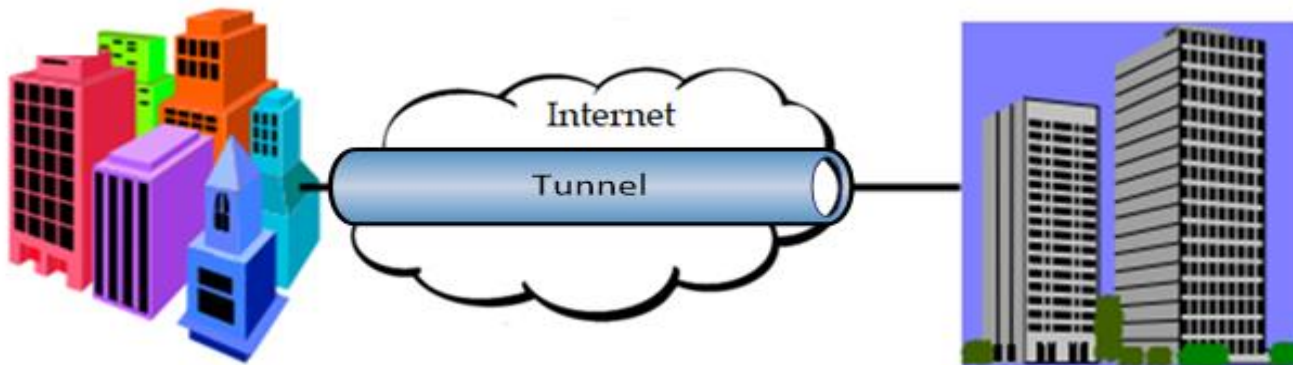
Một mạng VPN điển hình bao gồm mạng LAN tại trụ sở văn phòng chính, các mạng LAN khác tại những văn phòng chi nhánh, nhân viên di động truy cập đến từ bên ngoài.

## 2. VPN là gì?

- Phân biệt giữa **Private Network** và **Virtual Private Network**
- **Private Network:** sử dụng leased lines (dịch vụ thuê kênh riêng)



- **Virtual Private Network:** sử dụng đường ống (tunnel) dựa trên mạng công cộng (internet)



## 2. VPN là gì?

### Lợi ích của VPN

- Giảm thời gian và chi phí truyền dữ liệu đến người dùng ở xa. Giảm chi phí vận hành so với mạng WAN truyền thống
- Tăng tính bảo mật: các dữ liệu quan trọng gửi trên VPN đã được mã hóa
- Dễ mở rộng, nâng cấp, linh động cao: VPN xóa bỏ rào cản về mặt địa lý cho hệ thống mạng, kết nối các mạng riêng lại với nhau một cách dễ dàng thông qua môi trường Internet
- Kiến trúc mạng đường ống (tunnel) nên đơn giản hơn kiến trúc mạng truyền thống



## 2. VPN là gì?

### **Những hạn chế của VPN**

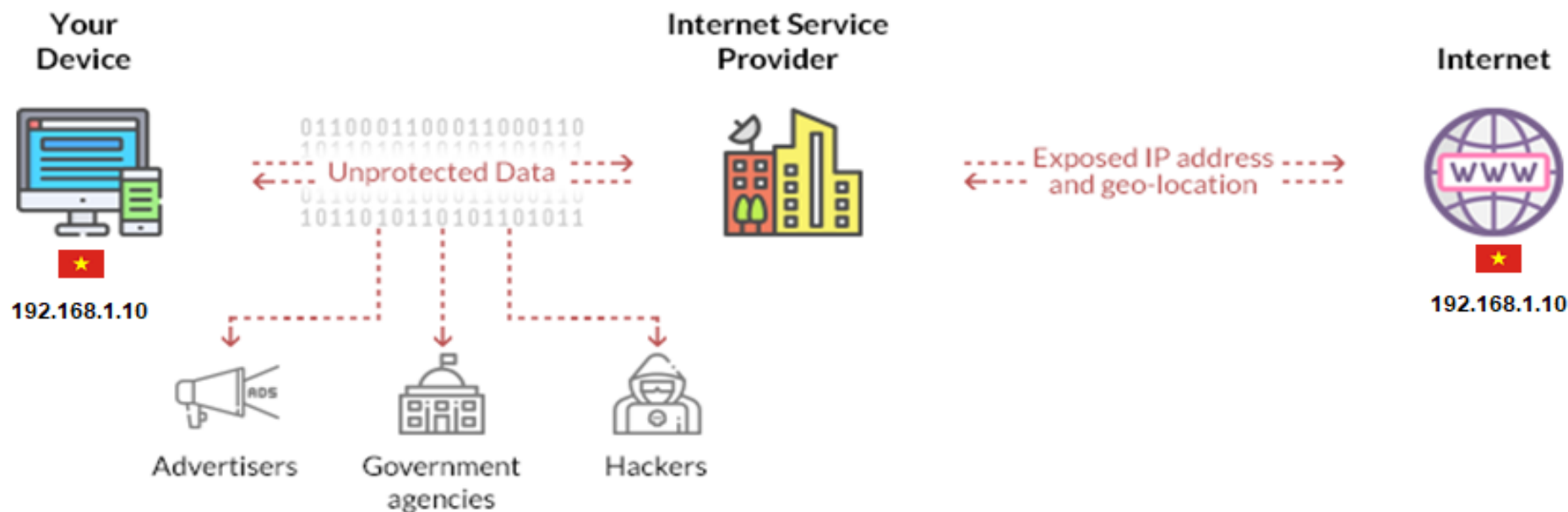
- VPN đòi hỏi hiểu biết rõ về an ninh mạng và cách cài đặt/cấu hình.
- Độ tin cậy và hiệu suất của VPN không dựa vào một tổ chức nào, mà dựa vào một ISP và chất lượng dịch vụ của họ.
- Do phải truyền dữ liệu thông qua Internet nên khi dữ liệu lớn như phim ảnh, âm thanh sẽ rất chậm

## 2. Các tính chất VPN

- **Đóng gói (encapsulation):** dữ liệu riêng tư khi truyền qua mạng phải được đóng gói kèm theo header có chứa thông tin định tuyến
- **Xác thực (authentication):** cung cấp danh tính identity của người dùng hoặc máy tính kết nối
- **Mã hóa (encryption):** dữ liệu phải được mã hóa trước khi truyền để người lạ không thể đọc. Khi nhận được, người nhận sẽ giải mã
- **Toàn vẹn dữ liệu (data integrity):** kiểm tra dữ liệu gửi qua kết nối VPN không sửa đổi trong quá trình truyền

# 3. Hoạt động của VPN

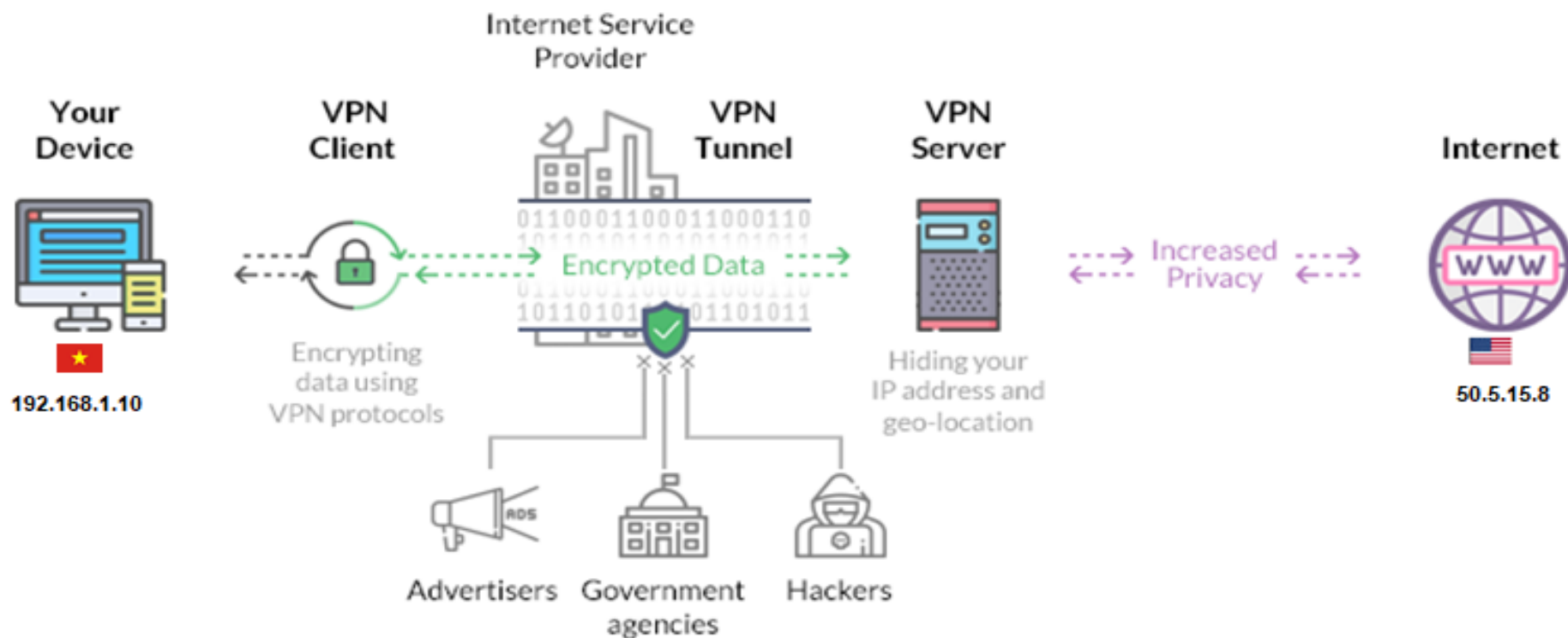
## Khi không dùng VPN



- Khi truy cập Internet, mọi dữ liệu đều đi qua ISP mà không được mã hóa
- ISP thấy mọi thứ khi online: lịch sử lướt web, download file ...
- Địa chỉ IP và vị trí địa lý đều được hiển thị trên Internet

# 3. Hoạt động của VPN

## Khi dùng VPN



- Có thêm VPN Client và VPN Server
- Dữ liệu được mã hóa. ISP không thấy được dữ liệu đi qua
- Địa chỉ IP và vị trí địa lý thay đổi

# 3. Hoạt động của VPN

## Khi dùng VPN

1. User sử dụng VPN Client kết nối tới VPN Server để truy cập web. Dữ liệu khi đến VPN Client bắt đầu được mã hóa
2. VPN Client thiết lập đường hầm VPN (VPN tunnel) tới VPN Server. Dữ liệu mã hóa được truyền qua tunnel này
3. VPN Server thay địa chỉ IP và vị trí địa lý của User bằng địa chỉ IP và vị trí địa lý của VPN Server. VPN Server giải mã dữ liệu và chuyển yêu cầu tới web
4. Ngay khi VPN Server nhận được trả lời từ web, nó sẽ mã hóa dữ liệu và trả ngược lại VPN Client theo tunnel đã tạo lúc trước.
5. VPN Client giải mã và gửi dữ liệu về thiết bị người dùng

# 4. Các dịch vụ phần mềm VPN

- Các phần mềm VPN không chỉ bảo vệ dữ liệu máy tính mà còn có thể truy cập vào những nội dung bị chặn trên mạng internet tại địa điểm hoặc quốc gia không cho phép hoạt động
- Ví dụ: Facebook bị chặn bởi các nhà mạng Việt Nam, nhưng sử dụng phần mềm VPN → truy cập Facebook một cách dễ dàng
- Hiện nay, có rất nhiều phần mềm VPN được tạo ra hỗ trợ cho đa nền tảng

# 4.1 ExpressVPN

[WHAT IS VPN? ▾](#)[PRODUCTS ▾](#)[SUPPORT](#)[BLOG](#)[MY ACCOUNT](#)[GET STARTED](#)[Er](#)

## Blazing-fast VPN speeds

Huge network of 2,000+ global VPN servers optimized for fast connections. Unlimited bandwidth, no throttling.



## Easy-to-use VPN service for Windows, Mac, iOS, Android, Linux, and routers

Get set up in minutes on any device. Download, install, and connect to ExpressVPN with the push of a button.



## No restrictions

Stream or download anything, from any of our servers, anywhere on Earth, with your IP address hidden from prying eyes.



## Offshore privacy protection

Based in the British Virgin Islands, a tropical oasis without data retention laws. No activity logs. No connection logs.

## ExpressVPN apps



Windows



Mac



iOS



Android



Linux



Routers

## Browser extensions

Chrome

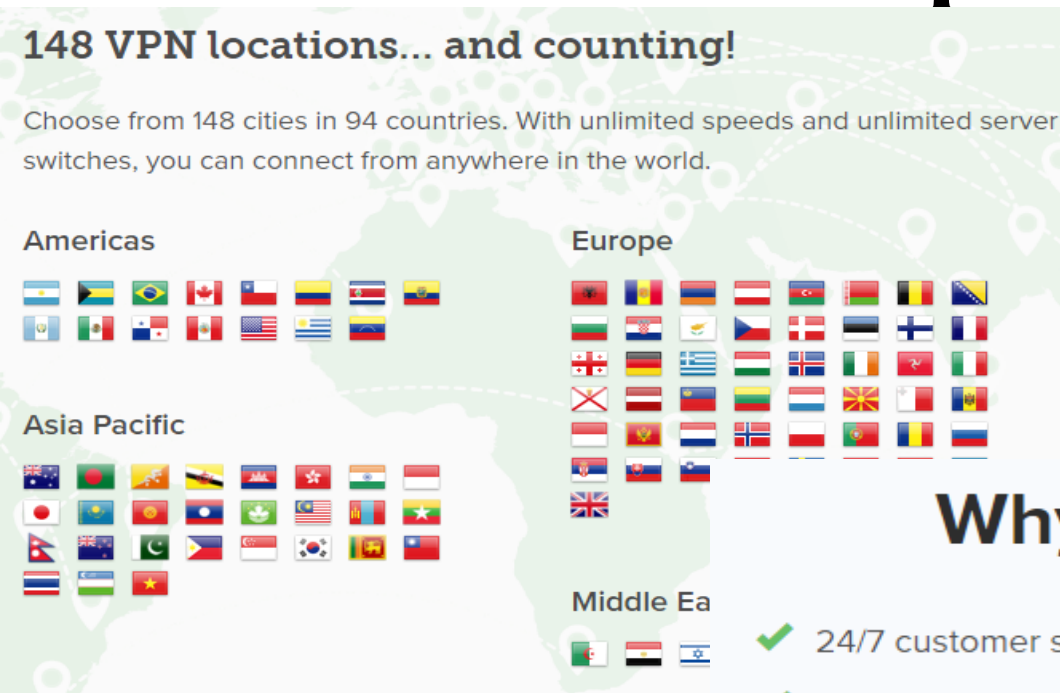
Firefox

Safari

# 4.1 ExpressVPN

**148 VPN locations... and counting!**

Choose from 148 cities in 94 countries. With unlimited speeds and unlimited server switches, you can connect from anywhere in the world.



**Americas**

**Europe**

**Asia Pacific**

**Middle Ea**

## Why choose ExpressVPN?

- ✓ 24/7 customer support through live chat
- ✓ 30-day money-back guarantee
- ✓ 148 VPN server locations in 94 countries
- ✓ Easy to use
- ✓ Apps for every device
- ✓ Speed-optimized network
- ✓ Unlimited bandwidth
- ✓ Best-in-class encryption
- ✓ Private, anonymous service
- ✓ Based in the BVI

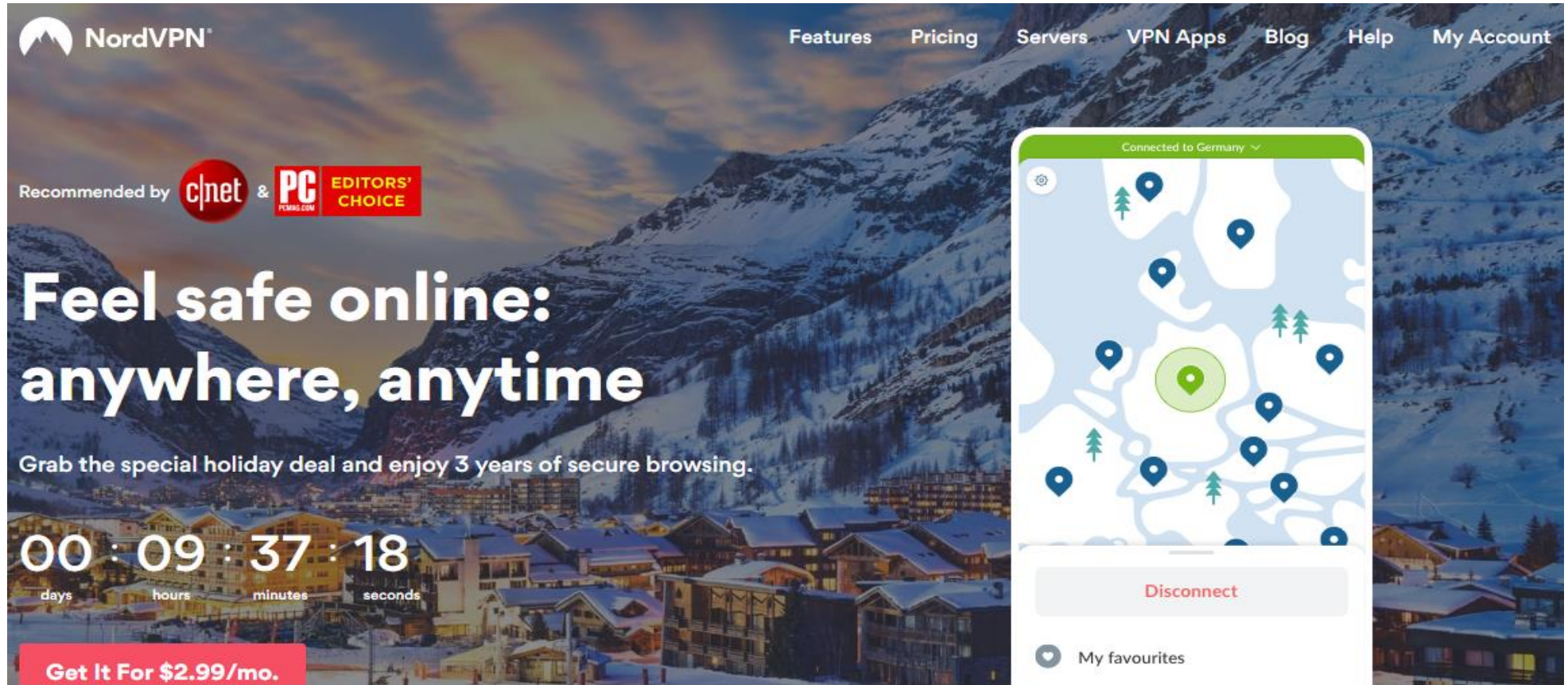
- Tham khảo:

[1] <https://www.expressvpn.com/>

[2] Review ExpressVPN <https://vi.wizcase.com/reviews/expressvpn/>



# 4.2 NordVPN



**NordVPN**

Features Pricing Servers VPN Apps Blog Help My Account

Recommended by **c|net** & **PC** **EDITORS' CHOICE**

## Feel safe online: anywhere, anytime

Grab the special holiday deal and enjoy 3 years of secure browsing.

00 : 09 : 37 : 18  
days hours minutes seconds

**Get It For \$2.99/mo.**

Connected to Germany

Disconnect

My favourites

# 4.2 NordVPN

## Download VPN for all your devices

NordVPN offers user-friendly applications for all major operating systems.



Android



Windows



macOS



iOS · iPhone · iPad



Android TV



Linux



Chrome



Firefox

## NordVPN servers

5206 servers · 62 countries

- Tham khảo:

[1] <https://nordvpn.com/>

[2] Review NordVPN

<https://vi.vpnmentor.com/reviews/nordvpn/>

# 4.3 CyberGhost



[VPN Insights](#) ▾ [The Apps](#) ▾ [Pricing](#) [Servers](#) [Help](#)



**Buy Now - 79% DISCOUNT**

[My Account](#)



Your ISP: **Vietnam Posts and Telecommu...**

Your Location: **Ho Chi Minh City (Vietnam)**

Your IP: **14.187.91.2**

Your Status: **EXPOSED** ⚠

Privacy so strong not even Santa can snoop on

**Get CyberGhost | Save 79%**

[Or try it for free for 24h](#)



# 4.3 CyberGhost

All you need from a truly complete VPN solution

- ✓ Automatic Kill Switch
- ✓ Highest possible speed
- ✓ Unlimited bandwidth and traffic
- ✓ Access to over 3000 servers worldwide
- ✓ DNS and IP Leak Protection
- ✓ Strict No Logs Policy
- ✓ 256-bit AES Encryption
- ✓ OpenVPN, L2TP-IPsec and PPTP protocols
- ✓ Simultaneous connections on up to 7 devices
- ✓ Apps for Windows, Mac, iOS, Android, Linux, Routers
- ✓ Friendly support: chat or email
- ✓ 45-day money back guarantee



**60**

COUNTRIES



**3,093**

SERVERS ONLINE



**36,527**

USERS ONLINE

- Tham khảo:

[1] [https://www.cyberghostvpn.com/en\\_US](https://www.cyberghostvpn.com/en_US)

[2] Review CyberGhost: phiên bản miễn phí thường không hỗ trợ mức mã hóa cao nhất cũng như băng thông bị giới hạn

<https://vi.vpnmentor.com/reviews/cyberghost-vpn/>

# 4.4 Pure VPN



PUREVPN

[Features](#)

[Why PureVPN](#)

[Server Locations](#)

[Pricing](#)

[Business VPN](#)

[My Account](#) ▼

[English](#) ▼



## The X-Mas Special

Get The World's Fastest VPN Service At

The **LOWEST PRICE Ever!**

**\$1.32** per month

ON 5-YEAR PLAN!

[Get A Trusted VPN →](#)

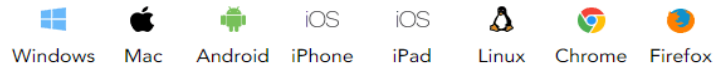
31-Day Money-Back Guarantee



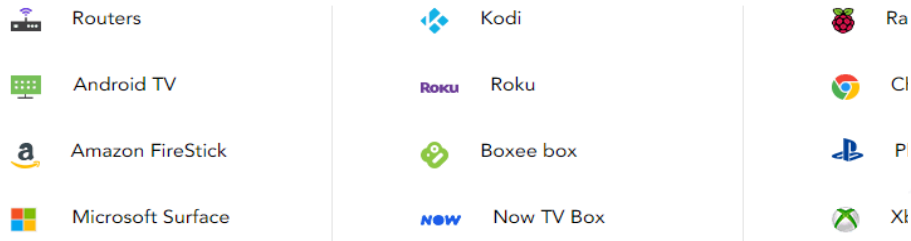
# 4.4 Pure VPN

## Devices Supported by our VPN Service

What good is a secure VPN if it doesn't support every internet-enabled device!



### Also Compatible With



## Our Footprint Covers 180+ Locations

Over 2,000+ servers and 300,000+ IPs are always there to ensure complete accessibility.

### North America

667 Servers



### South America

84 Servers



### Central America

12 Servers



### Oceania

### Europe

807 Servers



### Africa

150 Servers



### Asia

321 Servers



- Tham khảo:

[1] <https://www.purevpn.com/>

[2] Review PureVPN

<https://vi.vpnmentor.com/reviews/purevpn/>

# 5. Phân loại VPN

Tùy thuộc mô hình mạng và nhu cầu sử dụng, VPN được phân thành 2 loại cơ bản:

- **Remote Access VPN**
- **Site to Site VPN**

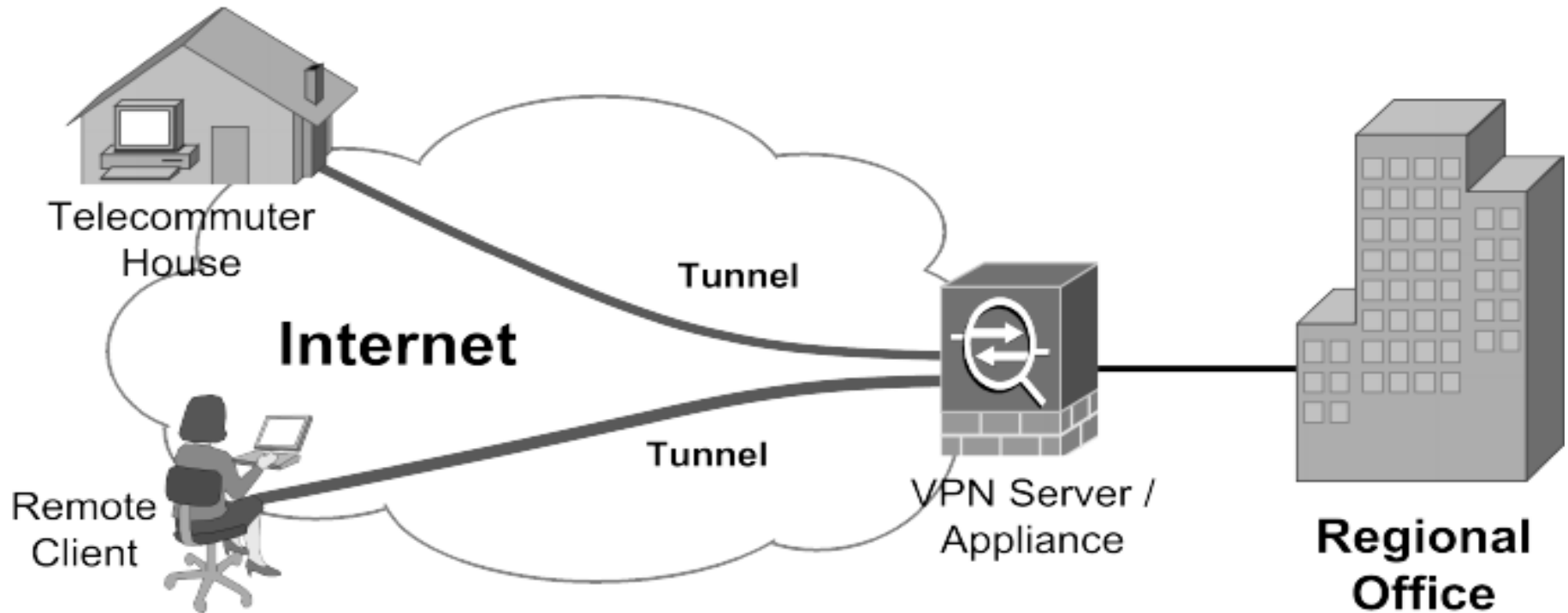


# 5.1 Remote Access VPN

- Áp dụng cho nhân viên làm việc lưu động hay làm việc ở nhà muốn kết nối vào mạng công ty một cách an toàn
- Cũng có thể áp dụng cho văn phòng nhỏ ở xa kết nối vào văn phòng trung tâm của công ty
- Remote Access VPN còn được xem như là dạng User-to-LAN, cho phép người dùng ở xa dùng phần mềm VPN Client kết nối với VPN Server



# 5.1 Remote Access VPN

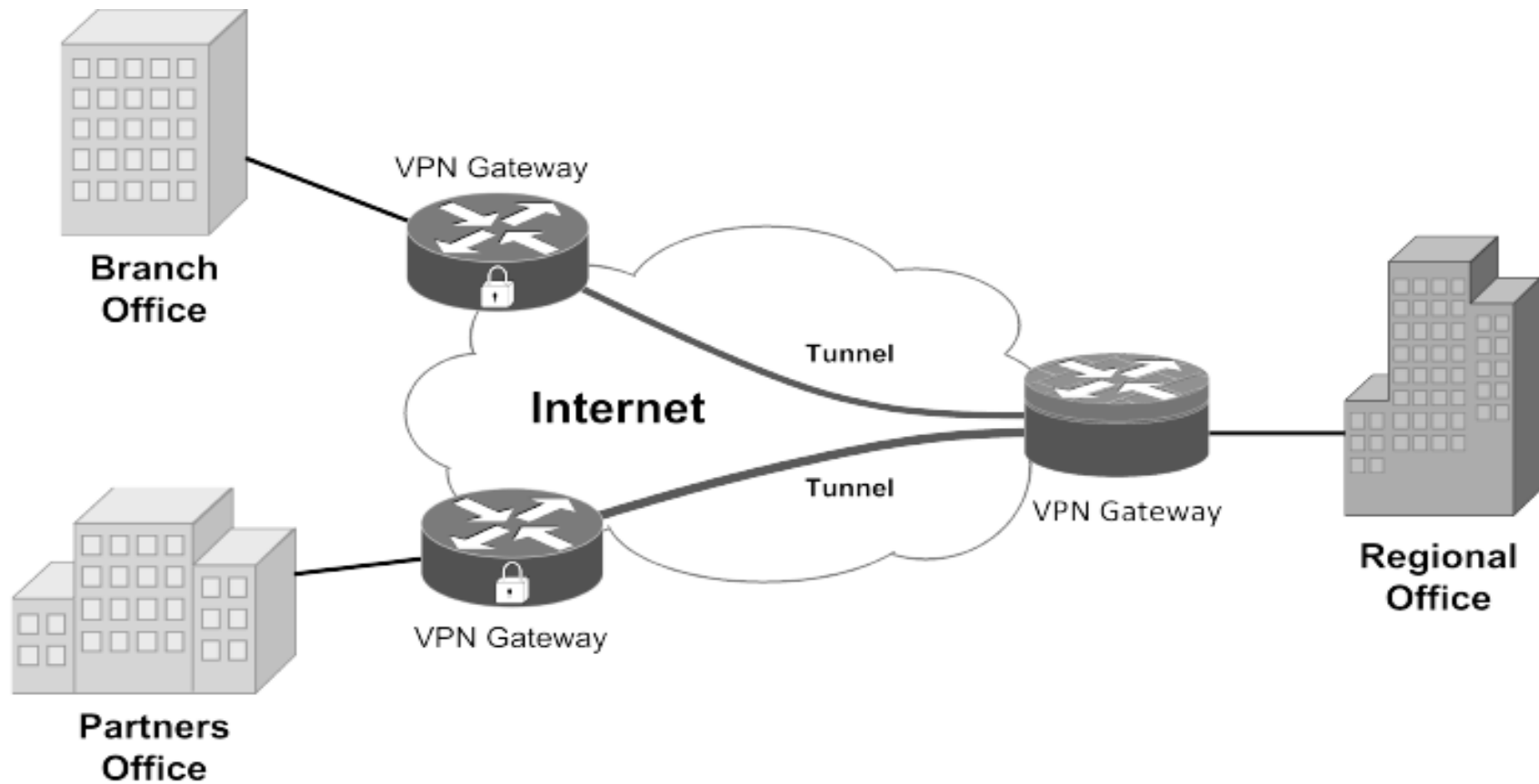


Minh họa Remote Access VPN

## 5.2 Site to Site VPN

- Còn được gọi là LAN-to-LAN cho phép kết nối nhiều văn phòng trụ sở xa nhau tạo thành một hệ thống mạng thống nhất
- Việc chứng thực phụ thuộc vào thiết bị đầu cuối ở các Site, các thiết bị này hoạt động như Gateway và đây là nơi đặt nhiều chính sách bảo mật nhằm truyền dữ liệu một cách an toàn giữa các Site

## 5.2 Site to Site VPN

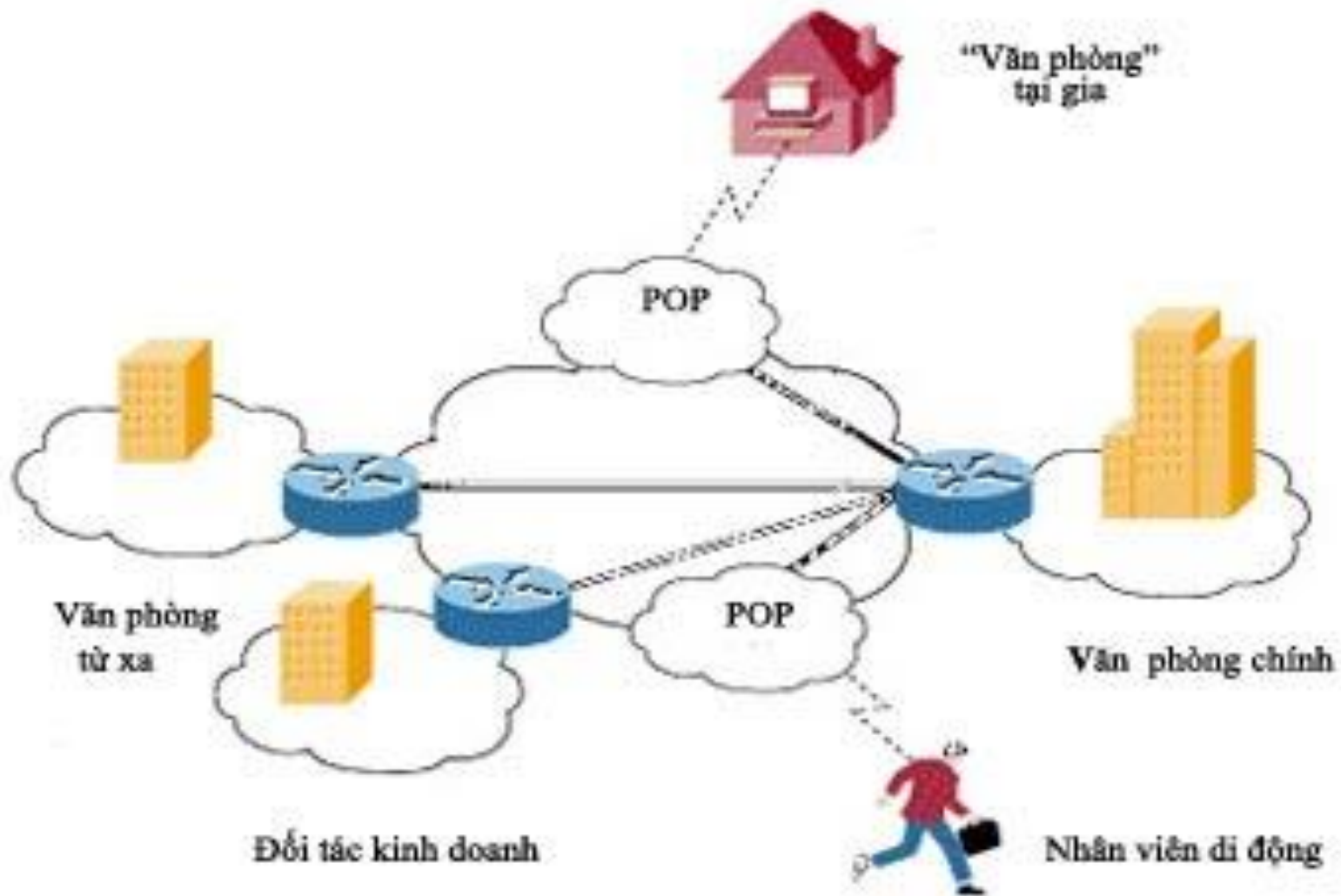


Minh họa Site to Site VPN

## 5.2 Site to Site VPN

- Gồm 2 loại:
  - ✓ Intranet Site to Site VPN
  - ✓ Extranet Site to Site VPN
- **Intranet**: Nếu một công ty có vài địa điểm từ xa muốn tham gia vào một mạng riêng duy nhất → tạo ra VPN nội bộ
- **Extranet**: Khi một công ty có mối quan hệ mật thiết với một công ty khác (đối tác cung cấp, khách hàng...) → tạo VPN mở rộng để nhiều tổ chức khác nhau có thể làm việc trên một môi trường chung

## 5.2 Site to Site VPN



Kết nối giữa văn phòng chính và văn phòng từ xa: ?

Kết nối giữa văn phòng chính và đối tác kinh doanh: ?

# 6. Các giao thức đường ống trong VPN

- Các giao thức trong VPN đều dựa vào **đường ống (tunnel)** để tạo ra mạng riêng trên nền Internet
- Các giao thức:
  - ✓ Point-to-Point Tunneling Protocol (PPTP)
  - ✓ Layer 2 Tunneling Protocol (L2TP)
  - ✓ Secure Socket Tunneling Protocol (SSTP)
  - ✓ Internet Key Exchange version 2 (IKEv2)
  - ✓ OpenVPN

# 6.1 PPTP

- Được phát triển bởi Microsoft, dựa trên kết nối quay số (dial-up)
- Là 1 trong các giao thức được sử dụng rộng rãi cho đến ngày nay. Các hệ điều hành khác như Linux, Mac OS, Android, iOS cũng hỗ trợ giao thức này → không cần cài thêm phần mềm để thiết lập PPTP
- Là giao thức được phát triển lâu nên lỗi thời → bảo mật không cao, dễ dàng bị giải mã bởi bên thứ 3
- Sử dụng TCP port 1723 và giao thức mã hóa GRE (Generic Routing Encapsulation) nên dễ dàng bị tường lửa (firewall) chặn lại

## 6.2 L2TP

- Được phát triển từ kết hợp các tính năng giao thức L2F (Layer 2 Forwarding) của Cisco và PPTP của Microsoft
- Cũng là giao thức được sử dụng rộng rãi ngày nay. Tất cả thiết bị và hệ điều hành đều được cài đặt sẵn giao thức này → dễ dàng thiết lập và cấu hình
- Không mã hóa dữ liệu mà phải nhờ giao thức khác mã hóa là IPsec → còn gọi là L2TP/IPsec
- Sử dụng UDP port 500, 1701, 4500 nên dễ dàng bị firewall chặn lại
- Chậm hơn so với các giao thức khác do đóng gói (encapsulation) dữ liệu 2 lần
- Tốt hơn PPTP



## 6.3 SSTP





- Được phát triển bởi Microsoft và là giao thức chỉ hỗ trợ hệ điều hành Windows
- Sử dụng SSL 3.0 nên bảo mật rất cao
- Dùng TCP port 443 nên khả năng vượt hầu hết firewalls
- Nếu máy dùng hệ điều hành Windows thì giữa các giao thức PPTP, L2TP thì SSTP được sử dụng do tính ổn định, dễ dùng và bảo mật tốt hơn

## 6.4 IKEv2

- Giao thức khá mới (2005) , được phát triển bởi Microsoft và Cisco
- Hỗ trợ ít hệ điều hành như Windows 7 trở đi, iOS, đặc biệt là thiết bị BlackBerry
- Cũng giống như L2TP, IKEv2 cũng sử dụng giao thức mã hóa IPSec
- Sử dụng UDP port 500 nên dễ dàng bị firewall chặn lại
- Hỗ trợ rất tốt cho người dùng lưu động: tạo lại kết nối một cách tự động khi kết nối bị ngắt tạm thời hoặc chuyển mạng
- Nhanh hơn PPTP, L2TP, SSTP

## 6.5 OpenVPN

- Là VPN mã nguồn mở (open source), xuất hiện 2001 cho đến nay có nhiều cải tiến → xem được code bên trong
- Chạy trên tất cả thiết bị, hệ điều hành nhưng để sử dụng phải cài thêm ứng dụng bên thứ 3 → cấu hình dễ
- Sử dụng thuật toán mã hóa AES (Advanced Encryption Standard) mới và không có điểm yếu nên được chính phủ và cơ quan Mỹ sử dụng để bảo vệ dữ liệu mật
- Dùng TCP port 443 nên khả năng vượt hầu hết firewalls
- Tốc độ nhanh, bảo mật và độ tin cậy cao

	PPTP	L2TP	SSTP	IKEv2	OPENVPN
PLATFORM					All platforms (3 <sup>rd</sup> party apps)
SECURITY	Basic encryption	IPsec encryption	SSL 3.0 encryption	IPsec encryption	AES encryption
FIREWALL	TCP port 1723, easy to block	UDP port 500, 1701, 4500, easy to block	TCP port 443, hard to block	UDP port 500, easy to block	TCP port 443, hard to block
RESULT	Old and outdated. Don't use	Better than PPTP	Good but mostly Windows	Automatic VPN connection	Faster, Secure, Cross- platform

# 7. Các giao thức xác thực trong VPN

- Trong Windows Server 2012 hỗ trợ các loại giao thức xác thực:
  - ✓ Password Authentication Protocol (PAP)
  - ✓ Challenge Handshake Authentication Protocol (CHAP)
  - ✓ Microsoft CHAP version 2 (MS-CHAP v2)
  - ✓ Extensible Authentication Protocol (EAP)

# 7. Các giao thức xác thực trong VPN

- **PAP**

- ✓ Password gửi đi dưới dạng plaintext, không mã hóa
- ✓ Xác thực kém nhất và không dùng hiện nay

- **CHAP**

- ✓ Cải tiến hơn PAP khi password dạng plaintext không được gửi
- ✓ Sử dụng phương thức challenge-response với MD5 hashing
- ✓ Được dùng trong các thiết bị mạng cũ nhưng vẫn còn phổ biến ngày nay

# 7. Các giao thức xác thực trong VPN

- **MS-CHAPv2**

- ✓ Cung cấp cơ chế xác thực lẫn nhau (mutual authentication)
- ✓ Bảo mật hơn CHAP
- ✓ Là giao thức duy nhất mà Windows Server 2012 cho phép thay đổi password hết hạn trong quá trình kết nối

- **EAP**

- ✓ Cơ chế bảo mật mạnh nhất: quét võng mạc, nhận diện giọng nói, xác định dấu vân tay, smart cards và chứng chỉ số

## 8. VPN Reconnect

- Là tính năng kết nối VPN mới được phát triển từ Windows 7 và Windows Server 2008.
- Thông thường, khi thực hiện kết nối VPN, nếu vì lý do nào đó mà kết nối internet bị gián đoạn thì kết nối VPN sẽ chấm dứt và người dùng buộc phải kích hoạt lại
- VPN reconnect : tự động tái kết nối ngay lập tức mà không cần bất kỳ sự can thiệp nào từ người dùng
- Muốn sử dụng VPN reconnect ta phải sử dụng giao thức đường ống IKEv2 và quyền xác thực là EAP



# 9. Câu hỏi ôn tập

Chọn tất cả đáp án đúng

**Câu hỏi 1.** Các dịch vụ nào dưới đây mà ta có thể cấu hình trong Routing and Remote Access (RRAS)?

- a. Routing                      b. OSPF                      c. RIP                      d. NAT

**Đáp án:**

- a. Routing, d. NAT



# 9. Câu hỏi ôn tập

Chọn 1 đáp án đúng nhất

**Câu hỏi 2.** Cách đơn giản nhất để thiết lập VPN client cho 1 user mà không cần đào tạo kỹ thuật?

- a. Sử dụng PAP
- b. Hướng dẫn và chụp màn hình step-by-step cho user
- c. Sử dụng Group Policy để cấu hình
- d. Sử dụng CMAK để tạo file thực thi để user chỉ cài đặt

**Đáp án:**

- d. Sử dụng CMAK để tạo file thực thi để user chỉ cài đặt

Sử dụng RAS CMAK là tính năng mới trên Windows Server 2012. Một file thực thi được tạo gồm tất cả cấu hình VPN sẽ được deploy cho user. User chỉ cần chạy file thực thi là kết nối VPN.

# 9. Câu hỏi ôn tập

Chọn 1 đáp án đúng nhất

**Câu hỏi 3.** Khi thiết lập kết nối VPN, tính chất nào xác định dữ liệu không bị chỉnh sửa trong quá trình truyền?

- a. Encapsulation      b. Authentication
- c. Data encryption    d. Data integrity

**Đáp án:**

d. Data integrity (toàn vẹn dữ liệu).  
Xem phần 2. các tính chất VPN.

# 9. Câu hỏi ôn tập

**Câu hỏi 4.** Chọn đúng giao thức VPN (PPTP, L2TP, SSTP, IKEv2) cho các phát biểu sau

- ..... a. Sử dụng MPPE để mã hóa (MPPE – Microsoft Point-to-Point Encryption)
- ..... b. Sử dụng UDP port 500, 1701, 4500
- ..... c. Hỗ trợ VPN reconnect
- ..... d. Chỉ sử dụng UDP port 500
- ..... e. Sử dụng port 1723
- ..... f. Sử dụng certificate hoặc preshared key và kết hợp IPsec để mã hóa
- ..... g. Sử dụng port 443

**Đáp án:**

a. PPTP, b. L2TP, c. IKEv2, d. IKEv2, e. PPTP, f. L2TP, g. SSTP

# 9. Câu hỏi ôn tập

**Câu hỏi 5.** Chọn đúng giao thức mã hóa (PAP, CHAP, MS-CHAPv2, EAP) cho các phát biểu sau

- ..... a. Sử dụng cho thiết bị mạng cũ và sử dụng phương thức challenge-response với md5 hashing
- ..... b. Cho phép thay đổi password đã hết hạn trong quá trình kết nối
- ..... c. Sử dụng smart card
- ..... d. Username và password được truyền dạng plaintext

**Đáp án:**

a. CHAP, b. MS-CHAPv2, c. EAP, d. PAP

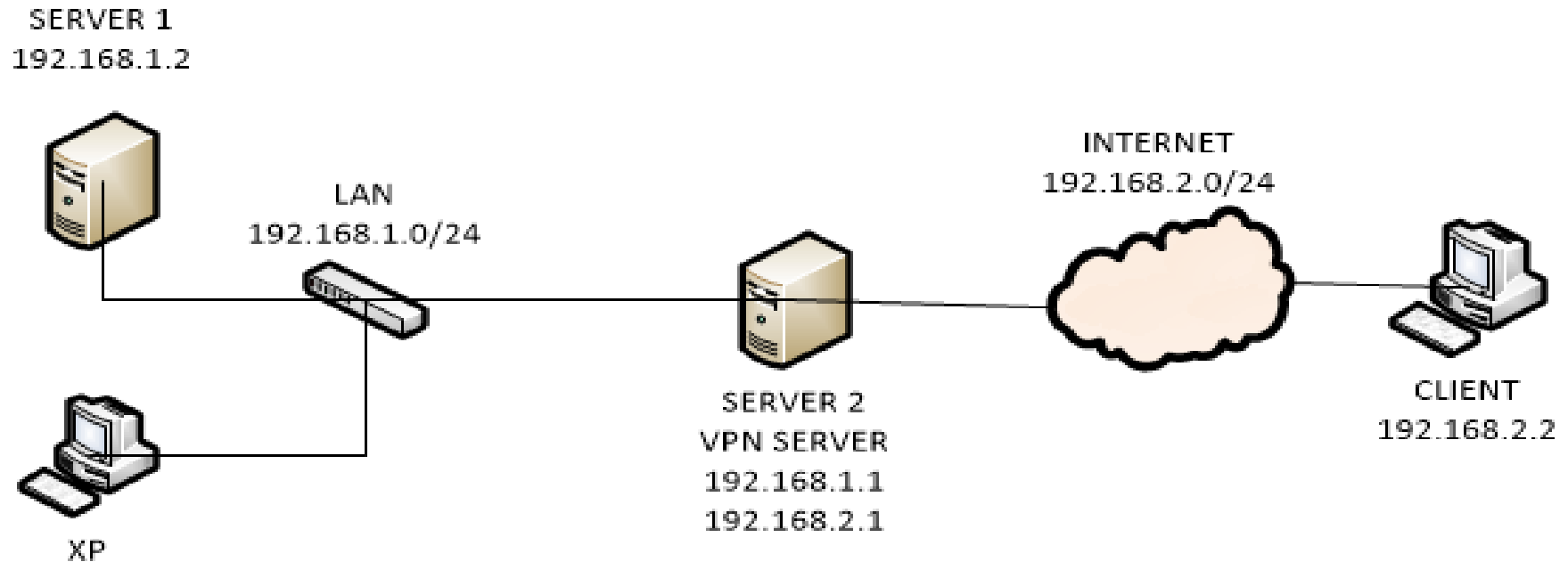
# 9. Câu hỏi ôn tập

**Câu hỏi 6.** Đánh số thứ tự các bước sau để cấu hình VPN Server. Không phải các bước dưới đây đều dùng.

- ...<sup>2</sup>... Chạy Configure and Enable Routing Remote Access Wizard
- ...<sup>3</sup>... Cấu hình thuộc tính trên VPN Server trong RRAS
- ...<sup>4</sup>.. Tạo kết nối trên client
- ..... Kích hoạt dịch vụ VPN
- ...<sup>1</sup>... Cài RRAS
- ..... Cài VPN console
- ..... Cài VPN service

**Đáp án**

# Thực hành 1: Remote Access VPN



## Chuẩn bị:

Máy SERVER2 làm VPN SERVER. Máy SERVER1 đại diện cho đường mạng nội bộ của công ty. Máy CLIENT là máy tính ngoài đường mạng truy xuất vào mạng nội bộ của công ty.

## Yêu cầu:

Cấu hình Remote Access VPN trên máy SERVER2 cho phép máy CLIENT ngoài mạng LAN có thể truy cập vào đường mạng LAN 192.168.1.0/24

# Hướng dẫn thực hành 1

## Hướng dẫn:

- Đặt IP tĩnh cho các máy tính
- Trên máy SERVER2, tạo tài khoản user vpn và cấu hình cho phép truy cập từ xa
- Trên máy SERVER2, cài đặt và cấu hình VPN remote access với dải IP 192.168.10.10 – 192.168.10.100 cho các máy client truy cập từ xa
- Trên máy CLIENT, tạo kết nối vpn và truy cập vào mạng LAN 192.168.1.0/24 để lấy dữ liệu đã được chia sẻ từ máy SERVER1



# Hướng dẫn thực hành 1

	CLIENT	SERVER1
VMNET	Vmnet3	Vmnet2
IP	192.168.2.2	192.168.1.2
SM	255.255.255.0	255.255.255.0
DG	192.168.2.1	192.168.1.1

	SERVER2	
VMNET	Vmnet3	Vmnet2
IP	192.168.2.1	192.168.1.1
SM	255.255.255.0	255.255.255.0
DG		

Bảng địa chỉ IP các máy

# Hướng dẫn thực hành 1

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

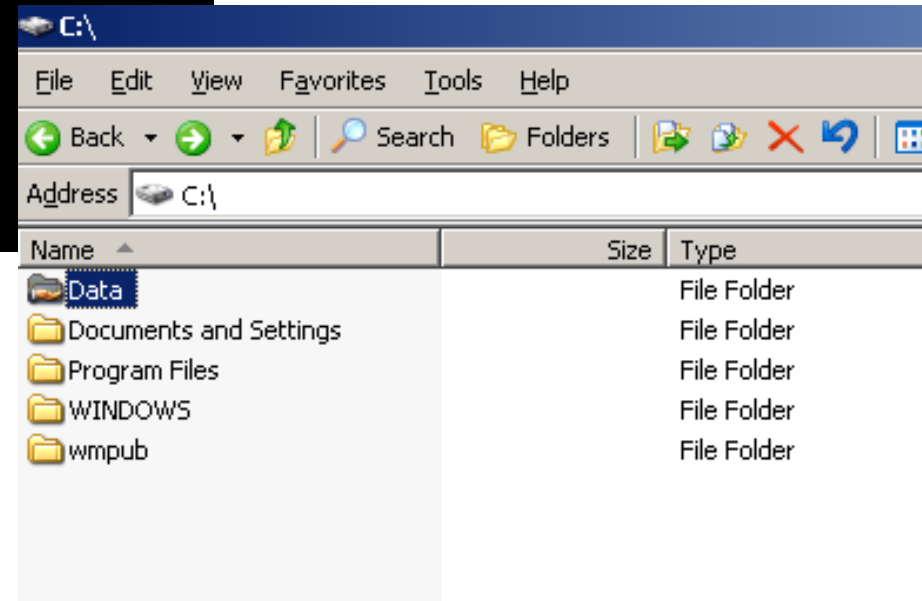
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter vmnet2-LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.2
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\Documents and Settings\Administrator>
```



Trên SERVER1, đặt IP và chia sẻ thư mục Data cho Everyone có quyền Read

# Hướng dẫn thực hành 1

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter vmnet2-LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter vmnet3-WAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>_
```

Trên SERVER2, đặt IP cho 2 card mạng VMnet 2 và VMnet3

# Hướng dẫn thực hành 1

```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\s\>ipconfig

Windows IP Configuration

Ethernet adapter vnet3-WAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.2.2
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.2.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . .             : Media disconnected

C:\Documents and Settings\s\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

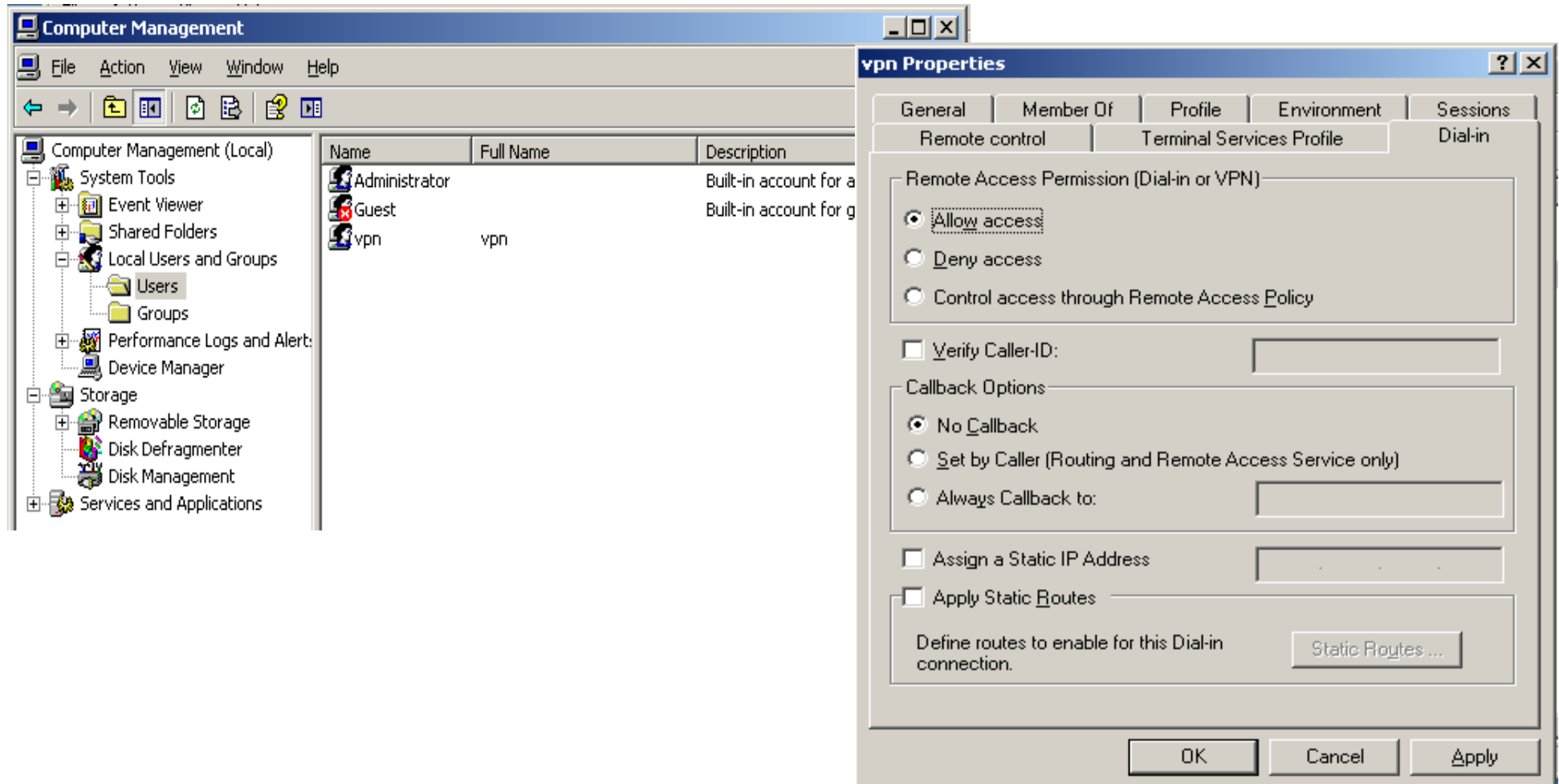
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\s\>_
```

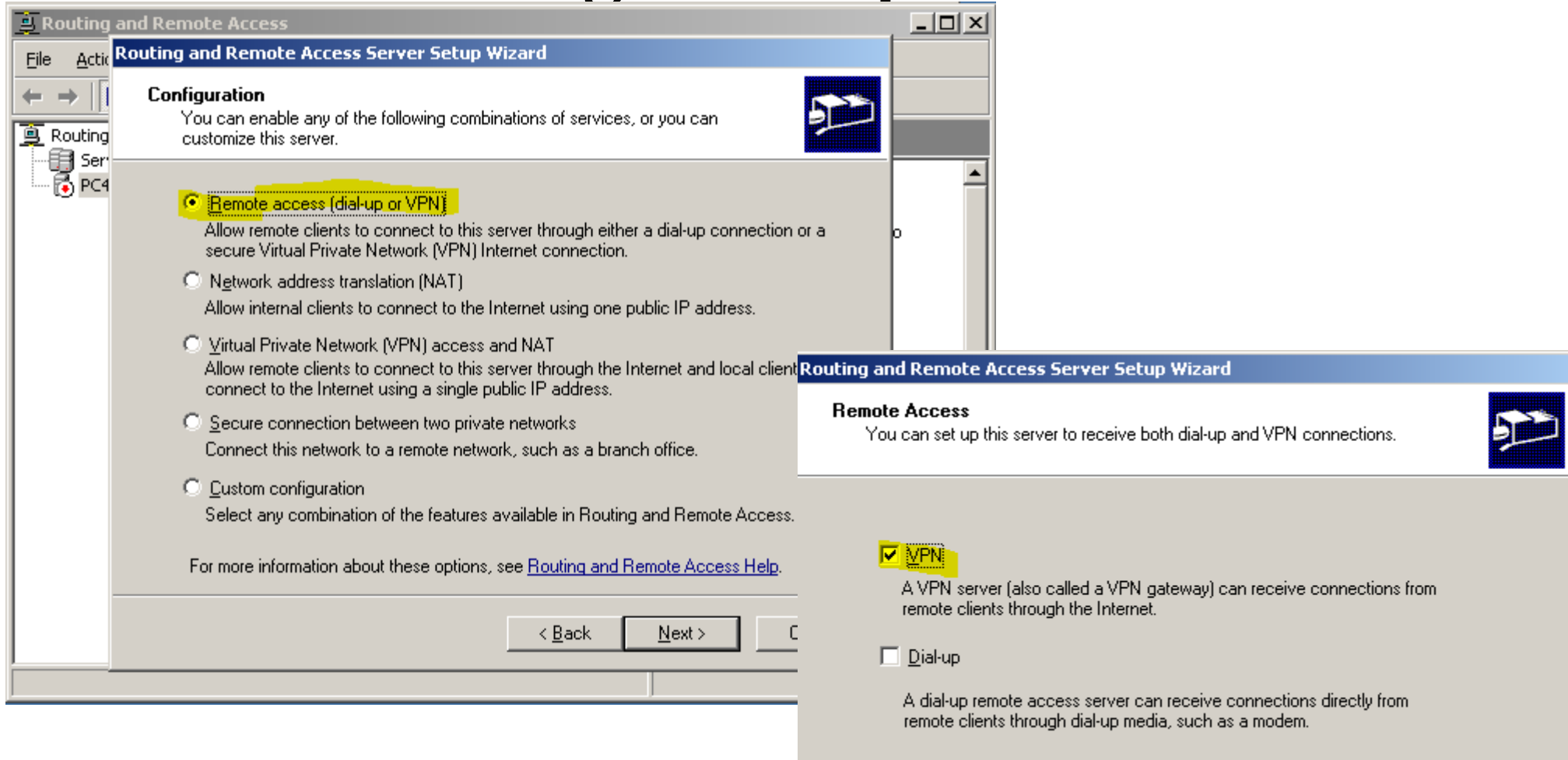
Trên CLIENT, đặt IP và ping tới máy SERVER1 → time out

# Hướng dẫn thực hành 1



Trên SERVER2, tạo user vpn với password là 123. Click phải vào user vpn, chọn Properties, vào tab Dial-in, check vào Allow access để cho user vpn truy cập từ xa

# Hướng dẫn thực hành 1



Trên SERVER2, cài đặt dịch vụ Routing and Remote Access, chọn RemoteAccess (dialup or VPN). Sau đó chọn VPN

# Hướng dẫn thực hành 1

**Routing and Remote Access Server Setup Wizard**

**VPN Connection**

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
vmnet2-LAN	Intel(R) PRO/1000 MT ...	192.168.1.1
vmnet3-WAN	Intel(R) PRO/1000 MT ...	192.168.2.1

☒ **Enable security on the selected interface by setting up static packet filters.**  
Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

For more information about network interfaces, see [Routing and Remote Access Help](#).

< Back   Next >   Cancel

**Routing and Remote Access Server Setup Wizard**

**IP Address Assignment**

You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

☐ Automatically  
If you use a DHCP server to assign addresses, confirm that it is configured properly.  
If you do not use a DHCP server, this server will generate the addresses.

☒ **From a specified range of addresses**

Trên SERVER2, chọn card mạng vmnet3WAN. Sau đó chọn From a specified range of addresses để gán khoảng địa chỉ cho các client truy cập từ xa

# Hướng dẫn thực hành 1

**Routing and Remote Access Server Setup Wizard**

**Address Range Assignment**

You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number
------	----	--------

**New...** **Edit...** **Delete**

**Routing and Remote Access Server Setup Wizard**

**Address Range Assignment**

You can specify the address ranges that this server will use to assign addresses to remote clients.

**New Address Range**

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192.168.10.10

End IP address: 192.168.10.100

Number of addresses: 91

**OK** **Cancel**

**< Back** **Next >** **Cancel**

Trên SERVER2, chọn New để nhập khoảng IP bắt đầu và kết thúc như hình




# Hướng dẫn thực hành 1

**Routing and Remote Access Server Setup Wizard**

**Managing Multiple Remote Access Servers**

Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.



Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

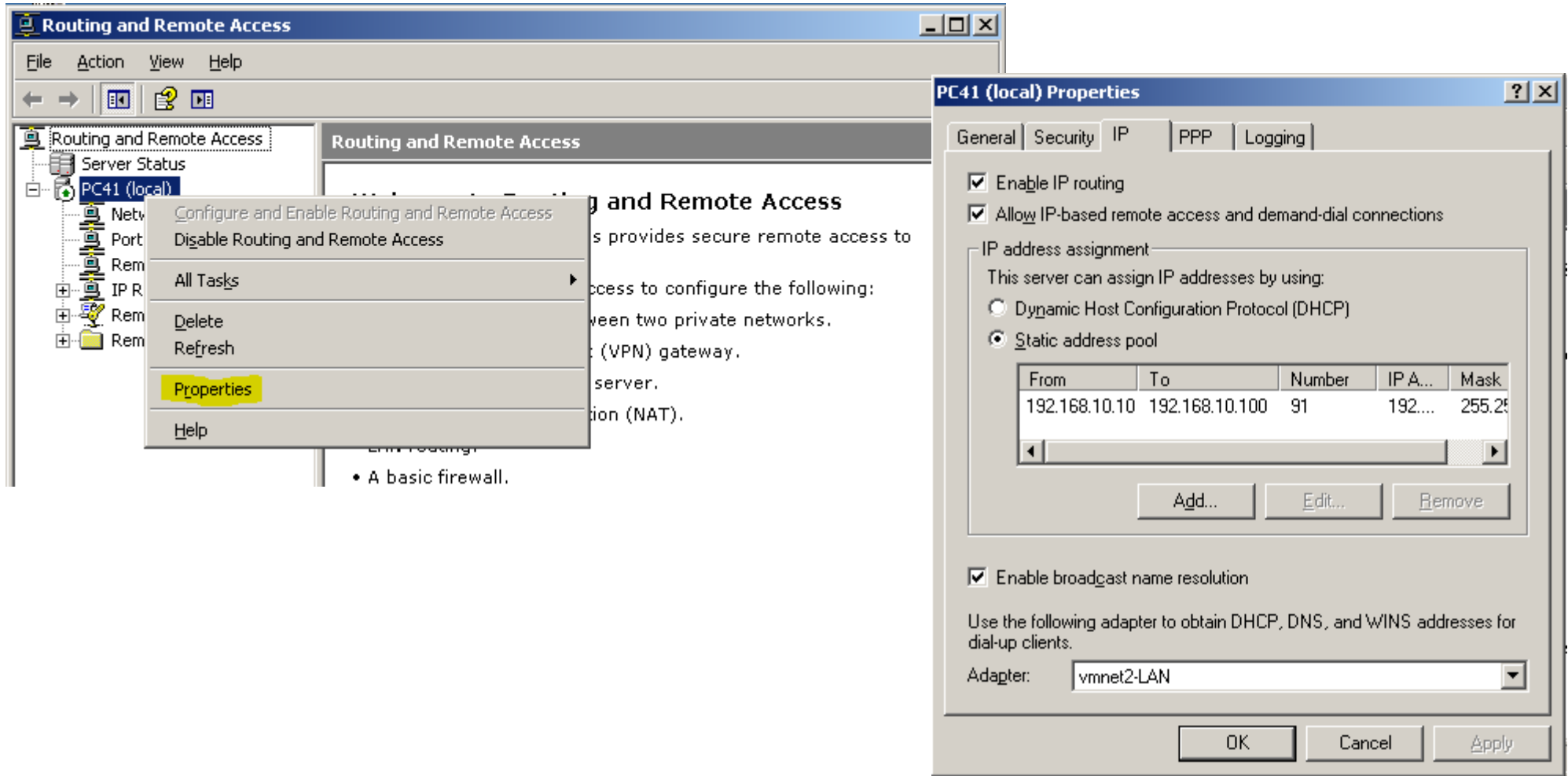
Do you want to set up this server to work with a RADIUS server?

☒ **No, use Routing and Remote Access to authenticate connection requests**

☐ Yes, set up this server to work with a RADIUS server

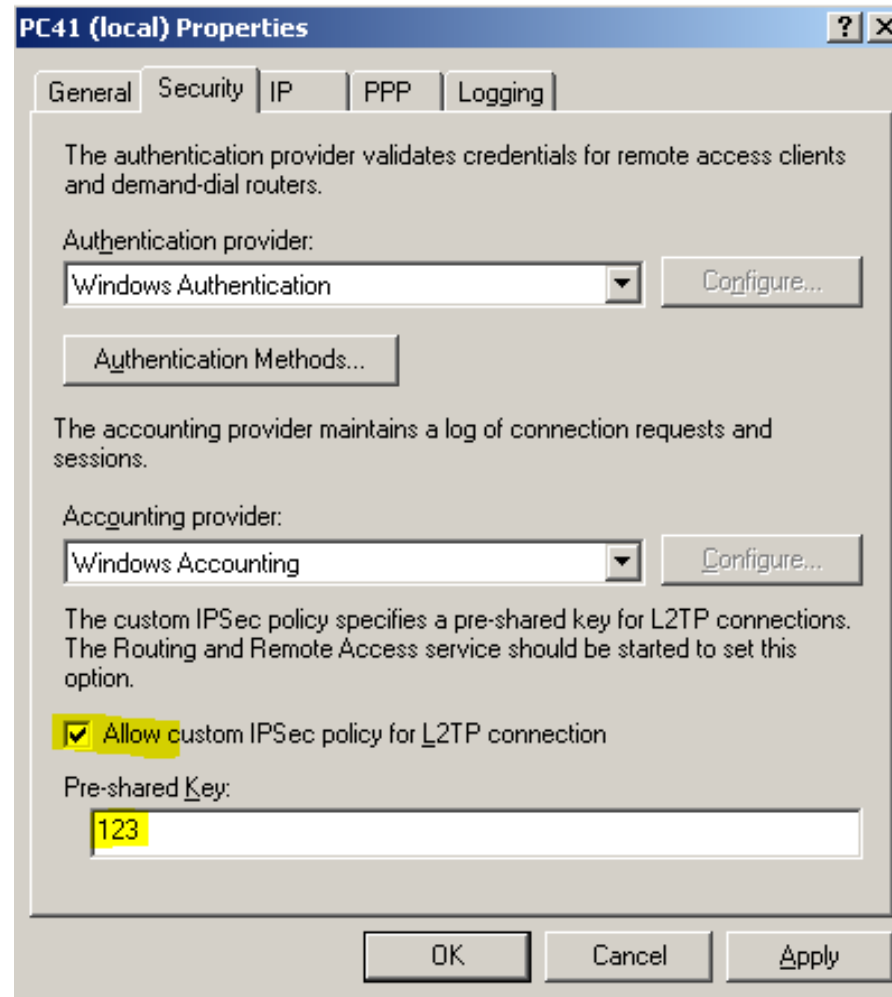
Trên SERVER2, chọn No, use ... do không cần máy RADIUS Server để xác thực truy cập từ xa. Sau đó Finish để kết thúc quá trình cấu hình VPN Server

# Hướng dẫn thực hành 1



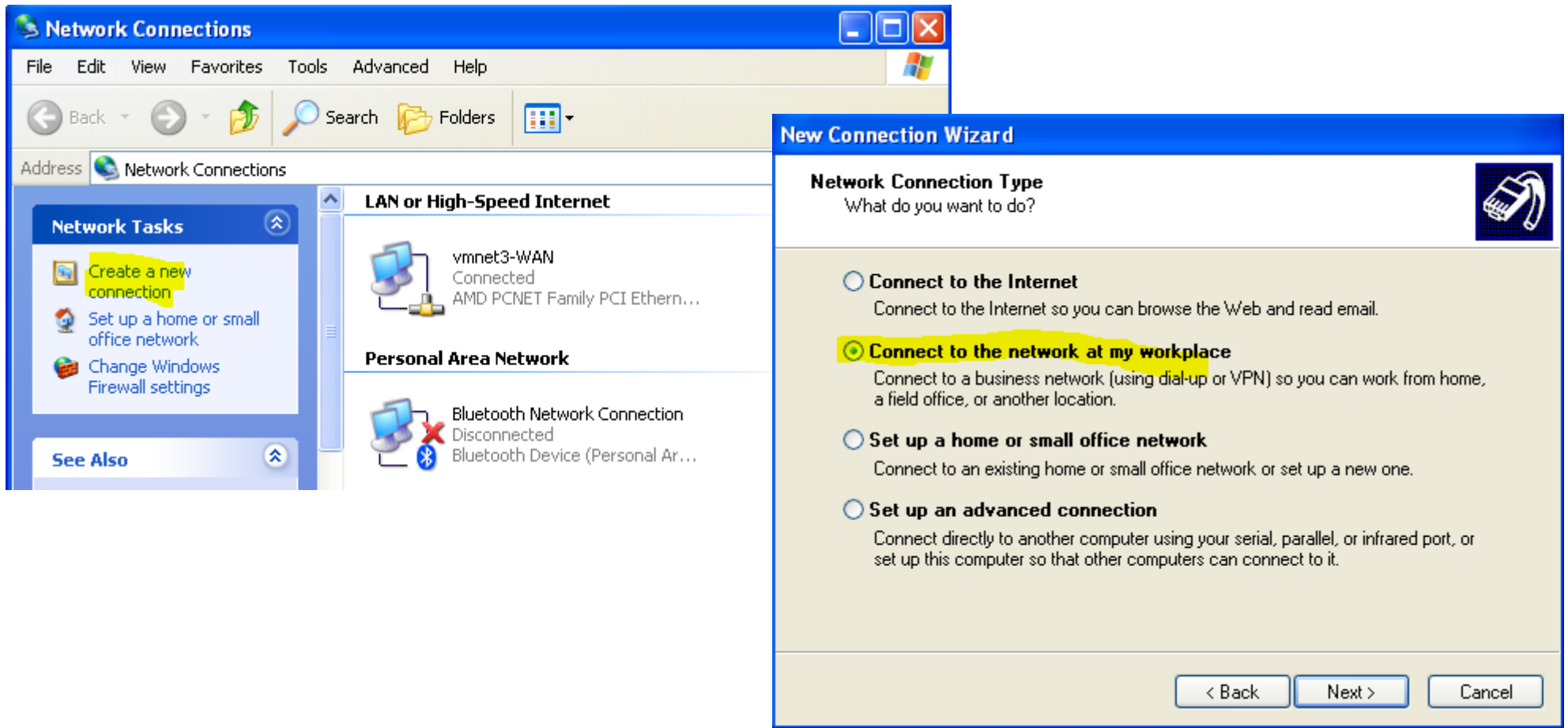
Trên SERVER2, để xem các thông tin đã cấu hình, click phải vào tên máy chọn Properties. Vào tab IP sẽ thấy khoảng IP đã gán

# Hướng dẫn thực hành 1



Trên SERVER2, mặc định là sử dụng giao thức PPTP. Nếu muốn dùng giao thức L2TP/IPSec thì check vào Allow custom ... trong tab Security, nhập Pre-shared Key: 123

# Hướng dẫn thực hành 1



Trên CLIENT, click chọn Create a new connection trong cửa sổ Network Connection. Sau đó chọn Connect to the network at my workplace

# Hướng dẫn thực hành 1

The image displays three overlapping screenshots of the Windows XP 'New Connection Wizard' interface, illustrating the steps to create a Virtual Private Network (VPN) connection.

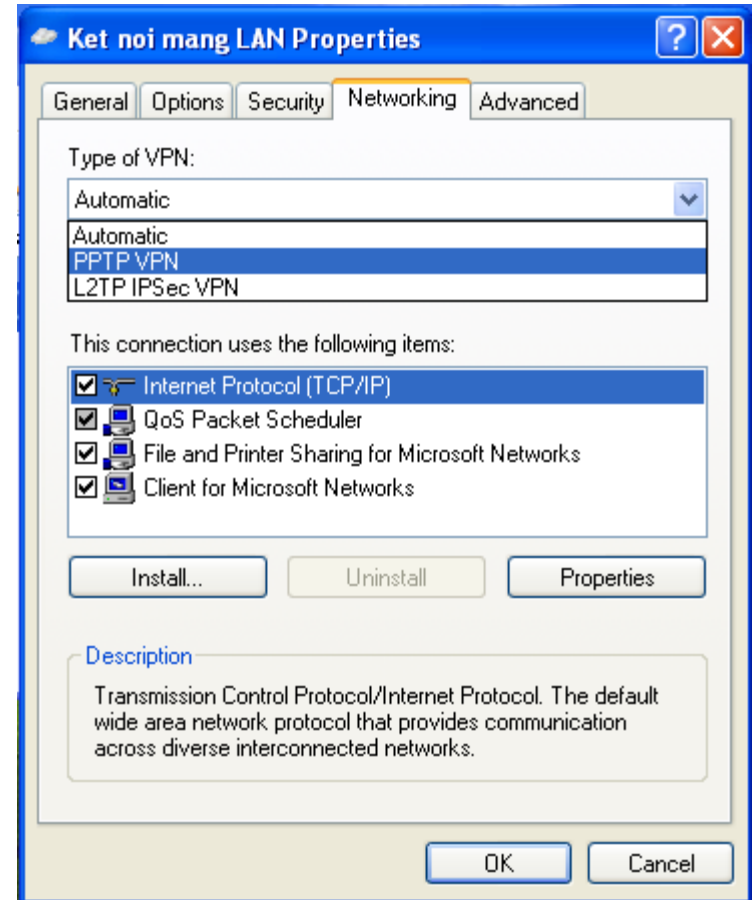
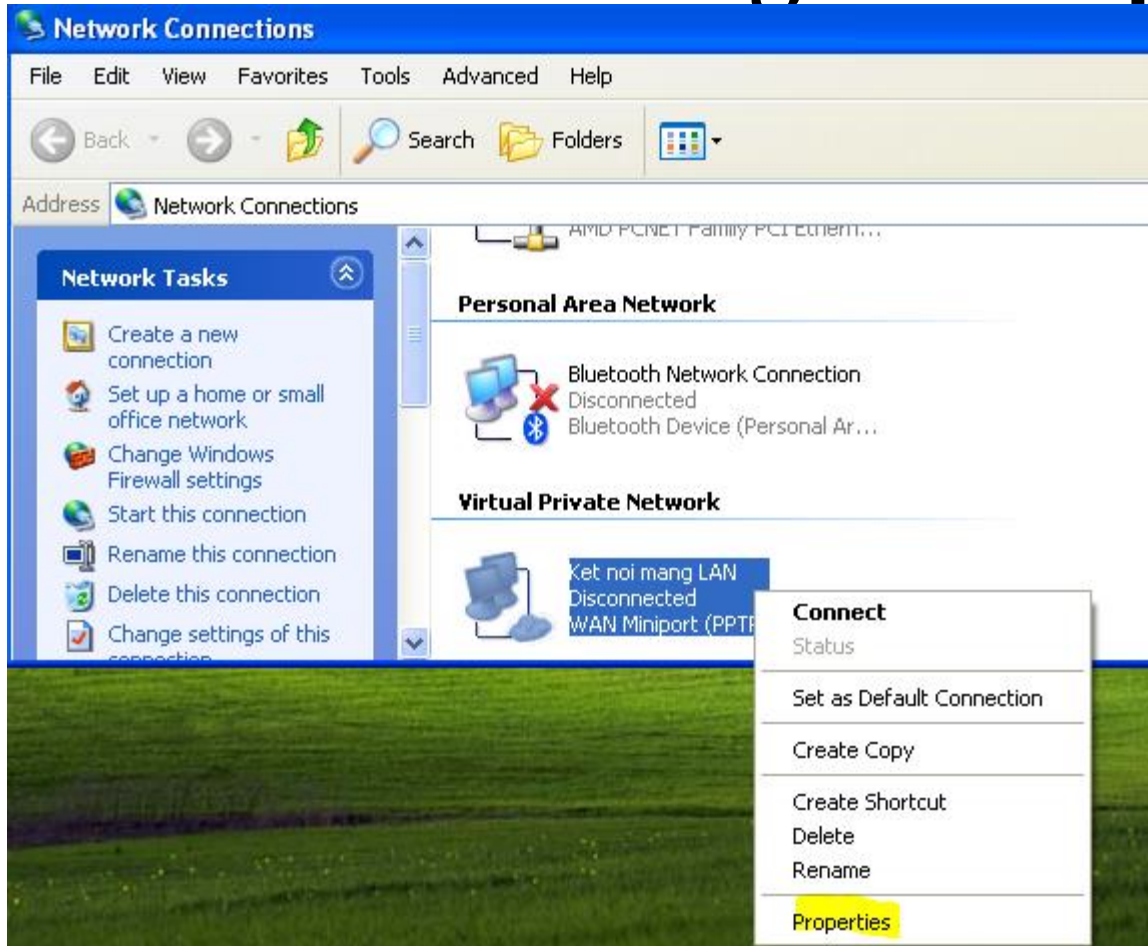
**Top Left Screenshot: Network Connection**  
The title bar reads 'New Connection Wizard'. The main heading is 'Network Connection' with the question 'How do you want to connect to the network at your workplace?'. Under 'Create the following connection:', two options are listed: 'Dial-up connection' (unselected) and 'Virtual Private Network connection' (selected and highlighted in yellow). The description for the selected option states: 'Connect to the network using a virtual private network (VPN) connection over the Internet.'

**Top Right Screenshot: Connection Name**  
The title bar reads 'New Connection Wizard'. The main heading is 'Connection Name' with the instruction 'Specify a name for this connection to your workplace.' Below this, a text box is labeled 'Type a name for this connection in the following box.' and 'Company Name'. The text box contains the text 'Kết nối mạng LAN' (highlighted in yellow). A small icon of a network card is visible in the top right corner.

**Bottom Screenshot: VPN Server Selection**  
The title bar reads 'New Connection Wizard'. The main heading is 'VPN Server Selection' with the question 'What is the name or address of the VPN server?'. Below this, a text box is labeled 'Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.' and 'Host name or IP address (for example, microsoft.com or 157.54.0.1 )'. The text box contains the IP address '192.168.2.1' (highlighted in yellow). A small icon of a network card is visible in the top right corner.

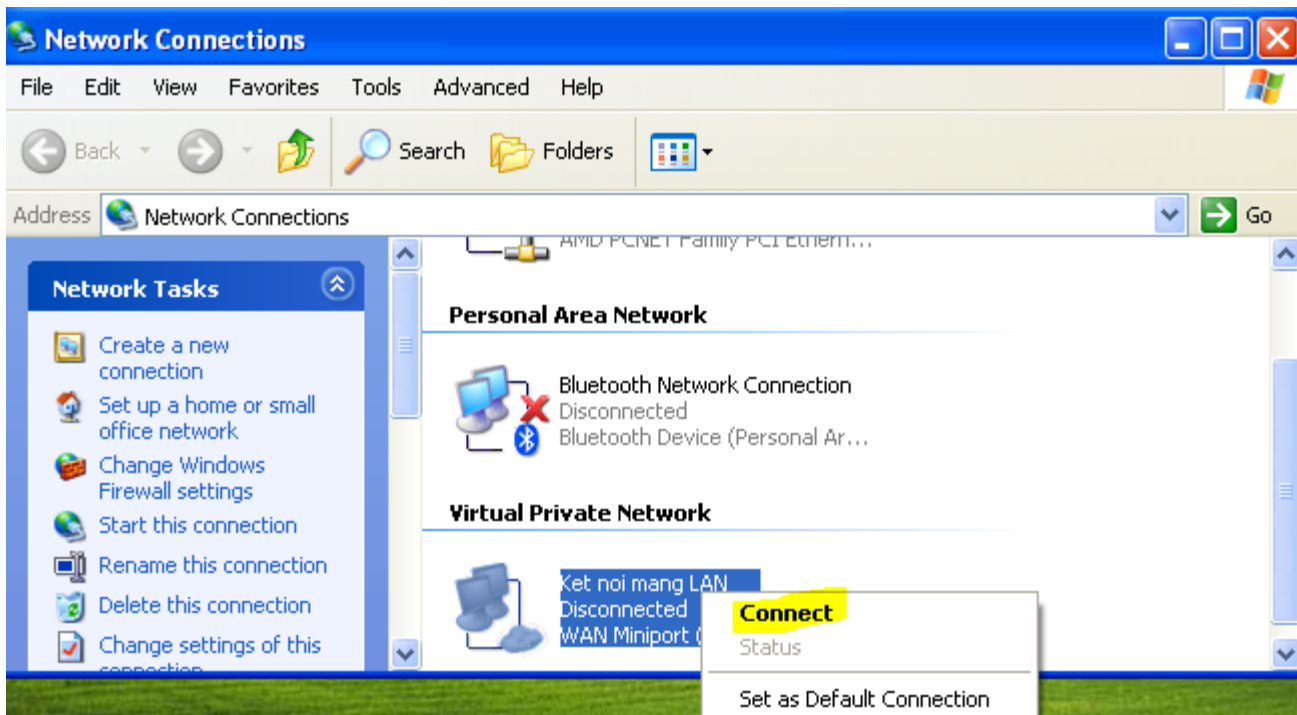
Trên CLIENT, chọn Virtual ... Sau đó nhập tên kết nối như hình. Nhập địa chỉ IP máy SERVER2 là 192.168.2.1. Cuối cùng Finish để hoàn tất tạo VPN Client

# Hướng dẫn thực hành 1



Trên CLIENT, click phải vào card mạng vừa tạo, chọn Properties. Trong tab Networking chọn PPTP VPN. Nếu VPN Server dùng giao thức L2TP/IPSec thì ở đây chọn L2TP IPSec VPN và nhập preshared key trong tab Security

# Hướng dẫn thực hành 1



Trên CLIENT, click phải vào card mạng vừa tạo, chọn Connect. Sau đó nhập username là vpn và password 123. Click chọn Connect

# Hướng dẫn thực hành 1

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\sv>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127
Reply from 192.168.1.2: bytes=32 time=4ms TTL=127
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Documents and Settings\sv>ipconfig

Windows IP Configuration

Ethernet adapter vmnet3-WAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

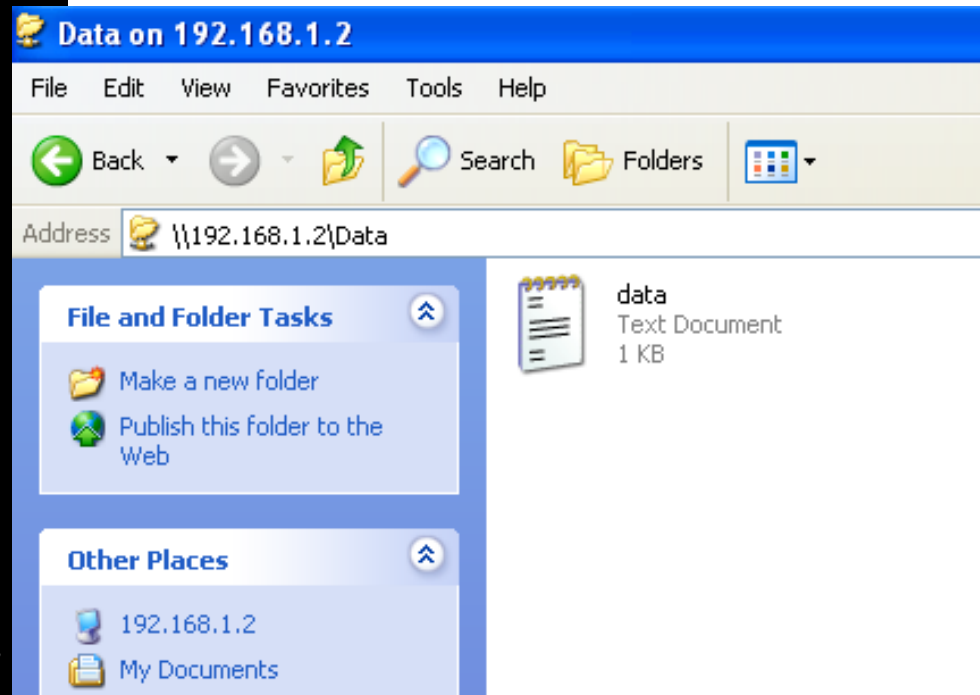
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

PPP adapter Ket noi mang LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.10.11
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 192.168.10.11

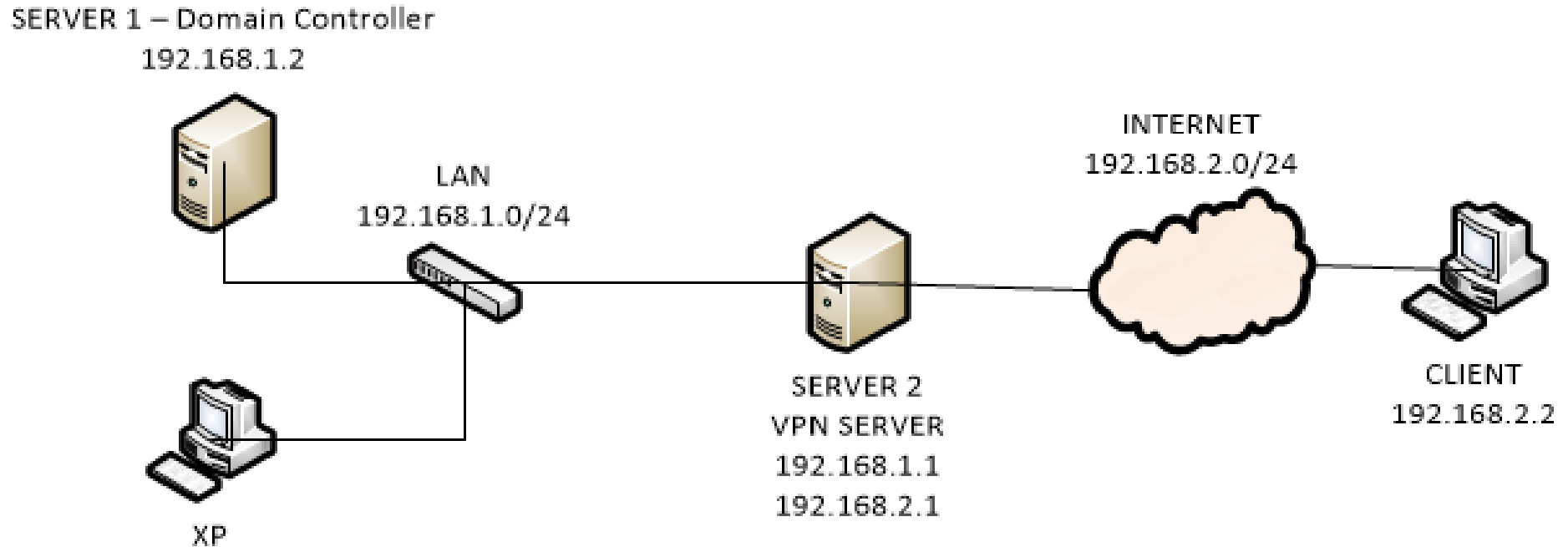
C:\Documents and Settings\sv>
```



Trên CLIENT, vào cmd ping lại đến máy SERVER1 → thành công. Truy cập đến thư mục Data đã được chia sẻ trên máy SERVER1 → thành công.



# Thực hành 1bis: Remote Access VPN



## Chuẩn bị:

Máy SERVER1 là DC quản lý miền caothang.edu.vn

Máy SERVER2 làm VPN SERVER gia nhập miền

Máy CLIENT là máy tính ngoài đường mạng truy xuất vào mạng nội bộ của trường.

## Yêu cầu:

Cấu hình Remote Access VPN trên máy SERVER2 cho phép máy CLIENT truy cập vào mạng nội bộ và truy cập thư mục dữ liệu đang chia sẻ trên máy SERVER1

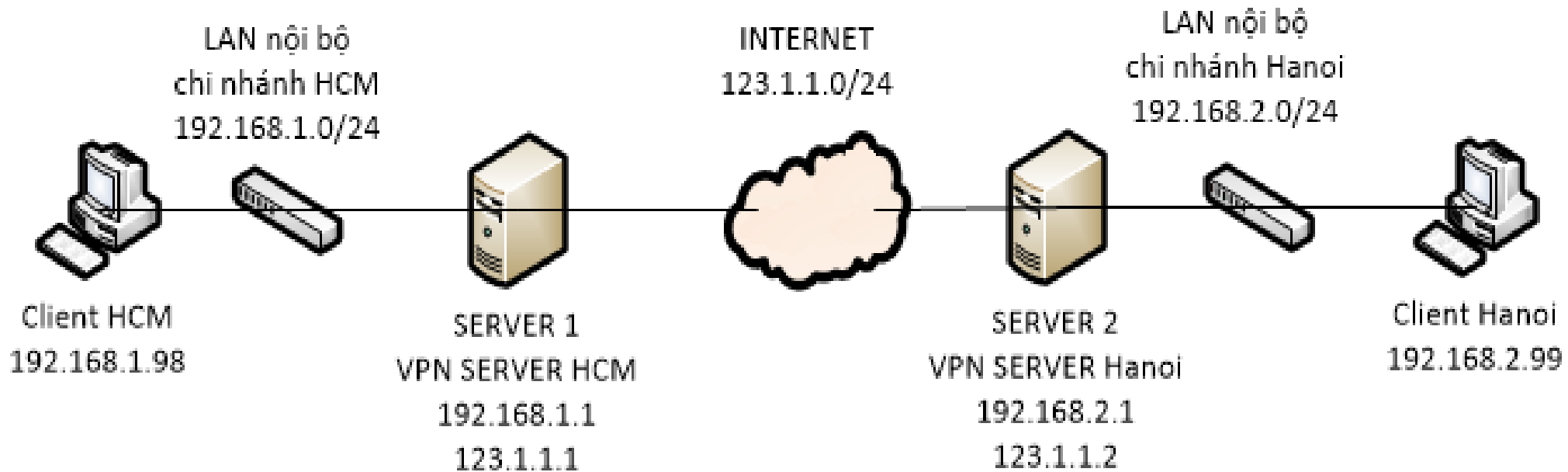
# Thực hành 1bis: Remote Access VPN

	CLIENT	SERVER1
VMNET	Vmnet3	Vmnet2
IP	192.168.2.2	192.168.1.2
SM	255.255.255.0	255.255.255.0
DG	192.168.2.1	192.168.1.1
P.DNS Server		192.168.1.2

	SERVER2	
VMNET	Vmnet3	Vmnet2
IP	192.168.2.1	192.168.1.1
SM	255.255.255.0	255.255.255.0
DG		
P.DNS Server		192.168.1.2

Bảng địa chỉ IP các máy

# Thực hành 2: Site to Site VPN



## Chuẩn bị:

1 máy VPN Server HCM, 1 máy client HCM  
1 máy VPN Server Hanoi, 1 máy client Hanoi

## Yêu cầu:

Cấu hình Site to Site VPN trên máy VPN Server HCM và VPN Server Hanoi cho phép máy client HCM kết nối máy client Hanoi

# Hướng dẫn thực hành 2

	Client HCM	VPN Server HCM	
VMNET	Vmnet2	Vmnet2	Vmnet3
IP	192.168.1.98	192.168.1.1	123.1.1.1
SM	255.255.255.0	255.255.255.0	255.255.255.0
DG	192.168.1.1		123.1.1.2

	Client Hanoi	VPN Server Hanoi	
VMNET	Vmnet4	Vmnet4	Vmnet3
IP	192.168.2.99	192.168.2.1	123.1.1.2
SM	255.255.255.0	255.255.255.0	255.255.255.0
DG	192.168.2.1		123.1.1.1

Bảng địa chỉ IP các máy

# Hướng dẫn thực hành 2

## Hướng dẫn:

- Đặt IP tĩnh cho các máy tính
- Trên VPN Server HCM, tạo User vpnhcm và cho phép truy cập qua VPN. Trên VPN Server Hanoi, tạo User vnphanoi và cho phép truy cập qua VPN
- Cài đặt và cấu hình Routing and Remote Access trên máy VPN Server HCM và VPN Server Hanoi
- Trên VPN Server HCM, tạo dãy IP 192.168.10.100 – 192.168.10.200 cho các máy bên ngoài kết nối vào LAN1. Trên VPN Server Hanoi, tạo dãy IP 192.168.20.100 – 192.168.20.200 cho các máy bên ngoài kết nối vào LAN2
- Trên VPN Server HCM, tạo mới Demand-dial Interface (cấu hình tài khoản VPN, routing cho các máy truy cập thông qua VPN). Trên VPN Server Hanoi, tạo mới Demand-dial Interface
- Tạo VPN Client trên các máy Client HCM và Client Hanoi. Kiểm tra kết nối giữa 2 hệ thống mạng LAN1 và LAN2

# Hướng dẫn thực hành 2



```
Administrator: Command Prompt

C:\Users\Administrator>ipconfig

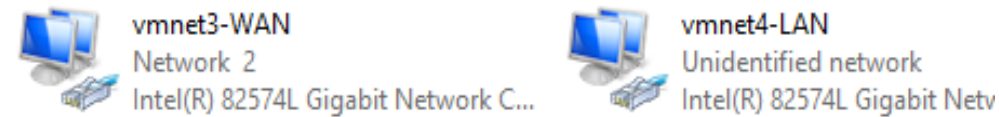
Windows IP Configuration

Ethernet adapter vmnet3-WAN:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 123.1.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 123.1.1.2

Ethernet adapter vmnet2-LAN:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```



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

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter vmnet4-LAN:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.2.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter vmnet3-WAN:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 123.1.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 123.1.1.1
```

Đặt IP tĩnh trên máy VPN Server HCM và VPN Server Hanoi

# Hướng dẫn thực hành 2

```
C:\ C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\sv>ipconfig

Windows IP Configuration

Ethernet adapter vmnet2-LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.98
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\sv>_
```

```
C:\ C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\sv>ipconfig

Windows IP Configuration

Ethernet adapter vmnet4-LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.99
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

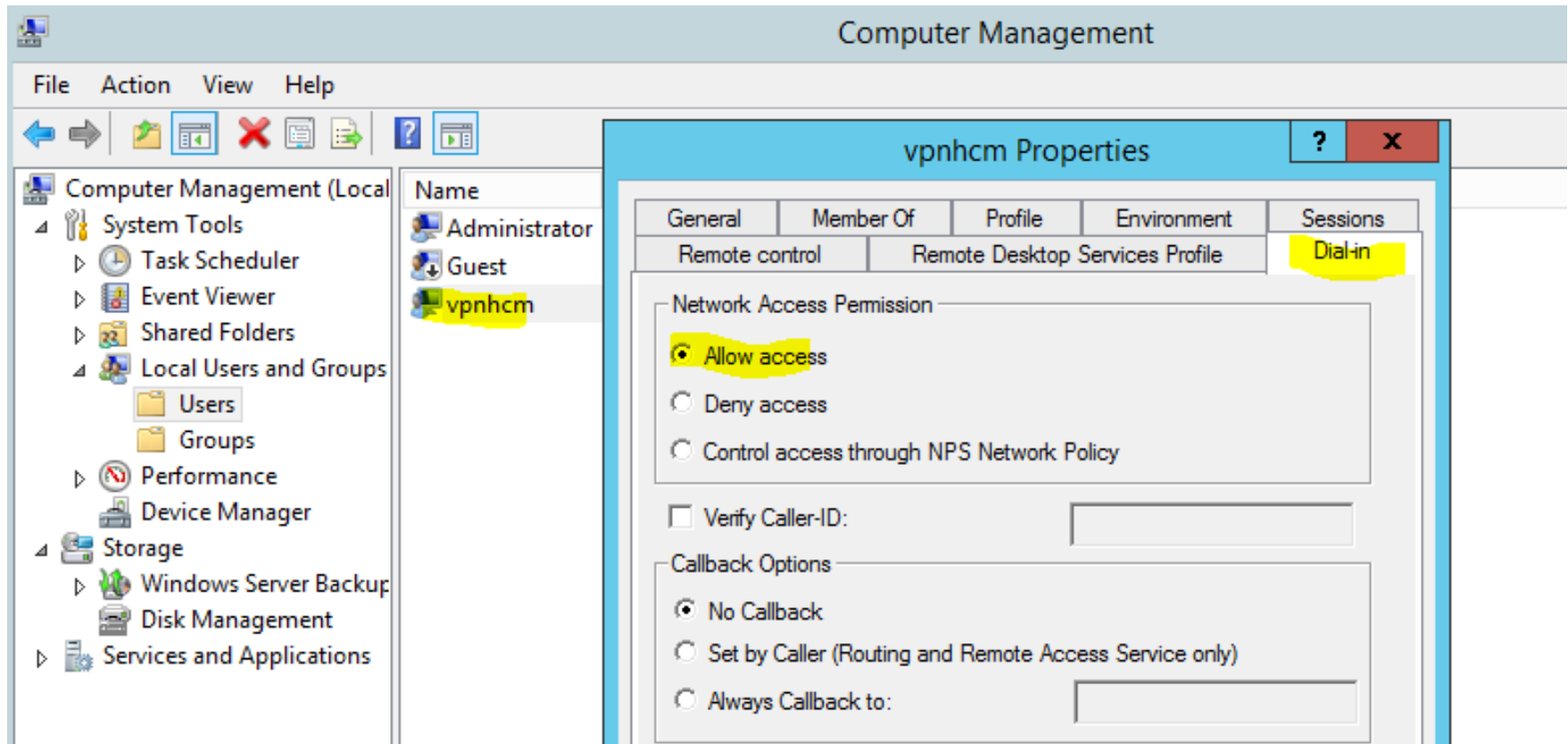
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\sv>
```

Đặt IP tĩnh trên máy Client HCM và Client Hanoi

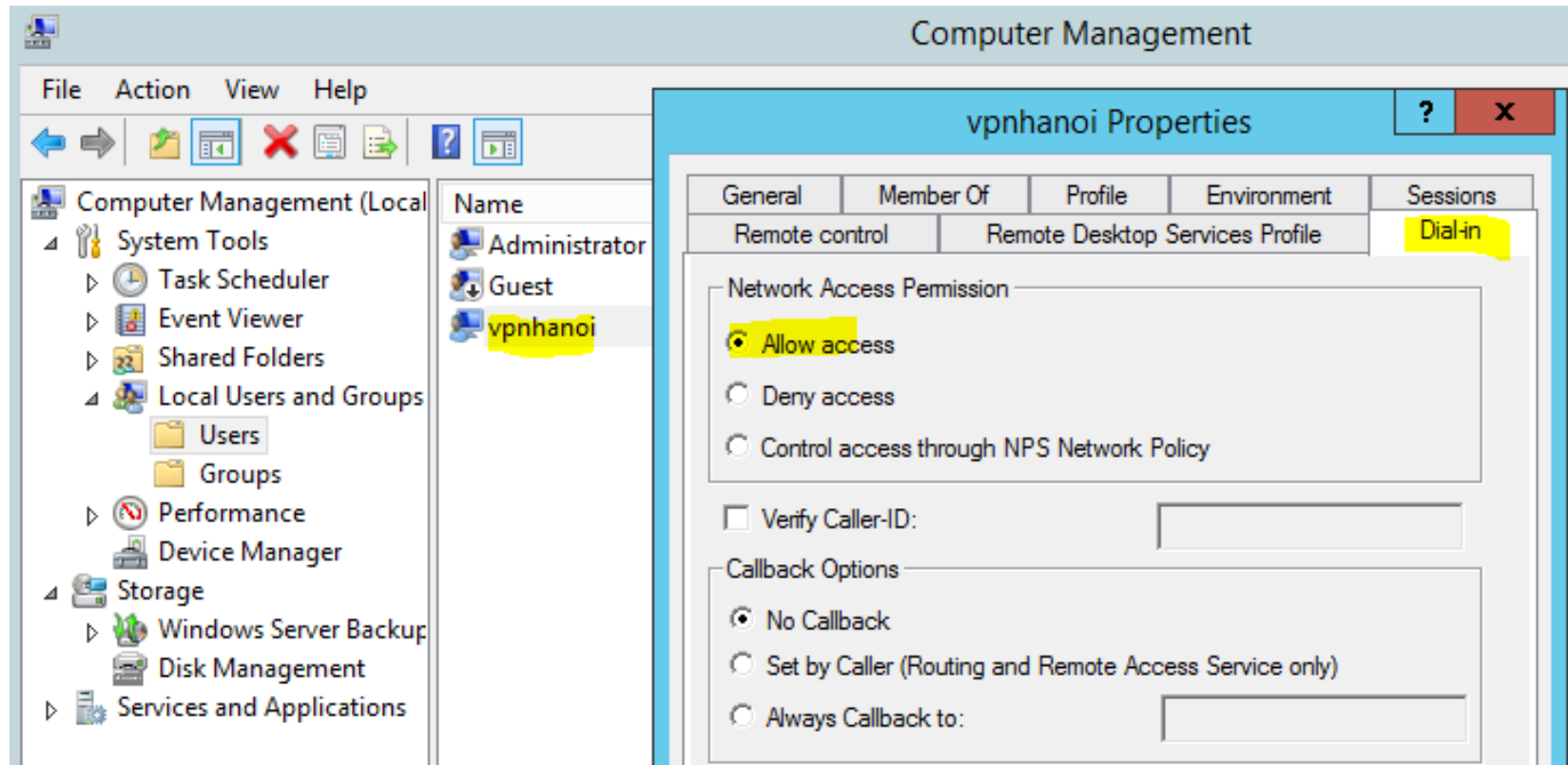
# Hướng dẫn thực hành 2



Trên VPN Server HCM, tạo User vpnhcm với password là 123456a@. Click phải lên User vpnhcm, chọn Properties, vào tab Dial-in, chọn Allow access. OK

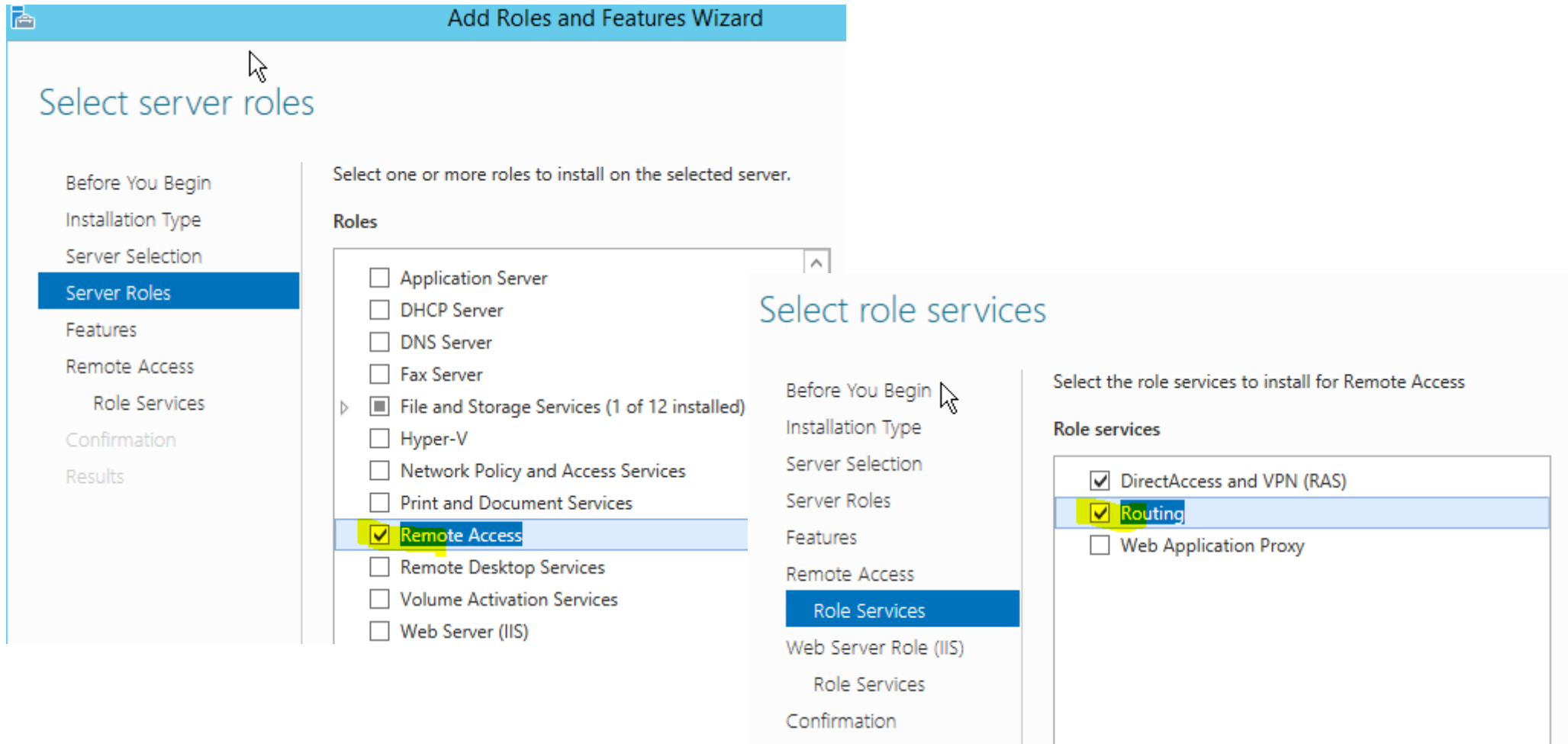


# Hướng dẫn thực hành 2



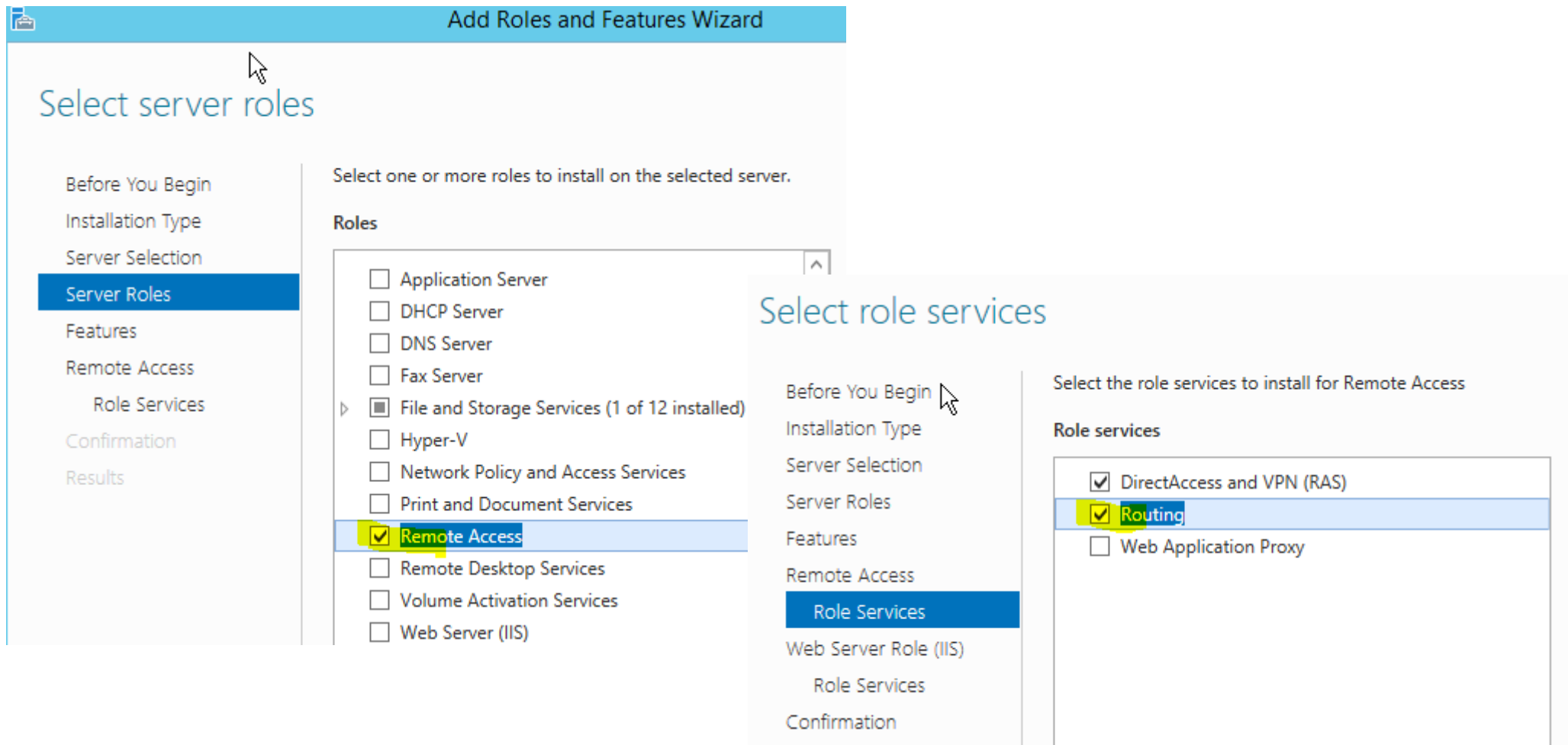
Trên VPN Server Hanoi, tạo User vpnhanoi với password là 123456a@. Click phải lên User vpnhanoi, chọn Properties, vào tab Dial-in, chọn Allow access. OK

# Hướng dẫn thực hành 2



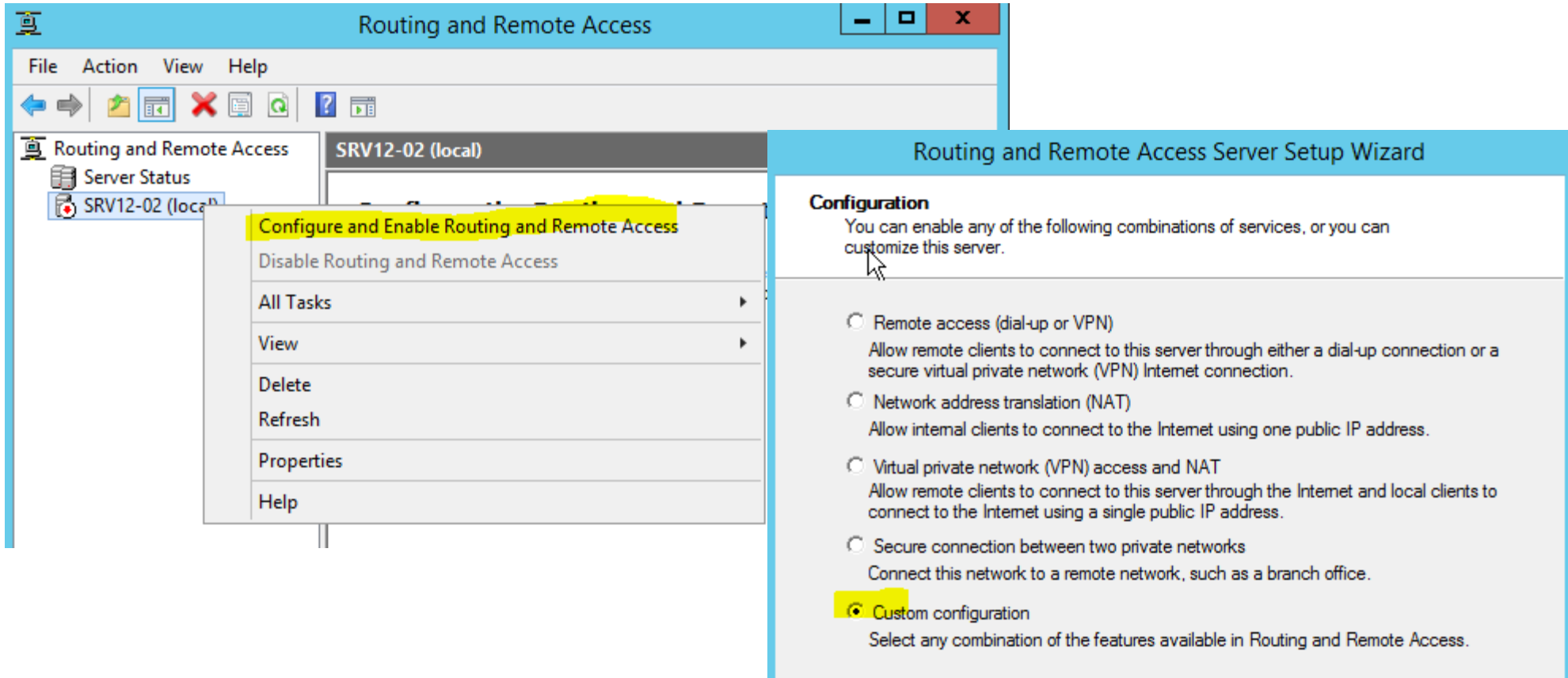
Trên VPN Server HCM, cài dịch vụ Remote Access. Trong Role Services, chọn Routing. Click Install để tiến hành cài

# Hướng dẫn thực hành 2



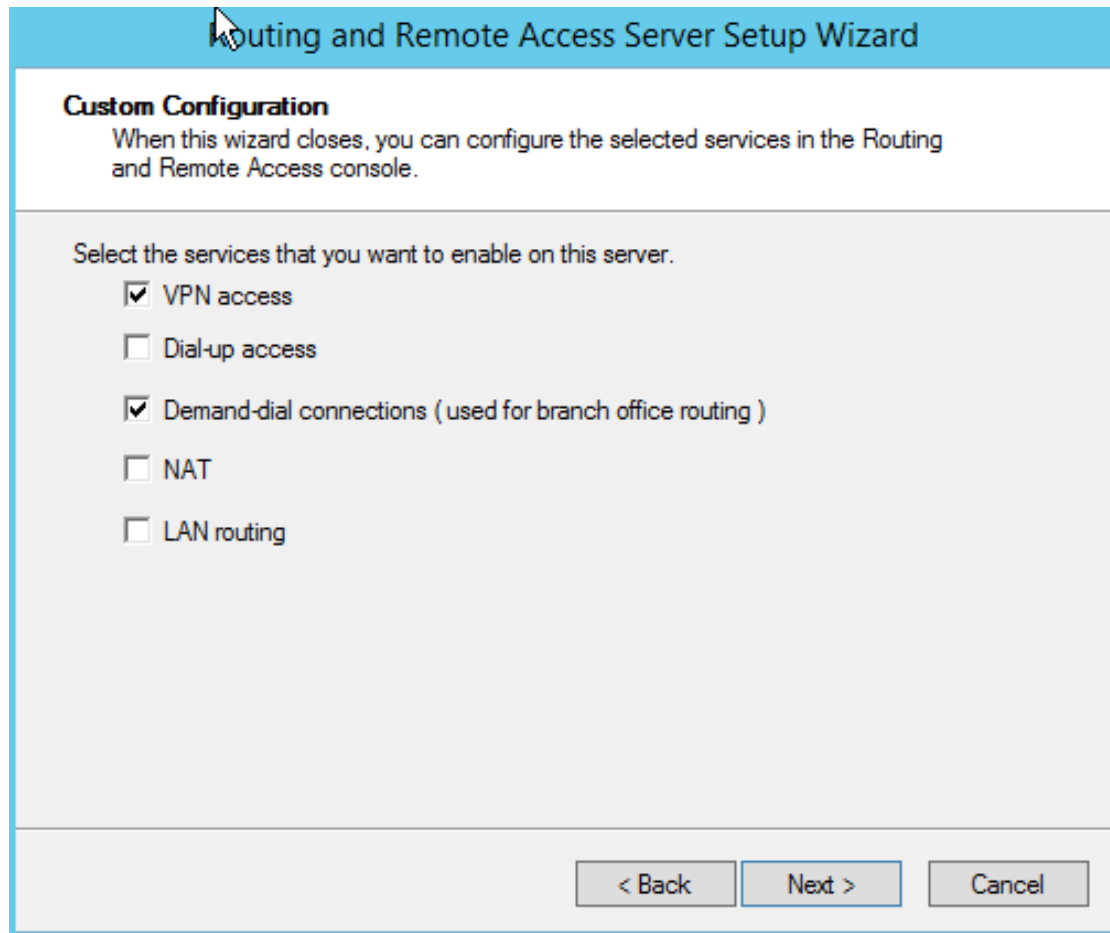
Trên VPN Server Hanoi, cài dịch vụ Remote Access. Trong Role Services, chọn Routing. Click Install để tiến hành cài

# Hướng dẫn thực hành 2



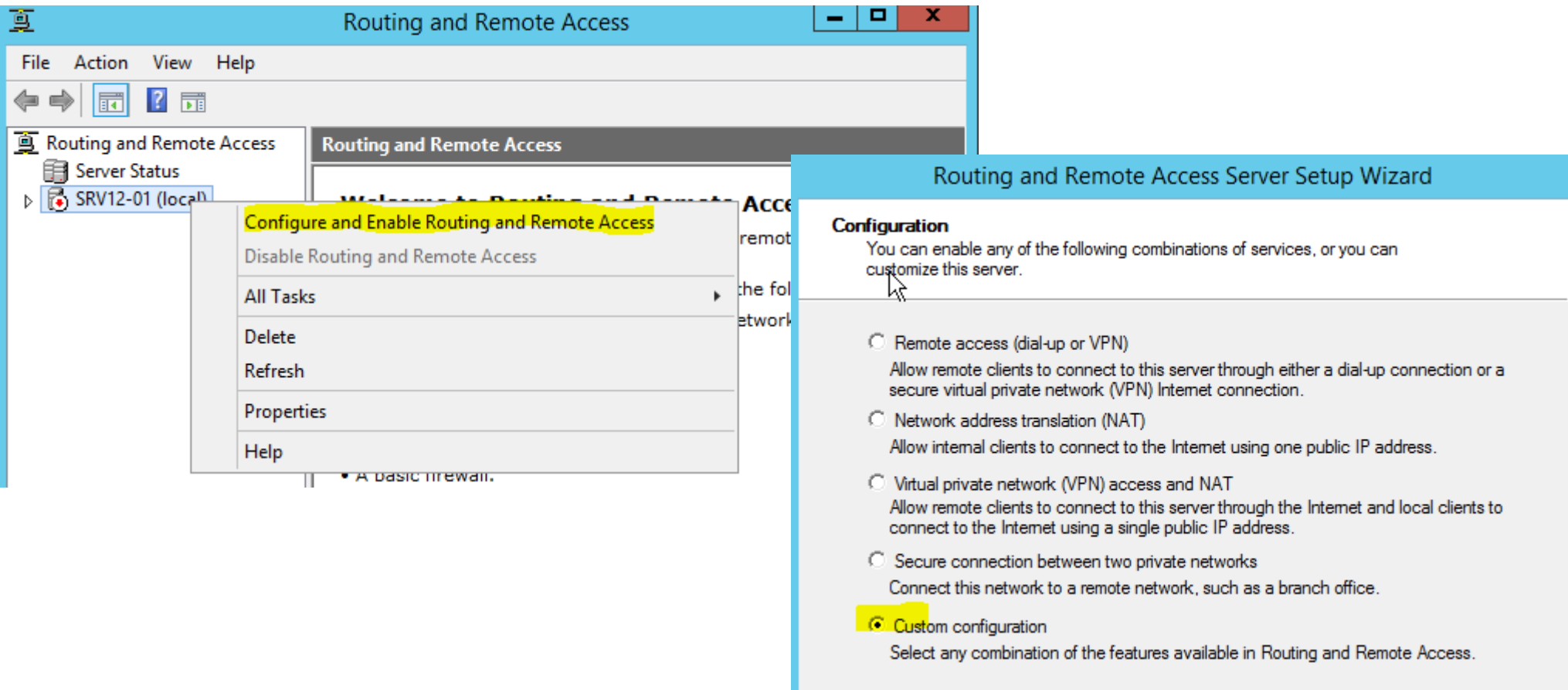
Trên VPN Server HCM, trong cửa sổ Routing and Remote Access, click phải vào tên máy chọn Configure ... Sau đó chọn Custom configuration

# Hướng dẫn thực hành 2



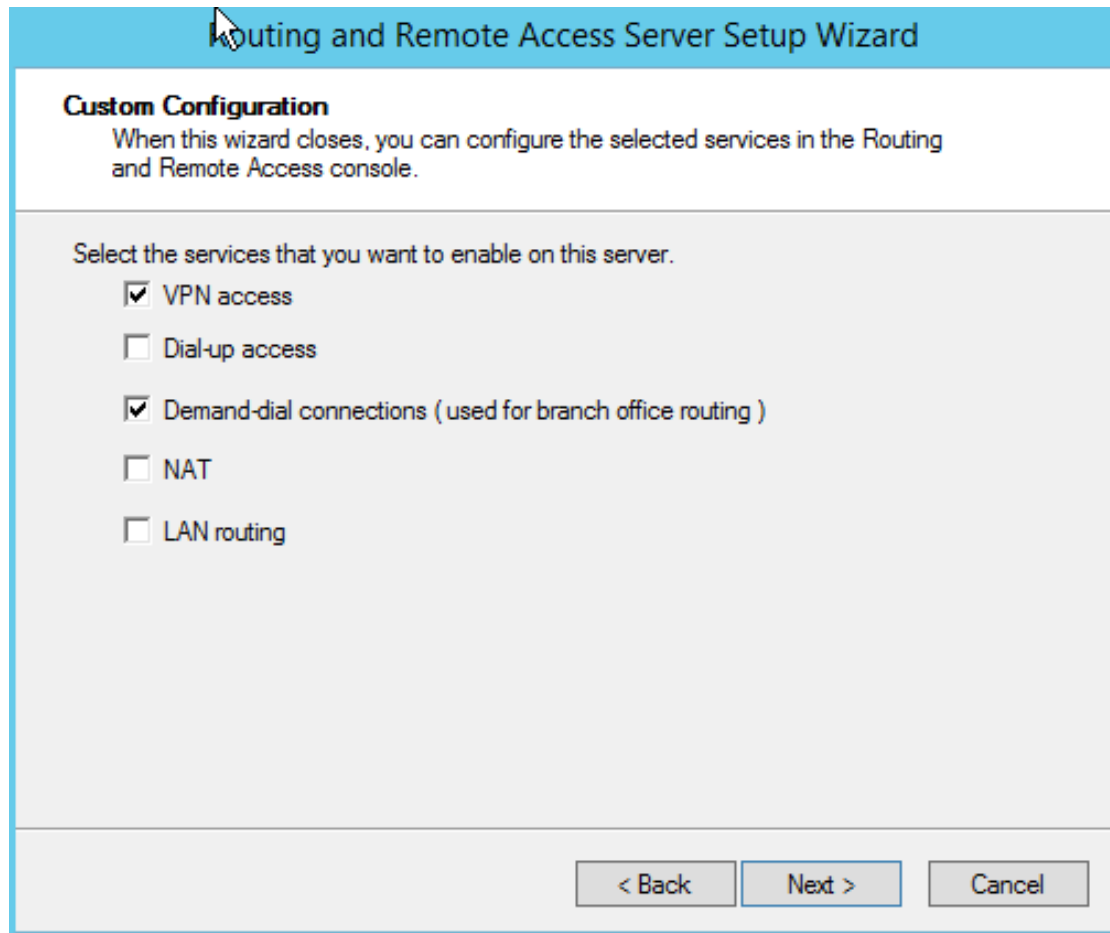
Trên VPN Server HCM, chọn VPN access và Demand-dial connections. Sau đó Finish và Start service để khởi động dịch vụ RRAS

# Hướng dẫn thực hành 2



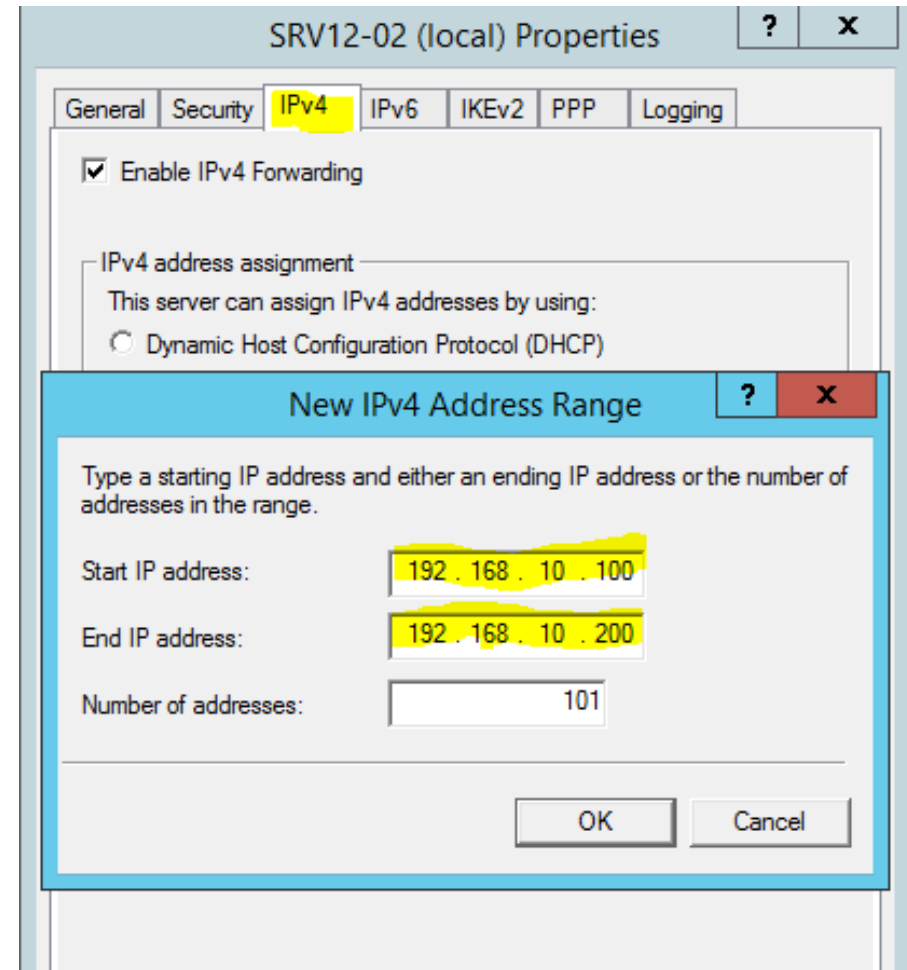
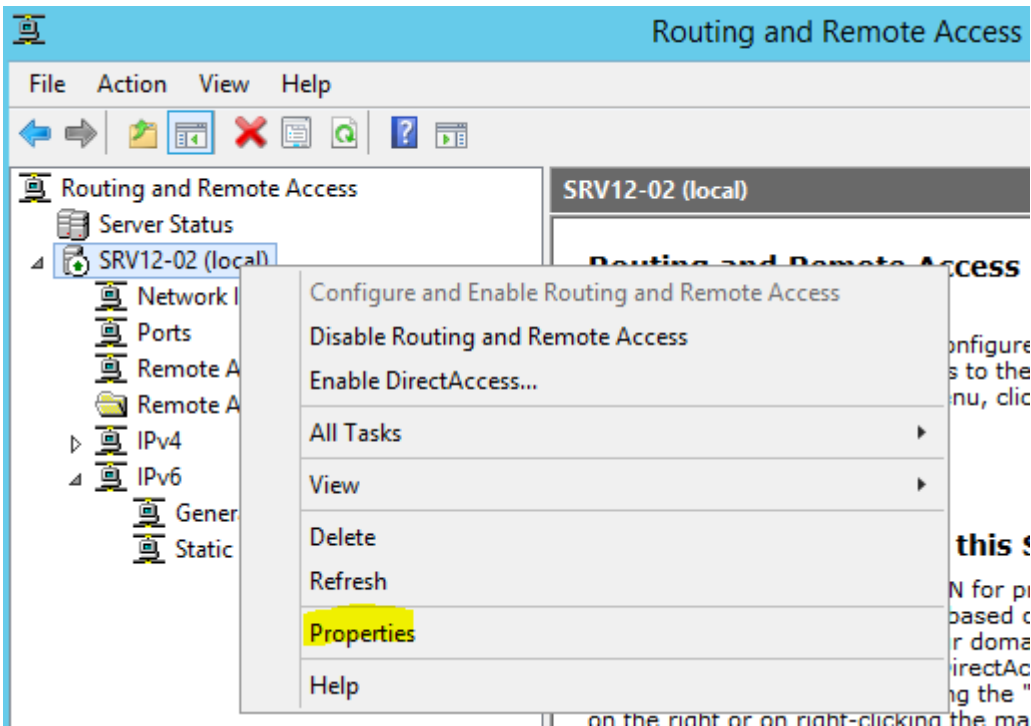
Trên VPN Server Hanoi, trong cửa sổ Routing and Remote Access, click phải vào tên máy chọn Configure ... Sau đó chọn Custom configuration

# Hướng dẫn thực hành 2



Trên VPN Server Hanoi, chọn VPN access và Demand-dial connections. Sau đó Finish và Start service để khởi động dịch vụ RRAS

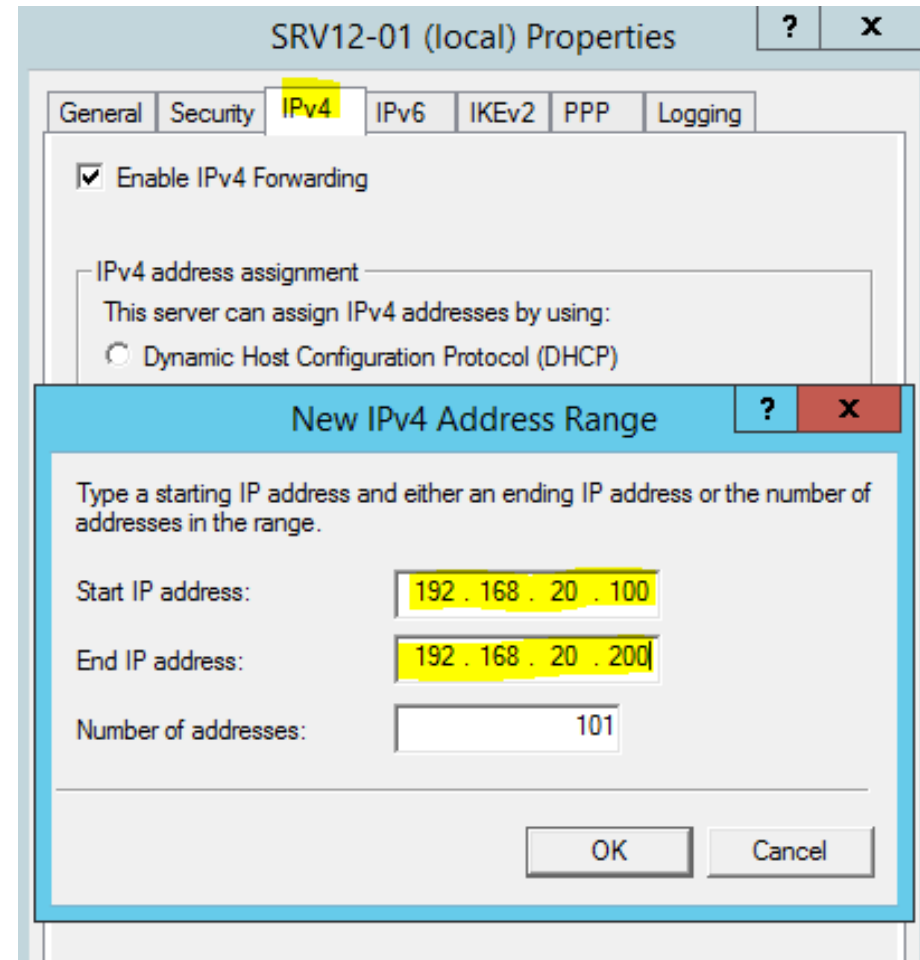
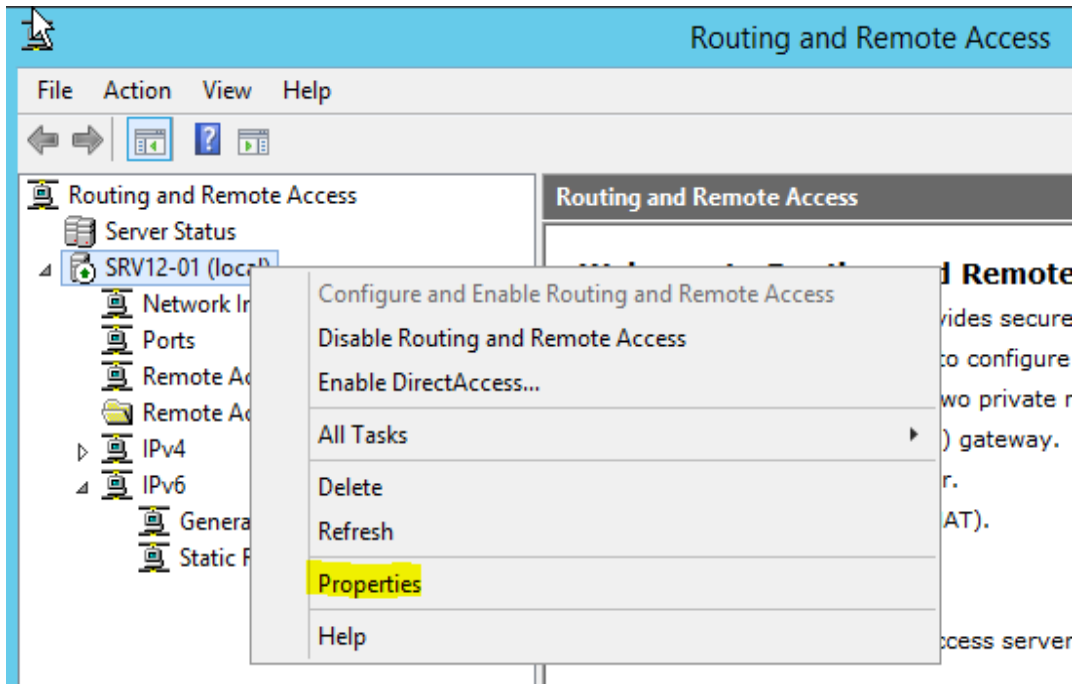
# Hướng dẫn thực hành 2



Trên VPN Server HCM, click phải lên tên máy chọn Properties. Vào tab IP, chọn Static address pool, chọn Add. Nhập vùng IP là 192.168.10.100 – 192.168.10.200 cấp phát cho các máy trạm truy cập bằng VPN. Sau đó OK

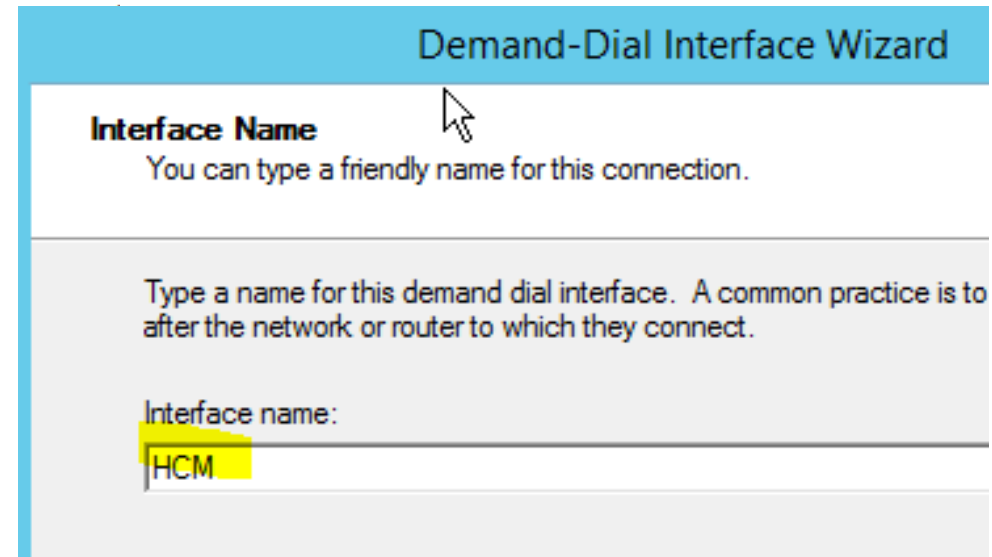
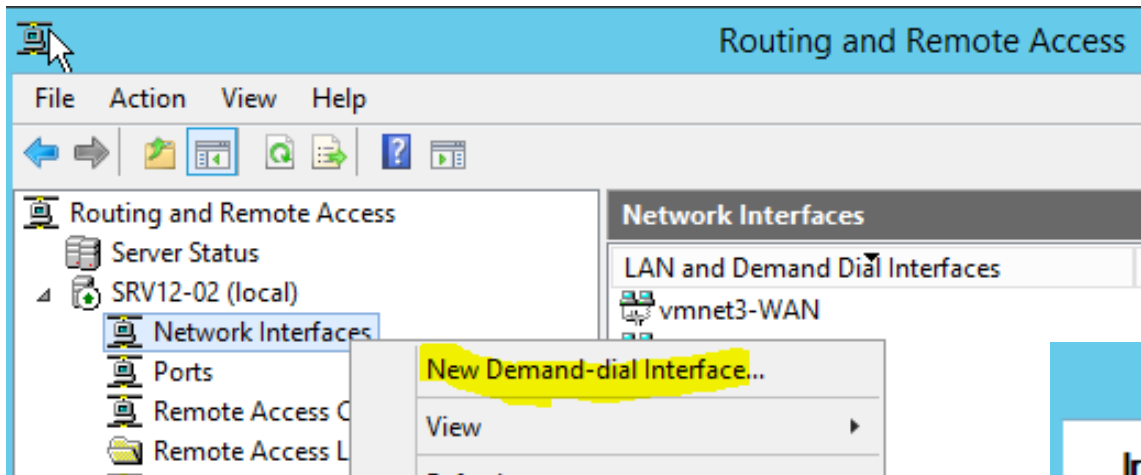


# Hướng dẫn thực hành 2



Trên VPN Server Hanoi, click phải lên tên máy chọn Properties. Vào tab IP, chọn Static address pool, chọn Add. Nhập vùng IP là 192.168.20.100 – 192.168.20.200 cấp phát cho các máy trạm truy cập bằng VPN. Sau đó OK

# Hướng dẫn thực hành 2



Trên VPN Server HCM, click phải lên Network Interface, chọn New Demand-dial Interface. Trong Interface Name, nhập tên HCM

# Hướng dẫn thực hành 2

The image displays three sequential screenshots of the 'Demand-Dial Interface Wizard' in a Windows operating system.

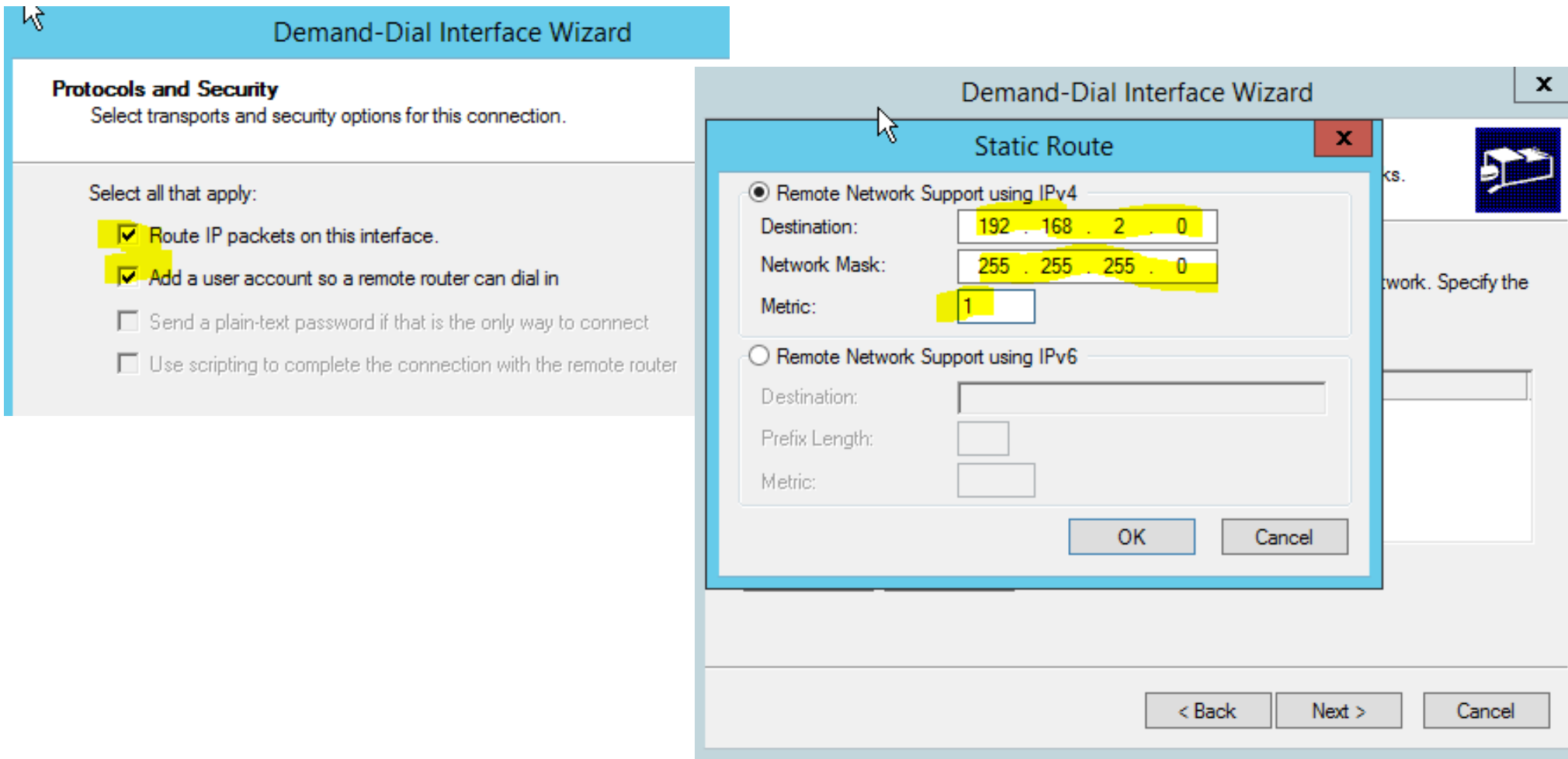
**Screenshot 1: Connection Type**  
The title bar reads 'Demand-Dial Interface Wizard'. The main heading is 'Connection Type' with the instruction 'Select the type of demand-dial interface you want to create.' There are three radio button options: 'Connect using a modem, ISDN adapter, or other device', 'Connect using virtual private networking (VPN)' (which is selected and highlighted with a yellow box), and 'Connect using PPP over Ethernet (PPPoE)'.

**Screenshot 2: VPN Type**  
The title bar reads 'Demand-Dial Interface Wizard'. The main heading is 'VPN Type' with the instruction 'Select the type of VPN connection you want to create.' There are three radio button options: 'Automatic selection', 'Point to Point Tunneling Protocol (PPTP)' (which is selected and highlighted with a yellow box), and 'Layer 2 Tunneling Protocol (L2TP)'.

**Screenshot 3: Destination Address**  
The title bar reads 'Demand-Dial Interface Wizard'. The main heading is 'Destination Address' with the instruction 'What is the name or address of the remote router?'. Below this, there is a text box with the prompt 'Enter the name or IP address of the router you are connecting to.' and another text box with the prompt 'Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1...)' where the IP address '123.1.1.2' has been entered and highlighted with a yellow box.

Trên VPN Server HCM, chọn Connect using VPN. Sau đó chọn kiểu VPN là PPTP. Kế đó nhập IP của máy VPN Server Hanoi là 123.1.1.2

# Hướng dẫn thực hành 2



Trên VPN Server HCM, check vào Route IP packets ... và Add a user account .... Sau đó chọn Add để thêm Static Route là địa chỉ đường mạng bên Hanoi là 192.168.2.0

# Hướng dẫn thực hành 2

**Demand-Dial Interface Wizard**

**Dial-In Credentials**

Configure the user name and password that the remote router will use when it dials in to this server.

You need to set the dial-in credentials that remote routers will use when connecting to this interface. A user account will be created on this router if one does not already exist. Enter the user name and password here.

User name: HCM

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

**Demand-Dial Interface Wizard**

**Dial-Out Credentials**

Supply the user name and password to be used when connecting to the remote router.

You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.

User name: vpnhanoi

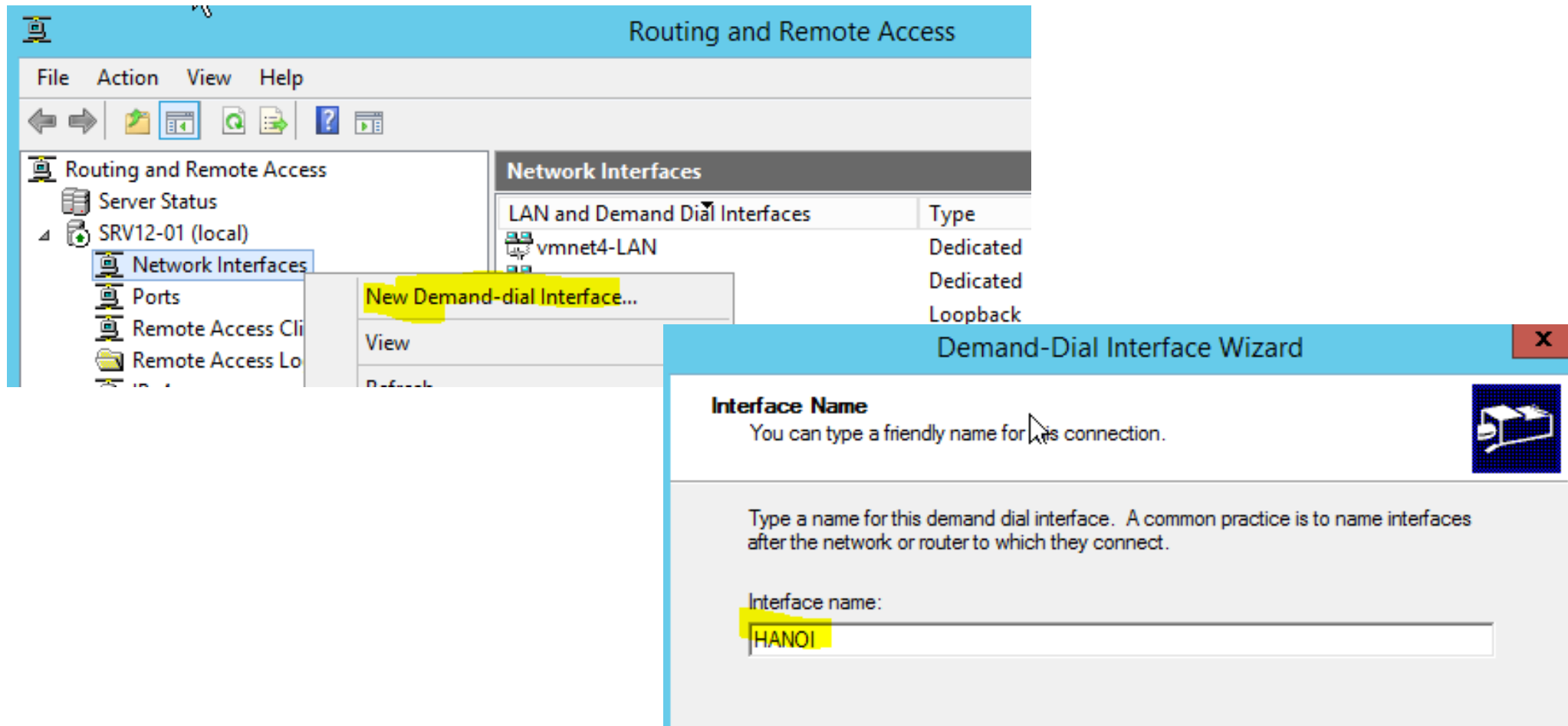
Domain:

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

Trên VPN Server HCM, nhập password 123456a@ cho username HCM. Sau đó nhập username cho dial-out là vpnhanoi và password 123456a@

# Hướng dẫn thực hành 2



Trên VPN Server Hanoi, click phải lên Network Interface, chọn New Demand-dial Interface. Trong Interface Name, nhập tên HANOI

# Hướng dẫn thực hành 2

The image displays three sequential screenshots of the 'Demand-Dial Interface Wizard' window, illustrating the configuration steps for a VPN connection.

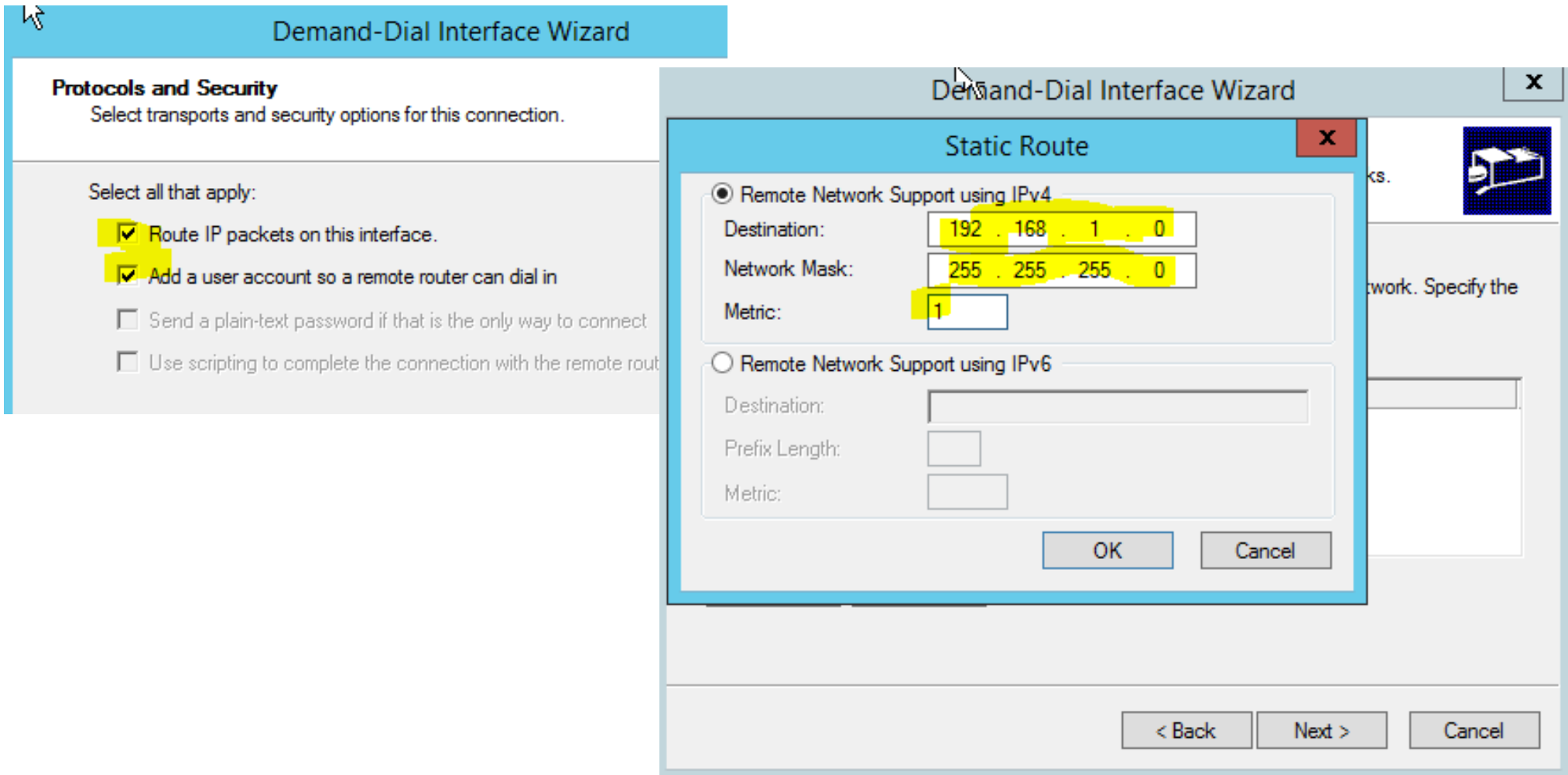
**Screenshot 1: Connection Type**  
The window title is 'Demand-Dial Interface Wizard'. The section is 'Connection Type' with the instruction 'Select the type of demand-dial interface you want to create.' Three radio button options are listed:  
☐ Connect using a modem, ISDN adapter, or other device  
☒ Connect using virtual private networking (VPN)  
☐ Connect using PPP over Ethernet (PPPoE)

**Screenshot 2: VPN Type**  
The window title is 'Demand-Dial Interface Wizard'. The section is 'VPN Type' with the instruction 'Select the type of VPN connection you want to create.' Three radio button options are listed:  
☐ Automatic selection  
☒ Point to Point Tunneling Protocol (PPTP)  
☐ Layer 2 Tunneling Protocol (L2TP)

**Screenshot 3: Destination Address**  
The window title is 'Demand-Dial Interface Wizard'. The section is 'Destination Address' with the instruction 'What is the name or address of the remote router?'. Below this, a text box prompts the user to 'Enter the name or IP address of the router you are connecting to.' and provides an example: 'Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):'. The text '123.1.1.1' is entered into the text box.

Trên VPN Server Hanoi, chọn Connect using VPN. Sau đó chọn kiểu VPN là PPTP. Kế đó nhập IP của máy VPN Server Hanoi là 123.1.1.1

# Hướng dẫn thực hành 2



Trên VPN Server Hanoi, check vào Route IP packets ... và Add a user account .... Sau đó chọn Add để thêm Static Route là địa chỉ đường mạng bên HCM là 192.168.1.0



# Hướng dẫn thực hành 2

**Demand-Dial Interface Wizard**

**Dial-In Credentials**

Configure the user name and password that the remote router will use when it dials in to this server.

You need to set the dial-in credentials that remote routers will use to connect to this interface. A user account will be created on this router with the name you enter here.

User name: HANOI

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

**Demand-Dial Interface Wizard**

**Dial-Out Credentials**

Supply the user name and password to be used when connecting to the remote router.

You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.

User name: vpngcm

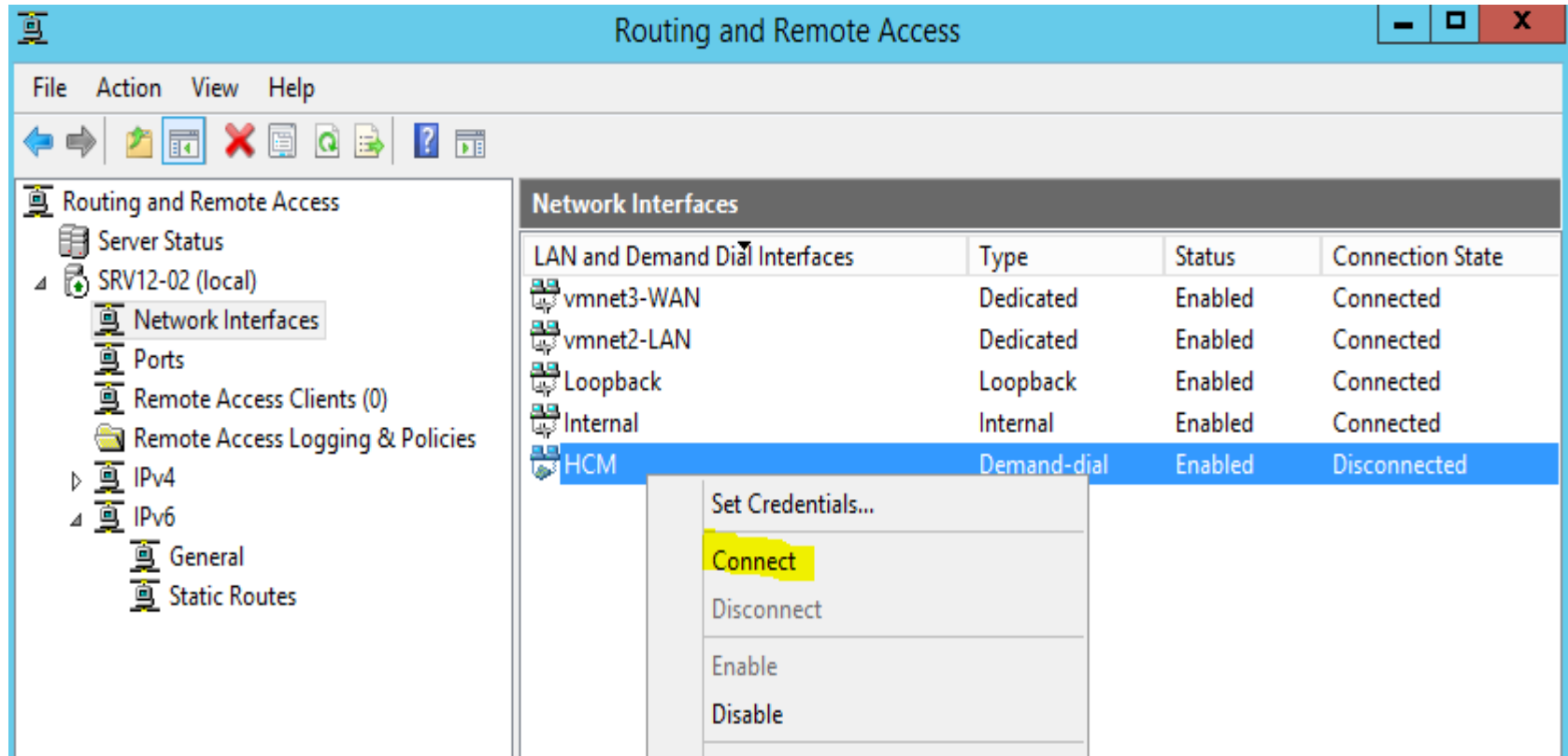
Domain:

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

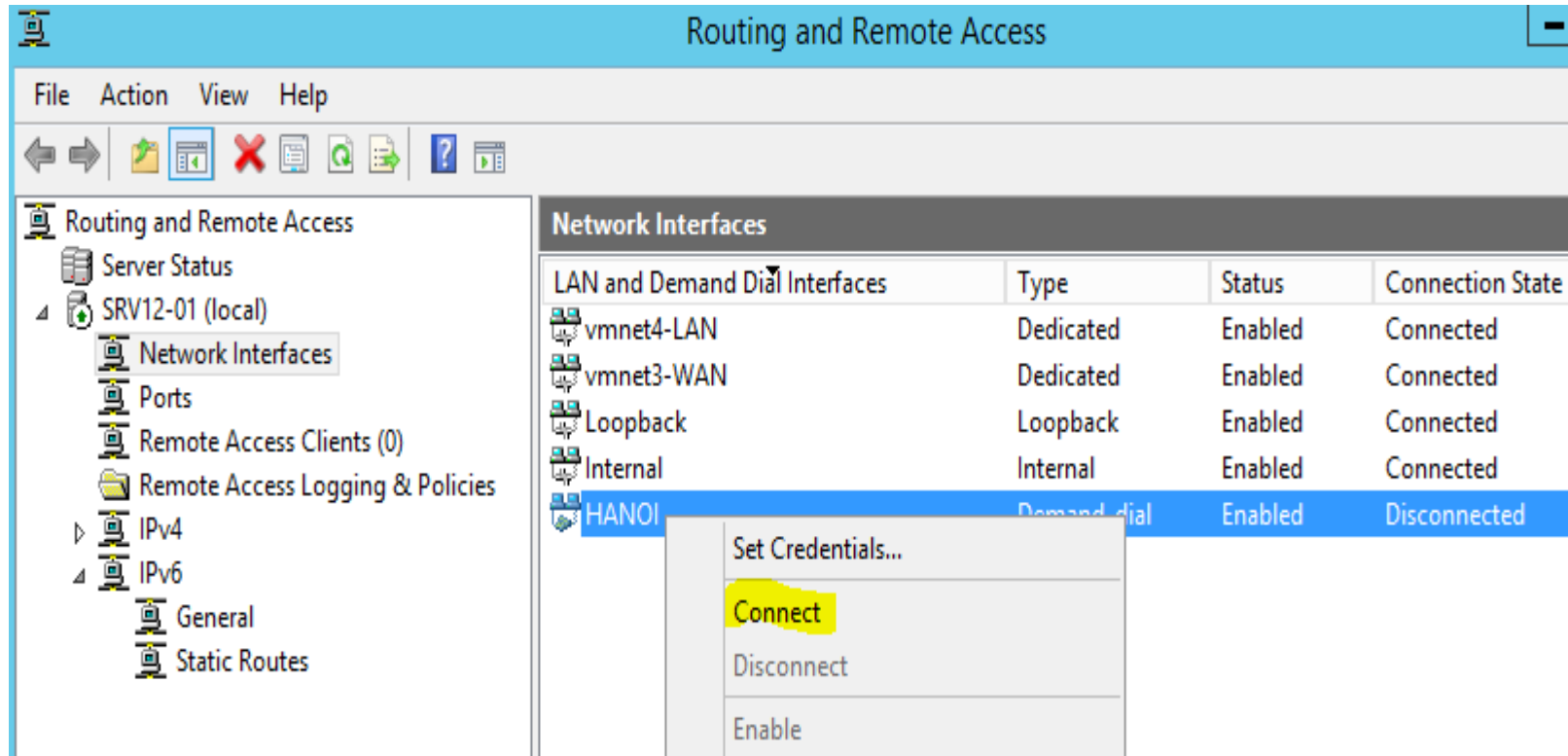
Trên VPN Server Hanoi, nhập password 123456a@ cho username HANOI. Sau đó nhập username cho dial-out là vpngcm và password 123456a@

# Hướng dẫn thực hành 2



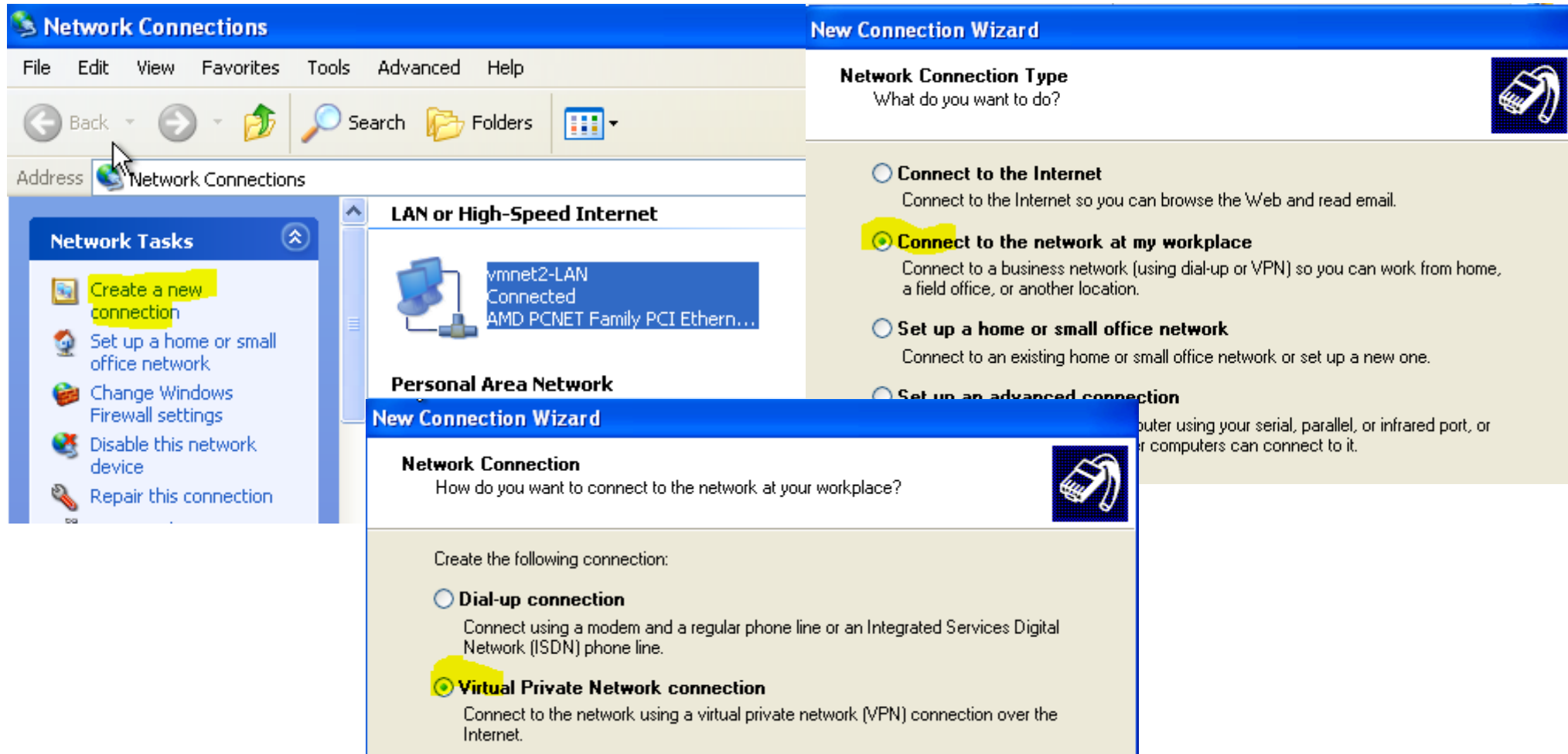
Trên VPN Server HCM, click chuột phải lên interface HCM, chọn Connect

# Hướng dẫn thực hành 2



Trên VPN Server Hanoi, click chuột phải lên interface HANOI, chọn Connect

# Hướng dẫn thực hành 2



Trên Client HCM, chọn Create a new connection. Chọn Connect to the ... và chọn Virtual Private ...

# Hướng dẫn thực hành 2

**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

Ket noi mang LAN Hanoi

For example, you could type the name of your workplace or the name of the server you will connect to.

**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?

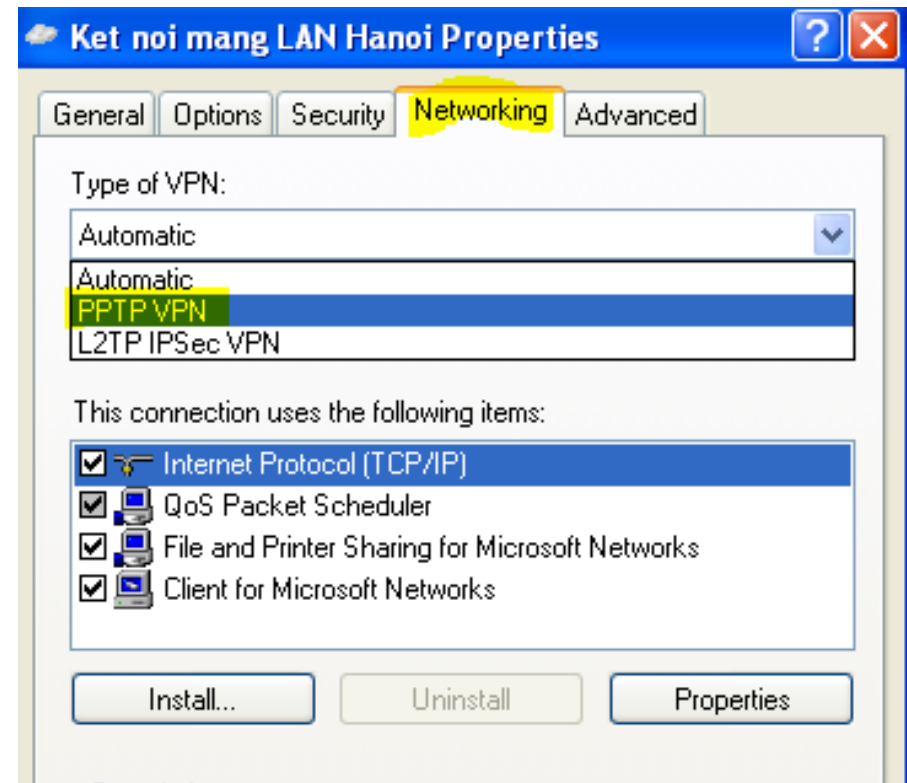
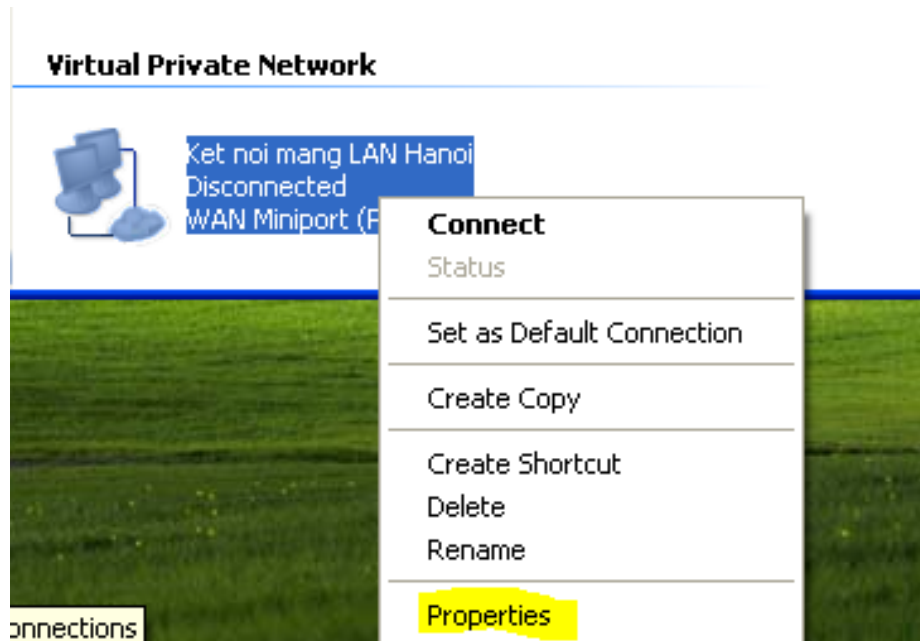
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1 ):

123.1.1.2

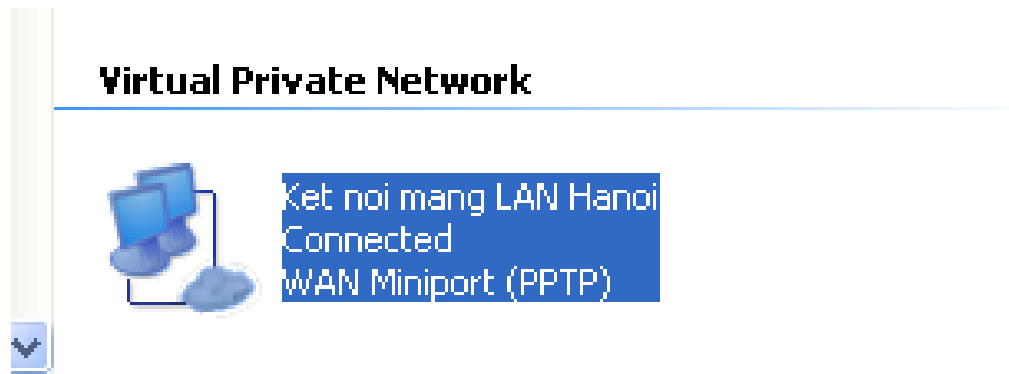
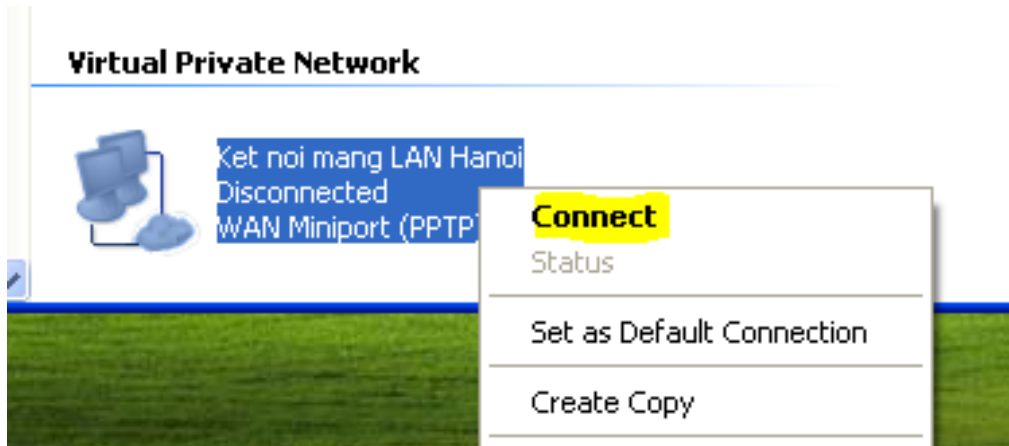
Trên Client HCM, nhập tên kết nối và địa chỉ IP của máy VPN Server Hanoi là 123.1.1.2

# Hướng dẫn thực hành 2



Trên Client HCM, click phải vào card mạng vừa tạo chọn Properties. Vào tab Networking, chọn kiểu giao thức VPN là PPTP

# Hướng dẫn thực hành 2



Trên Client HCM, click phải vào card mạng vừa tạo chọn Connect. Nhập username là vpnhanoi và password 123456a@. Chọn Connect. Và kết quả kết nối thành công

# Hướng dẫn thực hành 2

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\suv>ping 192.168.2.99

Pinging 192.168.2.99 with 32 bytes of data:

Reply from 192.168.2.99: bytes=32 time=1ms TTL=127
Reply from 192.168.2.99: bytes=32 time=1ms TTL=127
Reply from 192.168.2.99: bytes=32 time=3ms TTL=127
Reply from 192.168.2.99: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.2.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

C:\Documents and Settings\suv>ipconfig

Windows IP Configuration

Ethernet adapter vmnet2-LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.98
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

PPP adapter Ket noi mang LAN Hanoi:

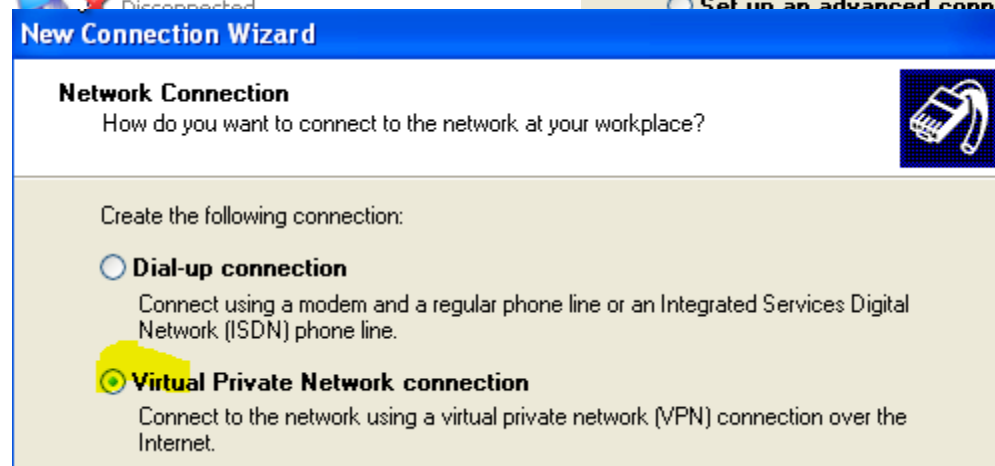
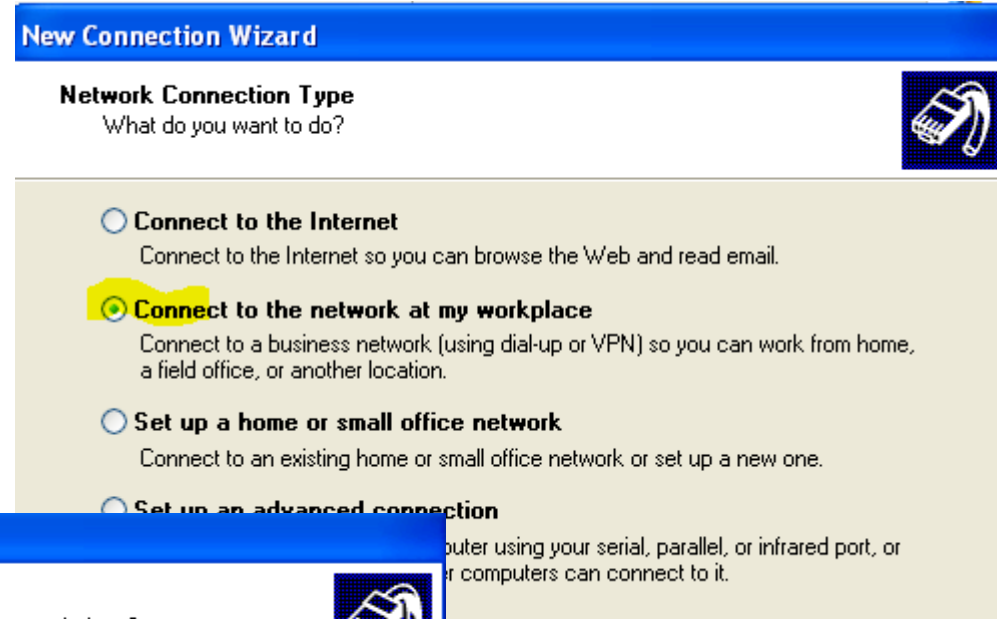
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.20.101
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 192.168.20.101

C:\Documents and Settings\suv>
```

Trên Client HCM, ping đến máy 192.168.2.99 → thành công



# Hướng dẫn thực hành 2



Trên Client Hanoi, chọn Create a new connection. Chọn Connect to the ... và chọn Virtual Private ...

# Hướng dẫn thực hành 2

**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

Kết nối mạng LAN HCM

For example, you could type the name of your workplace or the  
will connect to.

**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?

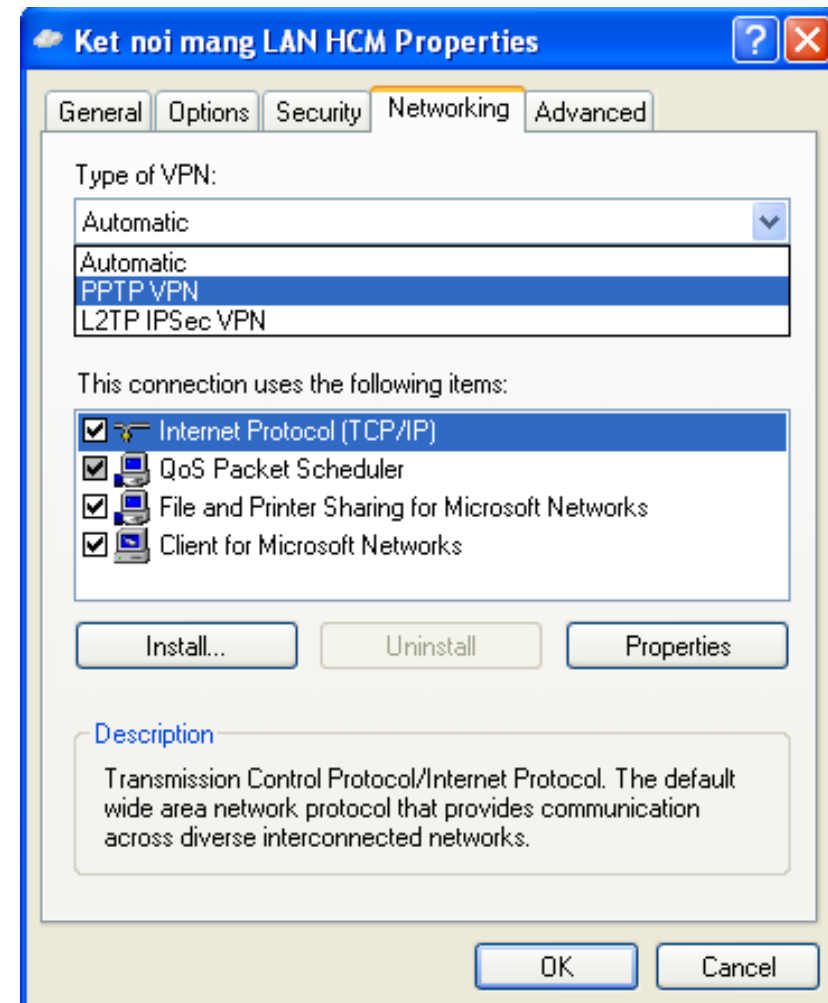
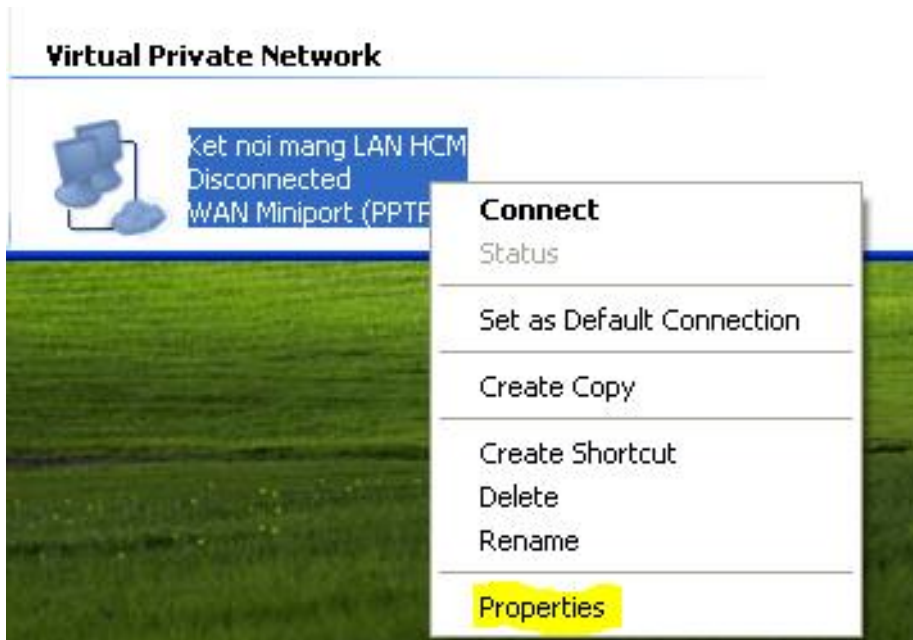
Type the host name or Internet Protocol (IP) address of the computer to which you are  
connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1 ):

123.1.1.1

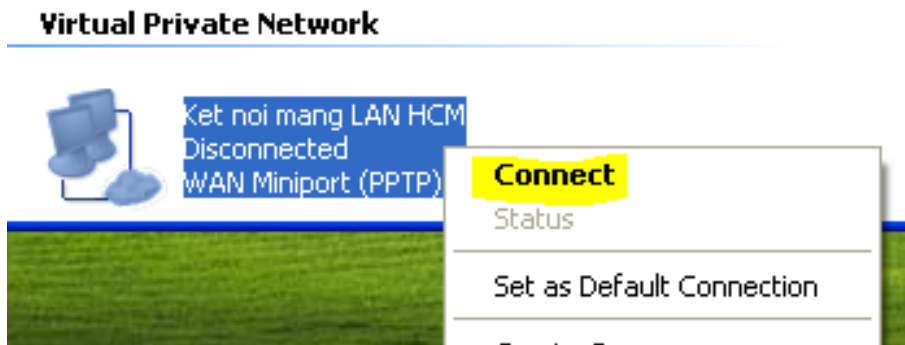
Trên Client Hanoi, nhập tên kết nối và địa chỉ IP của máy VPN Server Hanoi là 123.1.1.1

# Hướng dẫn thực hành 2



Trên Client Hanoi, click phải vào card mạng vừa tạo chọn Properties. Vào tab Networking, chọn kiểu giao thức VPN là PPTP

# Hướng dẫn thực hành 2



Trên Client Hanoi, click phải vào card mạng vừa tạo chọn Connect. Nhập username là vpnhcm và password 123456a@. Chọn Connect. Và kết quả kết nối thành công

# Hướng dẫn thực hành 2

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\sv>ping 192.168.1.98

Pinging 192.168.1.98 with 32 bytes of data:

Reply from 192.168.1.98: bytes=32 time=2ms TTL=126
Reply from 192.168.1.98: bytes=32 time=4ms TTL=126
Reply from 192.168.1.98: bytes=32 time=2ms TTL=126
Reply from 192.168.1.98: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\Documents and Settings\sv>ipconfig

Windows IP Configuration

Ethernet adapter vmnet4-LAN:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.99
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

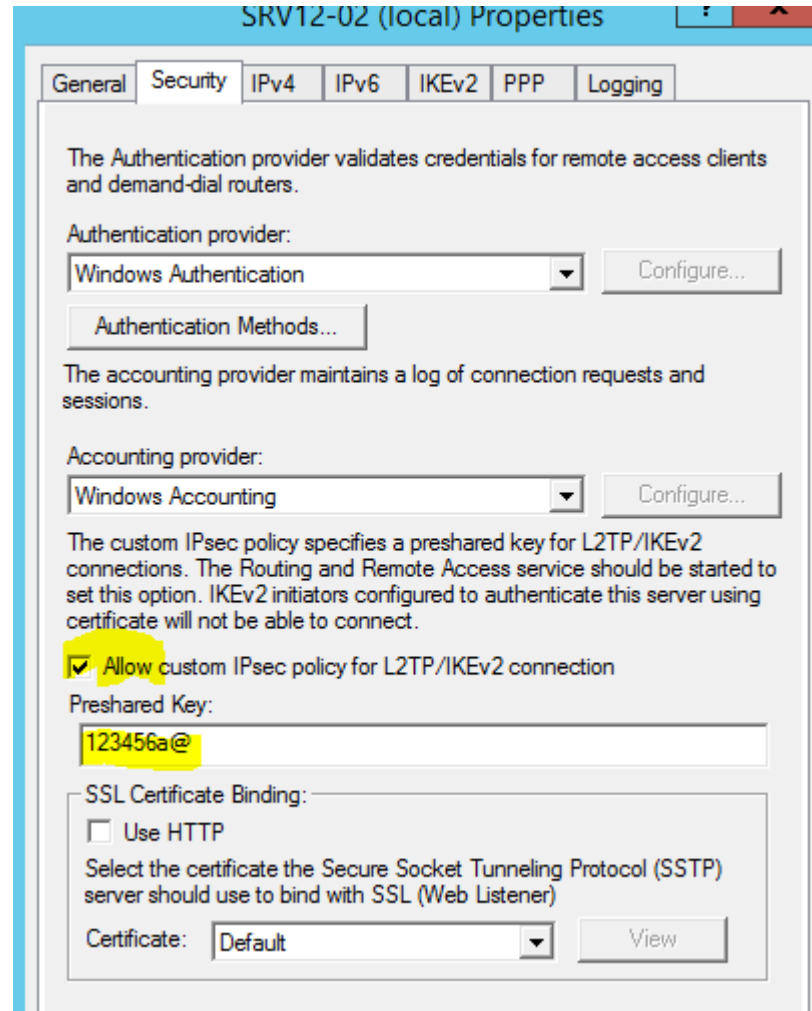
PPP adapter Ket noi mang LAN HCM:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.10.107
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 192.168.10.107

C:\Documents and Settings\sv>
```

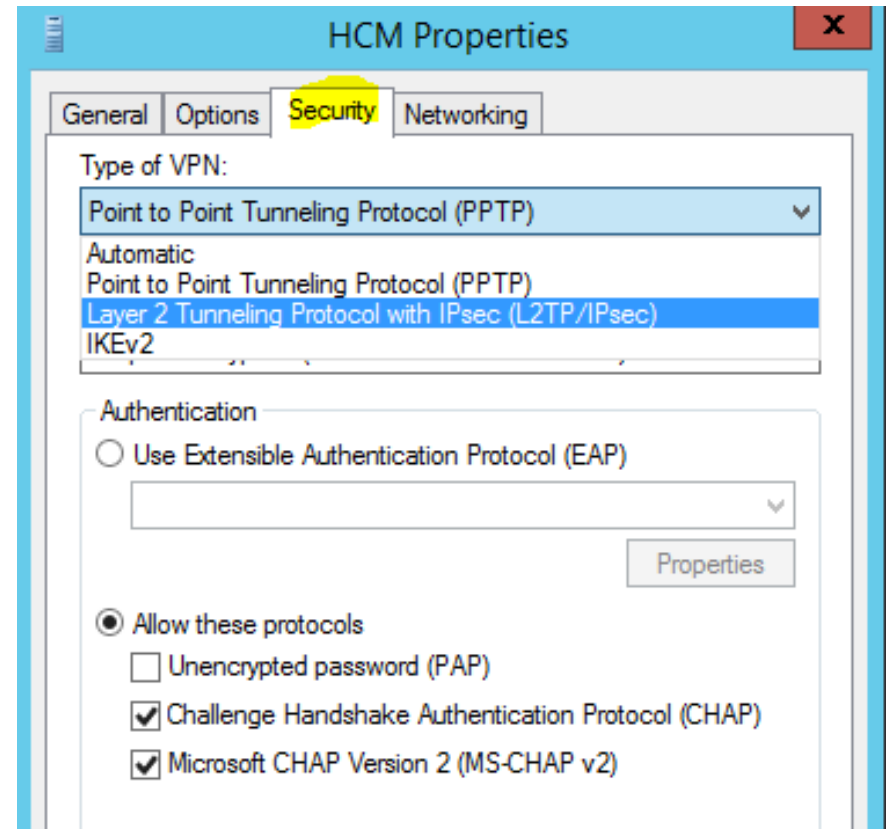
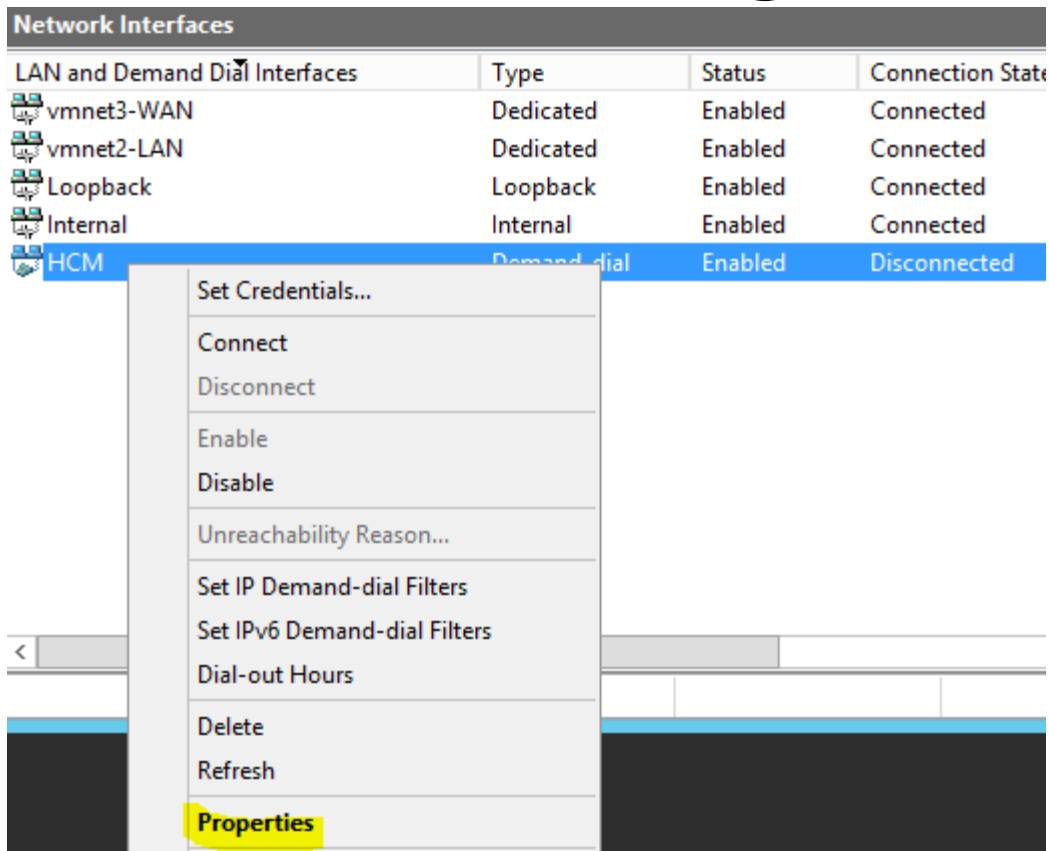
Trên Client Hanoi, ping đến máy 192.168.1.98 → thành công

# Hướng dẫn thực hành 2



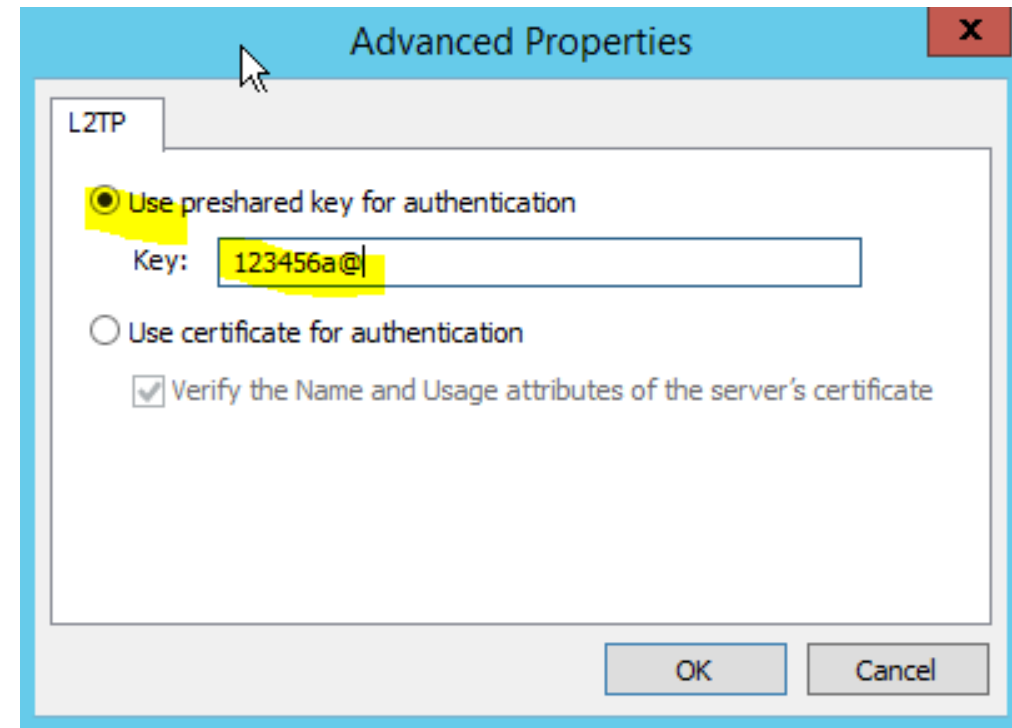
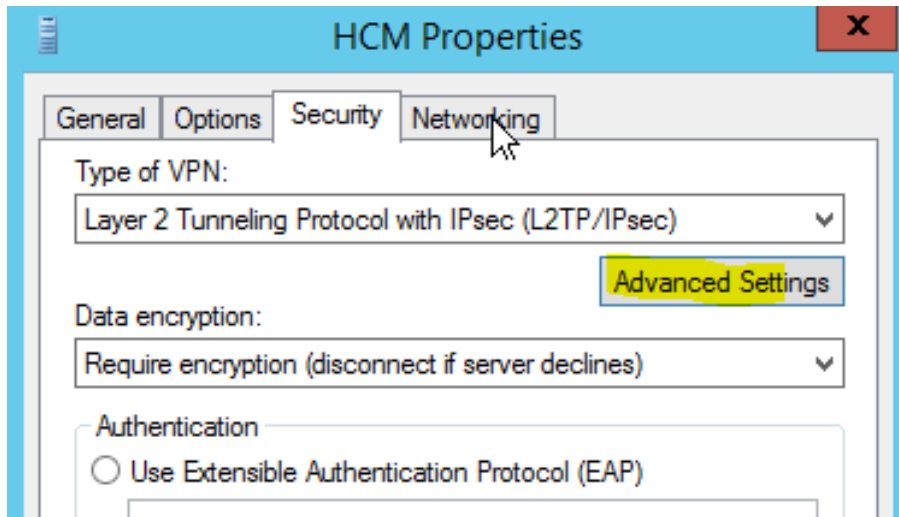
Nếu chọn giao thức L2PT để kết nối các máy, cần thêm các bước sau:  
Trên VPN Server HCM, click phải lên tên máy, chọn Properties, vào tab Security thêm phần Preshared Key. Làm tương tự với VPN Server Hanoi

# Hướng dẫn thực hành 2



Trên VPN Server HCM, click phải lên HCM, chọn Properties. Vào tab Security, chọn kiểu VPN là L2TP/IPSec. Làm tương tự trên VPN Server Hanoi

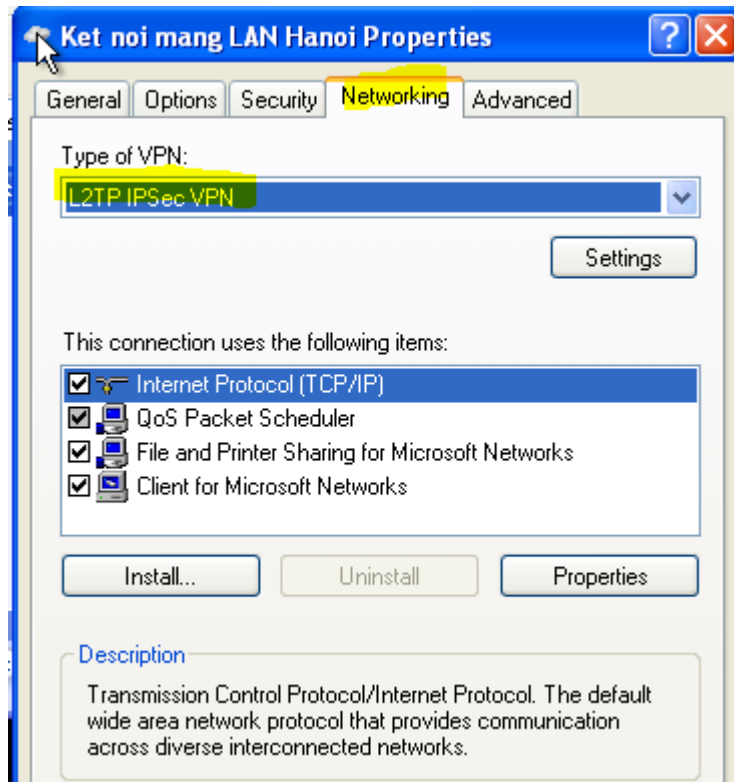
# Hướng dẫn thực hành 2



Trên VPN Server HCM, click chọn Advanced Settings, sau đó nhập preshared key.  
Làm tương tự trên VPN Server Hanoi

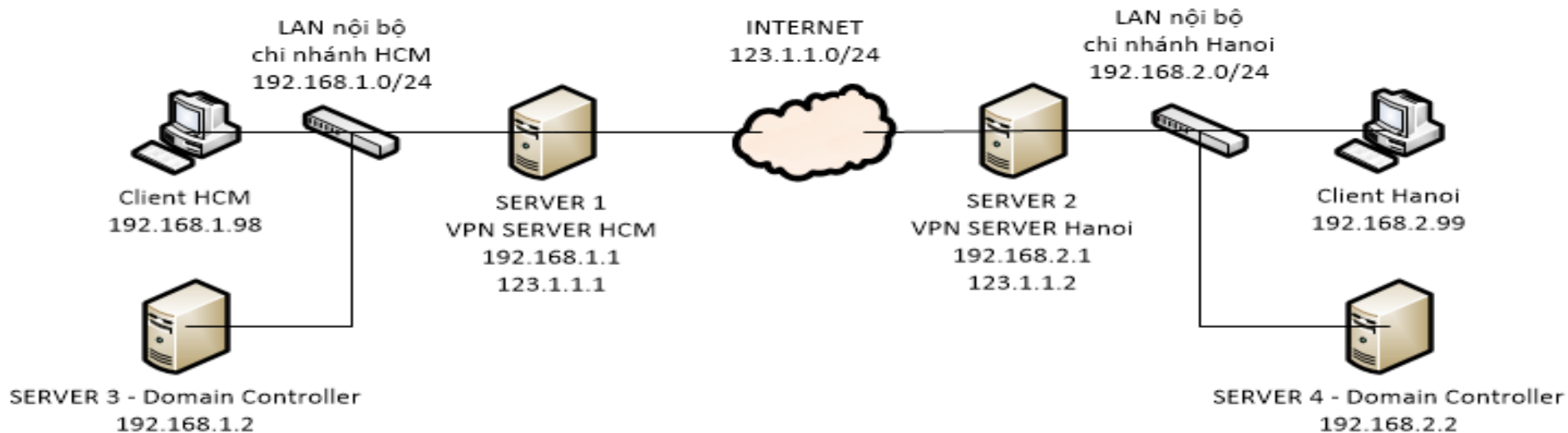


# Hướng dẫn thực hành 2



Trên Client HCM, click phải vào card mạng Ket noi mang LAN Hanoi, chọn Properties. Vào tab Networking, chọn kiểu giao thức L2TP IPSec. Vào tab Security, click chọn IPSec Settings, nhập preshared key. Làm tương tự trên Client Hanoi

# Thực hành 2bis: Site to Site VPN



## Chuẩn bị:

1 máy VPN Server HCM, 1 máy client HCM, 1 máy Server3 là DC quản lý miền cntt.caothang.edu.vn

1 máy VPN Server Hanoi, 1 máy client Hanoi, 1 máy Server4 là DC quản lý miền dt.caothang.edu.vn

## Yêu cầu:

Máy Client HCM, Server1 gia nhập miền cntt.caothang.edu.vn

Máy Client Hanoi, Server2 gia nhập miền dt.caothang.edu.vn

Cấu hình Site to Site VPN trên máy VPN Server HCM và VPN Server Hanoi cho phép máy client HCM kết nối máy client Hanoi

# Thực hành 2bis: Site to Site VPN

	Server3 (DC)	Client HCM	VPN Server HCM	
VMNET	Vmnet2	Vmnet2	Vmnet2	Vmnet3
IP	192.168.1.2	192.168.1.98	192.168.1.1	123.1.1.1
SM	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DG	192.168.1.1	192.168.1.1		123.1.1.2
P.DNS	192.168.1.2	192.168.1.2	192.168.1.2	

	Server4 (DC)	Client Hanoi	VPN Server Hanoi	
VMNET	Vmnet4	Vmnet4	Vmnet4	Vmnet3
IP	192.168.2.2	192.168.2.99	192.168.2.1	123.1.1.2
SM	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DG	192.168.2.1	192.168.2.1		123.1.1.1
P.DNS	192.168.2.2	192.168.2.2	192.168.2.2	

Bảng địa chỉ IP các máy