

CHƯƠNG 7

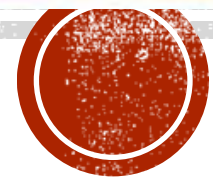
BẢO MẬT MẠNG

LẬP TRÌNH MẠNG CĂN BẢN





BẢO MẬT MẠNG



FIREWALL,
PROXY SERVER VÀ ROUTER

NỘI DUNG

- Giới thiệu
- Xây dựng hệ thống mạng từ đầu
- Xây dựng hệ thống mạng doanh nghiệp
- Tunneling trong mạng doanh nghiệp
- Vấn đề cần tránh khi xây dựng hệ thống mạng

XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU

Chọn kiến trúc mạng (topology):

- 3 kiểu kết nối vật lý chính:
 - UTP
 - BNC
 - Wireless

3 LOẠI KẾT NỐI VẬT LÝ



UTP VÀ STP



UTP Cable



STP Cable

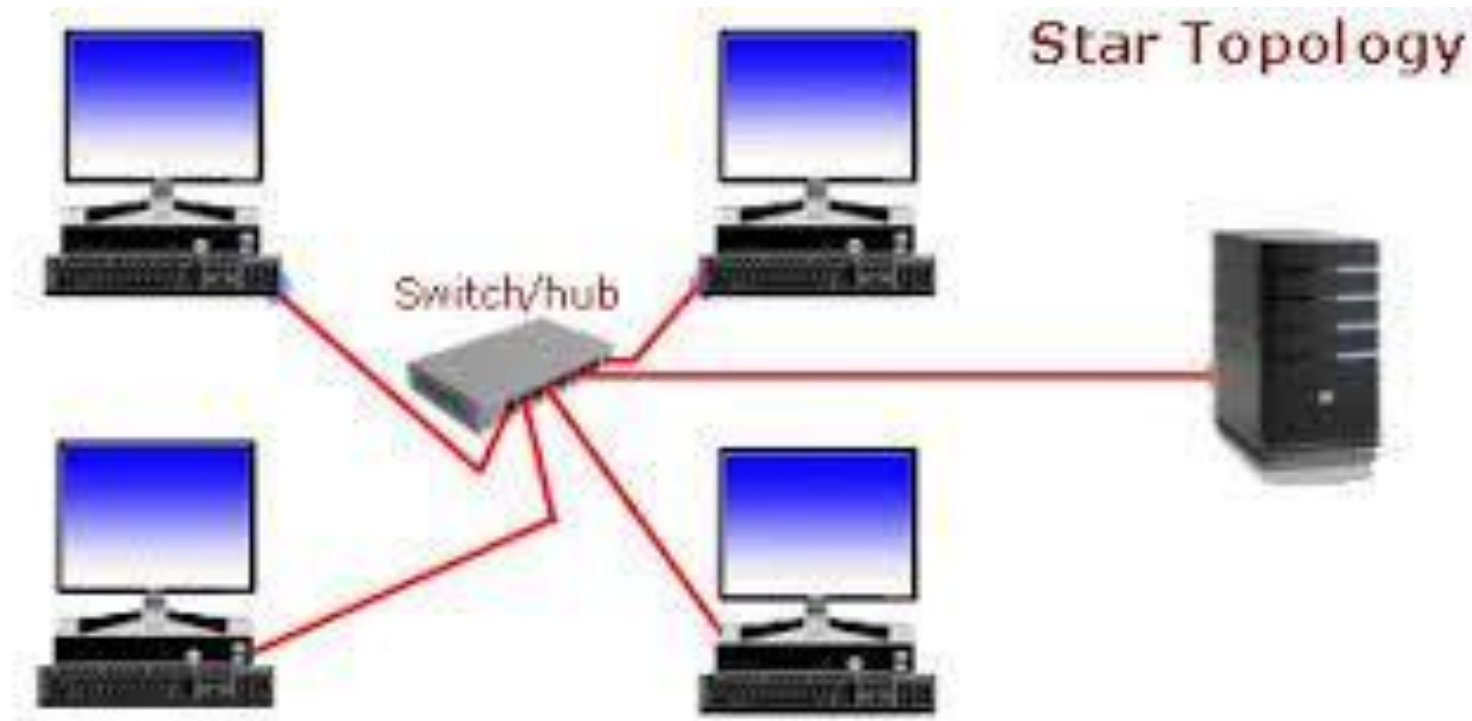
KHÁC NHAU GIỮA UTP VÀ BNC

- Loại cáp kết nối đến máy tính
- UTP giống cáp điện thoại, RJ45
- BNC cáp đồng trục, giống cáp tivi, đầu cắm tròn

XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU

Chọn kiến trúc mạng (topology)

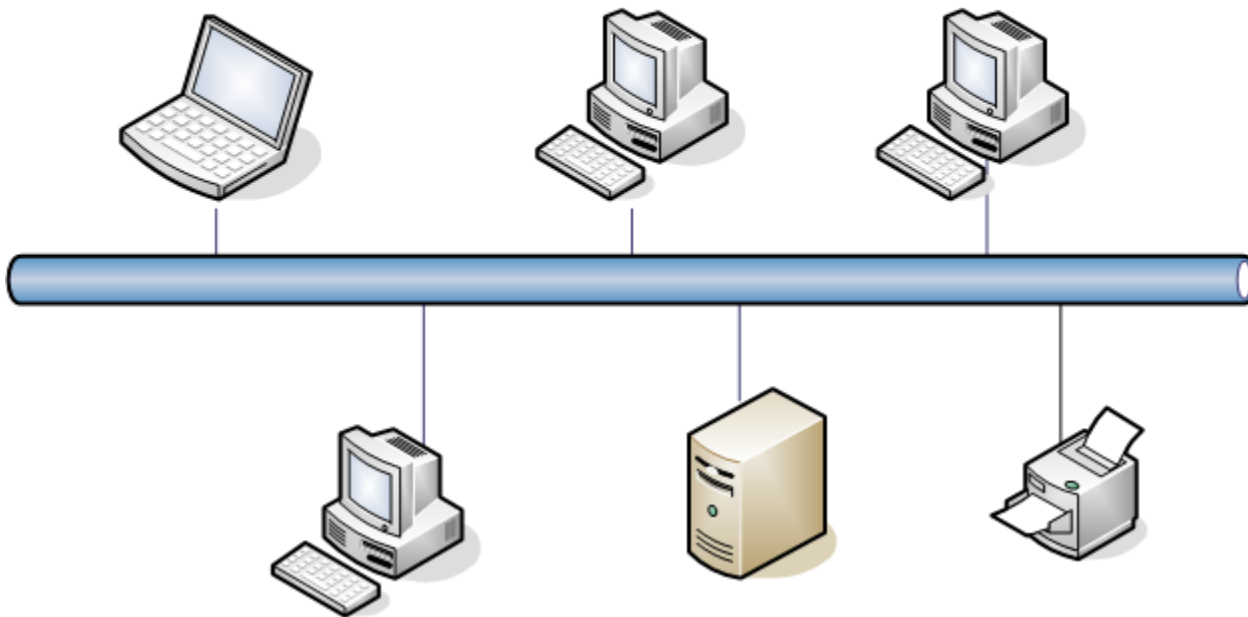
- UTP được dành cho dạng cấu trúc star



XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU

- BNC dùng cho kiến trúc bus (ít được sử dụng)

BUS Topology



KẾT NỐI KHÁC

- Vấn đề không tương thích



XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU

Cài đặt mạng

Người dùng sẽ mong đợi một cơ chế chia sẻ file trên mạng
→ nên cung cấp từ đầu:

- Chọn tên duy nhất cho máy tính trong mạng
- Mở các giao thức và dịch vụ
- Cấu hình TCP/IP
- Chia sẻ thư mục
- Hạn chế khả năng của người dùng truy cập từ xa

XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU

The screenshot shows the Windows 10 'System' control panel window. The title bar reads 'System'. The breadcrumb navigation shows 'Control Panel > All Control Panel Items > System'. The left sidebar includes 'Control Panel Home', 'Device Manager', 'Remote settings', 'System protection', and 'Advanced system settings'. The main content area is titled 'View basic information about your computer'. It displays 'Windows edition' as 'Windows 10 Education' with a copyright notice '© 2017 Microsoft Corporation. All rights reserved.' and the Windows 10 logo. The 'System' section lists hardware details: Processor (Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz 2.39 GHz), Installed memory (RAM) (8.00 GB), System type (64-bit Operating System, x64-based processor), and Pen and Touch (No Pen or Touch Input is available for this Display). The 'Computer name, domain, and workgroup settings' section shows the computer name as 'VanGiau-pc', full computer name as 'VanGiau-pc', computer description as 'VanGiau-pc', and workgroup as 'WORKGROUP'. A red box highlights the 'Change settings' link. The 'Windows activation' section shows 'Windows is activated' with a link to 'Read the Microsoft Software License Terms' and the product ID '00328-00073-76677-AA274'. A 'Change product key' link is also present. At the bottom, it says 'See also Security and Maintenance'.

System

Control Panel > All Control Panel Items > System

Control Panel Home

Device Manager

Remote settings

System protection

Advanced system settings

View basic information about your computer

Windows edition

Windows 10 Education

© 2017 Microsoft Corporation. All rights reserved.

Windows 10

System

Processor: Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz 2.39 GHz

Installed memory (RAM): 8.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: VanGiau-pc

Full computer name: VanGiau-pc

Computer description: VanGiau-pc

Workgroup: WORKGROUP

Change settings

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

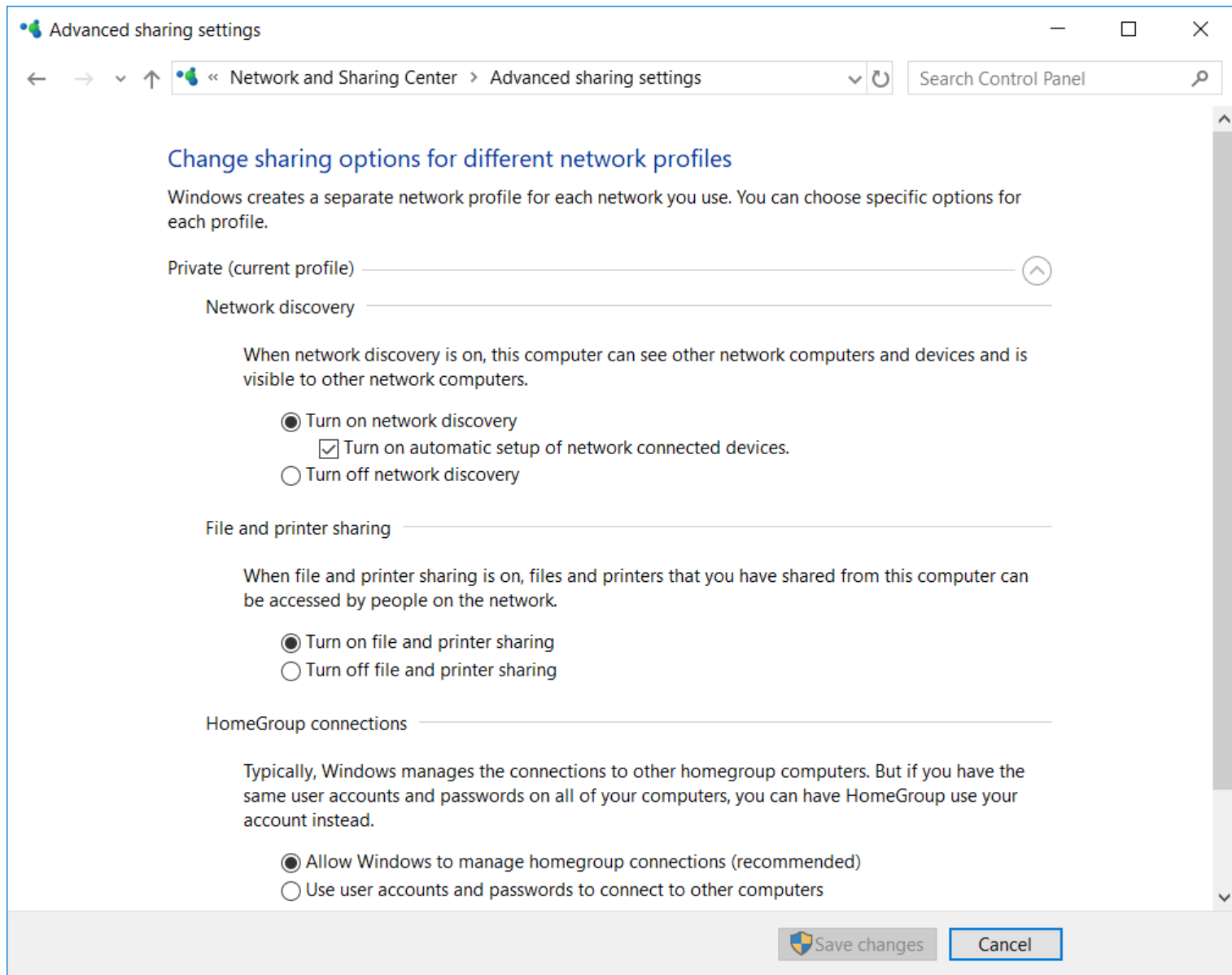
Product ID: 00328-00073-76677-AA274

Change product key

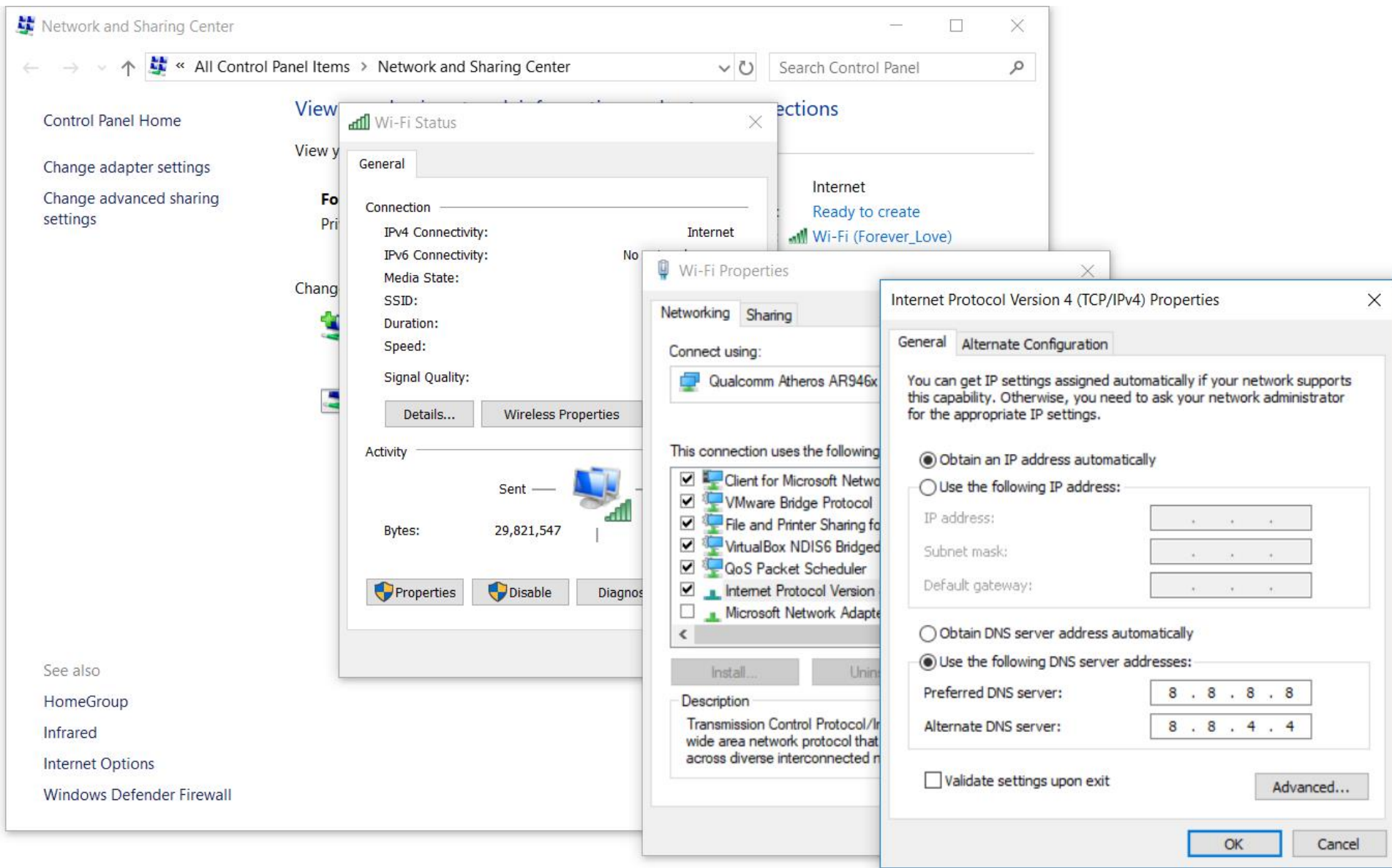
See also

Security and Maintenance

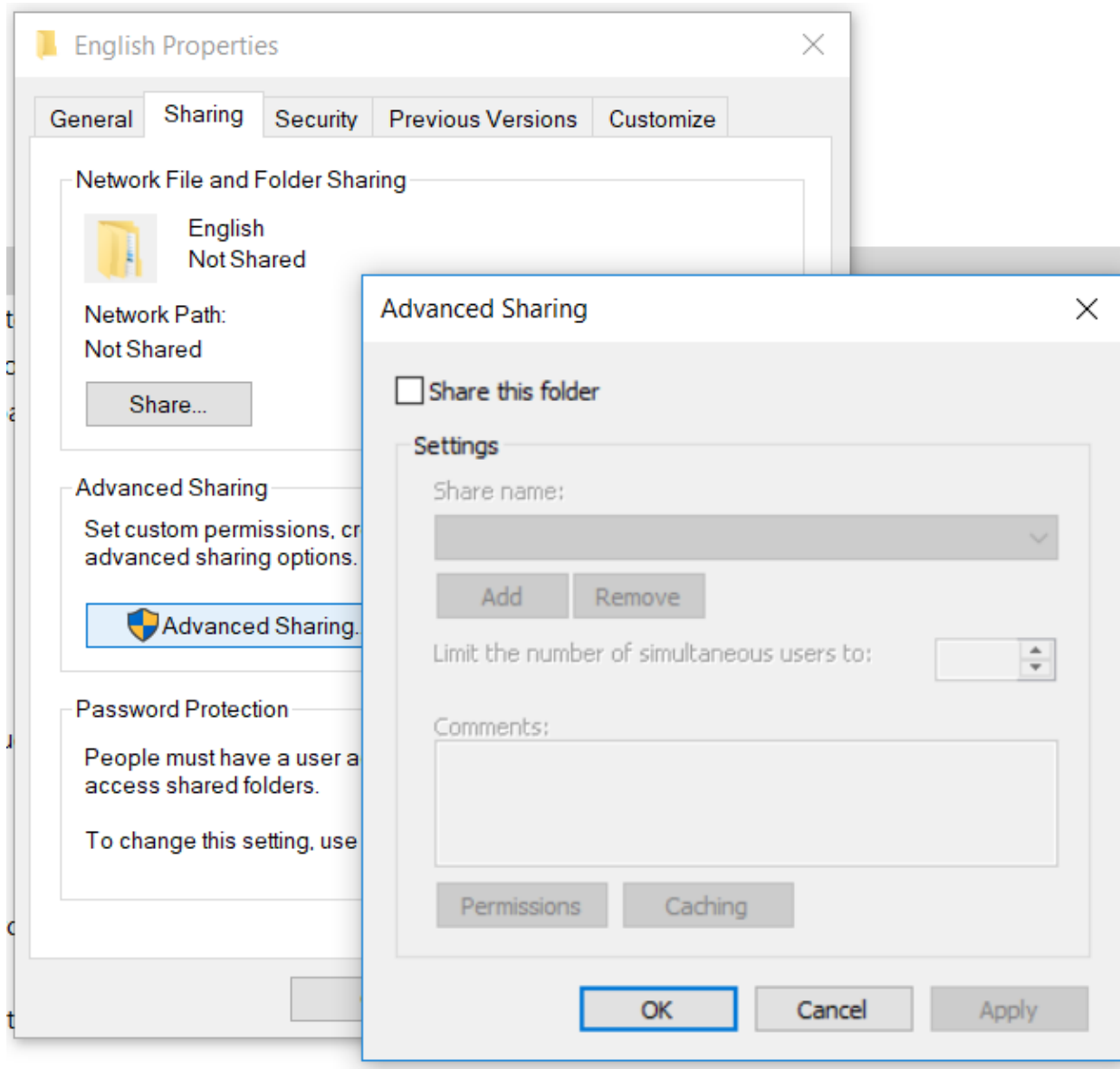
XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU



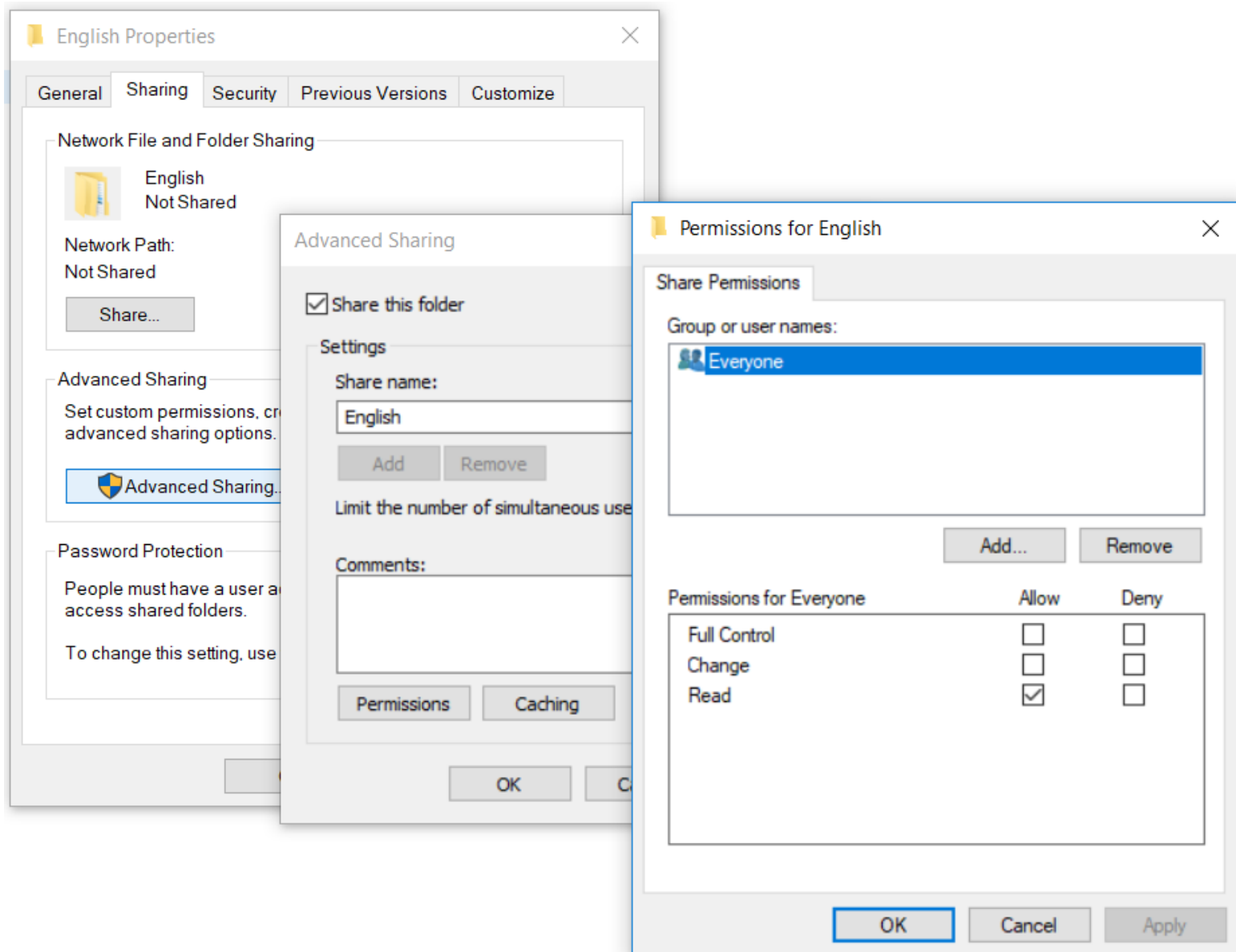
XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU



XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU



XÂY DỰNG HỆ THỐNG MẠNG TỪ ĐẦU

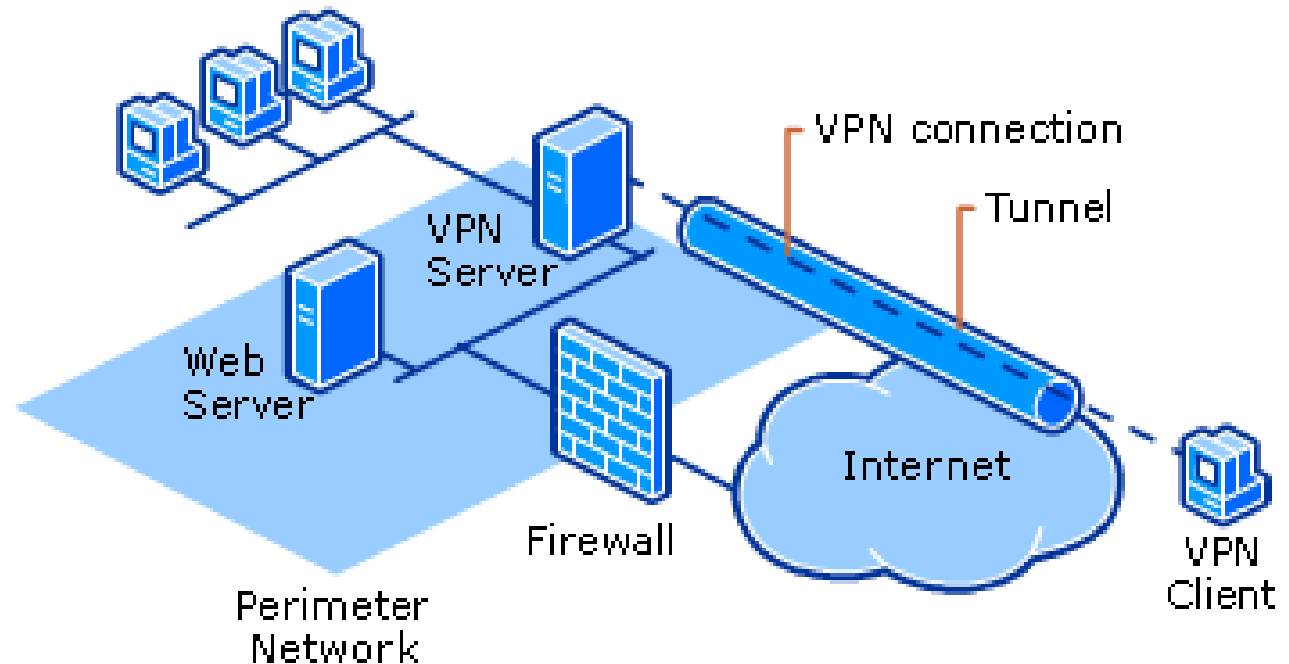


THIẾT LẬP VPN

- Virtual Private Network (VPN) cho phép các client từ xa truy xuất an toàn vào mạng LAN
- Việc thiết kế bảo đảm người dùng từ xa “trong suốt” với việc truy xuất đó để chia sẻ file, dùng máy in,...

THIẾT LẬP VPN

- VPN hoạt động trên giao thức:
 - PPTP
 - L2TP
 - IPSec
 - SSL



Network and Sharing Center



« All Control Panel Items » Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network settings

View your active networks

Forever_Love_2

Private network

Change your networking settings



Set up a new connection

Set up a broadband connection



Troubleshoot network problems

Diagnose and repair network problems

See also

HomeGroup

Infrared

Internet Options

Windows Defender Firewall

Set Up a Connection or Network

Choose a connection option



Connect to the Internet

Set up a broadband or dial-up connection to the Internet.



Set up a new network

Set up a new router or access point.



Manually connect to a wireless network

Connect to a hidden network or create a new wireless profile.



Connect to a workplace

Set up a dial-up or VPN connection to your workplace.

Next

Cancel



XÂY DỰNG HỆ THỐNG MẠNG THƯƠNG MẠI

- Việc **cấp phát cho mỗi người dùng một IP** public để truy cập trực tiếp vào Internet là việc **không thể** làm được (do khan hiếm địa chỉ)
- Khắc phục: nhóm người dùng kết nối với gateway, từ đó có kết nối trực tiếp đến Internet

XÂY DỰNG HỆ THỐNG MẠNG THƯƠNG MẠI

- Gateway là từ tổng quát chỉ thiết bị kết nối giữa mạng LAN và Internet
- Gateway:
 - một máy tính (proxy)
 - thiết bị chuyên dụng hoạt động độc lập (router)
- Proxy là phần mềm chạy trên một máy tính
- Router là thiết bị phần cứng chuyên dụng hoạt động độc lập

ROUTER

- Proxy có nhược điểm về hiệu suất hoạt động
- Router:
 - Xử lý ở mức gói tin (packet) → tốc độ xử lý vượt trội
 - Định tuyến các packet đến đúng hướng, thay vì gửi một cách mù quáng đến router kế tiếp
- Router gần như “trong suốt” đối với các client nên độ linh hoạt cao hơn

ROUTER

- Router phải có ít nhất 2 interface:
 - Kết nối đến mạng WAN (kết nối với ISP)
 - Mỗi port LAN có thể được nối vào 1 máy tính hoặc hub, switch

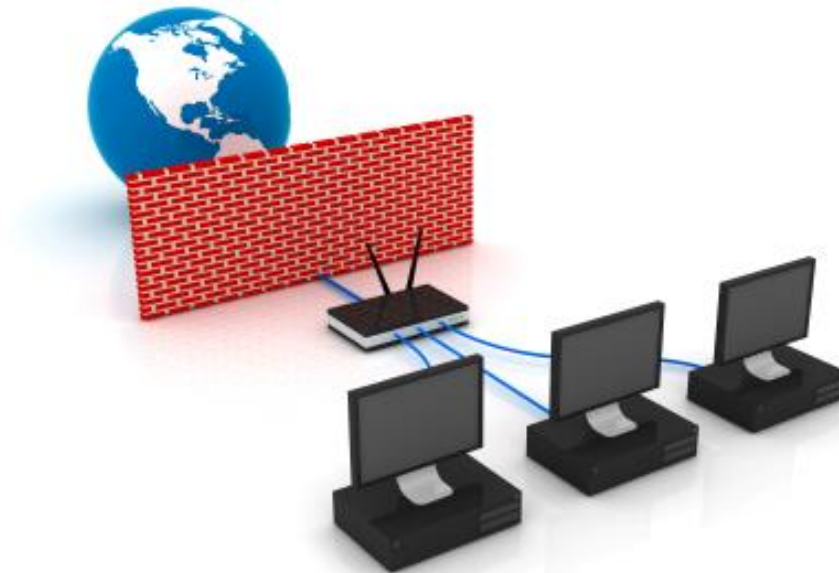


ROUTER

- Các thông tin cần nhận từ ISP:
 - Địa chỉ IP cố định được phép dùng
 - IP của default gateway
 - Subnet mask
 - Primary và secondary DNS
- Mỗi máy tính nằm sau router phải được thiết lập địa chỉ default gateway và DNS server

FIREWALL

- Thực hiện chức năng kiểm soát dòng dữ liệu đi vào và đi ra khỏi mạng LAN với tốc độ xử lý rất cao
- Có thể là phần mềm hoặc phần cứng





Customize Settings



<< Windows Defender Firewall > Customize Settings



Search Control Panel



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☐ Turn off Windows Defender Firewall (not recommended)

Public network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app




☐ Turn off Windows Defender Firewall (not recommended)

OK

Cancel

PROXY

- Phương án được xem xét nếu kinh phí ít hoặc số lượng host truy cập nhỏ
- Làm chậm tốc độ truy cập tương đối rõ
- Thiết kế bằng cách sử dụng 1 máy tính đóng vai trò proxy, chia sẻ kết nối Internet của nó cho các máy khác trong mạng
- Tất cả các máy khác cần phải biết địa chỉ IP của máy proxy

oe: Internet
up: [Ready to create](#)
ons:  Wi-Fi (Forever_Love)

a router or access point.

Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	<input type="text"/>	<input type="text"/>
Secure:	<input type="text"/>	<input type="text"/>
FTP:	<input type="text"/>	<input type="text"/>
Socks:	<input type="text"/>	<input type="text"/>

☐ Use the same proxy server for all protocols

Exceptions


Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.


OK Cancel

Internet Properties

General Security Privacy Content **Connections** Programs Advanced

 To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

 Viettel

Add... Add VPN... Remove... Settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☒ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced

☐ Bypass proxy server for local addresses

OK Cancel

LAN settings

Cancel Apply

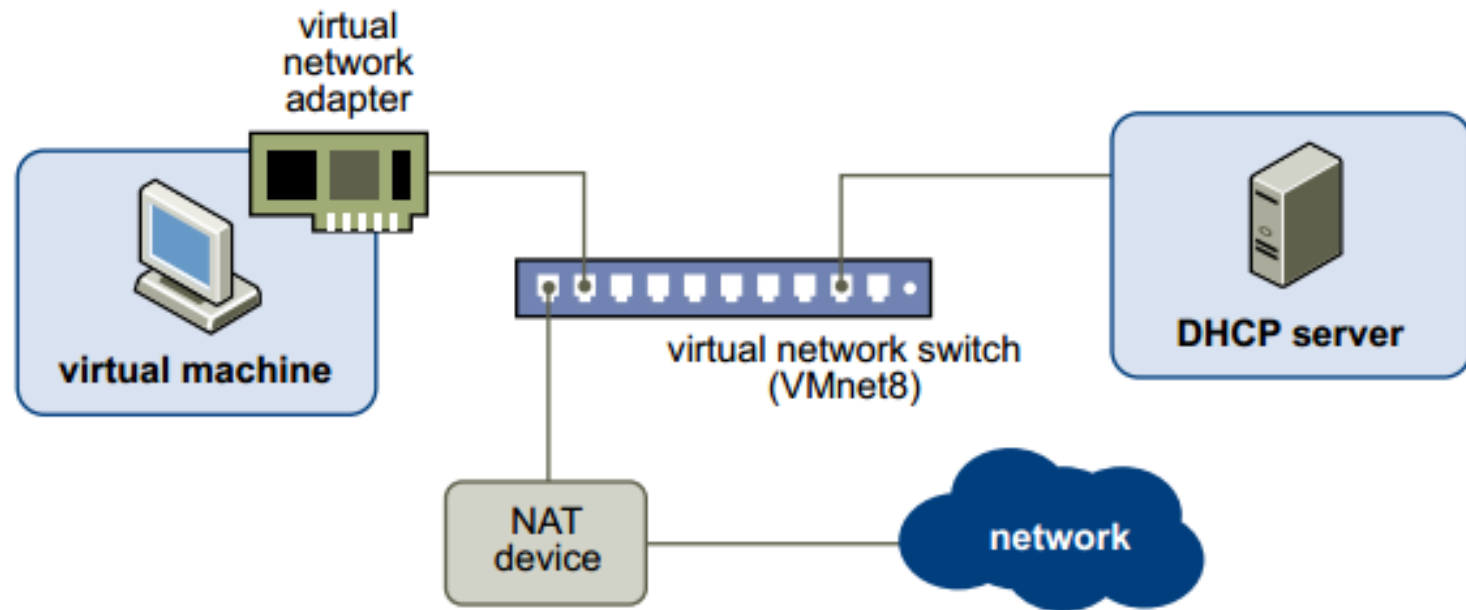
PROXY

- 2 dạng proxy:
 - Proxy mức ứng dụng: thông thường chấp nhận chỉ 1 giao thức như HTTP
 - Proxy mức mạch điện tử: có thể chấp nhận bất kỳ giao thức nào trên IP. Phổ biến là SOCKS (xem RFC 1928).

NAT

- Network address translator (NAT)
- NAT chuyển đổi địa chỉ IP từ private thành public khi gói tin đi ra khỏi mạng LAN, ghi nhận vào bảng chuyển đổi NAT
- Khi gói tin phản hồi đến, NAT sẽ tra trong bảng chuyển đổi và biết được IP private để chuyển đến đúng host bên trong

NAT



NAT

- NAT được phát triển bởi hãng CISCO, nhưng hiện đã trở thành chuẩn Internet (xem RFC 1631)
- Static NAT là kiểu mà mỗi địa chỉ private đều có địa chỉ public tương ứng → có nghĩa là mỗi máy tính đều phân biệt được đối với mạng ngoài, nhưng chưa được phép truy cập đến

NAT

- Dynamic NAT là kiểu mà mọi địa chỉ private được ánh xạ đến 1 địa chỉ public duy nhất, khác nhau bởi tham số bổ sung là local port
- NAT cần lưu thông tin gói tin đã gửi ra
- Một mạng có 100 máy có thể tạo ra 6 triệu phiên làm việc đồng thời

TUNNELING TRONG MẠNG DOANH NGHIỆP

- Nếu khách hàng đã có mạng hoạt động nhưng ứng dụng không làm việc được trên đó thì không thể bỏ qua vấn đề này được
- Tình huống:
Ứng dụng không làm việc được ở sau một firewall, thì khi đó có 3 phương án giải quyết:
 - chuyển server ra ngoài firewall
 - thiết lập port chuyển qua tunnel đến firewall (hoặc router)
 - dữ liệu được đưa lên một máy chủ proxy để tránh firewall

PROXY TUNNELING

- Không giống như router, các proxy không ‘trong suốt’ đối với client
- Cần phải chỉnh sửa code để tham chiếu đến proxy
- Khai báo và sử dụng proxy thông qua lớp WebProxy và HTTPWebRequest

PROXY TUNNELING

```
WebProxy myProxy= new WebProxy("proxyserver",8080);  
myProxy.BypassProxyOnLocal = true;  
String url = "http://www.yahoo.com";  
HttpWebRequest request =  
(HttpWebRequest)HttpWebRequest.Create(url);  
request.Proxy = myProxy;
```

FIREWALL TUNNELING

- Nếu firewall được thiết lập block tất cả các cổng thì có thể thay đổi firewall cho phép truy cập vào cổng yêu cầu
- Một số router cho phép thiết lập cổng được chuyển dữ liệu thẳng mà không qua firewall

FIREWALL TUNNELING

Tổng quát:

- Nếu không muốn truy cập vào firewall hoặc muốn cung cấp một giải pháp thân thiện người dùng thì ràng buộc dữ liệu trên 1 proxy.
- Máy tính ở sau firewall sẽ mở kết nối TCP với proxy, dữ liệu từ client đến proxy được chuyển qua kết nối đó.
- Đây là kỹ thuật mà các ứng dụng Instant Messenger dùng.

PHÒNG TRÁNH

- Phòng tránh luôn luôn là cách tốt hơn để xảy ra sự cố rồi mới tìm cách chữa trị
- Một số vấn đề:
 - Xung đột port
 - Vấn đề cấp phát IP động

XUNG ĐỘT PORT

- Nếu phần mềm không thể chạy trên port mặc định → nghĩ đến việc chuyển sang port khác, hoặc nhắc nhở cho người dùng chuyển sang port khác. Nếu không ta có thể gặp 2 vấn đề:
 - Người dùng sẽ không muốn ngừng phần mềm dùng trùng port
 - Firewall có thể đã được thiết lập để cho phép lưu thông qua một số port

XUNG ĐỘT PORT

- Các client đang chờ kết nối vào ứng dụng cần phải biết port đã thay đổi → cần hiển thị hộp thoại và cho phép người dùng nhập vào port mới, hoặc có thể dùng 1 DNS request để biết server đang lắng nghe trên port nào

VẤN ĐỀ CẤP PHÁT IP ĐỘNG

- Đây là vấn đề thường gặp phải
- Các ứng dụng thường mắc sai lầm là giả định địa chỉ IP cục bộ tĩnh trong suốt hoạt động của nó
- Cách giải quyết là dùng cơ chế theo dõi IP
- Phần mềm “No IP” có thể dùng kiểu ánh xạ một địa chỉ IP động từ DNS name
- Khi post 1 địa chỉ IP cần bảo đảm là địa chỉ public. Địa chỉ như 192.168.0.1 cho client không phải là ý tưởng tốt đối với thế giới bên ngoài

BÀI TẬP

- Đọc và nghiên cứu các tài liệu về RFC được giới thiệu trong chương
- Vận dụng khả năng cài đặt hệ thống ảo trên máy tính để hiện thực cơ chế hoạt động của các thiết bị router, firewall,...