

CHƯƠNG 2:

QUẢN TRỊ VẬN HÀNH HẠ TẦNG MẠNG

LAN-WAN-VLAN

Trình bày: Bùi Minh Quân

Email: bmquan@cit.ctu.edu.vn

Nội dung

- ❖ Bộ giao thức liên mạng
- ❖ LAN-WAN-VLAN
 - ❑ Qui trình thiết kế mạng PPDIOO – Cisco
 - ❑ Kỹ thuật thiết kế mạng phân cấp
 - ❑ Kỹ thuật mạng ảo (Vlan)
- ❖ Bài tập:
 - ❑ Phân tích mô hình mạng
 - ❑ Cấu hình thiết bị: switch, router

Bộ giao thức liên mạng (Internet Protocol Suite)

- ☐ Được phát triển bởi một dự án của Bộ quốc phòng Mỹ vào những năm 1970
- ☐ Liên nối kết các máy tính Unix, các mạng không đồng bộ thành một mạng của các mạng – ARPANET
- ☐ Mô hình của mạng TCP/IP hay mạng Internet
- ☐ Cung cấp dịch vụ truyền tải điểm cuối - điểm cuối qua một liên mạng
- ☐ Cung cấp các ứng dụng dạng client-server: làm việc từ xa, truyền tải file, chia sẻ tập tin, ...

Mạng TCP/IP

OSI Model

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

TCP/IP Model

5	Application
4	Transport Control Protocol (TCP) User Datagram Protocol (UDP)
3	Internet Protocol (IP)
2	Data Link
1	Physical

Giao thức IP

- ❖ Hoạt động ở tầng 3 của mô hình OSI
- ❖ Liên nối kết nhiều mạng cục bộ không đồng nhất
- ❖ Đảm bảo truyền tải các gói tin từ máy tính tới máy tính
- ❖ Vạch đường và chuyển tiếp các gói tin qua liên mạng
- ❖ Sử dụng địa chỉ IP để nhận dạng máy tính
 - ❑ Version 4: 32 bits
 - ❑ Version 6: 128 bits

Giao thức TCP & UDP

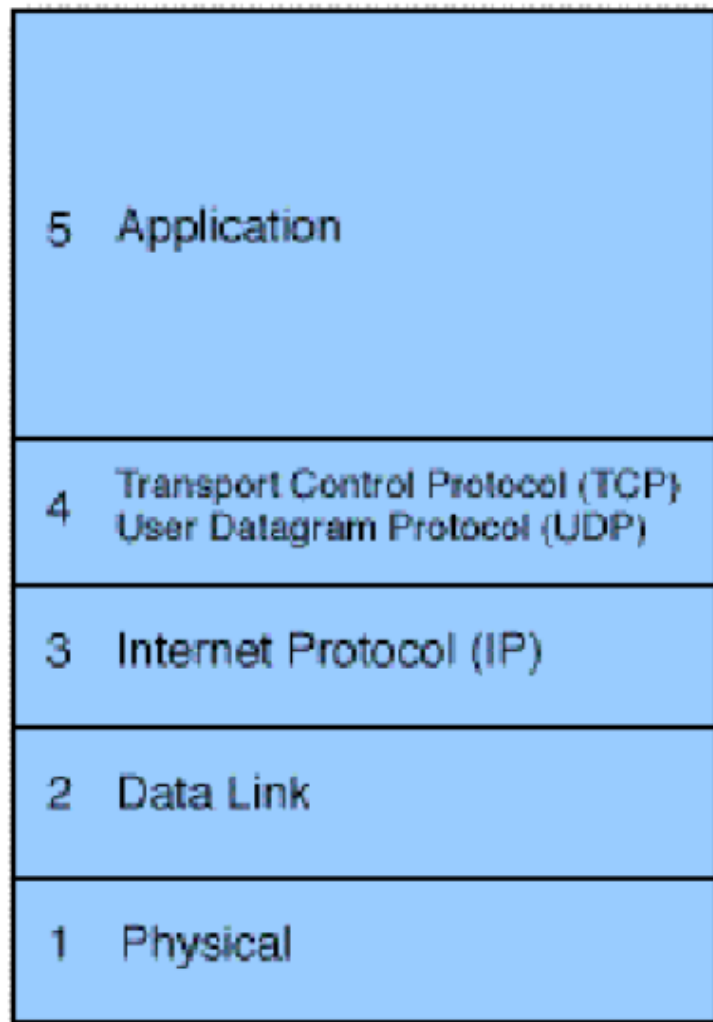
- ❖ Hoạt động ở tầng 4 trong mô hình OSI
- ❖ Đảm bảo truyền tải dữ liệu từ tiến trình đến tiến trình
 - ❑ TCP (Transport Control Protocol): có nối kết
 - ❑ UDP (User Datagram Protocol): không nối kết
- ❖ Cung cấp dịch vụ vận chuyển cho tầng ứng dụng thông qua Socket
 - ❑ Mỗi socket có một số hiệu cổng (port)
 - ❑ (IP,Port) địa chỉ gửi/nhận thông tin của một ứng dụng

Ứng dụng cơ bản trên TCP/IP

- ❖ Telnet: Đăng nhập và làm việc từ xa
- ❖ DNS (Domain Name Service): Phân giải tên miền
- ❖ FTP (File Transfer Protocol): Truyền tải tập tin
- ❖ NFS (Network File System): Tập tin trên mạng
- ❖ SMTP (Simple Mail Transfer Protocol): Gởi thư điện tử
- ❖ POP(Post Office Protocol): Nhận thư điện tử
- ❖ IMAP (Internet Mail Access Protocol): Nhận thư điện tử
- ❖ HTTP (Hyper-Text Transter Protocol): Dịch vụ Web

Cài đặt mạng TCP/IP

TCP/IP Model



Công việc thực hiện

Cài đặt các gói phần mềm được phát triển bởi các nhà phát triển ứng dụng độc lập.

Một giao thức ứng dụng có nhiều phần mềm:

- Web Server: Apache, Https, IIS
- Web client: Firefox, IE, Opera, Safari

Cài đặt và cấu hình các giao thức TCP/IP trên hệ điều hành: Unix, Linux, Windows, Netware, Mac OS.
Cấu hình Router.

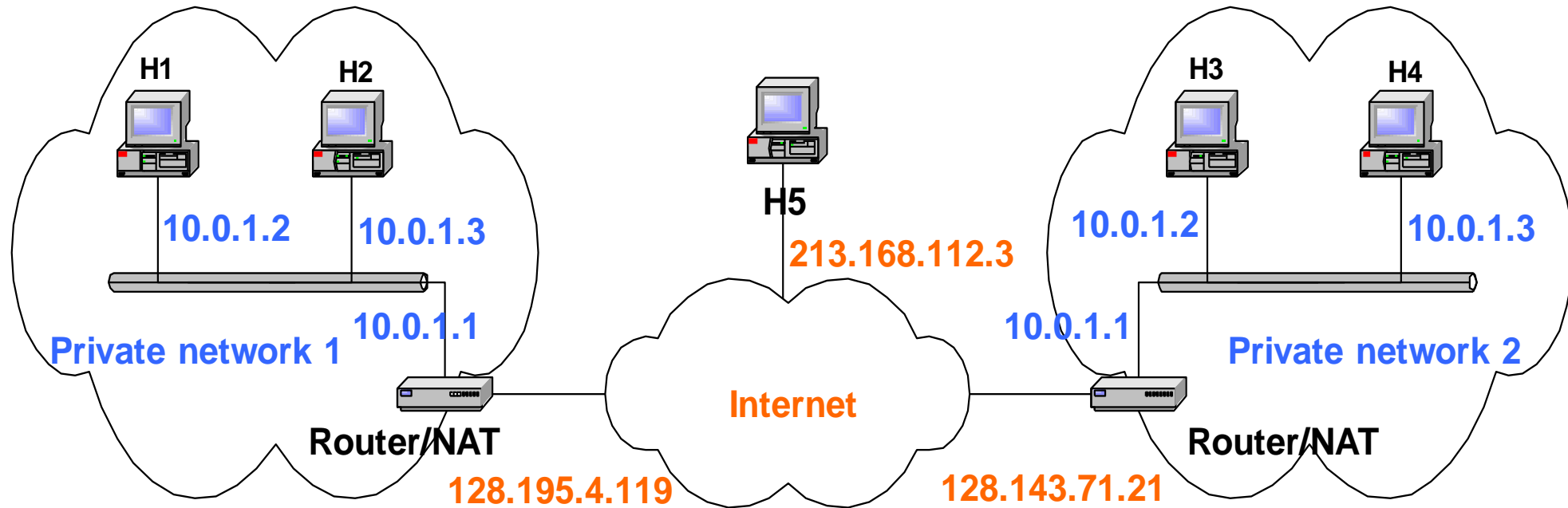
Cài đặt mạng cục bộ theo các chuẩn Ethernet, Fast Ethernet, Giga Ethernet, Token ring
Các thiết bị: NIC, dây dẫn, đầu nối, HUB, Switch

IP Private và Public

- ❖ Kết nối trực tiếp vào mạng internet phải có địa chỉ Public
- ❖ Do sự thiếu hụt của IPv4 Public
- ❖ Địa chỉ private được sử dụng trong các mạng riêng
 - ❑ 10.0.0.0/8
 - ❑ 172.16.0.0/16 - 172.31.0.0/16
 - ❑ 192.168.0.0/24 - 192.168.255.0/24
- ❖ Một IP riêng được ánh xạ tới một Public IP, khi máy tính phải truy cập vào Internet. Sử dụng kỹ thuật NAT

NAT (Network Address Translation)

(private IP, private port) <-> (public IP, public port)



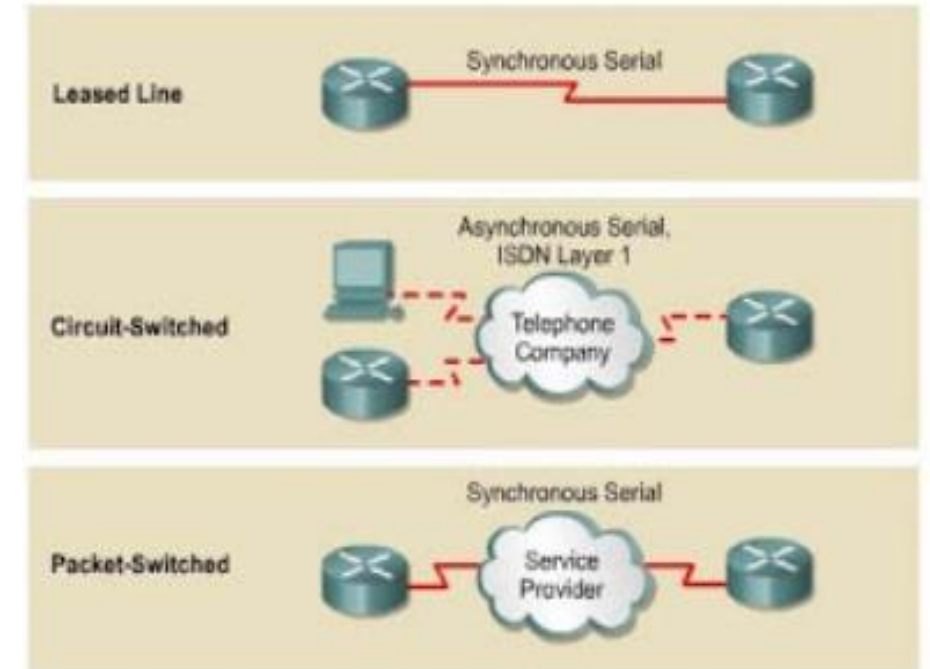
CÔNG NGHỆ MẠNG WAN

Công nghệ Wan

- ❖ ISDN
- ❖ Lease Line
- ❖ X25
- ❖ Frame Relay
- ❖ ATM
- ❖ DSL (Digital Subscriber Line): kênh thuê bao số

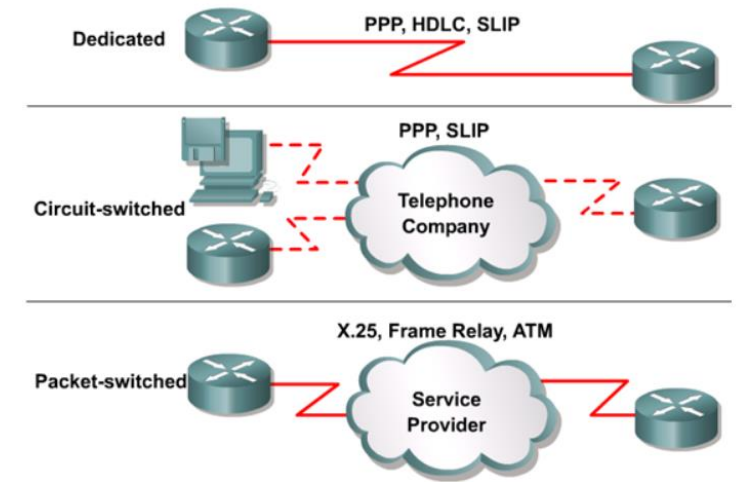
Công nghệ mạng Wan

- WAN sử dụng nhiều kỹ thuật khác nhau để thực hiện truyền dữ liệu qua một vùng địa lý rộng lớn.
- WAN thường được thuê từ nhà cung cấp dịch vụ.
- Các loại kết nối WAN như sau:
 - Kết nối thuê kênh riêng
 - Kết nối chuyển mạch - mạch
 - Kết nối chuyển mạch gói



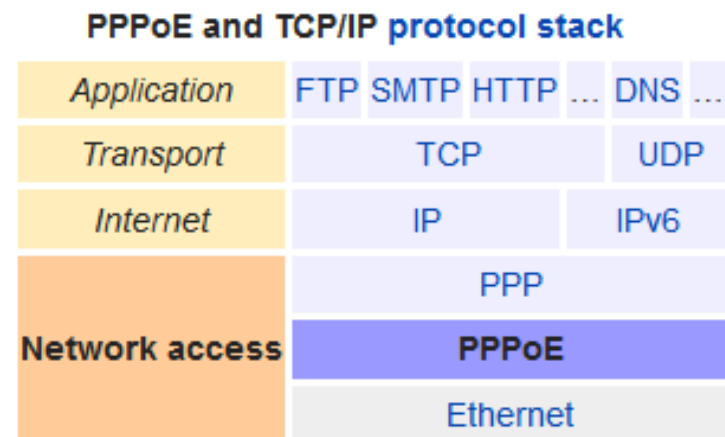
Công nghệ mạng Wan

- ❖ Kiểu đóng gói dữ liệu trên WAN:
 - ❑ HDLC (High-Level Data Link Control Protocol)
 - ❑ PPP (Point-to-Point Protocol)
 - ❑ SLIP (Serial Line Internet Protocol)
 - ❑ X.25/LAPB (Link Access Procedure for D-channel)
 - ❑ Frame Relay
 - ❑ ATM (Asynchronous Transfer Mode). (Cell switching)
 - ❑ ISDN (Integrated Services Digital Network)



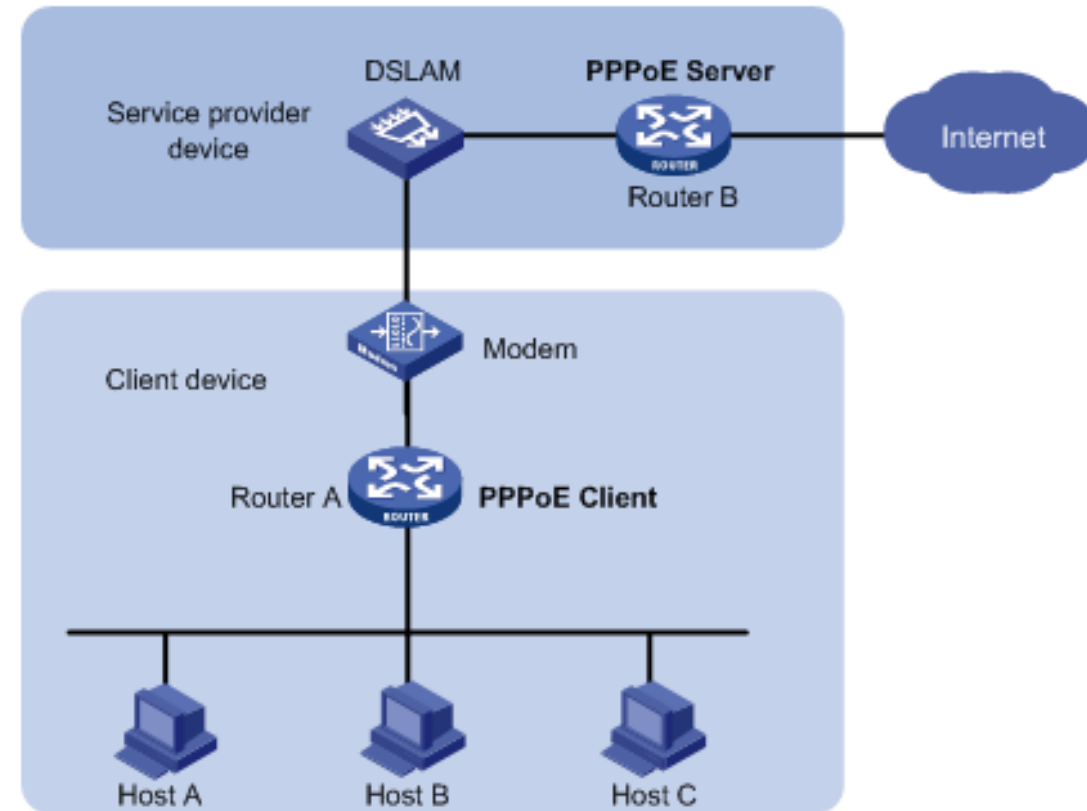
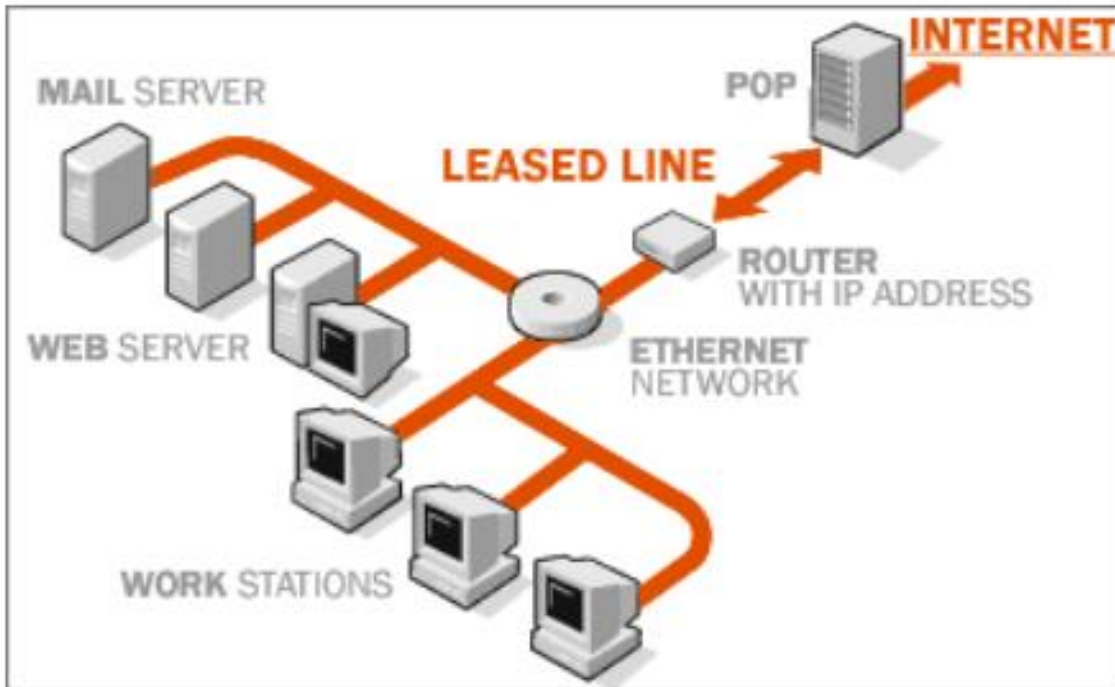
Point to Point Protocol (PPP)

- ❖ PPP: là một giao thức liên kết dữ liệu, thường được dùng để thiết lập một kết nối trực tiếp giữa 2 nút mạng như: router-to-router và host-to-network
- ❖ PPP cung cấp cơ chế xác thực Password Authentication Protocol (PAP) và Challenge Handshake Authentication Protocol (CHAP) và mã hóa việc truyền dữ liệu.
- ❖ Hai kiểu đóng gói dữ liệu của **PPP**:
 - ❑ **PPPoE** (Point-to-Point Protocol over Ethernet)
 - ❑ **PPPoA** (Point-to-Point Protocol over ATM)



Sự khác biệt internet Leased line và FTTH?

DSLAM (Digital Subscriber Line Access Multiplexor)



<http://maychuaoc.com.vn/su-khac-biet-internet-leased-line-voi-ftth/>

GIỚI THIỆU QUY TRÌNH THIẾT KẾ MẠNG LAN

Giới thiệu quy trình thiết kế mạng LAN

❖ PPDIOO là quy trình thiết kế mạng gồm 6 bước:

- ❑ Chuẩn bị (Prepare)
- ❑ Lập kế hoạch (Plan)
- ❑ Thiết kế (Design)
- ❑ Triển khai (implement)
- ❑ Vận hành (Operate)
- ❑ Tối ưu hóa (Optimize)

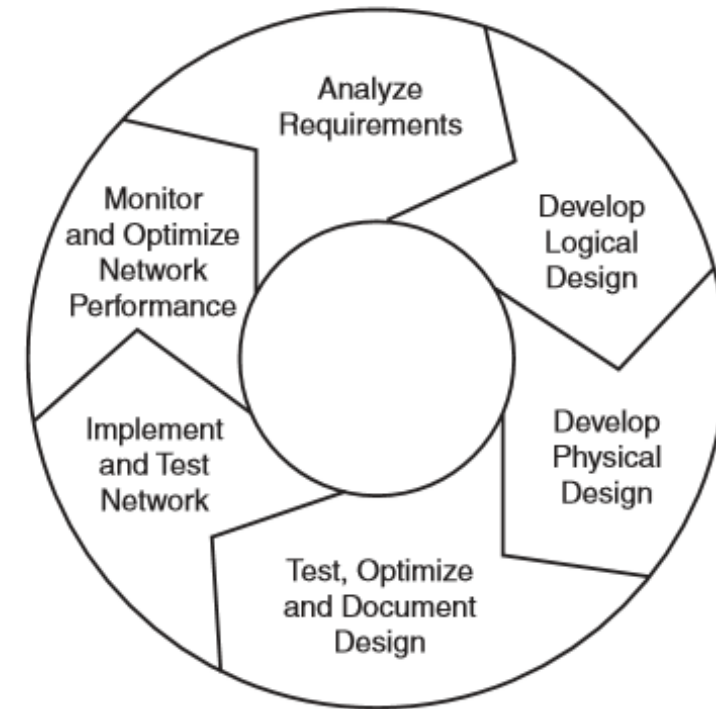


Figure 1-1 *Network Design and Implementation Cycle*

Giới thiệu quy trình thiết kế mạng LAN

❖ Chuẩn bị (Prepare):

- ❑ Thu thập thông tin về yêu cầu: yêu cầu người sử dụng, người điều hành và người quản lý hệ thống.
- ❑ “Quan sát địa hình thực tế” những nơi mạng sẽ đi qua
- ❑ Khả năng mở rộng và phát triển hạ tầng của đơn vị
- ❑ Phân tích đánh giá và chọn lọc ra những công nghệ thích hợp cho hệ thống mạng
- ❑ Đề xuất những mô hình phát thảo ban đầu

Giới thiệu quy trình thiết kế mạng LAN

❖ Lập kế hoạch (Plan):

□ Trong phần lên kế hoạch, cần sử dụng những bước sau:

- Lên kế hoạch mua các thiết bị mạng
- Lên kế hoạch cài hệ điều hành mạng và các ứng dụng
- Lên kế hoạch lập bảng báo giá
- Lên kế hoạch lập bản hợp đồng
- Lên kế hoạch lập bản thanh lý hợp đồng

Giới thiệu quy trình thiết kế mạng LAN

❖ Thiết kế (Design)

□ Bước này bao gồm các công việc:

- Thiết kế lớp ứng dụng và dịch vụ mạng
- Lựa chọn công nghệ mạng
- Quy hoạch địa chỉ IP
- Thiết kế về mặt định tuyến
- Thiết kế kiến trúc bảo mật
- Thiết kế hạ tầng mạng
- Thiết kế mô hình vật lý
- Thiết kế hệ thống tài liệu

Giới thiệu quy trình thiết kế mạng LAN

❖ Triển khai (implement)

- ☐ Cài đặt và cấu hình các thiết bị mới (hoặc nâng cấp, thay thế thiết bị đối với hạ tầng mạng đã có) phù hợp với những thiết kế đã quy định.
- ☐ Ghi chép các công việc đã thực hiện, thời gian thực hiện
- ☐ Lưu trữ dự phòng thông tin cấu hình
- ☐ Sẵn sàng khôi phục lại cấu hình khi có sự cố xảy ra

Giới thiệu quy trình thiết kế mạng LAN

❖ Vận hành (Operate)

- ❑ Quy trình này được tiến hành mỗi ngày nhằm đảm bảo sự vận hành liên tục của hệ thống.
- ❑ Các công việc cần thực hiện:
 - Giám sát các thành phần mạng
 - Duy trì hoạt động ổn định của hệ thống
 - Giám sát hiệu suất hoạt động mạng
 - Phát hiện và xử lý các sự cố phát sinh
 - Cung cấp thông tin cho qui trình tối ưu hóa.

Giới thiệu quy trình thiết kế mạng LAN

❖ Tối ưu hóa (Optimize)

- ☐ Xác định và thiết lập các thông số cải tiến hệ thống
- ☐ Xác định các ưu tiên cần cải tiến hệ thống.
- ☐ Xử lý sự cố, tối ưu hóa hệ thống.
- ☐ Có thể đề xuất thiết kế lại mạng mới nếu trong quá trình sử dụng có vấn đề về hệ thống hay phát sinh lỗi hoặc không đáp ứng được nhu cầu.

Vòng đời của quy trình PDIOO

- ❖ Nghỉ hưu (Retire): Khi mạng, hoặc một phần của mạng, đã lỗi thời, không còn sản xuất hoặc hỗ trợ từ nhà sản xuất
- ❖ Nghỉ hưu là giai đoạn không nằm trong vòng đời (PDIOO), tuy nhiên đây là một giai đoạn quan trọng. Giai đoạn nghỉ hưu bao trùm đến giai đoạn kế hoạch.
- ❖ Vòng đời PDIOO được lặp lại khi có yêu cầu về phát triển hệ thống mạng.

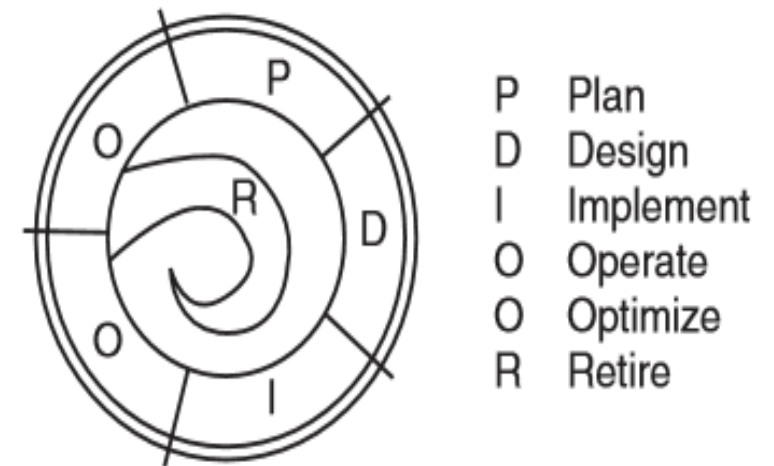


Figure 1-2 PDIOO Network Life Cycle

Phân tích và cân bằng các mục tiêu kỹ thuật

- ❖ Phân tích và cân bằng các mục tiêu kỹ thuật cho thiết kế.
- ❖ Các mục tiêu kỹ thuật điển hình bao gồm:
 - ☐ Khả năng mở rộng (scalability)
 - ☐ Tính sẵn sàng (availability)
 - ☐ Hiệu suất mạng (network performance)
 - ☐ Bảo mật (security)
 - ☐ Khả năng quản lý (manageability)
 - ☐ Tính dễ sử dụng (usability)
 - ☐ Khả năng thích ứng (adaptability)
 - ☐ Khả năng chi trả (affordability)

Tạo sự cân bằng trong thiết kế mạng

Mục tiêu kỹ thuật	Phần trăm
Khả năng mở rộng (scalability)	20
Tính sẵn sàng (availability)	30
Hiệu suất mạng (network performance)	15
Bảo mật (security)	5
Khả năng quản lý (manageability)	5
Tính dễ sử dụng (usability)	5
Khả năng thích ứng (adaptability)	5
Hiệu quả chi phí (affordability)	15
Tổng	100

KỸ THUẬT THIẾT KẾ MẠNG PHÂN CẤP

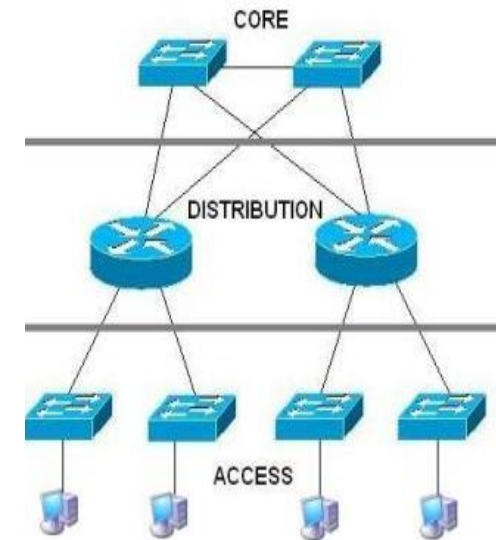
Kỹ thuật thiết kế mạng phân cấp

- ❖ Mô hình thiết kế mạng phân cấp (hierarchical network design) giúp phát triển một topology dưới dạng các lớp rời rạc.
- ❖ Mỗi lớp tập trung vào các chức năng cụ thể, cho phép chọn ra các hệ thống và đặc tính phù hợp
- ❖ Mô hình cisco giới thiệu có 3 lớp:
 - ❑ Core layer
 - ❑ Distribution layer
 - ❑ Access layer

Đặc trưng kỹ thuật của lớp core

❖ Lớp lõi (core):

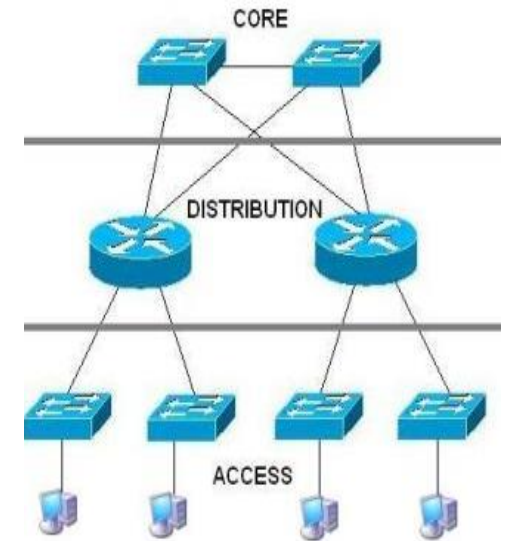
- ☐ Thiết bị có hiệu năng và tính sẵn sàng cao: tốc độ cao, độ trễ nhỏ, ổn định
- ☐ Định tuyến ra internet
- ☐ Core có thể dùng thiết bị: router hoặc switch
- ☐ Kết nối thiết bị lớp phân phối.



Đặc trưng kỹ thuật của lớp Distribution

❖ Lớp phân phối (Distribution):

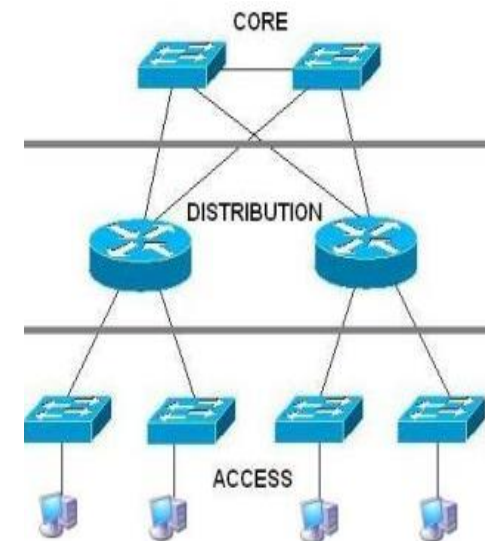
- ☐ Thiết lập chính sách an ninh mạng
- ☐ Kiểm soát lưu lượng
- ☐ Xác định miền quảng bá
- ☐ Định tuyến giữa các Vlan
- ☐ Tập hợp cho các thiết bị lớp Access
- ☐ Kết nối vào lớp Core
- ☐ Thiết bị sử dụng: router hoặc switch
- ☐ Trong các mô hình nhỏ có thể kết hợp lớp core và distribution.



Đặc trưng kỹ thuật của lớp Access

❖ Lớp phân phối (Access):

- ❑ Cung cấp truy cập mạng cho thiết bị đầu cuối: máy tính, máy in .v.v.
- ❑ Thiết bị sử dụng: switch layer 2 cấu hình thấp, access point
- ❑ Kết nối vào thiết bị lớp Distribution



Kỹ thuật thiết kế mạng phân cấp

- ❖ Ưu điểm mô hình:
 - ☐ Tiết kiệm chi phí
 - ☐ Dễ triển khai
 - ☐ Có khả năng mở rộng mạng
 - ☐ Dễ quản lí, khắc phục sự cố

VIRTUAL LAN

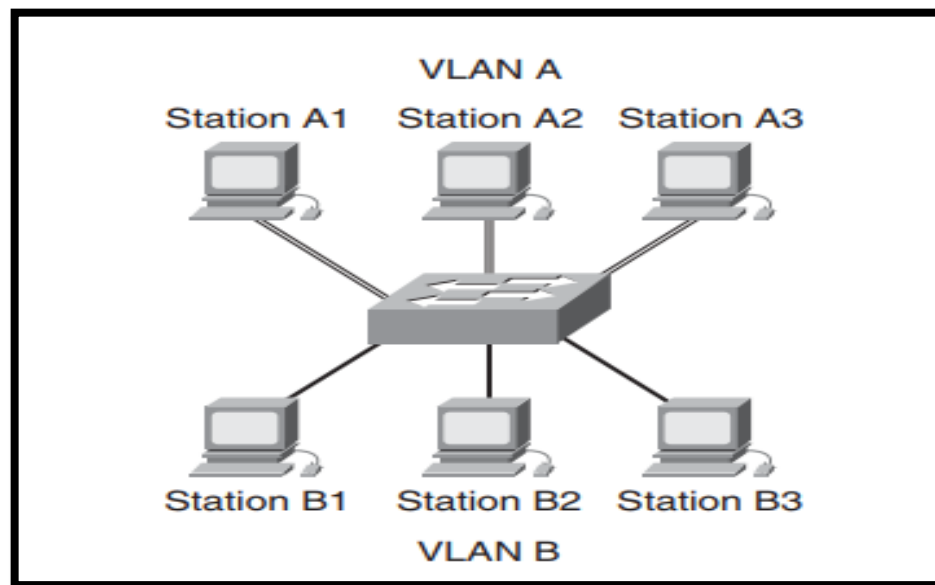
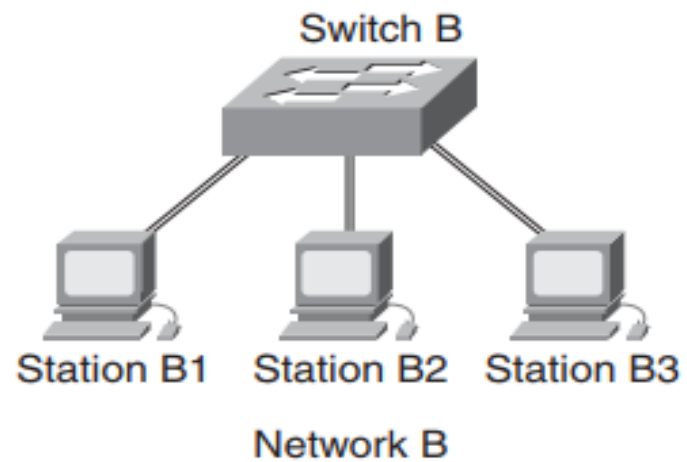
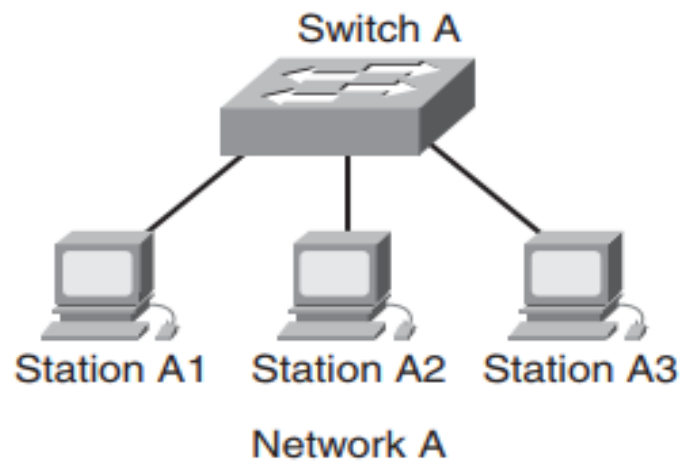
Mạng Lan ảo (Virtual LAN)

- ❖ Thiết kế mạng phải đảm bảo vùng đụng độ (*collision domain*) và vùng quảng bá (broadcast domains) càng nhỏ càng tốt.
- ❖ Các thiết bị nối vào Hub được xem cùng vùng đụng độ
- ❖ Một cổng của Switch là một vùng đụng độ, mặc định Switch không chia được vùng quảng bá.
- ❖ Một cổng của router là một vùng quảng bá
- ❖ Với kỹ thuật Vlan, switch chia được vùng quảng bá

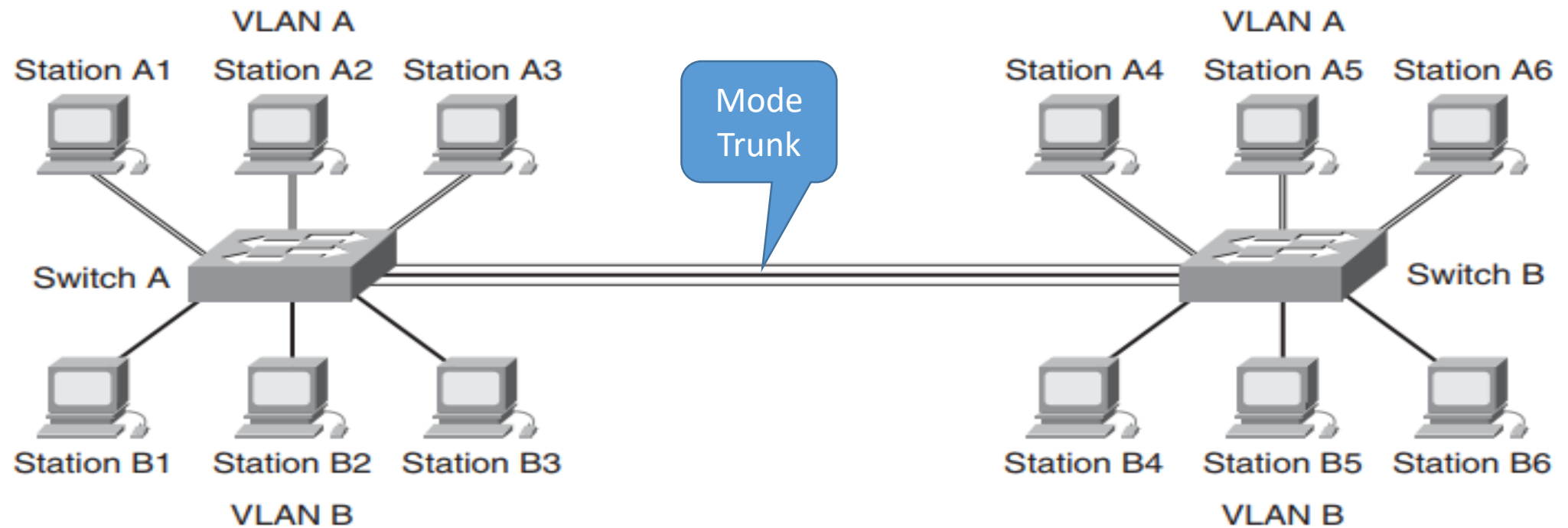
Mạng Lan ảo (Virtual LAN)

- ❖ Vlan là giải pháp truyền dữ liệu theo chuẩn LAN nhưng không bị hạn chế bởi các ràng buộc vật lý.
- ❖ Việc gán vào VLAN dựa trên nhu cầu ứng dụng, bảo mật, hiệu năng hay một đặc thù nào đó. Bất chấp vị trí vật lý của người dùng
- ❖ VLAN xuyên qua nhiều physical LAN
- ❖ Nhiều VLAN trên một physical LAN

Thiết kế VLAN

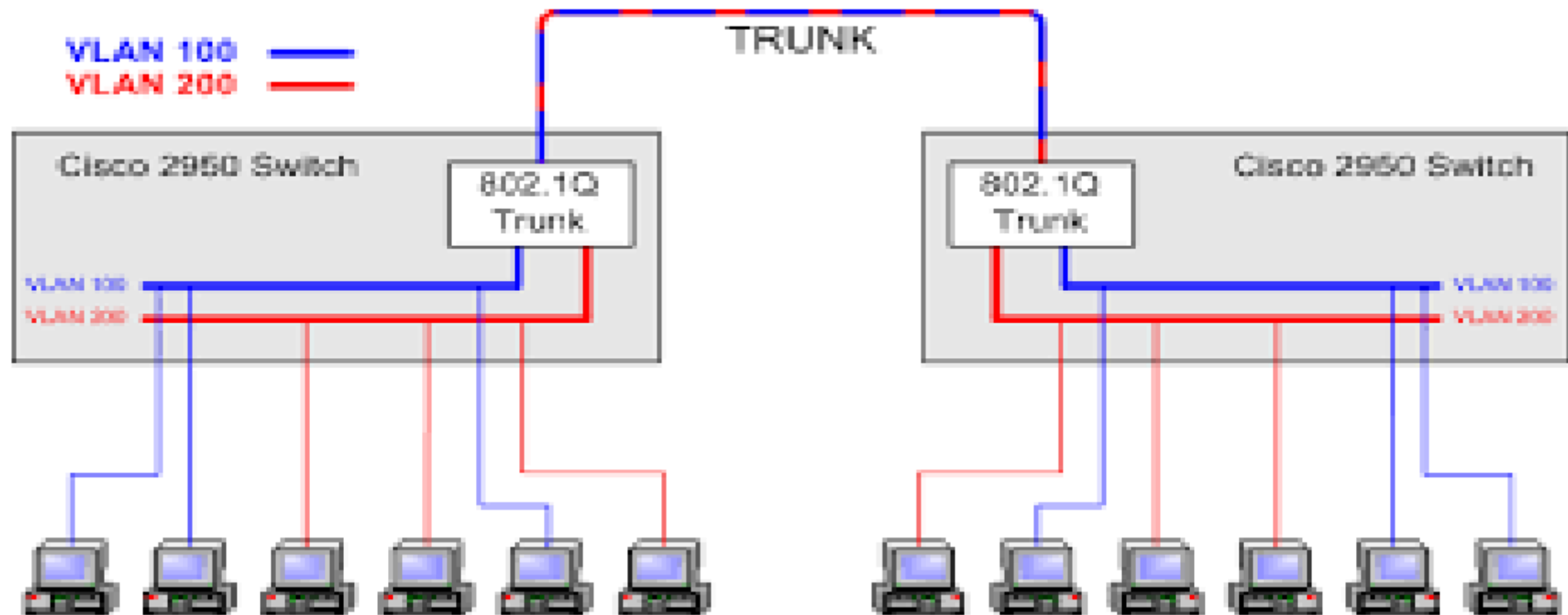


Thiết kế VLAN

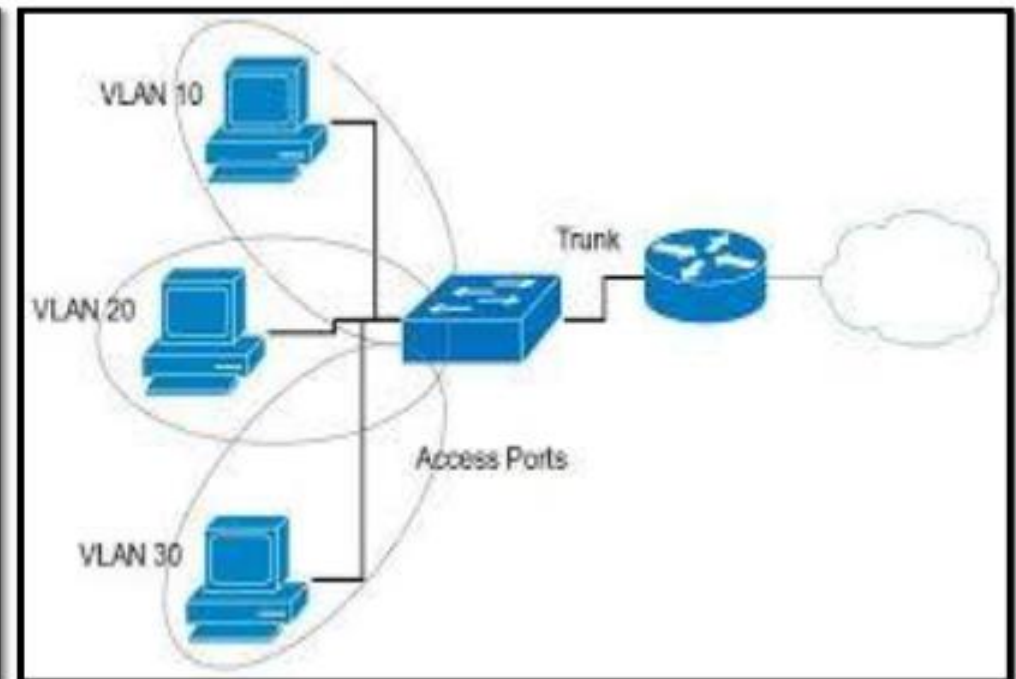
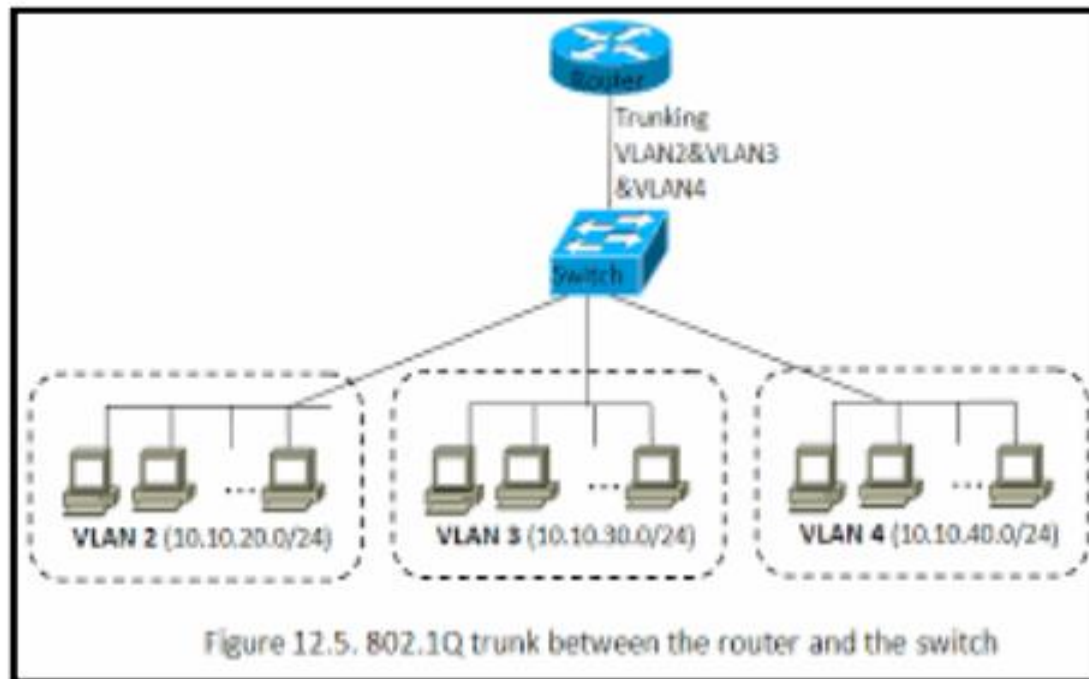
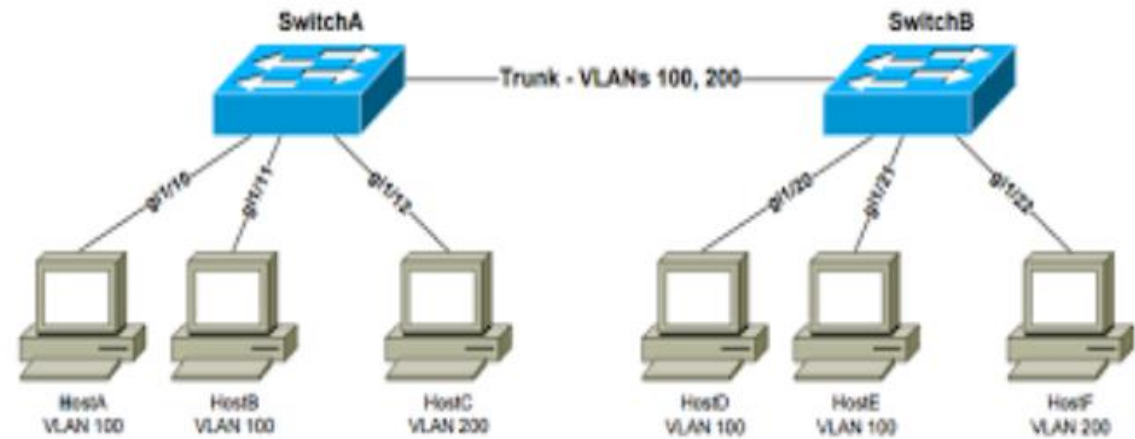


Vlan qua nhiều Switch

Mode trunk

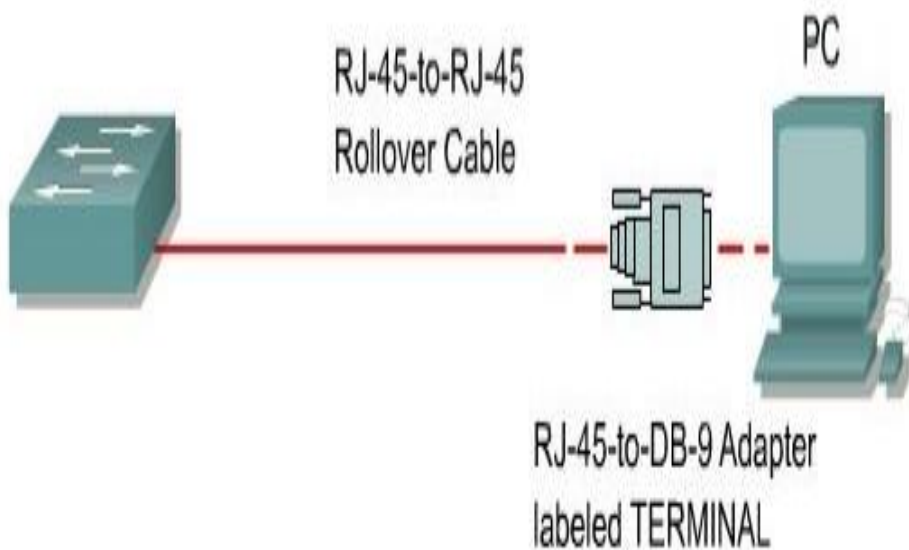


Mode trunk

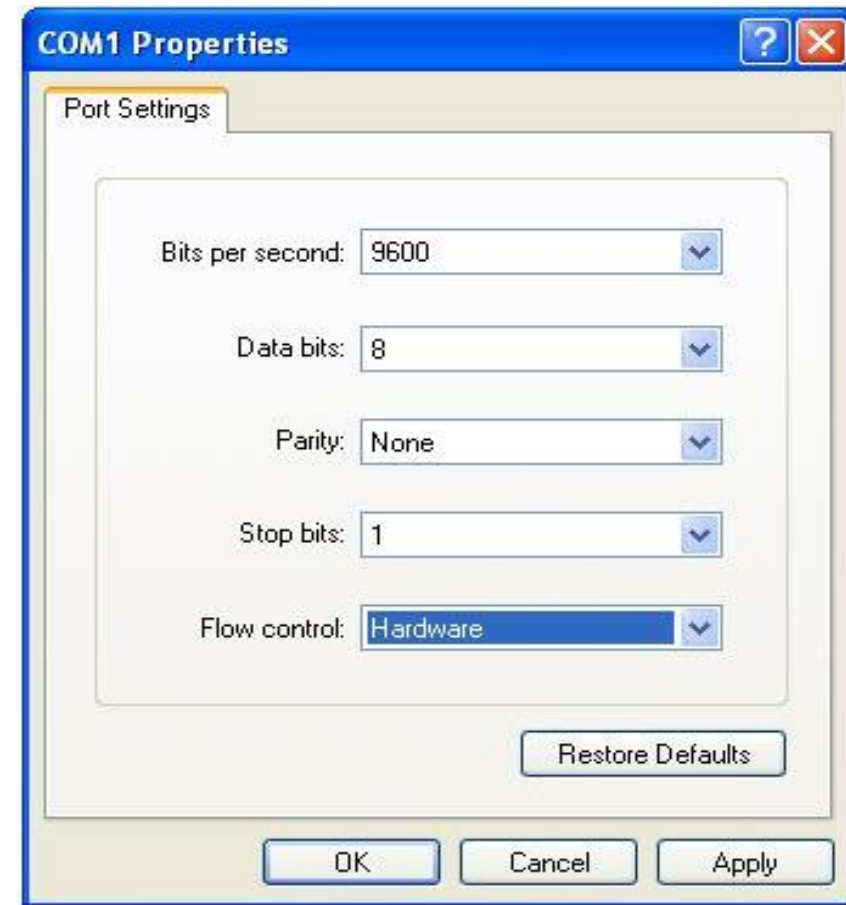


Cấu hình Switch và Router

Device with Console



Kết nối switch đến máy tính



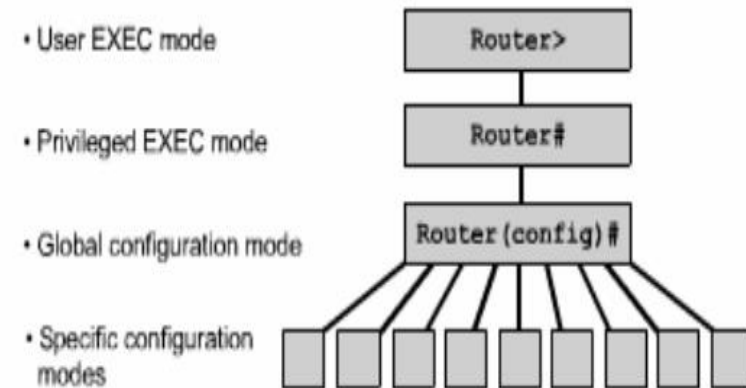
Cài đặt thông số cho Hyper Terminal

Cấu hình Switch và Router

❖ Chế độ giao tiếp dòng lệnh CLI

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fast
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Switch#write me
Switch#write memory
Building configuration...
[OK]
Switch#
```



Configuration Mode	Prompt
Interface	Router (config-if)#
Subinterface	Router (config-subif)#
Controller	Router (config-controller)#
Map-list	Router (config-map-list)#
Map-class	Router (config-map-class)#
Line	Router (config-line)#
Router	Router (config-router)#
IPX-router	Router (config-ipx-router)#
Route-map	Router (config-route-map)#

Cấu hình Switch và Router

Console Password

```
Router(config)#line console 0  
Router(config-line)#login  
Router(config-line)#password cisco
```



Virtual Terminal Password

```
Router(config)#line vty 0 4  
Router(config-line)#login  
Router(config-line)#password cisco
```



Enable Password

```
Router(config)#enable password san-fran
```

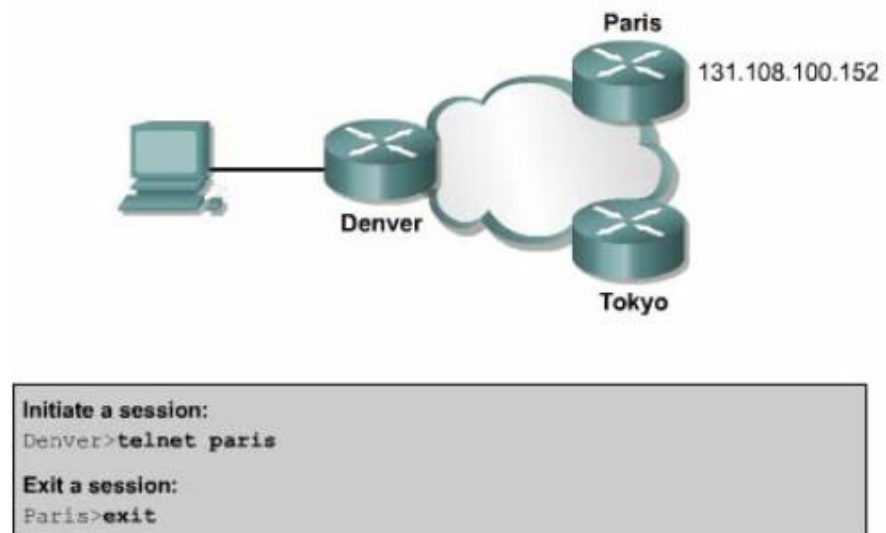
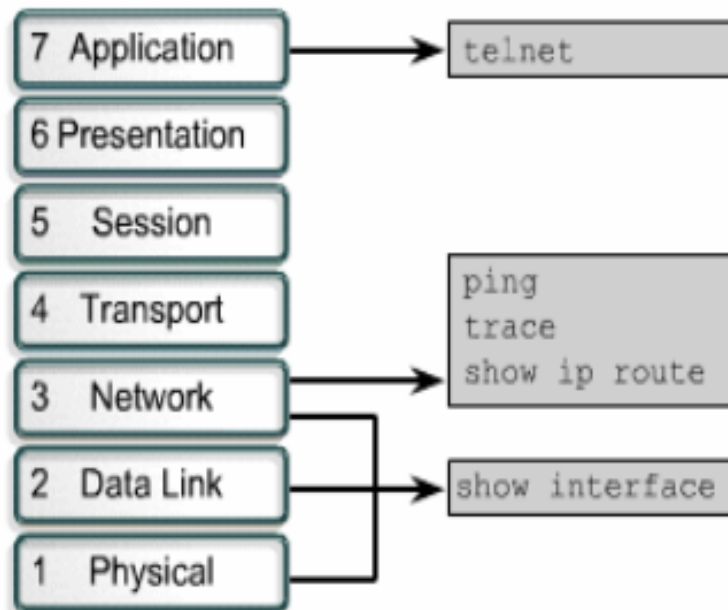


Perform Password Encryption

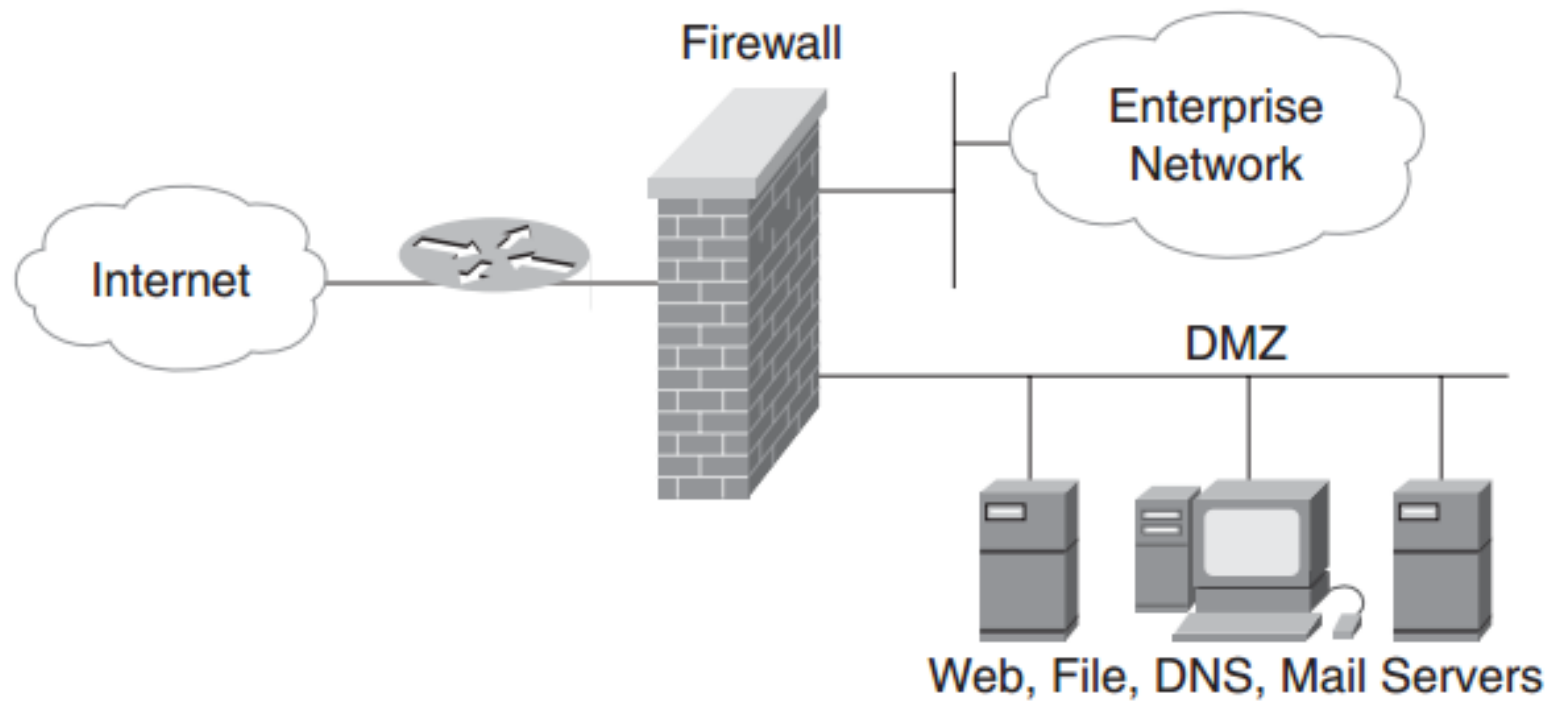
```
Router(config)#service password-encryption  
(set passwords here)  
Router(config)#no service password-encryption
```

Telnet hoặc SSH

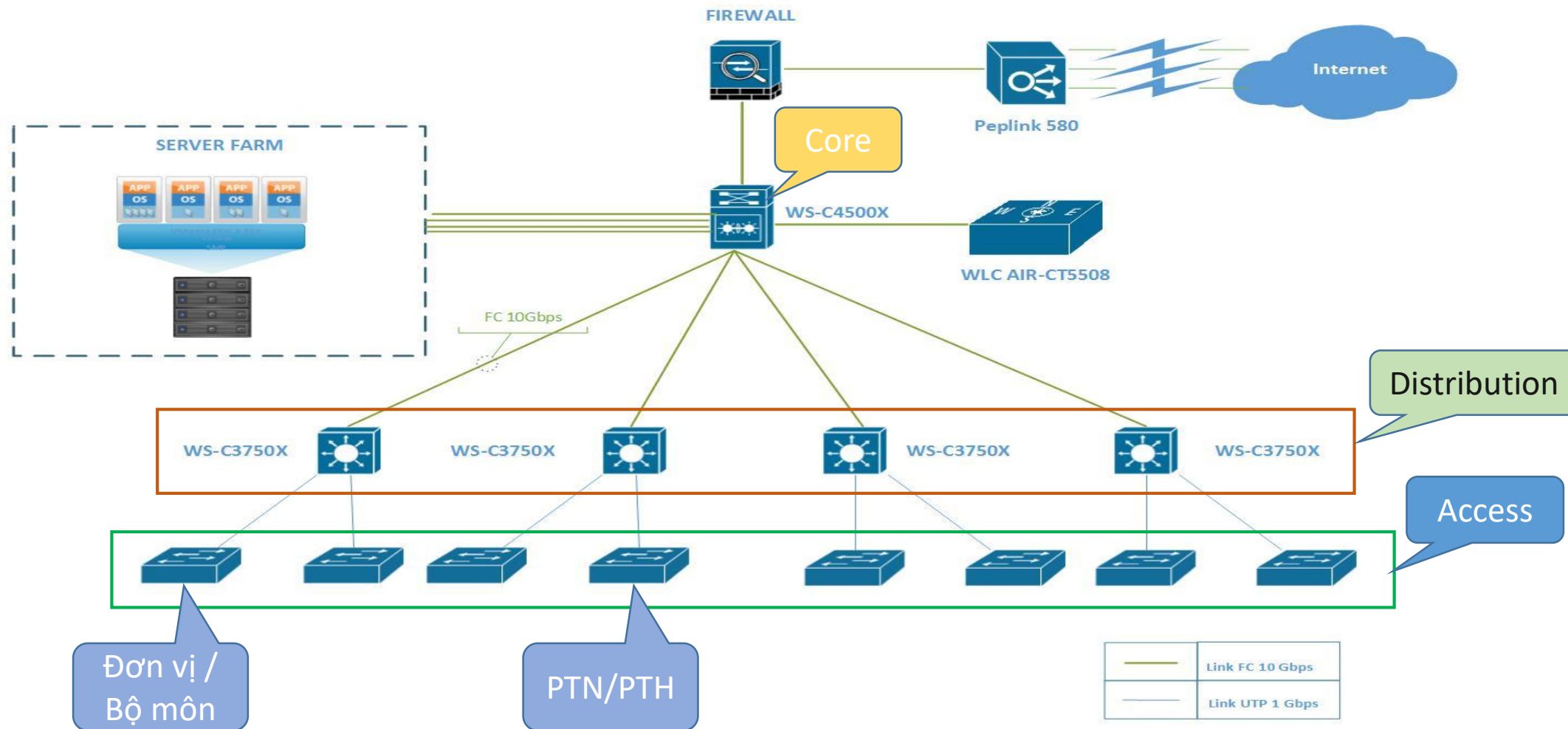
- ❖ Telnet/SSH là giao thức cho phép thiết lập kết nối từ xa.
- ❖ Secure Shell (SSH): sử dụng nhiều tính năng bảo mật
 - ❑ Xác thực mật khẩu mạnh hơn
 - ❑ Dữ liệu mã hóa khi vận chuyển



Mô hình mạng an toàn

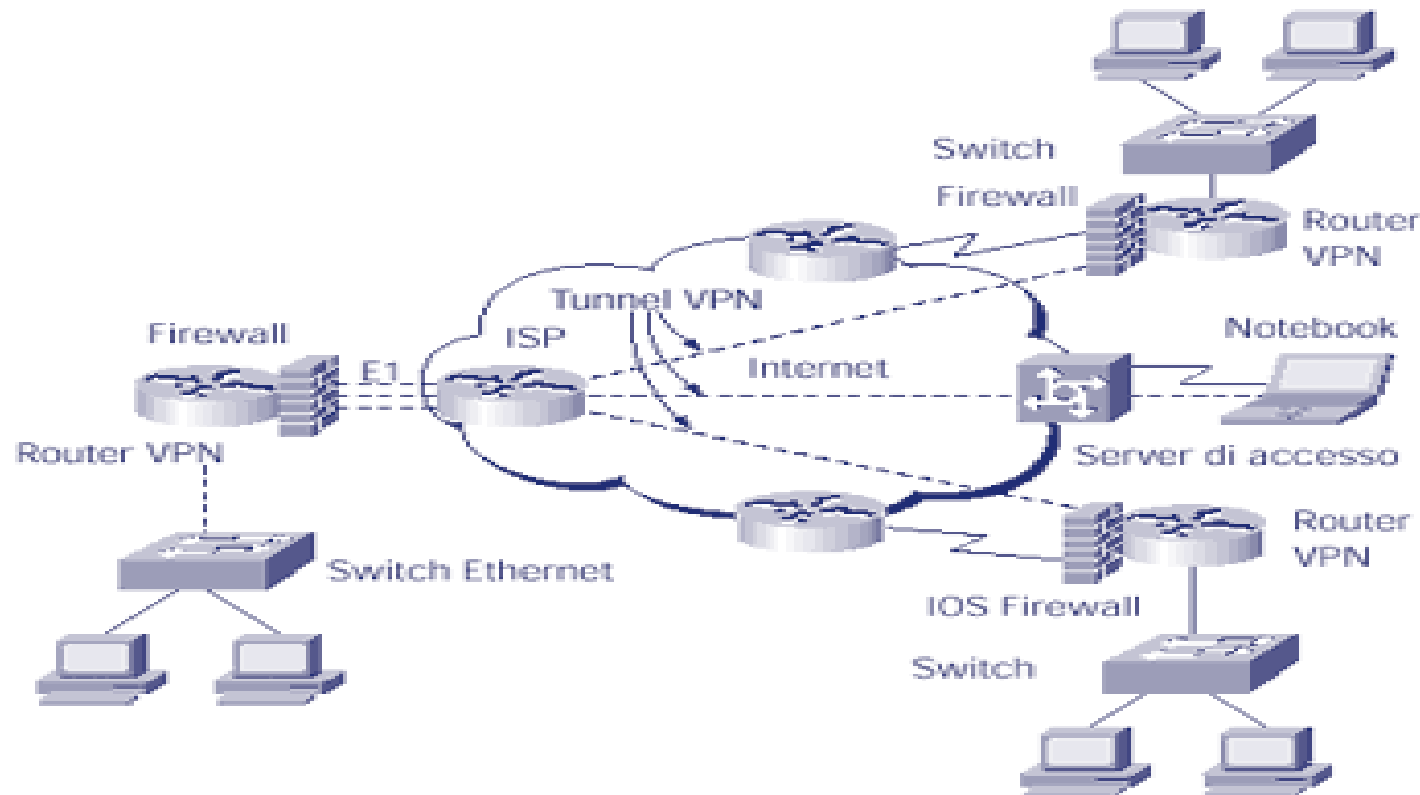


Phân tích mô hình mạng



VPN (Virtual private network)

- ❖ VPN là một công nghệ mạng riêng ảo: tạo kết nối mạng an toàn khi tham gia vào mạng công cộng (Internet), nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu.



Tài liệu tham khảo

- ❖ Principles of Network and System Administration, Mark Burgess, Oslo University College, Norway, Second Edition
- ❖ Network Management Fundamentals, Alexander Clemm Ph.D., Copyright© 2007 Cisco Systems, Inc.
- ❖ <https://www.cmc.com.vn/vi/san-pham/giai-phap-ha-tang-mang>
- ❖ <http://www.sunhitech.vn/trien-khai-he-thong-mang-cho-cong-ty-nhieu-chi-nhanh>