

CHƯƠNG 2

THIẾT KẾ MẠNG LAN

Bùi Trọng Tùng
Bộ môn TT&MMT - Khoa CNTT
Trường Đại học BKHN

1

Nội dung

1. Quy trình mạng
2. Khảo sát và phân tích yêu cầu
3. Thiết kế mạng

2

Nội dung

1. Quy trình mạng
2. Khảo sát và phân tích yêu cầu
3. Thiết kế mạng
4. Triển khai hạ tầng mạng
5. Quản trị mạng

3

1. Quy trình mạng

1.1. Khái niệm quy trình mạng

■ Khái niệm

- Tiến trình xây dựng và phát triển mạng máy tính
- Có sự kế thừa

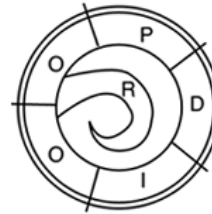
■ Mục đích

- Khai thác hệ thống mạng hiệu quả
- Tránh lãng phí tài nguyên
- Dễ dàng vận hành, bảo trì, phát triển

4

Quy trình mạng PDIOO

- Lập kế hoạch (Planning)
 - Xây dựng tiến trình công việc
 - Dự trù chi phí
 - Dự đoán rủi ro
- Thiết kế (Design)
 - Thu thập yêu cầu, khảo sát hiện trạng
 - Phân tích
 - Đề xuất giải pháp
 - Xây dựng sơ đồ thiết kế
 - Lập tài liệu



P Plan
 D Design
 I Implement
 O Operate
 O Optimize
 R Retire

5

Quy trình mạng PDIOO (tiếp)

- Triển khai cài đặt (Implementation)
 - Cài đặt phần cứng : đi dây mạng, lắp đặt, cấu hình thiết bị nối kết mạng (hub, switch, router)
 - Cài đặt phần mềm
 - Cấu hình server, máy trạm
 - Cài đặt, cấu hình các dịch vụ mạng
 - Tạo người dùng, phân quyền sử dụng

6

Quy trình mạng PDIOO (tiếp)

■ Vận hành (Operation)

□ Kiểm tra

- Sự kết nối giữa các máy tính
 - Hoạt động của các dịch vụ
 - Mức độ an toàn của hệ thống
- Dựa vào bảng đặc tả yêu cầu

□ Giám sát : hiệu năng, hiệu suất, độ an toàn mạng

7

Quy trình mạng PDIOO (tiếp)

■ Tối ưu hóa (Optimization)

- Đánh giá hiệu năng, hiệu quả mạng
- Xây dựng giải pháp tăng cường hiệu năng, cải thiện hiệu quả mạng
- Chuẩn bị mở rộng mạng

■ Bảo trì (Retirement)

- Khắc phục những vấn đề nảy sinh

8

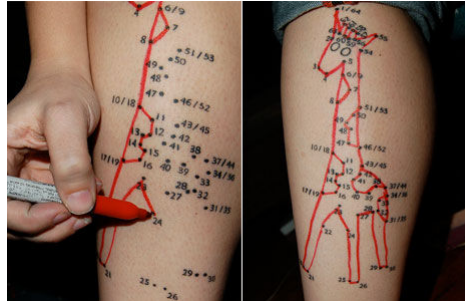
1.2. Phương pháp thiết kế top-down

- Phương pháp “connect-the-dots”

- Đặt tất cả các thiết bị lên bản vẽ
- Kết nối các thiết bị
- Hạn chế ???

- Thiết kế tốt ???

- Tính sẵn sàng
- Khả năng mở rộng
- Bảo mật
- Quản trị
- Hiệu năng
- Kinh tế



9

1.2. Phương pháp thiết kế top-down

- Bắt đầu từ tầng cao xuống tầng thấp (mô hình OSI)
- Phân tích mục đích, yêu cầu
 - Trước tiên !!!
 - Quan trọng
- Kiểu dữ liệu, lưu lượng, ứng dụng
- Các nhóm người dùng
- Thiết kế mức logic trước, mức vật lý sau
- Với mạng cỡ lớn cần module hóa

10

Nội dung

1. Quy trình thiết kế mạng
2. Khảo sát và phân tích yêu cầu
3. Thiết kế mạng
4. Triển khai hạ tầng mạng
5. Quản trị mạng

11

2.1. Phân tích yêu cầu khách hàng

- Tìm hiểu các đặc điểm chung của tổ chức (hoạt động, cơ cấu tổ chức...)
- Mục đích xây dựng mạng là gì ?
- Tìm hiểu đặc điểm các nhân viên trong tổ chức :
 - Nhân viên kỹ thuật ?
 - Người liên lạc ?
 - Người phê duyệt thiết kế ?
 - Trình độ tin học ?
- Các máy tính nào được nối mạng ?

12

2.1. Phân tích yêu cầu khách hàng (tiếp)

- Nhu cầu kết nối với mạng công cộng ?
- Nhu cầu truy cập từ bên ngoài ?
- Nhu cầu hỗ trợ các người dùng “di động” ?
- Các ứng dụng hỗ trợ nghiệp vụ ?

Tên ỨD	Loại ỨD	Ứng dụng mới (Y/N)?	Tính cần thiết	Ghi chú
--------	---------	---------------------	----------------	---------

- Yêu cầu về bảo mật, tính sẵn sàng ?
- Các yếu tố khác ảnh hưởng đến dự án : chính sách công ty, tài chính, thời gian hoàn thành...

13

2.2. Phân tích yêu cầu kỹ thuật

- Khả năng mở rộng
 - Kích thước
 - Phạm vi
 - Truy cập
- Tính sẵn sàng
 - Chịu lỗi
 - Dự phòng
 - Phục hồi

$$\text{Availability} = \text{Uptime} / \text{Total}$$

$$\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

MTBF : Mean Time Between Failure

MTTR : Mean Time To Repair

14

2.2. Phân tích yêu cầu kỹ thuật (tiếp)

■ Hiệu năng mạng

- Băng thông
- Băng thông tối thiểu
- Băng thông tối đa
- Thông lượng
- Tài
- Độ tin cậy
- Hiệu suất
- Trễ
- Thời gian đáp ứng

15

2.2. Phân tích yêu cầu kỹ thuật (tiếp)

■ Bảo mật

- Xác định tài nguyên mạng cần bảo vệ
- Phân tích các nguy cơ bảo mật
- Một số yêu cầu chính
 - Bảo mật dữ liệu
 - Toàn vẹn dữ liệu
 - Xác thực và phân quyền người dùng
 - Phân vùng DMZ (Demilitarized Zone)
 - Phát hiện tấn công
 - Xác thực băng định tuyến
 - Phòng chống virus
 - Đào tạo người dùng

16

2.2. Phân tích yêu cầu kỹ thuật (tiếp)

- Quản trị mạng
 - Quản trị hiệu suất
 - Quản trị lỗi
 - Quản trị cấu hình
 - Quản trị an toàn an ninh
 - Quản trị tài khoản
- Tiện lợi
- Tương thích

17

2.3. Khảo sát hiện trạng hệ thống mạng đang sử dụng

- Mô tả hạ tầng mạng
 - Sơ đồ vật lý : vị trí thiết bị, sơ đồ đi cáp, đặc điểm các đường cáp
 - Sơ đồ logic mạng
 - Nếu có thể hãy phát triển sơ đồ khối
 - Giao thức
 - Bảng thông
 - Dịch vụ hạ tầng đang sử dụng
 - Định địa chỉ/Định danh
 - Đặc điểm địa hình
- Phân tích hiệu năng

18

2.4. Phân tích lưu lượng mạng

■ Phân tích luồng dữ liệu

- Nguồn, đích, hướng, tốc độ truyền
- Các nhóm người dùng chính

Tên nhóm	Số lượng người dùng	Vị trí địa lý	Các ứng dụng đang sử dụng
----------	---------------------	---------------	---------------------------

- Kho dữ liệu

Tên kho	Vị trí địa lý	Các ứng dụng đang chạy	Nhóm người sử dụng
---------	---------------	------------------------	--------------------

- Luồng dữ liệu của hệ thống mạng đang sử dụng
- Phân loại các luồng dữ liệu : terminal/host, client/server, P2P, server/server, distributed computing

Tên ứng dụng	Luồng dữ liệu	Giao thức	Nhóm người dùng	Kho dữ liệu	Bảng thông yêu cầu	QoS
--------------	---------------	-----------	-----------------	-------------	--------------------	-----

19

2.4. Phân tích lưu lượng mạng (tiếp)

■ Phân tích tải

- Tải : tổng kích thước dữ liệu mà các máy trạm đưa lên đường truyền trong 1 khoảng thời gian
 - Tổng số máy trạm
 - Thời gian trung bình giữa 2 lần gửi dữ liệu
 - Thời gian trung bình để gửi dữ liệu
- Chi tiết hóa các ứng dụng trong mạng
 - Tần suất sử dụng
 - Thời gian một phiên làm việc trên ứng dụng
 - Số người sử dụng đồng thời
 - Bảng thông tối đa ???

20

Phân tích tải (tiếp)

■ Ước lượng tải phát sinh bởi ứng dụng

Type of Object	Size in Kbytes
Terminal screen	4
E-mail message	10
Web page (including simple GIF and JPEG graphics)	50
Spreadsheet	100
Word processing document	200
Graphical computer screen	500
Presentation document	2000
High-resolution (print-quality) image	50,000
Multimedia object	100,000
Database (backup)	1,000,000

■ Ước lượng tải phát sinh bởi giao thức

Ethernet	Token Ring	FDDI	IP	TCP
46	29	36	24	24

21

Nội dung

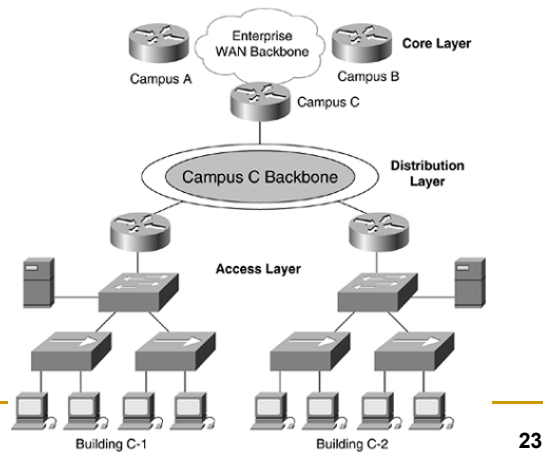
1. Quy trình mạng
2. Khảo sát và phân tích yêu cầu
3. Thiết kế mạng
4. Triển khai hạ tầng mạng
5. Quản trị mạng

22

3.1. Thiết kế mức logic

3.1.1. Thiết kế topo của mạng

- Mô hình phân cấp 3 lớp (3-layer hierarchical topology)



23

Mô hình phân cấp 3 lớp

- Lớp lõi (Core layer)
 - Lưu lượng mạng lớn
 - Tin cậy, nhanh, chịu lỗi
 - Lưu ý :
 - Hạn chế thực hiện các cấu hình làm chậm tốc độ xử lý : định tuyến VLAN, ACL, lọc gói tin...
 - Không kết nối trực tiếp máy trạm
 - Tránh mở rộng mạng ở lớp lõi
 - Switch layer 2 : nhanh, dễ mở rộng, rẻ
 - Switch layer 3, router : cân bằng tải, giám sát dữ liệu quảng bá

24

Mô hình phân cấp 3 lớp (tiếp)

- Lớp phân phối (Distribution Layer)
 - Triển khai các chính sách của mạng
 - ACL, lọc gói, QoS
 - Firewall
 - Cân bằng tải
 - VLAN routing
 - Cung cấp các kết nối dự phòng cho lớp truy cập

25

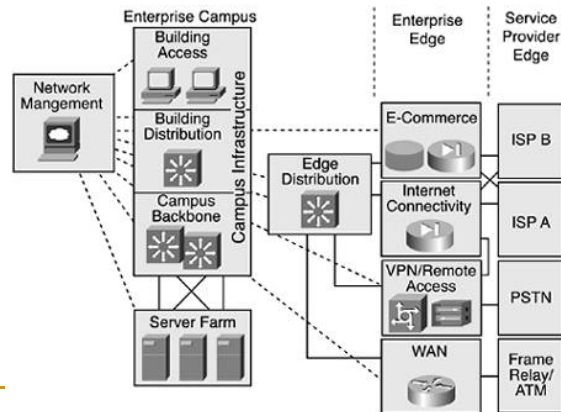
Mô hình phân cấp 3 lớp (tiếp)

- Lớp truy cập (Access Layer)
 - Có thể triển khai thêm các chính sách từ lớp phân phối
 - Cung cấp kết nối tới các nhóm máy trạm
 - Phân đoạn mạng
 - Lưu ý : không sử dụng router tại lớp này

26

3.1.1. Thiết kế topo của mạng (tiếp)

- Mô hình thiết kế mạng campus
 - Mô-đun hóa mạng theo chức năng



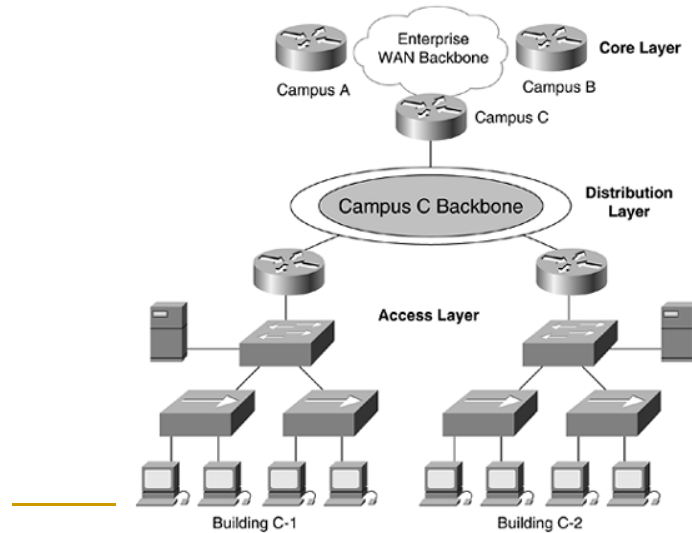
27

Mô hình thiết kế mạng campus

- Enterprise Campus
 - Mô-đun hạ tầng : mô hình 3 lớp
 - Lớp core (campus backbone) của các campus được kết nối với nhau
 - Mô-đun quản trị mạng : IDS, logging, SNMP...
 - Hệ thống máy chủ : DHCP, DNS, ứng dụng
 - Kết nối với mô-đun biên (Edge Distribution Module) : điều khiển truy cập, dung lượng đường truyền lớn, tính sẵn sàng cao

28

Enterprise Campus



29

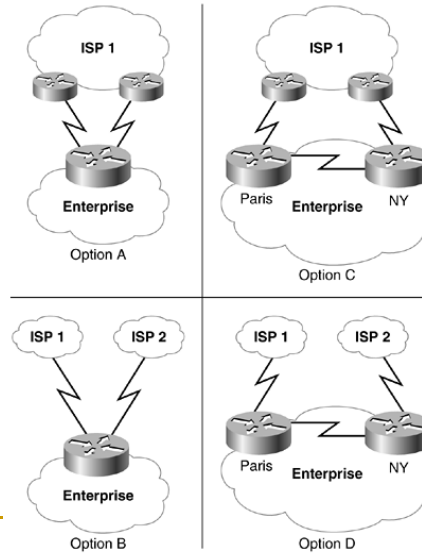
Mô hình thiết kế mạng campus

■ Enterprise Edge

- E-Commerce module : bao gồm các máy chủ ứng dụng phục vụ cho các nhu cầu truy cập từ bên ngoài
 - Cân bằng tải, cache
- Internet Connectivity module : cung cấp kết nối ra bên ngoài
 - Firewall, IDS, DNS
- VPN module : cung cấp các kết nối bảo mật
- WAN module : kết nối tới các mạng campus khác

30

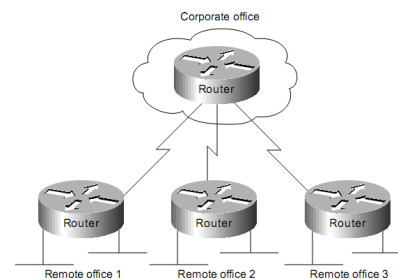
Internet Connectivity module



31

3.1.1. Thiết kế topo của mạng (tiếp)

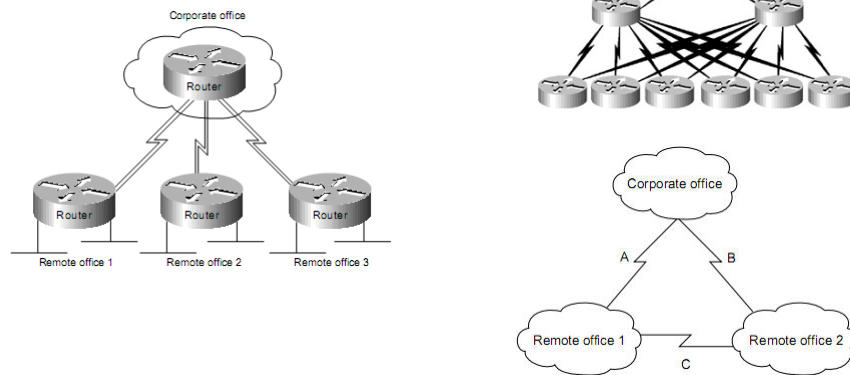
- Mô hình dự phòng
 - ❑ Không dự phòng
 - ❑ Topo dạng lưới
 - ❑ Dự phòng phần cứng
 - ❑ Dự phòng hệ thống nguồn



32

Mô hình dự phòng (tiếp)

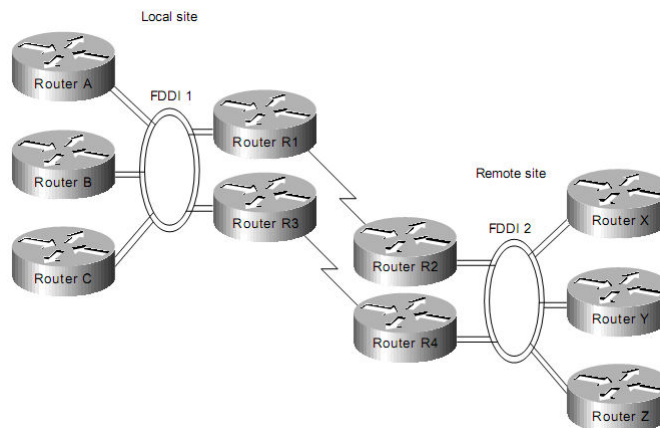
- Dự phòng kết nối với topo lù



33

Mô hình dự phòng

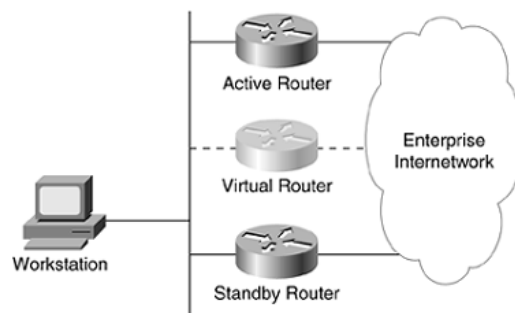
- Dự phòng phần cứng



34

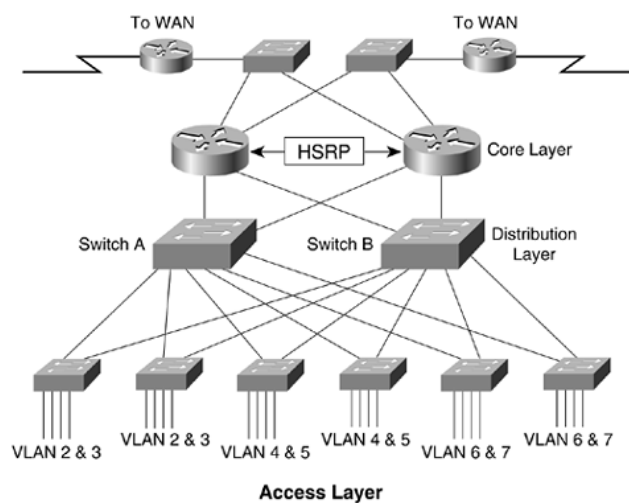
Mô hình dự phòng (tiếp)

■ Hot Standby Router Protocol



35

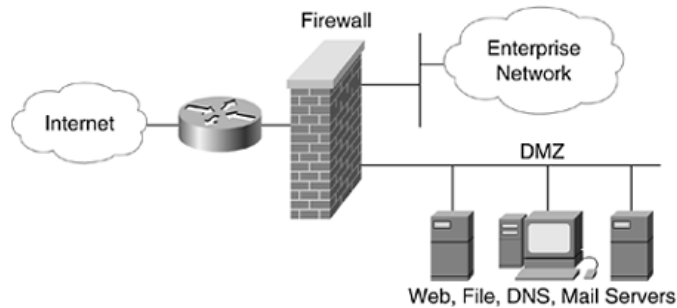
Mô hình dự phòng (tiếp)



36

3.1.1. Thiết kế topo của mạng (tiếp)

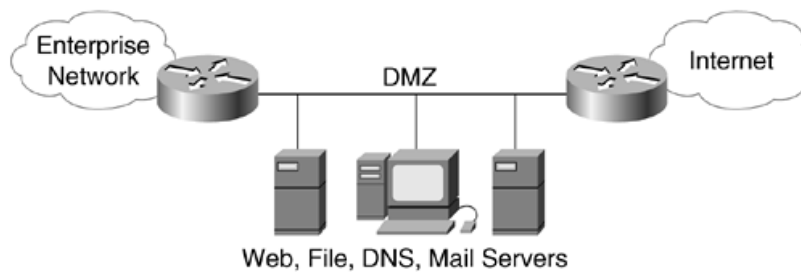
- Mô hình an toàn bảo mật
 - Phân vùng DMZ (Demilitarized Zone)



37

Mô hình an toàn bảo mật (tiếp)

- Tường lửa 3 lớp



38

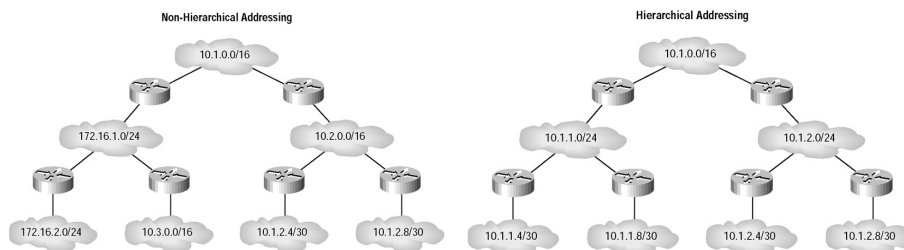
Mô hình an toàn bảo mật (tiếp)

- Dữ liệu : bảo mật, xác thực, tính sẵn sàng
- Router và switch :
 - Telnet, SNMP
 - Kiểm soát truy cập
 - Logging
 - An toàn thông tin định tuyến
- An toàn mạng
- An toàn máy trạm và ứng dụng

39

3.1.2. Định danh

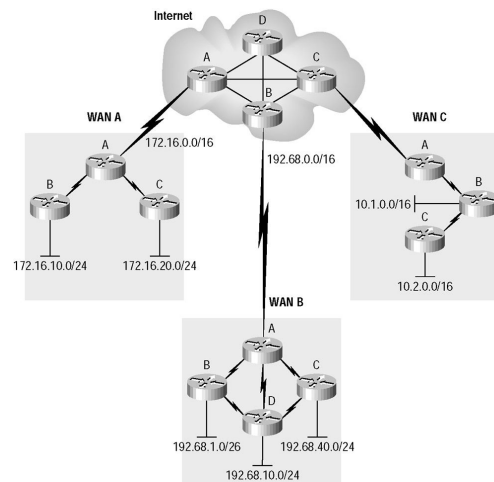
- Định danh có cấu trúc



40

3.1.2. Định danh (tiếp)

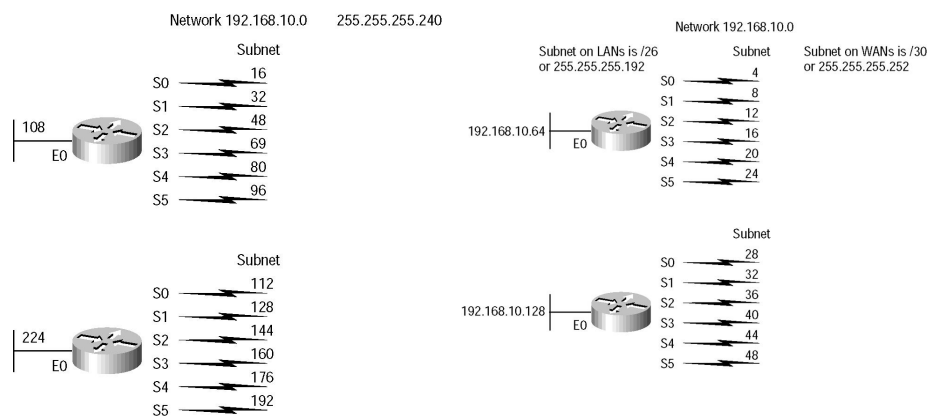
- Kết hợp đường đi trong định tuyến



41

3.1.2. Định danh (tiếp)

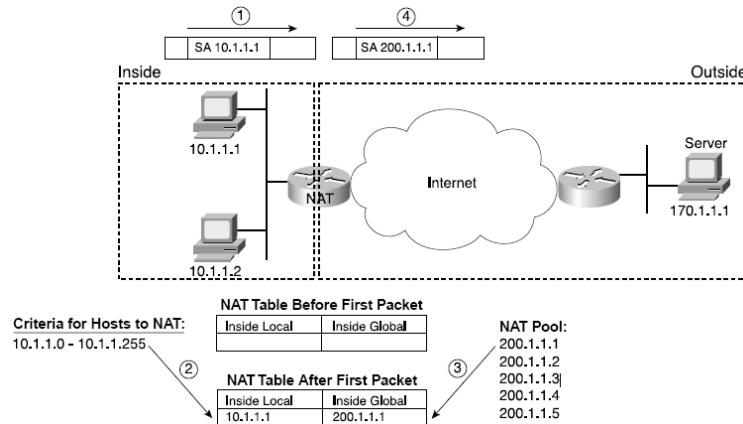
- Sử dụng mặt nạ mạng con có độ dài thay đổi



42

3.1.2. Định danh

■ NAT và PAT



43

3.1.3. Lựa chọn giao thức chuyển mạch và định tuyến

- Cầu trong suốt (transparent bridging)
 - Store-and-forward
- Chuyển mạch trong suốt (transparent switching)
 - Store-and-forward
 - Cut-and-through
- Chuyển mạch đa tầng
- Spanning Tree Protocol
- VLAN Trunk Protocol

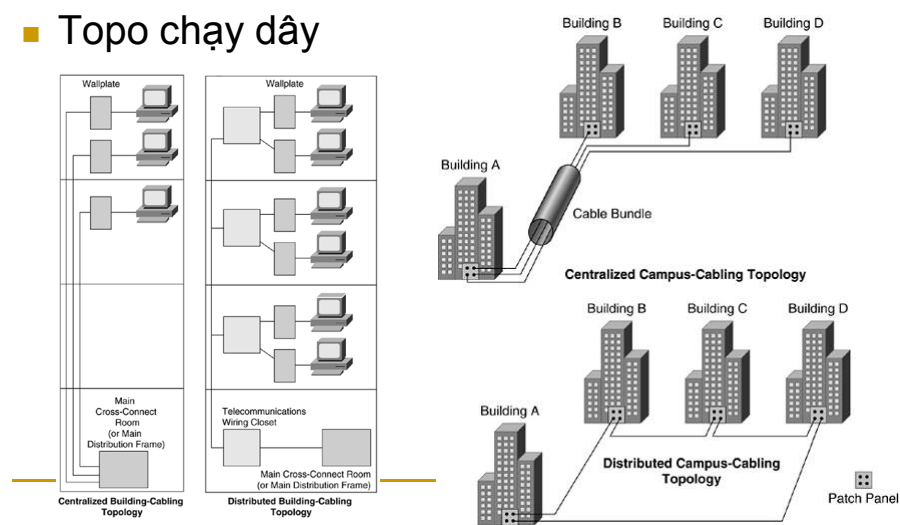
44

3.1.3. Lựa chọn giao thức chuyển mạch và định tuyến

Protocol	Classful ?	Metric	Scalability	Supports Security? Authenticates Routes?	Ease of config
RIP v1	Classful	Hop count	15	No	Easy
RIP v2	Classless	Hop count	30	Yes	Easy
IGRP	Classful	Bandwidth, delay, load	255	No	Easy
EIGRP	Classless	Bandwidth, delay, load	1000s	Yes	Easy
OSPF	Classless	Bandwidth	100s areas, 100s/area	Yes	Moderate
BGP	Classless	Path value	1000s	Yes	Moderate
IS-IS	Classless	Path value, delay, expense	100s areas, 100s/area	Yes	Moderate

3.2. Thiết kế mức vật lý

■ Topo chạy dây



3.2.2. Thiết kế mức vật lý – Lựa chọn thiết bị mạng

- Số cổng
- Thông lượng (pps)
- Băng thông
- Các công nghệ được hỗ trợ
- Các loại cáp được hỗ trợ
- MTBF, MTTR
- Các cơ chế an toàn-bảo mật
- Các tính năng năng hot-swap, dự phòng, QoS
- Cấu hình, quản trị, chi phí, hỗ trợ kỹ thuật, bảo hành...

47

Lựa chọn thiết bị mạng – Switch/Bridge

- Các công nghệ cầu nối được hỗ trợ
- STP
- Số địa chỉ MAC có thể học
- Kích thước bảng MAC (Switching Table)
- VLAN
- Định tuyến

48

Lựa chọn thiết bị mạng (tiếp)

- Router

- Các giao thức định tuyến được hỗ trợ
- Các ứng dụng quảng bá được hỗ trợ
- Nén, mã hóa

- Access Point

- Chuẩn WLAN
- Hỗ trợ các dịch vụ DHCP, NAT, định tuyến
- Hỗ trợ VLAN
- Phạm vi phủ sóng
- Các giao thức xác thực được hỗ trợ (WEP, WPA, WPA 2...)