Trường đại học Giao Thông Vận Tải Tp HCM
Khoa Điện-Điện tử viễn thông
Chuyên ngành Điện Tử Viễn Thông

Luận Văn Tốt Nghiệp

THIẾT KẾ MẠNG LAN 50 PCs

GVHD: Thạc sĩ Lê Anh Uyên Vũ
SVTH: Châu Phước Bảo Thiện-lớp DV04
MSSV: DV03055

TRƯỜNG ĐẠI HỌC GTVT TP.HCM
THƯ VIỆN
1.007
DV09-2009

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TPHCM
KHOA ĐIỆN - ĐIỆN TỬ VIỄN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc
- - - o O o - - -

NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP

(Chú ý: SV phải đóng bản nhiệm vụ này vào trang thứ nhất của đồ án)

Họ và tên SV: Châu Phước Bảo Thiện MSSV: DV03055

Ngành: Điện tử viễn thông Lớp: DV04

1. Tên đồ án tốt nghiệp:

...Thiết kế hệ thống mạng Lan 50 PCs.....
.....
.....
.....
.....

2. Nhiệm vụ (yêu cầu về nội dung và số liệu ban đầu):

- Tìm hiểu tổng quan CCNA , các kĩ thuật trong CCNA, kĩ thuật truyền dữ liệu trong mạng máy tính
- Phân chia Vlan trong mạng LAN gồm 50 PCs, tăng cường bảo mật trong VLAN
- Mô hình phải áp dụng được ngoài thực tế, có khả năng tự thiết kế hệ thống một cách tối ưu theo yêu cầu của doanh nghiệp.
- Sử dụng phần mềm mô phỏng (Boson..) để thực hiện đề tài

.....
.....
.....
.....
.....
.....

3. Ngày giao nhiệm vụ đồ án: 20/4/2009

4. Ngày hoàn thành nhiệm vụ: 20/7/2009

5. Họ tên người hướng dẫn: **Phần hướng dẫn**

1) Ths Lê Anh Uyên Vũ 1) .....
2) ..... 2) .....
3) ..... 3) .....

Nội dung và yêu cầu ĐATN đã được thông qua.
Ngày 25 tháng 04 năm 2009.

TRƯỞNG KHOA
(Ký và ghi rõ họ tên)

TRƯỞNG KHOA
PGS-TS. Trần Hoài An

NGƯỜI HƯỚNG DẪN CHÍNH
(Ký và ghi rõ họ tên)

Lê Anh Uyên Vũ

LỜI CẢM ƠN

Sự phát triển của khoa học thông tin liên lạc ngày nay đã mở ra một kỉ nguyên mới cho nhân loại, trong đó có vai trò của mạng máy tính, luận văn xin trình bày những khái niệm và cách xây dựng một mạng Lan phổ biến ngày nay.

Đầu tiên em xin gửi lời cảm ơn đến cô Lê Anh Uyên Vũ, người trực tiếp hướng dẫn em hoàn thành luận văn này.Những chỉ dẫn và ý kiến đóng góp của cô là vô cùng hữu ích, giúp em nhận ra những khuyết điểm của luận văn.

Dù rất cố gắng nhưng những tìm hiểu ban đầu về công nghệ không tránh khỏi những thiếu sót nhất định, kiến thức còn hạn chế, kính mong được các thầy cô và các bạn chỉ bảo nhiều hơn để lấp những lỗ hổng kiến thức này. Xin chân thành cảm ơn các thầy cô và các bạn trong khoa điện-điện tử viễn thông đã nhiệt tình giúp đỡ để em có thể hoàn thành tốt luận văn này!

Tp HCM, ngày19 tháng 7 năm 2009
SVTH

Châu Phước Bảo Thiện

Giới thiệu tóm tắt đề tài

Sự phát triển mạnh mẽ của máy vi tính trong thời đại bùng nổ thông tin đã mở rộng nhu cầu sử dụng không chỉ còn ở dạng cá nhân riêng rẽ như trước đây nữa. Ngày nay, tăng cường khả năng bảo mật trong nội bộ cũng như trước internet, sử dụng linh hoạt cho công việc, chứng thực người sử dụng, dự trữ, dự phòng dữ liệu để có thể phục hồi nhanh chóng, chính xác là một nhu cầu thiết yếu. Chính vì vậy, việc xây dựng một hệ thống đáp ứng tốt các yêu cầu trên đã dẫn đến việc tự xây dựng một hệ thống mạng Lan với một số lượng máy tính lớn là tất yếu. Đề tài thiết kế một hệ thống Lan tiêu biểu cho một trường đại học với sự tương đối đầy đủ các phòng ban.

Thiết bị kết nối các máy tính cần có sự thông minh, linh hoạt, tận dụng triệt để chức năng để giảm chi phí đầu tư xây dựng và phải đảm bảo được chất lượng. Một hãng chuyên sản xuất các thiết bị này với tên gọi là CISCO của USA đã đáp ứng được các yêu cầu đó. Đề tài sử dụng các switch và các router của CISCO để phân chia mạng con cho các phòng ban trong trường. Lan hay còn gọi là mạng cục bộ được chia thành 7 mạng Vlan cho 10 phòng và khoa trực thuộc là:

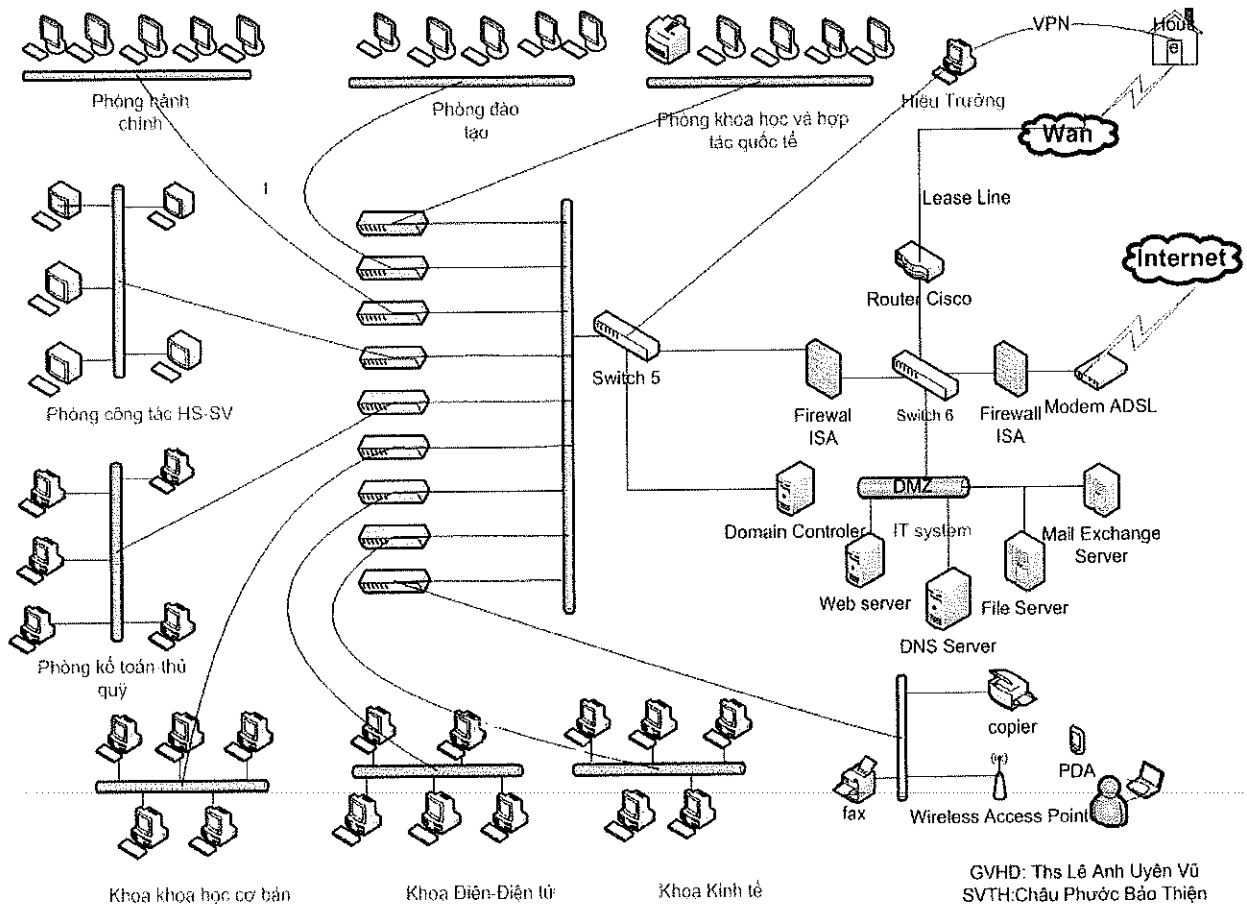
Phòng đào tạo, phòng khoa học và hợp tác quốc tế, khoa khoa học cơ bản, khoa điện-điện tử, phòng hiệu trưởng, khoa kinh tế, phòng hành chính, phòng công tác học sinh-sinh viên, phòng kế toán thủ quỹ, phòng hệ thống IT. Trong đó, phòng hệ thống IT là não bộ của toàn hệ thống, chứa các server quan trọng.

Phần đầu của đề tài là các kiến thức tổng quan của CCNA, một chương trình đào tạo của chính hãng CISCO đưa ra trên thế giới.

Phần nội dung chính của đề tài được dựa trên chương trình kiến thức CCNA: Các Vlan được chia trên các Switch 2950 series của CISCO, loại Switch này thể hiện sự thông minh ở chỗ nó không chỉ phân chia từ một mạng Lan thông thường thành nhiều mạng Lan (mà ta gọi là Vlan), Switch còn có thể chỉ định PC nào được phép kết nối vào cổng nào trên Switch bằng cách định nghĩa địa chỉ MAC cho chính cổng đó. Một Switch thường có số lượng cổng khoảng 24x trở lên. Vì nhu cầu sử dụng của chúng ta có lúc nhiều, lúc ít hơn con số trên Switch nên việc chia Vlan sẽ giúp giảm thiểu sự phức tạp khi gắn nhiều Switch thường (các Switch thường chỉ có một Lan khi được kết nối). Nhờ phân chia Vlan, các PC thuộc 2 phòng khoa khác nhau dù kết nối tới cùng một Switch nhưng thực tế vẫn hoạt động như trên hai Switch thuộc hai mạng Lan khác nhau. Giảm chi phí mua các Router. Đề tài sử dụng phần mềm mô phỏng Boson Netsim để giải quyết yêu cầu đặt ra. Mặc dù không đạt được như làm việc với thiết bị thật nhưng nó cũng đủ để ta có thể tìm hiểu, nghiên cứu và đạt được mục đích trong đề tài này. Để kiểm tra một

kết nối thành công, lệnh Ping được sử dụng. Đề tài cũng nêu các cách đi dây cáp, kiểm tra kết nối cáp, gán địa chỉ trên máy thật (chủ yếu là hệ điều hành thông dụng của Microsoft : window vista, XP, server 2k3)

Phần mở rộng của đề tài chủ yếu tập trung trên nền tảng của Microsoft : Hệ thống mạng Lan gồm 50 PC được thiết kế theo mô hình client/server để tạo khả năng bảo mật cao và quản lý trung tâm hoá. Trong đó có vai trò rất lớn của một máy tính gọi là domain controller, máy tính này thực hiện các dịch vụ thẩm định người dùng bằng cách theo dõi và kiểm tra username, password. Khả năng bảo mật hệ thống còn được thể hiện rõ ở vai trò của hai tường lửa là giới hạn và phân quyền truy cập tài nguyên từ các server lưu trữ dữ liệu như: FTP server lưu trữ data, mail server lưu trữ mail của các người dùng trong trường… Hai tường lửa này sẽ đánh chặn các tấn công từ bên trong (nội bộ) và các hiểm họa rất lớn từ bên ngoài internet vào hệ thống mạng. lấy cắp sửa đổi dữ liệu quan trọng của trường. Hình dưới đây thiết kế mô hình tổng quan của đề tài:



Hình giới thiệu mô hình tổng quan hệ thống

Mục tiêu, yêu cầu và hướng giải quyết đề tài:

A.Mục tiêu:

- Nắm bắt các kiến thức và kĩ thuật của CCNA.
- Xây dựng hệ thống mạng Lan sử dụng 50 PC có phân chia Vlan cho các phòng ban (ví dụ: các phòng ban trường đại học)

B. Yêu cầu:

- Có khả năng cấu hình thành công các Switch, Router
- Các Vlan dù cùng một Switch nhưng không thể trao đổi dữ liệu trực tiếp với nhau mà chỉ có thể trao đổi dữ liệu trong Vlan của mình.

C.Hướng giải quyết:

- Sử dụng phần mềm mô phỏng hệ thống Lan
- Cấu hình các thiết bị được mô phỏng để giải quyết yêu cầu đề tài.

Mục Lục

Phần 1: Tổng quan về CCNA: **11**
I. Giới thiệu về router trong mạng WAN 11
I.1 Nhiệm vụ 12
I.2 Phân loại 13
II. Các khái niệm cơ bản về Router và cơ chế routing 14
II.1 Nguyên tắc hoạt động của Router – ARP Protocol 14
II.2 Một số khái niệm cơ bản 17
II.3 Các routing protocol tiêu biểu 21
III. Khái niệm về cấu hình Router 23
III.1 Cấu trúc router 24
III.2 Các mode config 26
IV. Cấu hình các tính năng chung của router: 30
IV.1 Một số quy tắc về trình bày câu lệnh 30
IV.2 Các phím tắt cần sử dụng khi cấu hình router 30
IV.3 Các khái niệm về console, telnet. Cách xác định các tên và password cho router 32
IV.3.1 Console port 32
IV.3.2 Telnet sesstion 35
IV.3.3 Xác định tên cho router và enable password 36
IV.4 Làm việc với file cấu hình và IOS image 36
IV.4.1 Một số khái niệm cơ bản 36
IV.4.2 Làm việc với file cấu hình và IOS 39
Phần 2:Tính toán thiết kế và thi công mạng Lan: **46**
V. Giới thiệu phần mềm mô phỏng Boson netsim 46
VI. Sơ đồ thiết kế hệ thống 51
VI.1 Mạng máy tính cục bộ (LAN) 51
VI.2 Mạng riêng ảo (VPN) trong đề tài 52
VI.3 Tiến trình đóng gói chi tiết 54
VII. Cáp 55
VII.1 Loại cáp sử dụng 58
VII.2 Nối cáp: 60
VII.3 Kiểm tra cáp: 60
VIII. Ethernet Switching 61

VIII.1 Bắc cầu ở lớp 2: 61
VIII.2 Chuyển mạch ở lớp 2 63
VIII.3 Giới thiệu về luồng dữ liệu (data flow) 64
IX. Các địa chỉ IP lớp A, B, C, D và E 65
X. Sự gán tĩnh một địa chỉ IP 68
XI. Các thuật toán định tuyến và các metric 71
XII. Phân chia Vlan trong hệ thống mạng 73
XII.1 Vlan 73
XII.2 Khái niệm, hoạt động của mạch nối (trunk) 74
XIII. Bức tường lửa 81
XIII.1 Chức năng 81
XIII.2 Cấu trúc của FireWall 81
XIV. Domain controller 84
XV. Cấu trúc tổng quát các lệnh thiết yếu sử dụng trong đề tài 86
XV.1 Các lệnh trên Switch 86
XV.2 Các lệnh trên router 86
XVI. Kiểm tra tính kết nối bằng lệnh Ping 87

Phần 3: Phụ Lục 92
Một số cấu hình hiện có trên Switch 92

Danh sách bảng biểu, hình vẽ

Hình 1: Cấu trúc Router
Hình 1.1: Tiến trình đóng gói dữ liệu
Hình 3: Giao thức ARP
Hình 4: Giao thức ARP (tt)
Hình 5: Phân giải địa chỉ dùng proxy ARP.
Bảng 6: Ví dụ về routing table.
Hình 7: Quá trình chuyển packet qua một hệ thống bao gồm nhiều router
Hình 8: Thuật toán Distance Vector
Hình 2.1
Hình 2.2
Hình 9: Một số mode config của Cisco Router
Bảng 10
Hình 11
Hình 12: Quy trình cập nhật IOS image
Hình 13: Configuration register
Hình 14: Mô hình cơ bản của một kết nối leased line
Hình 15: Các loại cáp kết nối giữa router và NTU (CSU/DSU)
Hình 5.1: Giao diện của phần mềm Bosson Netsim
Hình 5.2: Các lệnh hỗ trợ trên Switch của phần mềm
Hình 5.3: Giao diện Netsim Designer
Hình 5.4: Hệ thống Lan 50 PCs được thiết kế bằng phần mềm Designer
Hình 6.1: Hệ thống mạng Lan phân chia các phòng ban trong đề tài
Hình 6.2: Vpn kết nối đến một máy tính trong trường
Hình 6.3: Các kết nối VPN
Hình 6.4: Tiến trình đóng gói chi tiết
Hình 7.1: Cáp UTP
Hình 7.2 Chuẩn kết nối T568A và T568B
Hình7.3: Đầu nối RJ45 (male
Hình 7.4: Đầu nối RJ45 (female)
Hình 7.5: Sơ đồ nối cáp thẳng
Hình 7.6: Sơ đồ nối cáp chéo
Hình 7.7: Sơ đồ nối cáp đảo
Hình 7.8: Chuẩn kiểm thử cáp

Hình 8.1: Hoạt động của Bridge
Hình 8.2: Hoạt động của Switch
Hình 8.3: Luồng dữ liệu xuyên qua một mạng
Hình 9.1: Các tiền tố lớp địa chỉ
Hình 9.2: Địa chỉ lớp A
Hình 9.2: Địa chỉ lớp B
Hình 9.3: Địa chỉ lớp C
Hình 9.4: Các địa chỉ IP private
Hình 10.1: Gán tĩnh IP trên hệ điều hành Windows Vista (PC)
Hình 10.2: Gán tĩnh IP trên hệ điều hành Windows Vista (tt)
Hình 10.3: Gán tĩnh ip trên phần mềm mô phỏng Bosson Netsim
Hình 11.1: Định tuyến đi qua mạng
Hình 11.2: Điều khiển tốc độ
Hình 12.1: Sơ đồ hệ thống mạng (Visio)
Hình 12.2: Sơ đồ hệ thống mạng (designer)
Bảng 12.3: Thống kê các thiết bị được sử dụng
Hình 13.1: Sơ đồ hệ thống tường lửa và khu vực phi quân sự của đề tài theo mô hình Screened-Subnet
Hình 13.2: Các địa chỉ IP của một số server hay dùng
Hình15.1: Lệnh Ping
Hình 15.2: Ping cùng VLAN và khác VLAN
Hình15.3: Ping lên router của vlan 1

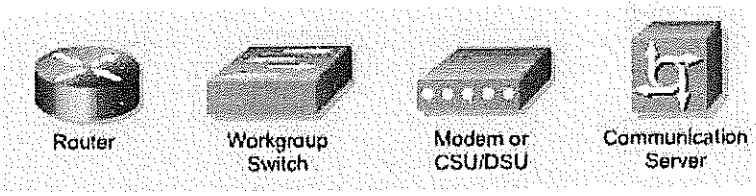
Phần 1

Tổng quan về CCNA

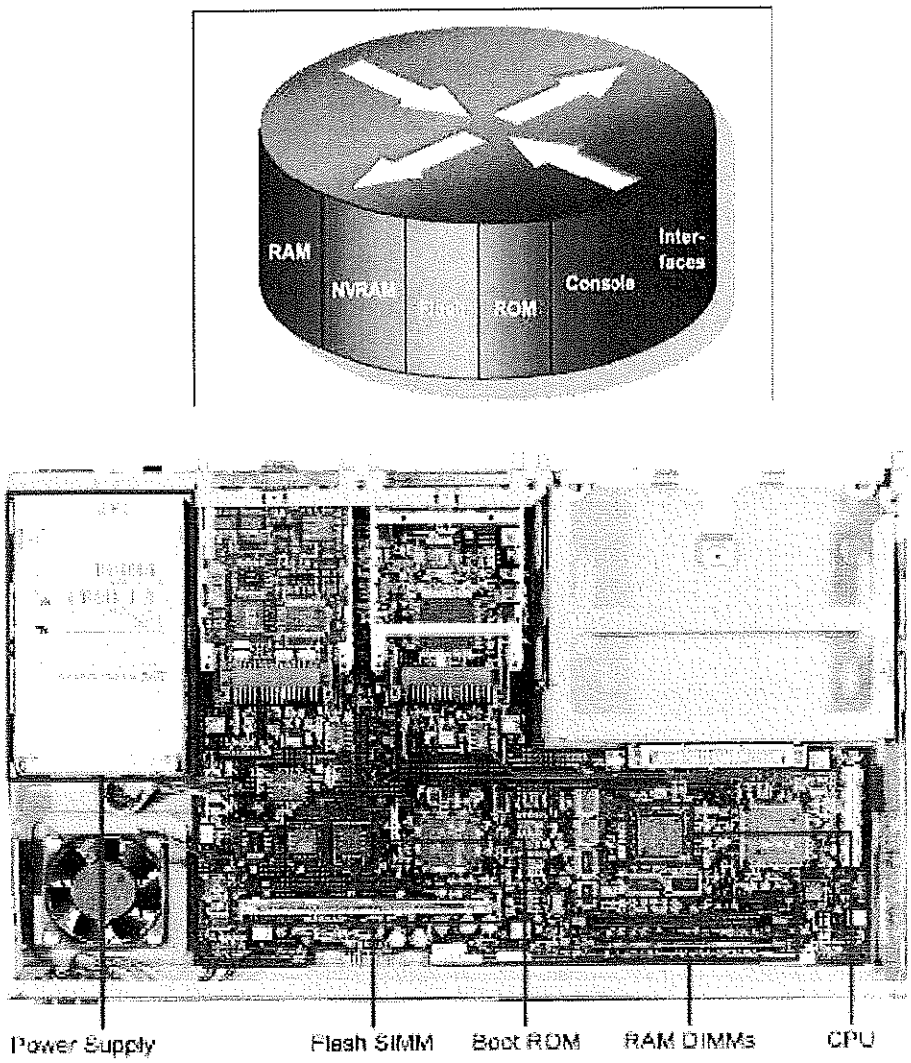
WAN – ROUTER

Mạng diện rộng (WAN) là mạng truyền dữ liệu qua những vùng địa lý rất lớn. Mạng WAN hoạt động chủ yếu ở lớp Vật lý và lớp Liên kết dữ liệu mô hình OSI. WAN kết nối các mạng LAN lại với nhau. Do đó, WAN thực hiện chuyển đổi các gói dữ liệu giữa các router, switch và các mạng LAN mà nó kết nối. Các thiết bị được sử dụng trong WAN:

- Router: cung cấp nhiều dịch vụ khác nhau, bao gồm Internet và các giao tiếp WAN.
- Loại switch được sử dụng trong WAN cung cấp kết nối cho hoạt động thông tin liên lạc băng thoại video và dữ liệu.
- Modem: bao gồm: giao tiếp với dịch vụ truyền thoại; CSU/DSU (Chanel service units/ Digital service units) để giao tiếp với dịch vụ T1/E1; TA/NT1 (Terminal Adapters /Network Terminal 1) để giao tiếp với dịch vụ ISDN (Integrate Services Digital Network).
- Server thông tin liên lạc: tập trung xử lý cuộc gọi của người dùng



I. Giới thiệu về router trong mạng WAN:



Hình 1: Cấu trúc Router

I.1.Nhiệm vụ:

Router là thiết bị mạng hoạt động ở tầng thứ 3 của mô hình OSI-tầng network. Router được chế tạo với hai mục đích chính:

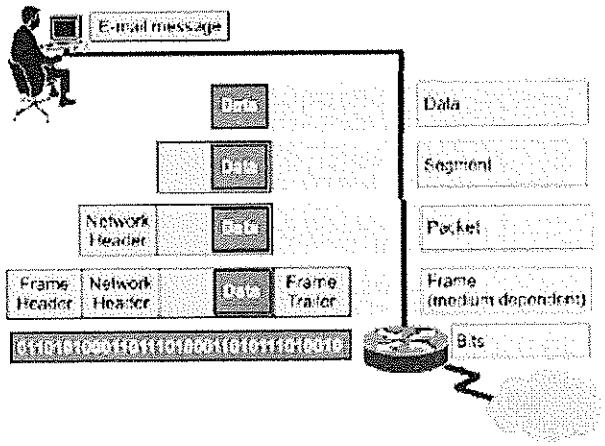
Phân cách các mạng máy tính thành các segment riêng biệt để giảm hiện tượng đụng độ, giảm broadcast hay thực hiện chức năng bảo mật.

Kết nối các mạng máy tính hay kết nối các user với mạng máy tính ở các khoảng cách xa với nhau thông qua các đường truyền thông: điện thoại, ISDN, T1,

X.25...Cùng với sự phát triển của switch, chức năng đầu tiên của router ngày nay đã được switch đảm nhận một cách hiệu quả. Router chỉ còn phải đảm nhận việc thực hiện cáckết nối truy cập từ xa (remote access) hay các kết nối WAN cho hệ thống mạng LAN.

Do hoạt động ở tầng thứ 3 của mô hình OSI, router sẽ hiểu được các protocol quyết định phương thức truyền dữ liệu. Các địa chỉ mà router hiểu là các địa chỉ "giả" được quy định bởi các protocol. Ví dụ như địa chỉ IP đối với protocol TCP/IP, địa chỉ IPX đối với protocol IPX... Do đó tùy theo cấu hình, router quyết định phương thức và đích đến của việc chuyển các packet từ nơi này sang nơi khác. Một cách tổng quát router sẽ chuyển packet theo các bước sau:

- Đọc packet.
- Gỡ bỏ dạng format quy định bởi protocol của nơi gửi.
- Thay thế phần gỡ bỏ đó bằng dạng format của protocol của đích đến.
- Cập nhật thông tin về việc chuyển dữ liệu: địa chỉ, trạng thái của nơi gửi, nơi nhận.
- Gửi packet đến nơi nhận qua đường truyền tối ưu nhất.



Hình 1.1: Tiến trình đóng gói dữ liệu

I.2 Phân loại:

Router có nhiều cách phân loại khác nhau. Tuy nhiên người ta thường có hai cách phân loại chủ yếu sau:

Dựa theo công dụng của Router: theo cách phân loại này người ta chia router thành

remote access router, ISDN router, Serial router, router/hub...

Dựa theo cấu trúc của router: fixed configuration router, modular router.

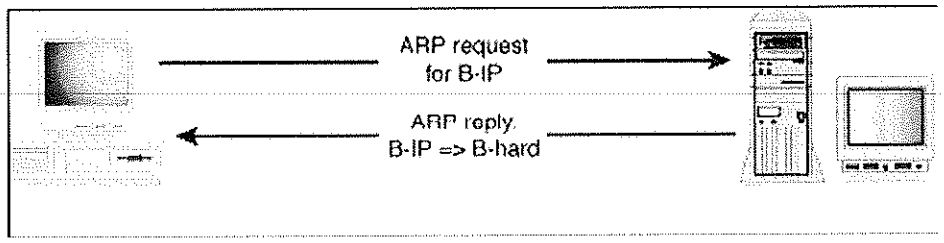
Tuy nhiên không có sự phân loại rõ ràng router: mỗi một hãng sản xuất có thể có các tên gọi khác nhau, cách phân loại khác nhau.

II. Các khái niệm cơ bản về Router và cơ chế routing:

II.1 Nguyên tắc hoạt động của Router – ARP Protocol:

Như ta đã biết tại tầng network của mô hình OSI, chúng ta thường sử dụng các loại địa chỉ mang tính chất quy ước như IP, IPX... Các địa chỉ này là các địa chỉ có hướng, nghĩa là chúng được phân thành hai phần riêng biệt là phần địa chỉ network và phần địa chỉ host. Cách đánh số địa chỉ như vậy nhằm giúp cho việc tìm ra các đường kết nối từ hệ thống mạng này sang hệ thống mạng khác được dễ dàng hơn. Các địa chỉ này có thể được thay đổi theo tùy ý người sử dụng. Trên thực tế, các card mạng chỉ có thể kết nối với nhau theo địa chỉ MAC, địa chỉ cố định và duy nhất của phần cứng. Do vậy ta phải có một phương pháp để chuyển đổi các dạng địa chỉ này qua lại với nhau. Từ đó ta có giao thức phân giải địa chỉ: Address Resolution Protocol (ARP).

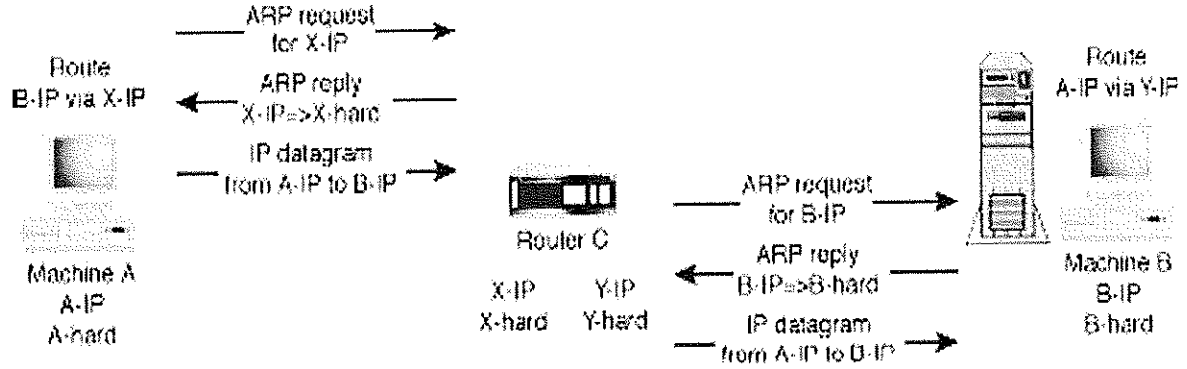
- **ARP** là một protocol dựa trên nguyên tắc: Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng network (IP, IPX...) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng network của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một packet (trong đó có chứa địa chỉ MAC của mình). Trong một hệ thống mạng đơn giản như hình 3, ví dụ như máy A muốn gửi packet đến máy B và nó chỉ biết được địa chỉ IP của máy B. Khi đó máy A sẽ phải gửi một ARP broadcast cho toàn mạng để hỏi xem "địa chỉ MAC của máy có địa chỉ IP này là gì". Khi máy B nhận được broadcast này, có sẽ so sánh địa chỉ IP trong packet này với địa chỉ IP của nó. Nhận thấy địa chỉ đó là địa chỉ của mình, máy B sẽ gửi lại một packet cho máy B trong đó có chứa địa chỉ MAC của B. Sau đó máy A mới bắt đầu truyền packet cho B.



Hình 3

Trong một môi trường phức tạp hơn: hai hệ thống mạng gắn với nhau thông qua một router C. Máy A thuộc mạng A muốn gửi packet đến máy B thuộc mạng B. Do các broadcast không thể truyền qua router nên khi đó máy A sẽ xem router C như một cầu nối để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của router C (port X) và biết được rằng để truyền packet tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng routing (routing table). Bảng routing table theo cơ chế này được lưu giữ trong mỗi máy. Routing table chứa thông tin về các gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của router C. Routing table sẽ có chứa địa chỉ IP của port X. Quá trình truyền dữ liệu theo từng bước sau:

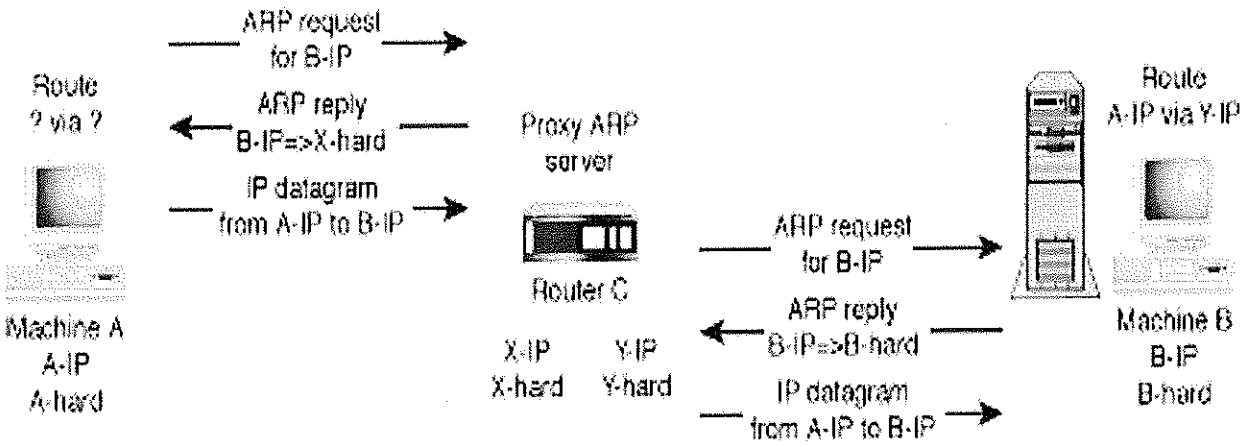
- Máy A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.
- Router C trả lời, cung cấp cho máy A địa chỉ MAC của port X.
- Máy A truyền packet đến port X của router.
- Router nhận được packet từ máy A, chuyển packet ra port Y của router. Trong packet có chứa địa chỉ IP của máy B.
- Router sẽ gửi ARP request để tìm địa chỉ MAC của máy B.
- Máy B sẽ trả lời cho router biết địa chỉ MAC của mình.
- Sau khi nhận được địa chỉ MAC của máy B, router C gửi packet của A đến B.



Hình 4

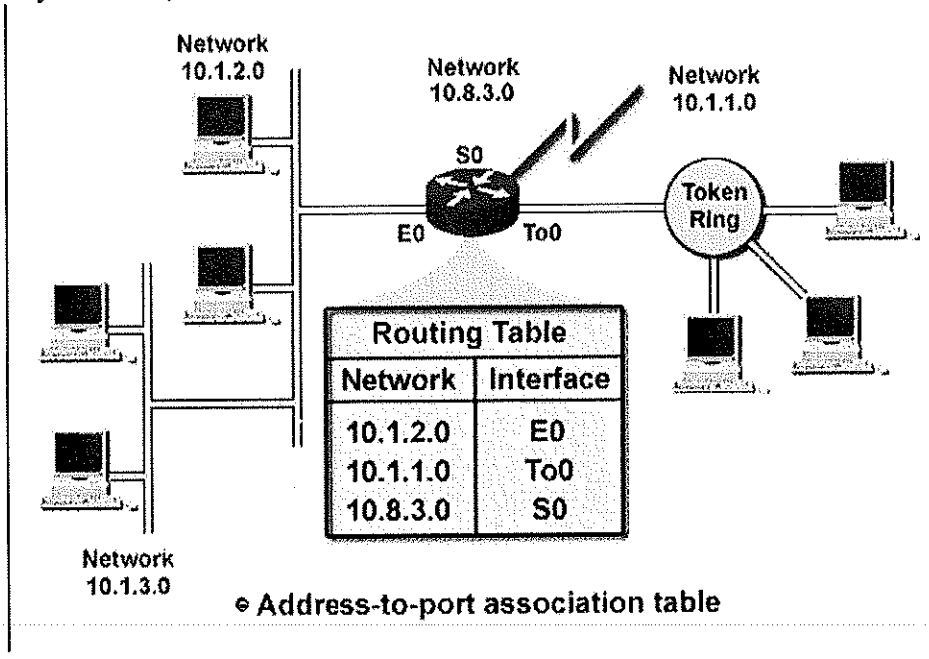
Trên thực tế ngoài dạng routing table này người ta còn dùng phương pháp proxy ARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác.

Quá trình này được trình bày trong hình 5.



Hình 5: Phân giải địa chỉ dùng proxy ARP.

Theo đó các máy trạm không cần giữ bảng routing table nữa router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy trong các mạng kết nối với nó. Router sẽ có một bảng routing table riêng biệt chứa tất cả các thông tin cần thiết để chuyển dữ liệu.



Bảng 6: ví dụ về routing table.

Trong bảng, dòng đầu tiên có nghĩa là tất cả các packet gửi cho một máy bất kỳ thuộc mạng 10.1.2.0 subnet mask 255.255.255.0 sẽ thông qua port ethenet 0 (eth0) có địa chỉ IP là 10.1.2.1. Flag = U có nghĩa là port trong trạng thái hoạt động ("up").

II.2.Một số khái niệm cơ bản:

Path determination:

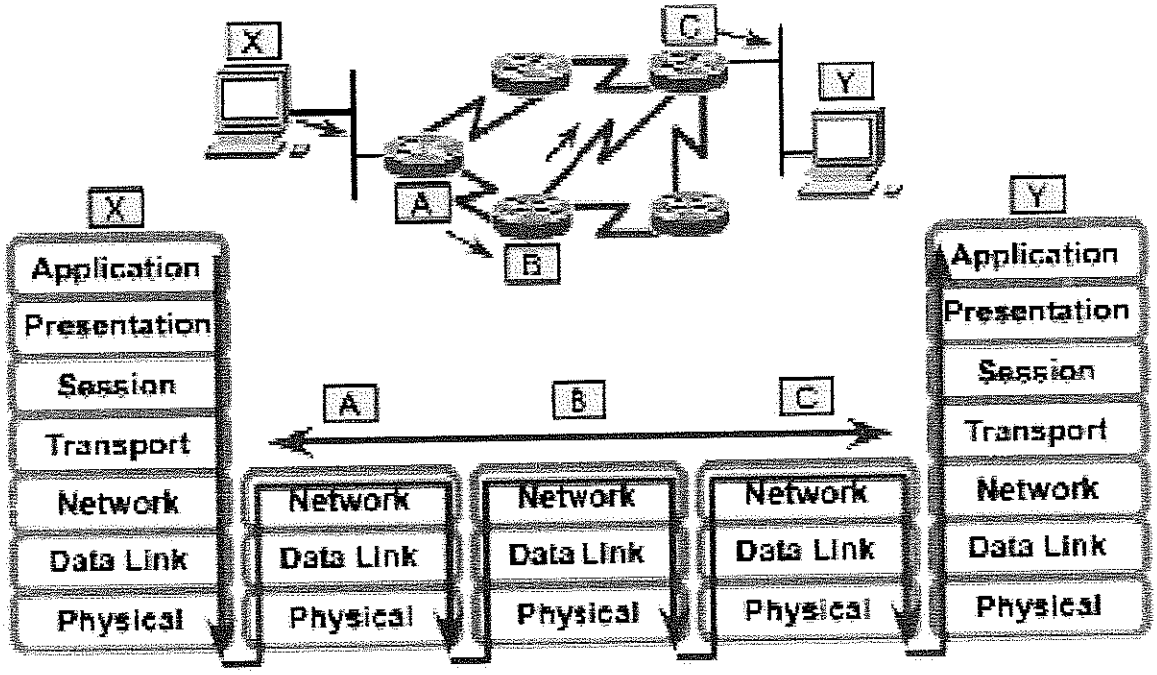
Như đã được đề cập ở phần trên, router có nhiệm vụ chuyển dữ liệu theo một đường liên kết tối ưu. Đối với một hệ thống gồm nhiều router kết nối với nhau, trong đó các router có nhiều hơn hai đường liên kết với nhau, vấn đề xác định đường truyền dữ liệu (path determination) tối ưu đóng vai trò rất quan trọng. Router phải có khả năng lựa chọn đường liên kết tối ưu nhất trong tất cả các đường có thể, mà dữ liệu có thể truyền đến đích nhanh nhất. Việc xác định đường dựa trên các thuật toán routing, các routing protocol, từ đó rút ra được một số đo gọi là metric để so sánh giữa các đường với nhau.

Sau khi thực hiện việc kiểm tra trạng thái của các đường liên kết bằng các thuật toán dựa trên routing protocol, router sẽ rút ra được các metric tương ứng cho mỗi đường, cập nhật vào routing table. Router sẽ chọn đường nào có metric nhỏ nhất để truyền dữ liệu.

Switching:

Quá trình chuyển dữ liệu (switching) là quá trình cơ bản của router, được dựa trên ARP protocol. Khi một máy muốn gửi packet qua router cho một máy thuộc mạng khác, nó gửi packet đó đến router theo địa chỉ MAC của router, kèm theo địa chỉ protocol (network address) của máy nhận. Router sẽ xem xét network address của máy nhận để biết xem nó thuộc mạng nào. Nếu router không biết được phải chuyển packet đi đâu, nó sẽ loại bỏ (drop) packet. Nếu router nhận thấy có thể chuyển packet đến đích, nó sẽ bổ sung MAC address của máy nhận vào packet và gởi packet đi.

Việc chuyển dữ liệu có thể phải đi qua nhiều router, khi đó mỗi router phải biết được thông tin về tất cả các mạng mà nó có thể truyền dữ liệu tới. Vì vậy, các thông tin của mỗi router về các mạng nối trực tiếp với nó sẽ phải được gửi đến cho tất cả các router trong cùng một hệ thống. Trong quá trình truyền **địa chỉ MAC của packet luôn thay đổi nhưng địa chỉ network không thay đổi**. Hình 7 trình bày quá trình chuyển packet qua một hệ thống bao gồm nhiều router.



Hình 7: Quá trình chuyển packet qua một hệ thống bao gồm nhiều router.

Thuật toán routing:

– Mục đích và yêu cầu:

o *Tính tối ưu*: Là khả năng chọn đường truyền tốt nhất của thuật toán. Mỗi một thuật toán có thể có cách phân tích đường truyền riêng, khác biệt với các thuật tóan khác, tuy nhiên mục đích chính vẫn là để xác định đường truyền nào là đường truyền tốt nhất.

o Tính đơn giản: Một thuật toán đòi hỏi phải đơn giản, dễ thực hiện, ít chiếm dụng băng thông đường truyền.

o *Ổn định, nhanh chóng, chính xác*: Thuật toán phải ổn định và chính xác để bảo đảm hoạt động tốt khi xảy ra các trường hợp hư hỏng phần cứng, quá tải đường truyền... Mặt khác thuật toán phải bảo đảm sự nhanh chóng để tránh tình trạng lặp trên đường truyền như hình 5 do không cập nhật kịp trạng thái đường truyền.

o *Sự linh hoạt*: Tính năng này bảo đảm sự thay đổi kịp thời và linh hoạt trong

bất cứ mọi trường hợp xảy ra trong hệ thống.

– Phân loại:

Thuật toán routing có thể thuộc một hay nhiều loại sau đây:

o Static hay dynamic.

-Static routing: là cơ chế trong đó người quản trị quyết định, gán sẵn protocol cũng như địa chỉ đích cho router: đến mạng nào thì phải truyền qua port nào, địa chỉ là gì... Các thông tin này chứa trong routing table và chỉ được cập nhật hay thay đổi bởi người quản trị.

Static routing thích hợp cho các hệ thống đơn giản, có kết nối đơn giữa hai router, trong đó đường truyền dữ liệu đã được xác định trước.

-Dynamic routing: dùng các routing protocol để tự động cập nhật các thông tin về các router xung quanh. Tùy theo dạng thuật toán mà cơ chế cập nhật thông tin của các router sẽ khác nhau. Dynamic routing thường dùng trong các hệ thống phức tạp hơn, trong đó các router được liên kết với nhau thành một mạng lưới, ví dụ như các hệ thống router cung cấp dịch vụ internet, hệ thống của các công ty đa quốc gia.

o Single-Path hay Multipath.

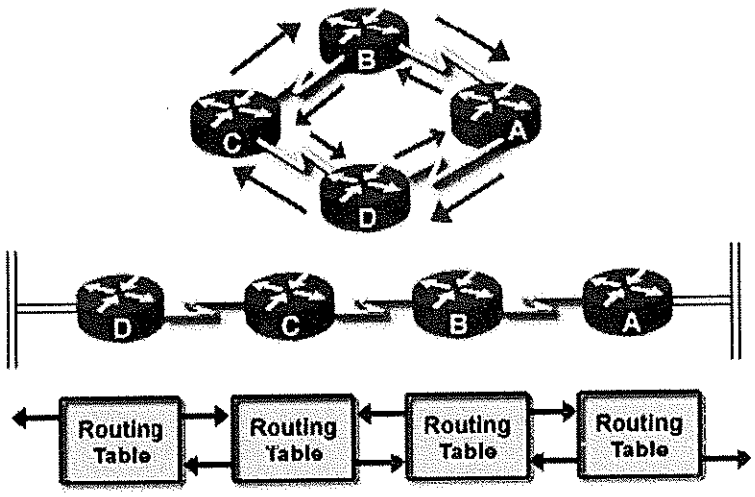
Thuật toán multipath cho phép việc đa hợp dữ liệu trên nhiều liên kết khác nhau còn thuật toán single path thì không. Multi path cung cấp một lưu lượng dữ liệu và độ tin cậy cao hơn single path.

o Flat hay Hierarchical.

Thuật toán flat routing dùng trong các hệ thống có cấu trúc ngang hàng với nhau, được trải rộng với chức năng và nhiệm vụ như nhau. Trong khi đó thuật toán hierachical là thuật toán phân cấp, có cấu trúc cây như mô hình phân cấp của một domain hay của một công ty. Tùy theo dạng hệ thống mà ta có thể lựa chọn thuật toán thích hợp.

o Link State or Distance Vector.

Thuật toán link state (còn được gọi là thuật toán shortest path first) cập nhật tất cả các thông tin về cơ chế routing cho tất cả các node trên hệ thống mạng. Mỗi router sẽ gửi một phần của routing table, trong đó mô tả trạng thái của các liên kết riêng của mình lên trên mạng. Chỉ có các thay đổi mới được gửi đi.



Hình 8: Thuật toán Distance Vector.

-Thuật toán distance vector: (còn gọi là thuật toán Bellman-Ford) bắt buộc mỗi router phải gửi toàn bộ hay một phần routing table của mình cho router kết nối trực tiếp với nó theo một chu kỳ nhất định (Hình 8)

Về mặt bản chất, thuật toán link state gửi bảng cập nhật có kích thước nhỏ đến khắp nơi trong mạng, trong khi thuật toán distance vector gửi các bảng cập nhật có kích thước lớn hơn chỉ cho router kết nối với nó.

Thuật toán distance vector có ưu điểm là dễ thực hiện, dễ kiểm tra, tuy nhiên nó có một số hạn chế là thời gian cập nhật lâu, chiếm dụng băng thông lớn trên mạng. Ngoài ra nó cũng làm lãng phí băng thông do tính chất cập nhật theo chu kỳ của mình.

Thuật toán distance vector thường dùng trong các routing protocol: RIP(IP/IPX), IGRP (IP), RTMP(AppleTalk)... và thường áp dụng cho hệ thống nhỏ.

-Thuật toán link state: có ưu điểm là có tốc độ cao, không chiếm dụng băng thông nhiều như thuật toán distance vector. Tuy nhiên thuật toán này đòi hỏi cao hơn về bộ nhớ, CPU cũng như việc thực hiện khá phức tạp.

Thuật toán link state được sử dụng trong routing protocol: OSPF, NLSP... và thích hợp cho các hệ thống cỡ trung và lớn. Ngoài ra còn có sự kết hợp hai thuật toán này trong một số routing protocol như: IS-IS, EIGRP.

– Các số đo cơ bản trong thuật toán routing:

Metric là số đo của thuật toán routing để từ đó quyết định đường đi tối ưu nhất cho dữ

liệu. Một thuật toán routing có thể sử dụng nhiều metric khác nhau. Các metric được kết hợp với nhau để thành một metric tổng quát, đặc trưng cho liên kết. Mỗi thuật toán có thể sử dụng kiểu sử dụng metric khác nhau. Các metric thường được dùng là.

o Path Length:

Là metric cơ bản, thường dùng nhất. Path length trong router còn được xác định bằng số hop giữa nguồn và đích. Một hop được hiểu là một liên kết giữa hai router.

o Reliability:

Là khái niệm chỉ độ tin cậy của một liên kết. Ví dụ như độ tin cậy được thể hiện thông qua bit error rate... Khái niệm này nhằm chỉ khả năng hoạt động ổn định của liên kết.

o Delay:

Khái niệm delay dùng để chỉ khoảng thời gian cần để chuyển packet từ nguồn đến đích trong hệ thống. Delay phụ thuộc vào nhiều yếu tố: khoảng cách vật lý, băng thông của liên kết, đụng độ, tranh chấp đường truyền. Chính vì thế yếu tố này là một metric đóng vai trò rất quan trọng trong thuật toán routing.

o Bandwidth

Là một metric quan trọng để đánh giá đường truyền. Bandwidth chỉ lưu lượng dữ liệu tối đa có thể truyền trên liên kết.

o Load

Load nhằm chỉ phần trăm network resource đang trong trạng thái bận {busy). Load có thể là lưu lượng dữ liệu trên liên kết, là độ chiếm dụng bộ nhớ, CPU...

Routed protocol và Routing Protocol

– Phân biệt giữa hai khái niệm:

Routed protocol quy định dạng format và cách sử dụng của các trường trong packet nhằm chuyển các packet từ nơi này sang nơi khác (đến tận người sử dụng) Ví dụ: IP, IPX...

Routing protocol: cho phép các router kết nối với nhau và cập nhật các thông tin của nhau nhờ các bảng routing. Routing protocol có thể sử dụng các routed protocol để truyền thông tin giữa các router. Ví dụ: RIP (Router Information Protocol), IGRP (Interior Gateway Routing Protocol)...Routing protocol quyết định:

o Router nào cần biết thông tin về các router khác.

o Việc cập nhật thông tin như thế nào.

II.3.Các routing protocol tiêu biểu:

Các routing protocol được trình bày trong bảng 1.3.

Tên	Tên đầy đủ	Routed Protocol hỗ trợ
RIP	Routing Information Protocol	TCP/IP, IPX
IGRP	Interior Gateway Routing Protocol	TCP/IP
OSPF	Open Shortest Path First	TCP/IP
EGP	Exterior Gateway Protocol	TCP/IP
BGP	Border Gateway Protocol	TCP/IP
IS-IS	Intermediate System to Intermediate System	TCP/IP
EIGRP	Enhanced Interior Gateway Routing Protocol	TCP/IP
NLSP	NetWare Link Services Protocol	IPX/SPX
RTMP	Routing Table Maintenance Protocol	AppleTalk

Bảng 1.3: Các routing protocol tiêu biểu

o RIP:

RIP là chữ viết tắt của Routing Information Protocol, là 1 trong những routing protocol đầu tiên được sử dụng. RIP dựa trên thuật toán distance vector, được sử dụng rất rộng rãi tuy nhiên chỉ thích hợp cho các hệ thống nhỏ và ít phức tạp. RIP tự động cập nhật thông tin về các router bằng cách gửi các broadcast lên mạng mỗi 30 giây. RIP xác định đường bằng hop count (path length). Số lượng hop tối đa là 15.

o IGRP:

Là loại routing protocol hiện nay đang thường dùng nhất, được phát triển bởi Cisco, có các đặc điểm sau:

♦ Dùng cơ chế advanced distance vector. Chỉ cập nhật thông tin khi có sự thay đổi cấu trúc.

♦ Việc xác định đường được thực hiện linh hoạt thông qua nhiều yếu tố: số hop, băng thông, độ trì hoãn, độ tin cậy...

♦ Có khả năng vượt giới hạn 15 hop.

♦ Có khả năng hỗ trợ cho nhiều đường liên kết với khả năng cân bằng tải cao.

♦ Linh hoạt, thích hợp cho các hệ thống lớn, do dựa trên cơ chế link state kết hợp với distance vector.

o OSPF:

Là loại routing protocol tiên tiến, dựa trên cơ chế link-state có khả năng cập nhật sự thay đổi một cách nhanh nhất. Sử dụng IP multicast làm phương pháp truyền nhận thông tin. Thích hợp với các hệ thống lớn, gồm nhiều router liên kết với nhau.

III. Khái niệm về cấu hình Router.

Cấu hình router là sử dụng các phương pháp khác nhau để định cấu hình cho router thực hiện các chức năng cụ thể: liên kết leased line, liên kết dial-up, firewall, Voice Over IP...trong từng trường hợp cụ thể. Đối với Cisco Router thường có 03 phương pháp để định cấu hình cho router:

Sử dụng CLI:

CLI là chữ viết tắt của Command Line Interface, là cách cấu hình cơ bản áp dụng cho hầu hết các thiết bị của Cisco. Người sử dụng có thể dùng các dòng lệnh nhập từ các Terminal (thông qua port Console hay qua các phiên Telnet) để định cấu hình cho Router.

Sử dụng Chương trình ConfigMaker:

ConfigMaker là chương trình hỗ trợ cấu hình cho các Router từ 36xx trở xuống của Cisco. Chương trình này cung cấp một giao diện đồ họa và các Wizard thân thiện, được trình bày dưới dạng "Question – Answer", giúp cho việc cấu hình router trở nên rất đơn giản. Người sử dụng có thể không cần nắm vững các câu lệnh của Cisco mà chỉ cần một kiến thức cơ bản về hệ thống là có thể cấu hình được router. Tuy nhiên ngoài hạn chế về số sản phẩm router hỗ trợ như ở trên, chương trình này cũng không cung cấp đầy đủ tất cả các tính năng của router và không có khả năng tuỳ biến theo các yêu cầu cụ thể đặc thù.

Hiện nay version mới nhất của ConfigMaker là ConfigMaker 2.4.

Sử dụng chương trình FastStep:

Khác với chương trình ConfigMaker, FastStep được cung cấp dựa trên từng loại sản phẩm cụ thể của Cisco. Ví dụ như với Cisco router 2509 thì có FastStep for Cisco Router 2509... Chương trình này cung cấp các bước để cấu hình các tính năng cơ bản cho từng loại sản phẩm. Các bước cấu hình cũng được trình bày dưới dạng giao diện đồ họa, "Question – Answer" nên rất dễ sử dụng. Tuy vậy cũng như chương trình

ConfigMaker, FastStep chỉ mới hỗ trợ cho một số sản phẩm cấp thấp của Cisco và chỉ giúp cấu hình cho một số chức năng cơ bản của router.

Tóm lại, việc sử dụng CLI để cấu hình Cisco Router tuy phức tạp nhưng vẫn là cách cấu hình router thường gặp nhất. Hiểu biết việc cấu hình bằng CLI sẽ giúp người sử dụng linh hoạt trong việc cấu hình và dễ dàng khắc phục sự cố. Hiện nay việc sử dụng CLI có thể kết hợp với một trong 02 cách cấu hình còn lại để đẩy nhanh tốc độ cấu hình router. Khi đó, các chương trình cấu hình sẽ sử dụng để tạo các file cấu hình thô, phương pháp CLI sẽ được sử dụng sau cùng để tùy biến hay thực hiện các tác vụ mà chương trình không thực hiện được. Trong tài liệu này các hướng dẫn cấu hình đều là phương pháp CLI – phương pháp dùng dòng lệnh.

III.1. Cấu trúc router.

Cấu trúc router là một trong các vấn đề cơ bản cần biết trước khi cấu hình router. Cấu trúc của router được trình bày trong hình 2.1.Các thành phần chính của router bao gồm:

NVRAM:

NVRAM (Nonvolatile random-access memory) là loại RAM có thể lưu lại thông tin ngay cả khi không còn nguồn nuôi. Trong Cisco Router NVRAM thường có nhiệm vụ sau:

– Chứa file cấu hình startup cho hầu hết các loại router ngoại trừ router có Flash file system dạng Class A. (7xxx)

– Chứa Software configuration register, sử dụng để xác định IOS image dùng trong quá trình boot của router.

Flash memory:

Flash memory chứa Cisco IOS software image. Đối với một số loại, Flash memory có thể chứa các file cấu hình hay boot image..

Tùy theo loại mà Flash memory có thể là EPROMs, single in-line memory (SIMM) module hay Flash memory card:

-Internal Flash memory:

o Internal Flash memory thường chứa system image.

o Một số loại router có từ 2 Flash memory trở lên dưới dạng single in-line memory modules (SIMM). Nếu như SIMM có 2 bank thì được gọi là *dual-bank Flash memory*. Các bank này có thể được phân thành nhiều phần logic nhỏ

- Bootflash

o Bootflash thường chứa boot image.

o Bootflash đôi khi chứa ROM Monitor.

– Flash memory PC card hay PCMCIA card.

Flash memory card để gắn vào Personal Computer Memory Card International Association (PCMCIA) slot. Card này dùng để chứa system image, boot image và file cấu hình.

Các loại router sau có PCMCIA slot:

o Cisco 1600 series router: 01 PCMCIA slot.

o Cisco 3600 series router: 02 PCMCIA slots.

o Cisco 7200 series Network Processing Engine (NPE): 02 PCMCIA slots

o Cisco 7000 RSP700 card và 7500 series Route Switch Processor (RSP) card chứa 02 PCMCIA slots.

DRAM:

Dynamic random-access memory (DRAM) bao gồm 02 loại:

– Primary, main, hay processor memory, dành cho CPU dùng để thực hiện Cisco IOS software và lưu giữ running configuration và các bảng routing table.

– Shared, packet, or I/O memory, which buffers data transmitted or received by the router's network interfaces.

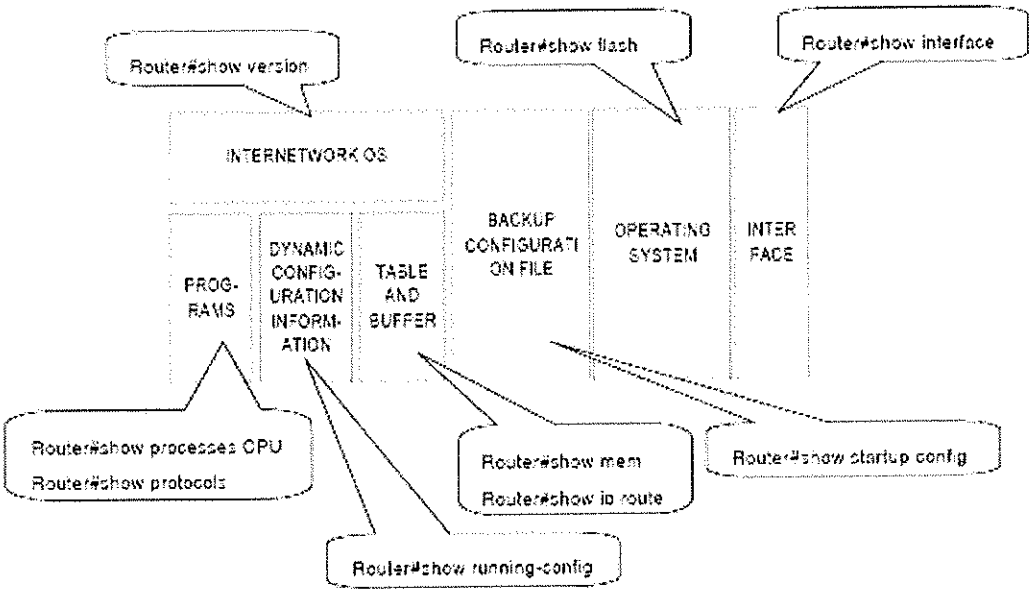
Tùy vào IOS và phần cứng mà có thể phải nâng cấp Flash RAM và DRAM.

ROM

Read only memory (ROM) thường được sử dụng để chứa các thông tin sau:

– ROM monitor, cung cấp giao diện cho người sử dung khi router không tìm thấy các file image không phù hợp.

– Boot image, giúp router boot khi không tìm thấy IOS image hợp lệ trên flash memoty.



Hình 2.1

III.2 Các mode config:

Cisco router có nhiều chế độ (mode) khi config, mỗi chế độ có đặc điểm riêng, cung cấp một số các tính năng xác dịnh để cấu hình router. Các mode của Cisco router được trình bày trong hình 9.

User Mode hay User EXEC Mode:

Đây là mode đầu tiên khi bạn bắt đầu một phiên làm việc với router (qua Console hay Telnet). Ở mode này bạn chỉ có thể thực hiện được một số lệnh thông thường của router. Các lệnh này chỉ có tác dụng một lần như lệnh **show** hay lệnh **clear** một số các counter của router hay interface. Các lệnh này sẽ không được ghi vào file cấu hình của router và do đó không gây ảnh hưởng đến các lần khởi động sau của router.

Privileged EXEC Mode:

Để vào Privileged EXEC Mode, từ User EXEC mode gõ lệnh **enable** và password (nếu cần). Privileged EXEC Mode cung cấp các lệnh quan trọng để theo dõi hoạt động của router, truy cập vào các file cấu hình, IOS, đặt các password... Privileged EXEC Mode là khóa để vào Configuration Mode, cho phép cấu hình tất cả các chức năng hoạt động của router.

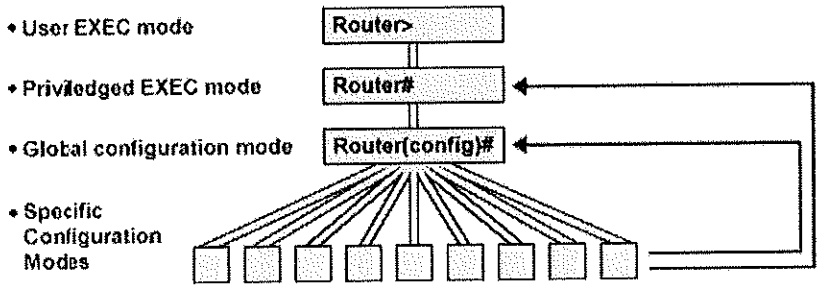
Configuration Mode:

Như trên đã nói, configuration mode cho phép cấu hình tất cả các chức năng của Cisco router bao gồm các interface, các routing protocol, các line console, vty (telnet), tty (async connection). Các lệnh trong configuration mode sẽ ảnh hưởng trực tiếp đến cấu hình hiện hành của router chứa trong RAM (running-configuration). Nếu cấu hình này được ghi lại vào NVRAM, các lệnh này sẽ có tác dụng trong những lần khởi động sau của router.

Configurarion mode có nhiều mode nhỏ, ngoài cùng là global configuration mode, sau đó là các interface configration mode, line configuration mode, routing configuration mode.

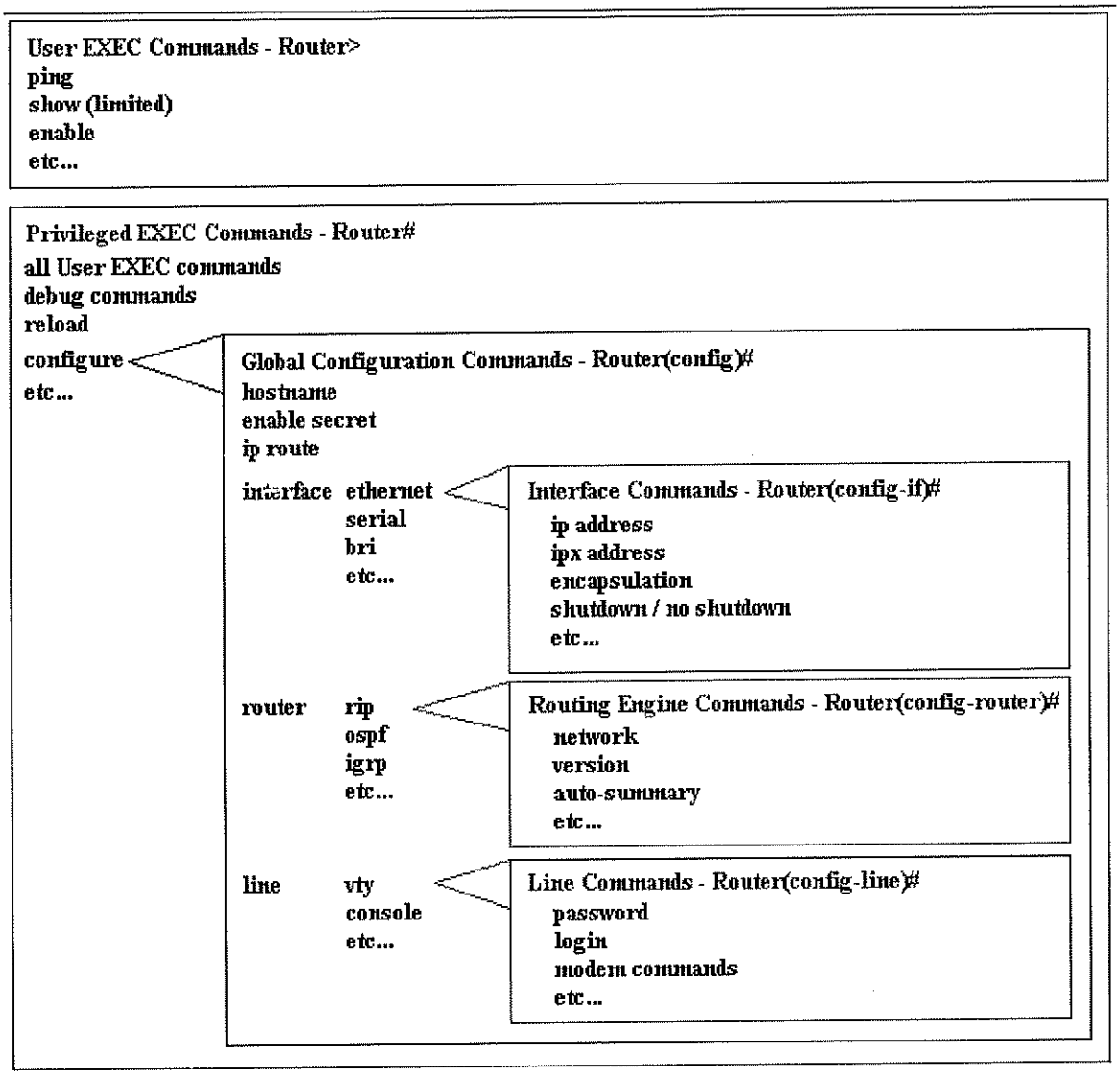
ROM Mode

ROM mode dùng cho các tác vụ chuyên biệt, can thiệp trực tiếp vào phần cứng của router như Recovery password, maintenance. Thông thường ngoài các dòng lệnh do người sử dụng bắt buộc router vào ROM mode, router sẽ tự động chuyển vào ROM mode nếu không tìm thấy file IOS hay file IOS bị hỏng trong quá trình khởi động.



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)#

Hình 2.2



Hình 9: Một số mode config của Cisco Router.

Bảng 10 trình bày các mode cơ bản của Cisco router và một số đặc điểm của chúng:

Mode	Cách thức truy cập	Dấu nhắc	Cách thức thoát
User EXEC	Log in.	Router>	**logout** command.
Privileged EXEC	Từ user EXEC mode, sử dụng lệnh **enable**.	Router#	Để trở về user EXEC mode, dùng lệnh **disable**. Để vào global configuration mode, dùng lệnh **configure terminal**.
Global configuration	Từ privileged EXEC mode, dùng lệnh **configure terminal**	Router(config)#	Để ra privileged EXEC mode, dùng lệnh **exit** hay **end** hay gõ **Ctrl-Z**. Để vào interface configuration mode, gõ lệnh **interface**.
Interface configuration	Từ global configuration mode, gõ lệnh **interface**.	Router(config-if)#	Để ra global configuration mode, dùng lệnh **exit** Để ra privileged EXEC mode, dùng lệnh **exit** hay gõ **Ctrl-Z**. Để vào subinterface configuration mode, xác định subinterface bằng lệnh **interface**
Subinterface configuration	Từ interface configuration mode, xác định subinterface bằng lệnh **interface**.	Router(config-subif)#	To exit to global configuration mode, use the exit command. To enter privileged EXEC mode, use the end command or press Ctrl-Z.
ROM monitor	Từ privileged EXEC mode, dùng lệnh **reload** nhấn phim Break trong 60s khi router khởi động Dùng lệnh **boot system rom**.	>	Để ra user EXEC mode, gõ lệnh **continue**

Bảng 10

IV.Cấu hình các tính năng chung của router:

IV.1 Một số quy tắc về trình bày câu lệnh:

Các quy tắc trình bày tại bảng sau được sử dụng trong đề tài này cũng như trong tất cảcác tài liệu khác của Cisco

Cách trình bày	Ý nghĩa
^ hay Ctrl	Phím Ctrl.
Screen	Hiển thị các thông tin sẽ được trình bày trên màn hình.
Boldface	Hiển thị các thông tin (dòng lệnh) mà bạn phải nhập vào từ bàn phím.
< >	Biểu hiện các ký tự không hiển thị trên màn hình, ví dụ như password.
!	Biểu hiện các câu chú thích.
( )	Biểu hiện dấu nhắc hiện tại
[ ]	Biểu hiện các tham số tùy chọn (không bắt buộc) cho câu lệnh.
Italics	Biểu hiện các tham số của dòng lệnh. Các tham số này là bắt buộc phải có và bạn phải chọn giá trị phù hợp cho tham số đó để đưa vào câu lệnh.
{ x | y | z }	Biểu hiện bạn phải chọn một trong các giá trị x, y, z trong câu lệnh.

Bảng 3.1

3.2 Các phím tắt cần sử dụng khi cấu hình router

Cisco router được cấu hình bằng chuỗi các lệnh, để thuận tiện và nhanh chóng hơn trong việc nhập lệnh một số các phím tắt thường được sử dụng được trình bày ở bảng 3.2:

Phim	Công dụng
Delete	Xóa ký tự bên phải con trỏ
Backspace	Xóa ký tự bên trái con trỏ
Left Arrow hay Ctrl-B	Di chuyển con trỏ về bên trái một ký tự
Right Arrow hay Ctrl-F	Di chuyển con trỏ về bên phải một ký tự
Esc-B	Di chuyển con trỏ về bên trái một từ
Esc-F	Di chuyển con trỏ về bên phải một từ
TAB	Hiển thị toàn bộ lệnh (chỉ có tác dụng khi phần đã gõ của lệnh tương ứng đủ để giúp Cisco IOS xác định lệnh đó là duy nhất)
Ctrl-A	Di chuyển con trỏ lên đầu hàng lệnh.
Ctrl-E	Di chuyển con trỏ về cuối hàng lệnh.
Ctrl-R	Hiển thị lại dòng lệnh.
Ctrl-U	Xóa dòng lệnh.
Ctrl-W	Xóa một từ
Ctrl-Z	Kết thúc Configuration Mode, trở về EXEC mode.
Up Arrow hay Ctrl-P	Hiển thị dòng lệnh trước.
Down Arrow hay Ctr-N	Hiển thị dòng lệnh tiếp theo.

Bảng 3.2

Ngoài ra khi cấu hình router, dấu **?** thường được sử dụng ở tất cả các mode để liệt kê danh sách các câu lệnh có thể sử dụng được tại mode đó.

Ví dụ:

```
Router> ?
Exec commands:
<1-99>          Session number to resume
connect         Open a terminal connection
disconnect      Disconnect an existing telnet session
enable          Turn on privileged commands
exit            Exit from the EXEC
help            Description of the interactive help system
```

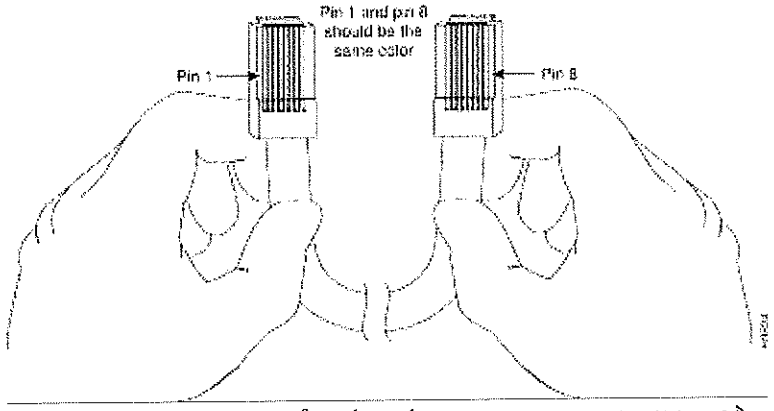
lat	Open a lat connection
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
menu	Start a menu-based user interface
mbranch	Trace multicast route for branch of tree
mrbranch	Trace reverse multicast route to branch of tree
mtrace	Trace multicast route to group
name-connection	Name an existing telnet connection
pad	Open a X.29 PAD connection
ping	Send echo messages
resume	Resume an active telnet connection
show	Show running system information
systat	Display information about terminal lines
telnet	Open a telnet connection
terminal	Set terminal line parameters
tn3270	Open a tn3270 connection
trace	Trace route to destination
where	List active telnet connections
x3	Set X.3 parameters on PAD
xremote	Enter XRemote mode

IV.3 . Các khái niệm về console, telnet. Cách xác định các tên và password cho router.

IV.3.1 Console port

Console port có trên tất cả các loại router dùng để cho các terminal có thể truy cập vào router để định cấu hình cũng như thực hiện các thao tác khác trên router. Console port thường có dạng lỗ cắm cho RJ-45 connector. Để kết nối vào console port ta cần các thiết bị sau:

- 1 terminal, có thể là terminal chuyên dụng của UNIX hay máy PC Windows chạy chương trình HyperTerminal.
- 1 Roll-over cable: sợi cáp này đi kèm với mỗi router (hình 3.1), là cáp UTP có 4 cặp dây và được bấm RJ-45 đảo thứ tự 2 đầu.



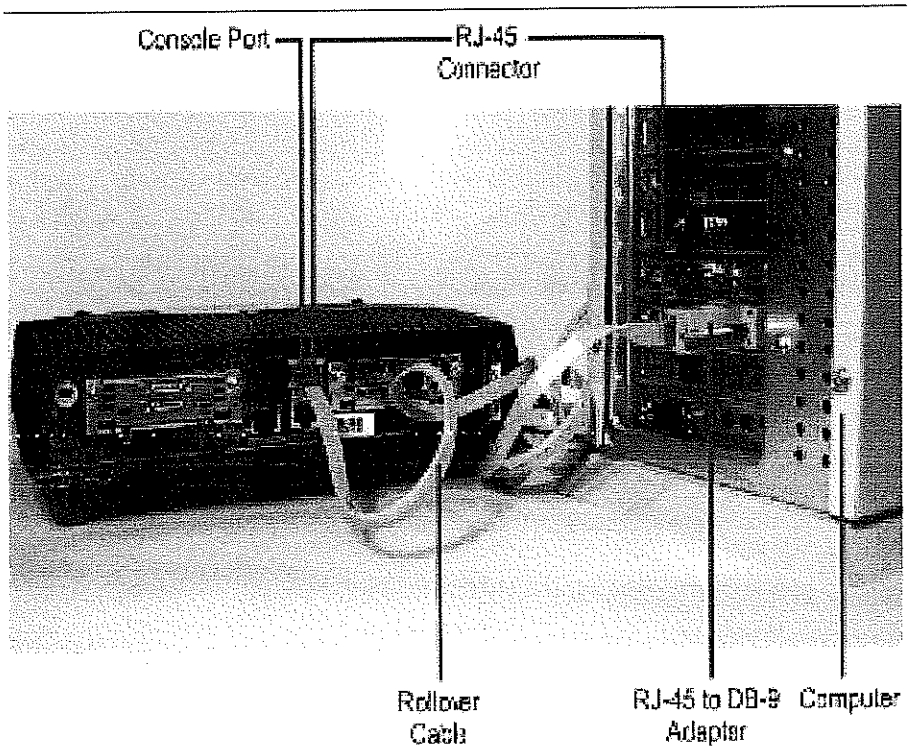
-1 đầu DB-25 hay DB-9 dùng để kết nối vào Terminal. Các đầu nối này có port nối RJ-45 ở phía sau. Các đầu nối này thường được gọi là RJ-45 to DB-9 hay RJ-45 to DB-25 adapter. Kết nối vào console port được thực hiện như hình.

Khi kết nối đã được thực hiện, chạy chương trình (ví dụ như HyperTerminal) của Windows để truy cập vào router. Một số điểm lưu ý khi sử dụng chương trình là:

Chọn đúng COM port kết nối (direct to COM1 hay COM2).

Các thông số của console port là: 9600 baud, 8 data bits, no parity, 2 stop bits. Console port không hỗ trợ cho flow control và modem control.

Nếu không được đặt password cho console port, khi khởi động chương trình HyperTerminal, xác lập đúng các thông số như trên và gõ vài lần Enter, bạn sẽ vào ngay user EXEC mode với dấu nhắc "router>". Password với console port là không bắt buộc, tuy nhiên để bảo đảm an toàn cho hệ thống, ta có thể dùng các bước sau đây để xác định password cho console port của router.



Câu lệnh	Dấu nhắc ban đầu	Dấu nhắc sau khi gõ	Giải thích
enable	Router>	Router#	Vào chế độ Privileged mode, gõ password nếu cần
config terminal	Router#	Router#(config)	Vào global configuration mode
line con0	Router#(config)	Router#(config-line)	Vào line configuration mode.
login	Router#(config-line)	Router#(config-line)	Cho phép login vào router và hiển thị câu hỏi password khi truy cập.
password *password*	Router#(config-line)	Router#(config-line)	Đặt password cho console port.
^ Z	Router#(config-line)	Router#	Trở về Privileged mode.

Bảng 3.3

IV.3.2 Telnet sesstion

Trong hệ thống mạng sử dụng TCP/IP, Telnet là một dịch vụ rất hữu ích giúp cho người sử dụng có thể truy cập và cấu hình thiết bị từ bất cứ nơi nào trong hệ thống hay thông qua các dịch vụ remote access. Để sử dụng được Telnet cho việc truy cập và cấu hình cisco router cần phải có các điều kiện sau:

- Hệ thống mạng sử dụng giao thức TCP/IP
- Gán địa chỉ IP cho ít nhất 01 trong các ethernet port của router và kết nối cổng đó vào hệ thống mạng.
- 1 PC kết nối vào mạng thông qua TCP/IP.

Sau khi thỏa mãn các điều kiện trên, tại PC ta có thể gõ lệnh **telnet** *ip address của ethernet port trên router* để có thể truy cập vào router.

Do mức độ dễ dàng và thuận tiện của telnet trong việc truy cập vào router, việc đặt password cho telnet là rất cần thiết và quan trọng. Bảng sau sẽ trình bày các bước để xác lập password cho các đường telnet.

Câu lệnh	Dấu nhắc ban đầu	Dấu nhắc sau khi gõ	Giải thích
enable	Router>	Router#	Vào chế độ Privileged mode, gõ password nếu cần
config terminal	Router#	Router#(config)	Vào global configuration mode
line vty 0 4	Router#(config)	Router#(config-line)	Vào line configuration mode.
login	Router#(config-line)	Router#(config-line)	Cho phép login vào router và hiển thị câu hỏi password khi truy cập.
password *password*	Router#(config-line)	Router#(config-line)	Đặt password cho console port.
^ Z	Router#(config-line)	Router#	Trở về Privileged mode.

Đường telnet trong Cicso router được ký hiệu là **vty.** Cisco router hỗ trợ 05 phiên telnet đồng thời (ký hiệu từ 0 đến 4). Ta có thể xác định password cho từng đường telnet. Tuy nhiên cả 05 đường thường được cấu hình chung 01 password duy nhất để tăng khả năng bảo mật và dễ quản lý.

IV.3.3 Xác định tên cho router và enable password:

Khi chưa xác định tên cho router, dấu nhắc mặc định của router sẽ là "router>". Việc xác định tên cho router nhằm mục đích quản lý và làm thay đổi dấu nhắc này. Ngoài ra việc xác định enable password cho phép ngăn chặn thêm một lần nữa (ngoài password vào console hay telnet) việc truy cập và thay đổi cấu hình router. Bảng sau trình bày các bước để đặt (hay thay đổi) tên và enable password cho router.

Câu lệnh	Dấu nhắc ban đầu	Dấu nhắc sau khi gõ lệnh	Giải thích
enable	Router>	Router#	Vào chế độ Privileged mode, gõ password nếu cần
config terminal	Router#	Router#(config)	Vào global configuration mode
hostname *name*	Router#(config)	(name)#(config-line)	Xác định tên cho router, dấu nhắc sẽ thay đổi đúng theo tên đã nhập.
enable password *password*	(name)#(config-line)	(name)#(config-line)	Xác định enable password
enable secret *password*	(name)#(config-line)	(name)#(config-line)	Xác định enable password đồng thời mã hóa password trong file cấu hình. Phải đi chung với lệnh **service password-encryption**.
^ Z	(name)#(config-line)	(name)#	Trở về Privileged mode.

Bảng 3.5

IV.4. Làm việc với file cấu hình và IOS image.

IV.4.1 Một số khái niệm cơ bản.

File cấu hình (configuration file):

Là một file dạng text có cấu trúc, trong đó chứa tất cả các lệnh quan trọng của router, quyết định hoạt động của router. Sau khi cấu hình ban đầu, file cấu hình này được ghi vào NVRAM của router và sẽ được sử dụng trong suốt thời gian hoạt động

của router (trong một số loại router, file này có thể chứa ở bootflash RAM, slot 0 hay slot 1 của PCMCIA card). Khi router khởi động file cấu hình này được nạp từ NVRAM vào RAM và thi hành một cách tự động. Việc mất hay hư hỏng file cấu hình này sẽ khiến router rơi vào ROM mode hay setup mode. File cấu hình nằm trong NVRAM được gọi là startupconfig còn nằm trong RAM được gọi là running-config. Ngoại trừ trong quá trình cấu hình router, hai file này thường giống nhau.

*Ví dụ về một file cấu hình của router:

```
Current configuration:
!
version 11.2
! Version of IOS on router, automatic command
!
no service udp-small-servers
no service tcp-small-servers
!
hostname Critter
prompt Emma
! Prompt overrides the use of the hostname as the prompt
!
enable password lu
! This sets the priviledge exec mode password
!
no ip domain-lookup
! Ignores all names resolutions unless locally defined on the router.
!
ipx routing 0000.3089.b170
! Enables IPX rip routing
!
interface Serial0
ip address 137.11.12.2 255.255.255.0
ipx network 12
!
interface Serial1
```

```
description this is the link to Albuquerque
ip address 137.11.23.2 255.255.255.0
ipx network 23
!
interface TokenRing0
ip address 137.11.2.2 255.255.255.0
ipx network CAFE
ring-speed 16
!
router rip
network 137.11.0.0
!
no ip classless
!
banner motd ^C This Here's the Rootin-est Tootin-est Router in these here Parts! ^C
! Any text between the Ctl-C keystroke is considered part of the banner, including
!the return key.!
line con 0
password cisco
login
! login tells the router to supply a prompt; password defines what the user must type!
!
line aux 0
line vty 0 4
password cisco
login
!
end
```

IOS image:

IOS là chữ viết tắt của Internetworking Operating System. IOS thực sự là trái tim của Cisco router. Nó quyết định tất cả các chức năng của thiết bị và bao gồm tất cả các dòng lệnh dùng để cấu hình thiết bị đó. IOS image là thuật ngữ dùng để chỉ file chứa IOS, nhờ đó mà ta có thể backup hay upgrade IOS một cách dễ dàng và thuận tiện. Trong Cisco router IOS thường được chứa trong Flash RAM.

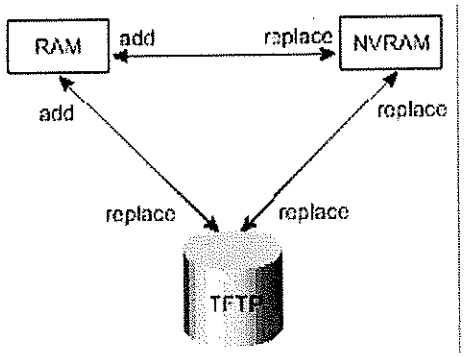
TFTP server.

TFTP là chữ viết tắt của Trial File Transfer Protocol, một protocol chuẩn của giao thức TCP/IP. TFTP là một connectionless, reliable protocol. TFTP Server có thể là một workstation UNIX hay một PC thường chạy chương trình giả lập TFTP server trên một hệ thống mạng TCP/IP. TFTP Server thường được dùng làm nơi backup các file cấu hình, IOS image hay ngược lại là nơi chứa các file cấu hình mới, các IOS image mới để update cho router.

IV.4.2 Làm việc với file cấu hình và IOS.

Với file cấu hình:

Các quá trình làm việc với file cấu hình được mô tả trong hình 11:



Hình 11

Như hình 11 cho thấy, ta có thể chuyển đổi qua lại file cấu hình từ RAM, NVRAM và TFTP Server. Các chuyển đổi đến NVRAM và TFTP thường có nghĩa là thay thế (replace) trong khi các chuyển đổi tới RAM có nghĩa là bổ sung (add).

– Để chuyển đổi file cấu hình trong Cisco router dùng lệnh sau ở privileged mode:

copy {tftp | running-config | startup-config} {tftp | running-config | startup-config}

Ví dụ:

– Để copy file cấu hình từ RAM vào NVRAM ta dùng lệnh sau:

copy running-config startup-config

– Để xem một file cấu hình ta dùng lệnh sau:

show {running-config | startup-config}

– Để xóa một file cấu hình ta dùng lệnh sau:

erase nvram

Ngoài ra ta còn có thể sử dụng các câu lệnh khác có tác dụng tương tự. Các lệnh này là các lệnh cũ thường được sử dụng trong các IOS version 11.0 trở về trước.

Câu lệnh	Câu lệnh tương đương (lệnh cũ)
show running-config	write terminal
show startup-config	show config
copy running-config startup config	write mem
copy running-config tftp	write network
erase nvram	write erase hay erase startup-config.

Làm việc với IOS image.

Như trên đã nói IOS image đóng vai trò rất quan trọng đối với router. Làm việc với IOS image nghĩa là thực hiện việc lưu giữ các IOS image, cập nhật các IOS image từ Cisco, quản lý các IOS image trong router và có khả năng xác định các IOS image dùng để khởi động router.

– Lưu giữ IOS image.

IOS image thường được lưu giữ ở TFTP server bằng câu lệnh sau:

copy flash tftp

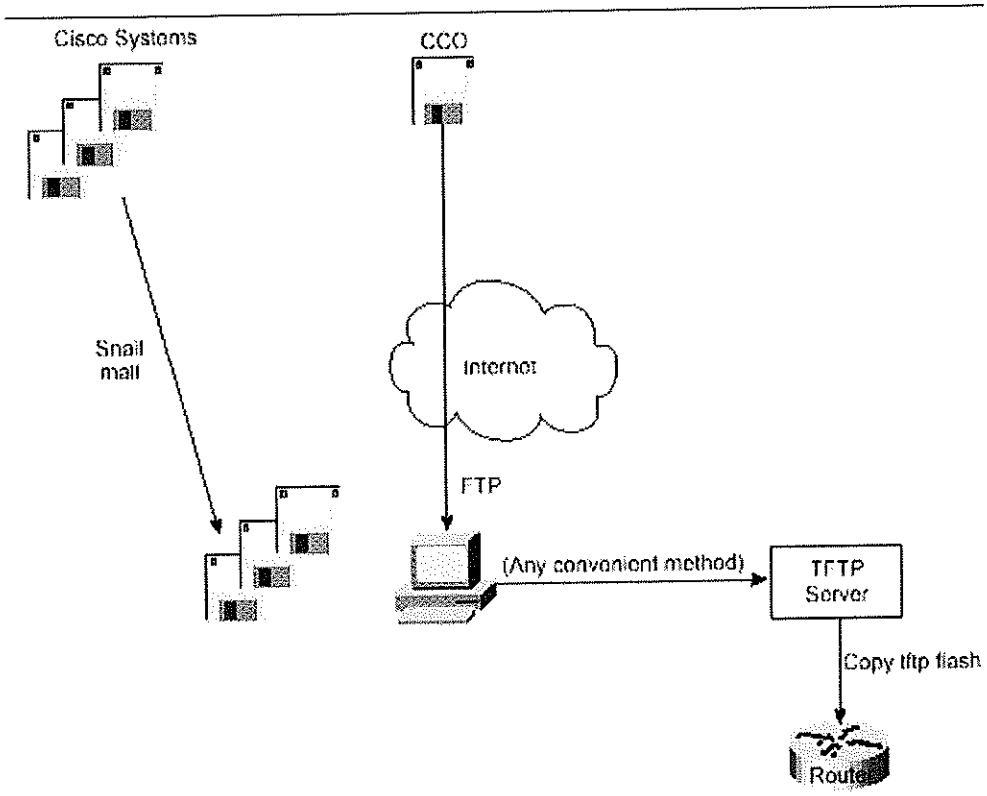
– Cập nhật IOS image từ Cisco.

Thiết kế dùng IOS image của Cisco giúp cho thiết bị có khả năng nâng cấp nhanh chóng và linh hoạt. Các IOS image của Cisco thường xuyên được cập nhật để khắc phục các lỗi của version trước và bổ sung các tính năng mới cho router. Việc cập nhật này có thể được mô tả bằng hình 12.

Lệnh để cập nhật IOS image là:

Copy tftp flash

Sau khi gõ lệnh này router sẽ hiện ra tên các IOS image hiện có trong flash RAM, hỏi bạn địa chỉ IP của TFTP và chờ bạn xác nhận trước khi copy. Ví dụ sau sẽ trình bày chi tiết về điều này.



Hình 12: Quy trình cập nhật IOS image.

Ví dụ:

R1#**copy tftp flash**
System flash directory:
File Length Name/status
1 7530760 c2500-ainr-l_112-31.bin
[7530824 bytes used, 857784 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 134.141.3.33
Source file name? c2500-ainr-l_112-11.bin
Destination file name [c2500-ainr-l_112-11.bin]?
Accessing file 'c2500-ainr-l_112-11.bin' on 134.141.3.33...
Loading c2500-ainr-l_112-11.bin from 134.141.3.33 (via TokenRing0): ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'c2500-ainr-l_112-11.bin' from server

as 'c2500-ainr-l_112-11.bin' into Flash WITH erase? [yes/no]y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading c2500-ainr-l_112-11.bin from 134.141.3.33 (via TokenRing0):
!!
!!
!!
!!
!!
!!
!!
!!
....
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7530760/8388608 bytes]
Verifying checksum... OK (0xA93E)
Flash copy took 0:04:26 [hh:mm:ss]
R1#

– Xem nội dung của flash RAM

Dùng lệnh **show flash** để xem thông tin về IOS image chứa trong flash RAM

Ví dụ:

fred#**show flash**
System flash directory:
File Length Name/status
1 4181132 c2500-i-l.112-7a
[4181196 bytes used, 4207412 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)

– Chọn IOS image để khởi động router.

Trong mỗi router có 01 thanh ghi gọi là configuration register. Đây là một thanh ghi 16-bit (Hình 3.5) trong đó 4 bit cuối cùng được gọi là boot field quyết định quá trình khởi động của router. Giá trị của boot field cho biết router sẽ khởi động từ ROM hay từ RAM. Can thiệp vào quá trình khởi động của router thông qua configuration register thường dùng trong quá trình password recovery.

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0

Hình 13: configuration register.

Một cách khác đơn giản và thường được sử dụng là dùng lệnh **boot system** của IOS. Lệnh này thường được đặt và trong startup-config của router. Bảng sau sẽ tổng kết lại cả hai phương pháp trên

Giá trị của boot field	Câu lệnh boot system	Kết quả
0x0	Không ảnh hưởng	ROM monitor mode.
0x1	Không ảnh hưởng	ROM mode.
0x2 đến 0xF	**Boot system rom**	ROM mode
0x2 đến 0xF	**Boot system flash**	IOS đầu tiên trong flash sẽ được dùng để khởi động.
0x2 đến 0xF	**Boot system flash** *filename*	IOS image trong flash được chỉ định sẽ được dùng để khởi động.
0x2 đến 0xF	**Boot system tftp** *ip address filename*	IOS image có tên là *filename* trong TFTP server có địa chỉ *ip address* sẽ được dùng để khởi động.
0x2 đến 0xF	Nhiều lệnh **boot system**	Router sẽ sử dụng các lệnh từ trên xuống dưới cho đến khi có một lệnh được thực hiện hoàn tất. Nếu tất cả các lệnh đều không thi hành được, router sẽ khởi động về ROM mode.

V. Cấu hình router cho đường leased line.

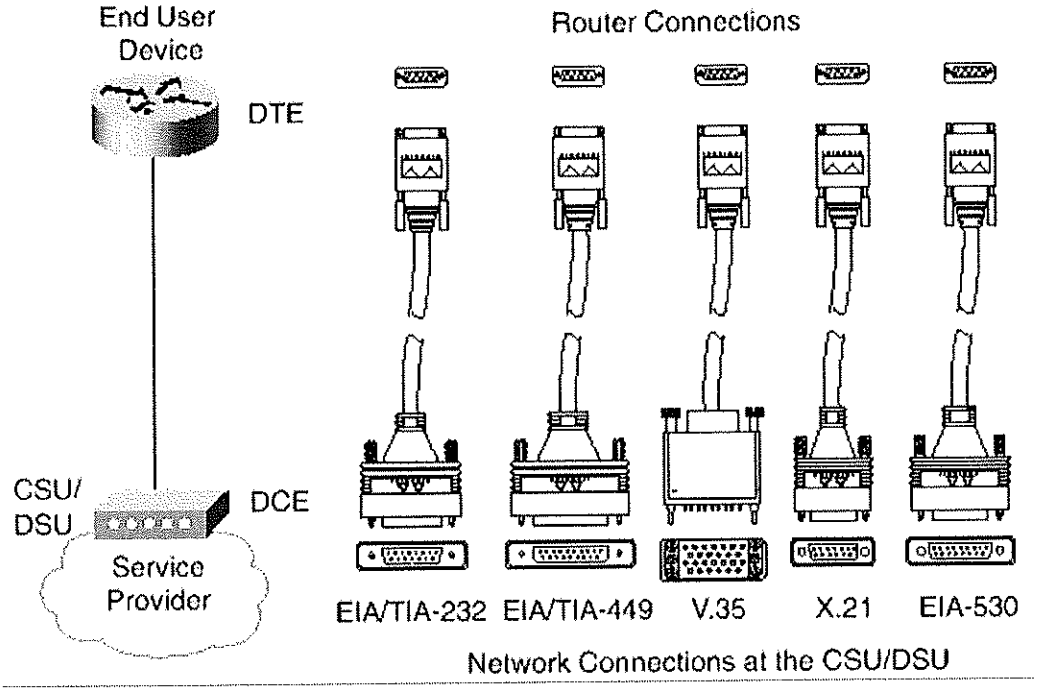
V.1 Khái niệm về liên kết leased line.

Đường liên kết leased line là đường liên kết kỹ thuật số do Bưu điện cung cấp, thường là một đường cáp đồng 1 pair, kết nối điểm-điểm với hai đầu cần kết nối. Mô hình cơ bản của một kết nối leased line như hình 14:



Hình 14

Liên kết trên đường leased line là liên kết tín hiệu số, có tốc độ lên tới 2.048Mbps (với cáp đồng). Thiết bị đầu cuối là NTU (Network Terminal Unit) còn gọi là DSU/CSU (Channel Service Unit/ Data Service Unit) tác dụng như một DCE (Data Circuit Equipment). Các NTU có thể có nhiều loại với nhiều tốc độ khác nhau. Router trong trường hợp này đóng vai trò như một DTE (Data Terminal Equipment). Các NTU thường cung cấp giao tiếp V.35 hay RS232 để kết nối với Router. Tùy theo NTU mà phải chọn loại cáp kết nối cho cổng Serial của router cho thích hợp (xem hình 12)



Hình15: Các loại cáp kết nối giữa router và NTU (CSU/DSU)

Tùy theo nhu cầu sử dụng mà khách hàng có thể chọn tốc độ cho đường leased line, thường là từ 64Kbps trở lên, từ đó chọn NTU và router thích hợp. Ví dụ cho thiết bị NTU thường dùng hiện nay là: ACD-3 của hãng Timeplex, ASM-31, ASM-40 của RAD.

Hầu hết các loại Cisco Router đều có thể hỗ trợ cho liên kết leased line thông qua các serial port của mình. Ngoại trừ Cisco router 7xx chỉ hỗ trợ cho ISDN. Tất cả các loại router từ series 8xx trở lên đều có thể hỗ trợ từ 01 đến hàng chục cổng serial.

Các cáp serial của router dùng cho các kết nối leased line thường là V.35 DTE và RS232 DTE đối với các serial port 60 chân và V35 SS DTE, RS232 SS DTE đối với cổng Smart Serial (WIC-2T, WIC-2A/S...)..

V.2.3 Cấu hình static routing hay hay dynamic routing:

Như phần trình bày đầu tiên về khái niệm router ở phần đầu của đề tài này, ta có thể chọn một trong hai cơ chế routing khi cấu hình Cisco router: static hay dynamic:

Static routing là cơ chế trong đó người quản trị quyết định, gán sẵn protocol cũng như địa chỉ đích cho router: đến network nào thì phải truyền qua port nào, địa chỉ là gì... Các thông tin này chứa trong routing table và chỉ được cập nhật hay thay đổi bởi người quản trị. Static routing thích hợp cho các hệ thống đơn giản, có kết nối đơn giữa hai router, trong đó đường truyền dữ liệu đã được xác định trước.

Dynamic routing dùng các routing protocol để tự động cập nhật các thông tin về các router xung quanh. Tùy theo dạng thuật toán mà cơ chế cập nhật thông tin của các router sẽ khác nhau. Dynamic routing thường dùng trong các hệ thống phức tạp hơn, trong đó các router được liên kết với nhau thành một mạng lưới, ví dụ như các hệ thống router cung cấp dịch vụ internet, hệ thống của các công ty đa quốc gia.

Phần 2

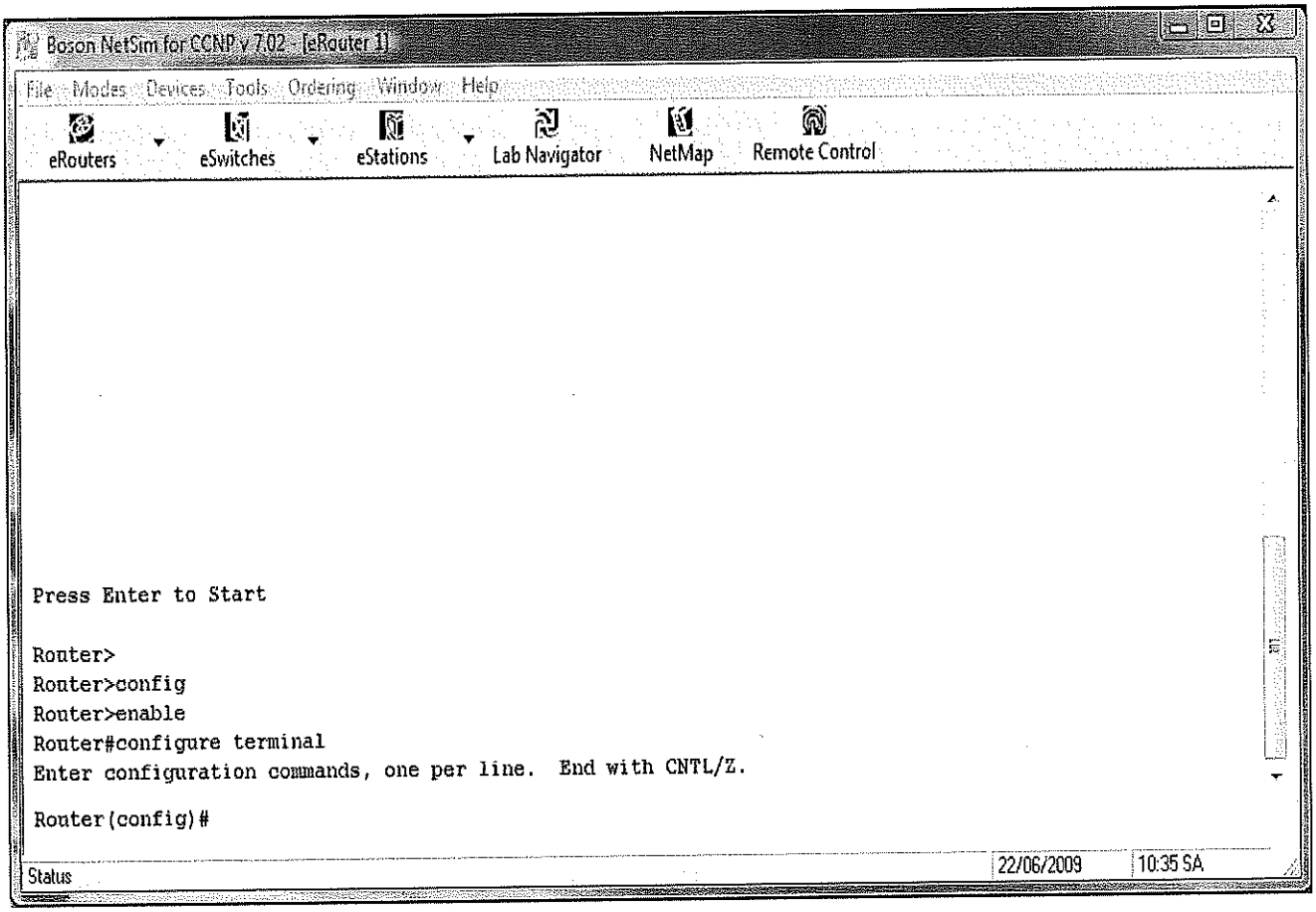
Tính toán thiết kế và thi công mạng Lan

V. Giới thiệu phần mềm mô phỏng Boson netsim:

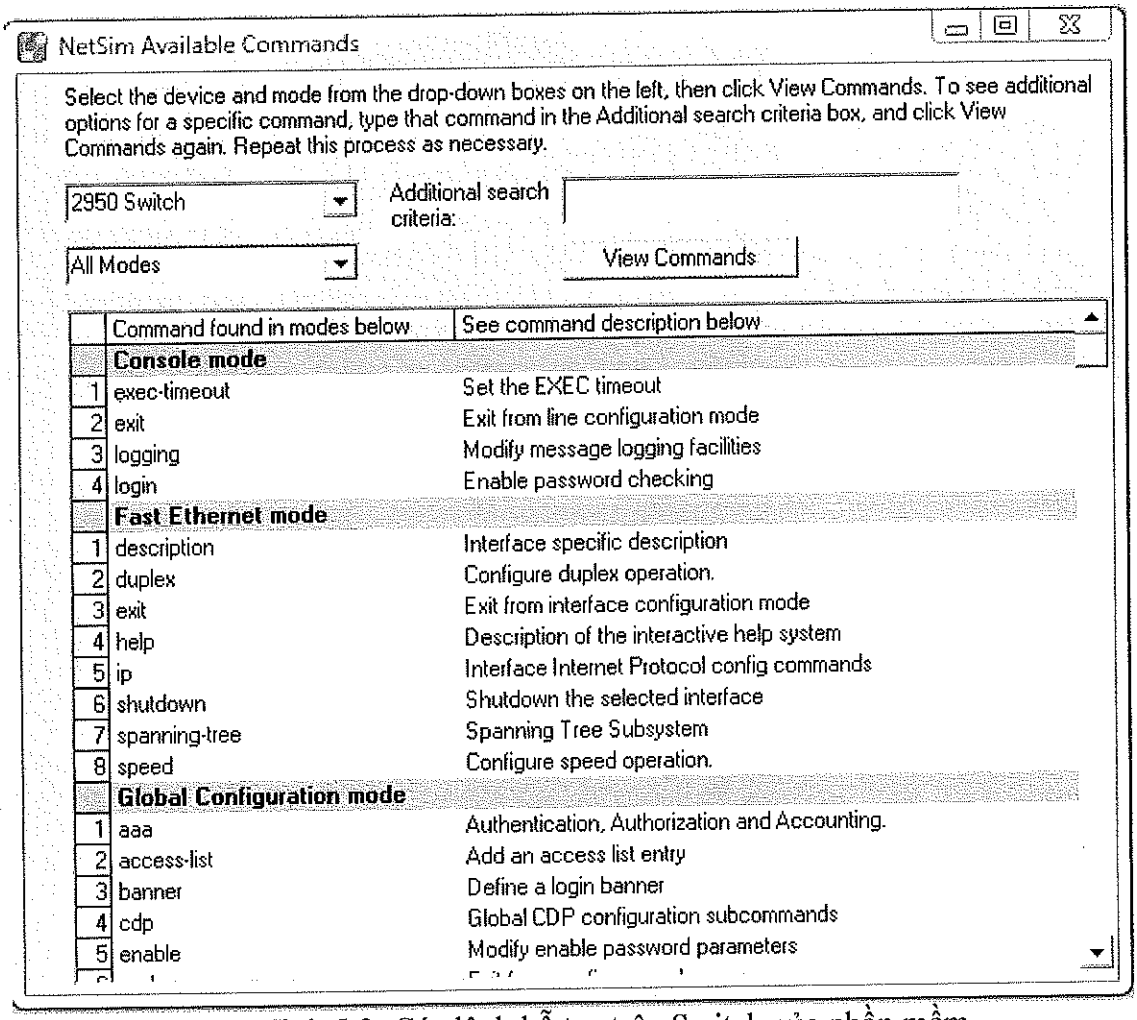
Kiến trúc mạng Internet là chằng chịt và phức tạp nhưng ta chỉ cần hiểu rằng có hai khối chức năng vô cùng quan trọng được phân chia một cách rõ ràng: đó là chuyển mạch (switching) và định tuyến (routing).

Hai khối chức năng này được tìm hiểu một cách cơ bản thông qua mô hình OSI tại tầng 2 và tầng 3 (layer 2 & layer 3) và ta có thể hiểu được rõ hơn thông qua 2 thiết bị đặc trưng tại hai tầng này đó là Switch (layer 2 device) & Router (layer 3 device).

Để giúp cho người học có thể tiếp cận nhanh nhất đến các thiết bị này mà không phải chi phí quá nhiều, hãng Boson đã đưa ra phần mềm giả lập Boson **Netsim** for CCNA or CCNP,…. Mặc dù không đạt được như làm việc với thiết bị thật nhưng nó cũng đủ để ta có thể tìm hiểu, nghiên cứu và đạt được mục đích trong đề tài này.

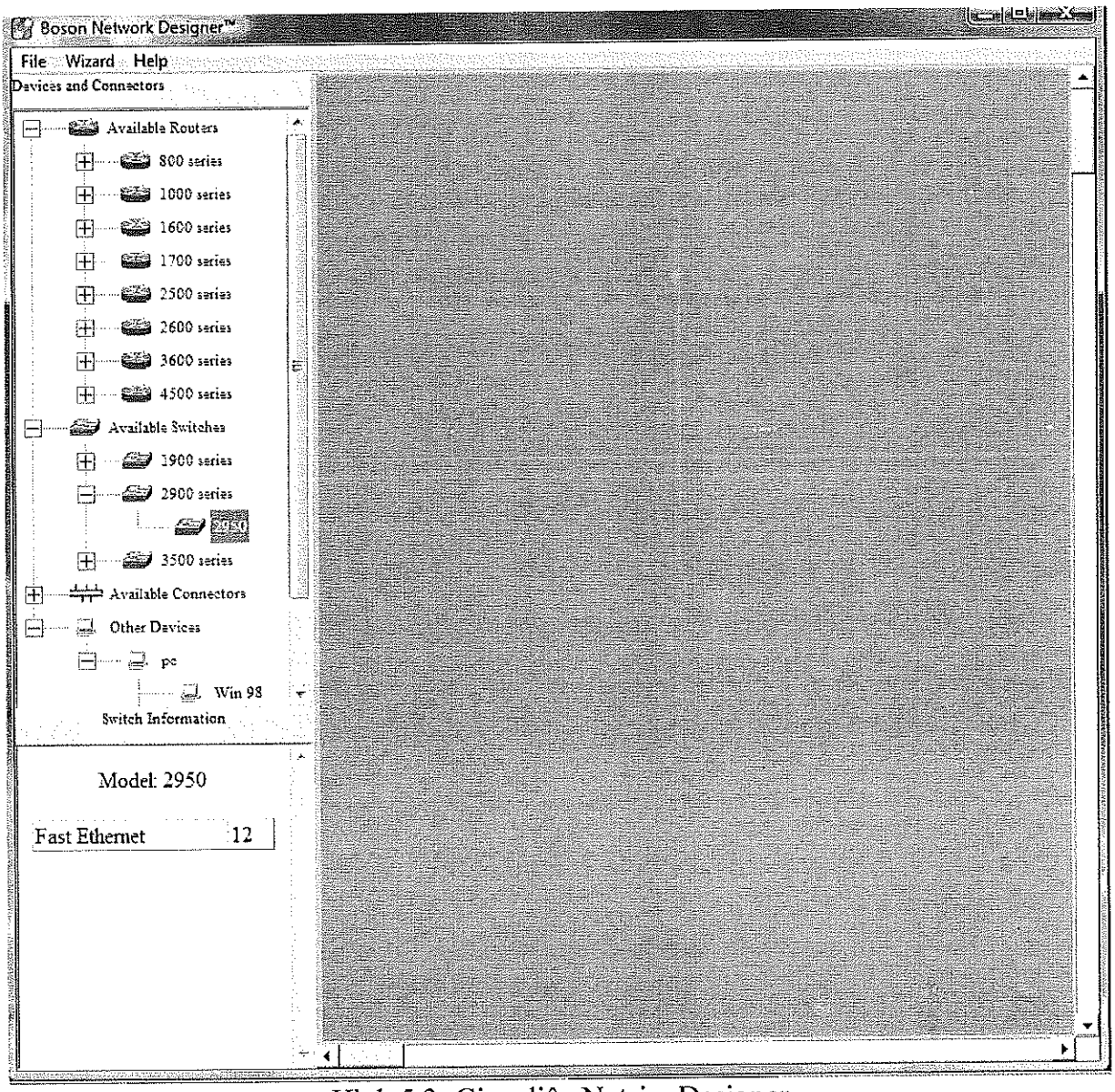


Hình 5.1: Giao diện của phần mềm Bosson Netsim.

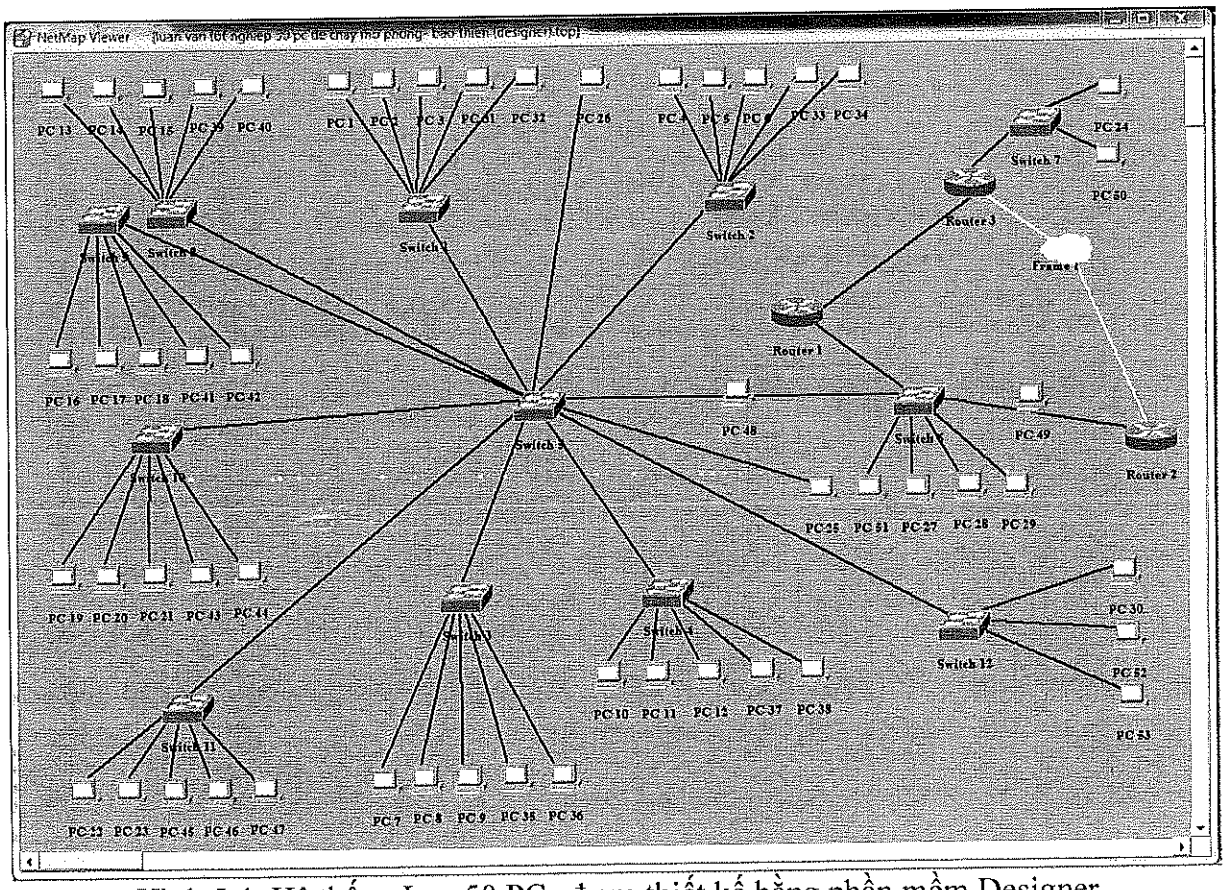


Hình 5.2: Các lệnh hỗ trợ trên Switch của phần mềm.

Trước khi có thể mô phỏng hoạt động của Switch và các thiết bị, ta cần phải thiết kế mô hình cho hệ thống. Netsim Designer của Boson sẽ giúp ta thực hiện dễ dàng công việc này (hình 5.3). Việc thiết kế lắp đặt một sơ đồ mạng về mặt logic nhưng nó có nghĩa như ta đang lắp bên ngoài vậy.



Hình 5.3: Giao diện Netsim Designer



Hình 5.4: Hệ thống Lan 50 PCs được thiết kế bằng phần mềm Designer

- **Thuật ngữ networking**:

Mạng Lan có từ khi nào?

Vào giữa thập niên 1980 các user dùng máy tính bắt đầu chia sẻ các tập tin bằng cách dùng modem kết nối với các máy tính khác. Cách thức này gọi là điểm nối điểm (point to point), hay truyền theo kiểu quay số.

Sau đó khái niệm này được mở rộng bằng cách dùng các máy tính trung tâm truyền tin trong một kết nối quay số. Các máy tính này được gọi là sàn thông báo(bulletin boards). Các user sẽ kết nối đến các sàn thông báo này, để lại đó hay lấy đi các thông điệp, cũng như gửi lên hay tải về các tập tin. Điểm yếu của hệ thống này là có rất ít hướng truyền tin và chỉ với những ai biết về sàn thông báo này. Hạn chế khác là các máy tính tại sàn thông báo cần một modem cho mỗi kết nối. Nếu có năm người kết nối đồng thời sẽ cần đến năm modem được kết nối với năm đường điện thoại riêng biệt. Do đó khi số lượng người muốn kết nối tăng lên , hệ thống không thể đáp ứng được nhu cầu. Ví dụ, nếu có 500 người muốn kết nối đến cùng một lúc thì…

Sau này bộ quốc phòng Hoa Kì đã phát triển một công nghệ khác với truyền tin điểm điểm được dùng tại sàn thông báo. Nó cho phép nhiều máy tính kết nối lại với nhau bằng các đường truyền dẫn khác nhau. Bản thân mạng sẽ xác định dữ liệu di chuyển từ máy tính này đến máy tính khác như thế nào, thay vì chỉ có thể thông tin với một máy tính tại một thời điểm, có thể thông tin với nhiều máy tính cùng lúc bằng cùng một kết nối. DOD WAN về sau trở thành Internet.

VI.Sơ đồ thiết kế hệ thống:

VI.1.Mạng máy tính cục bộ (LAN):

LAN bao gồm các thành phần sau:

-PC

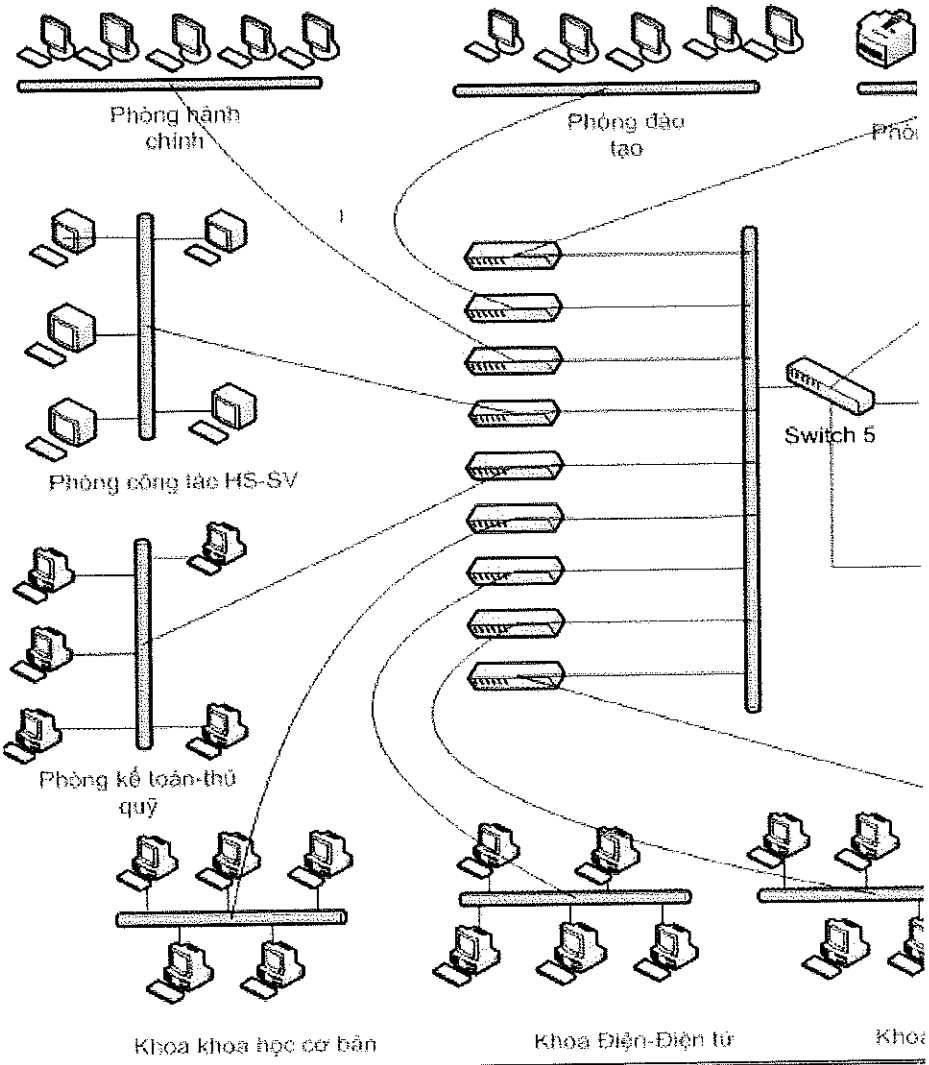
-Các card giao tiếp mạng (NIC)

-Các thiết bị ngoại vi

-Đường truyền thiết lập mạng

- Các thiết bị mạng

Các phòng ban được chia thành mỗi VLAN riêng biệt, cho phép kết nối với nhau trong VLAN của mình.

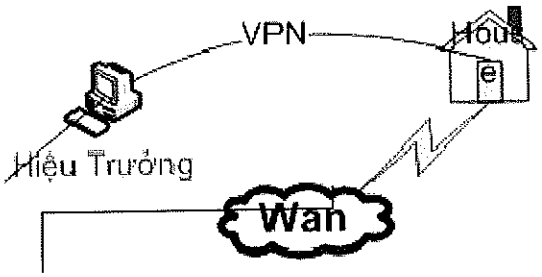


Hình 6.1: Hệ thống mạng Lan phân chia các phòng ban trong đề tài

Lan tạo điều kiện cho kinh doanh và đào tạo trong đó dùng kĩ thuật máy tính để chia sẻ tập tin và máy in cục bộ một cách hiệu quả và mở ra khả năng truyền thông nội bộ.

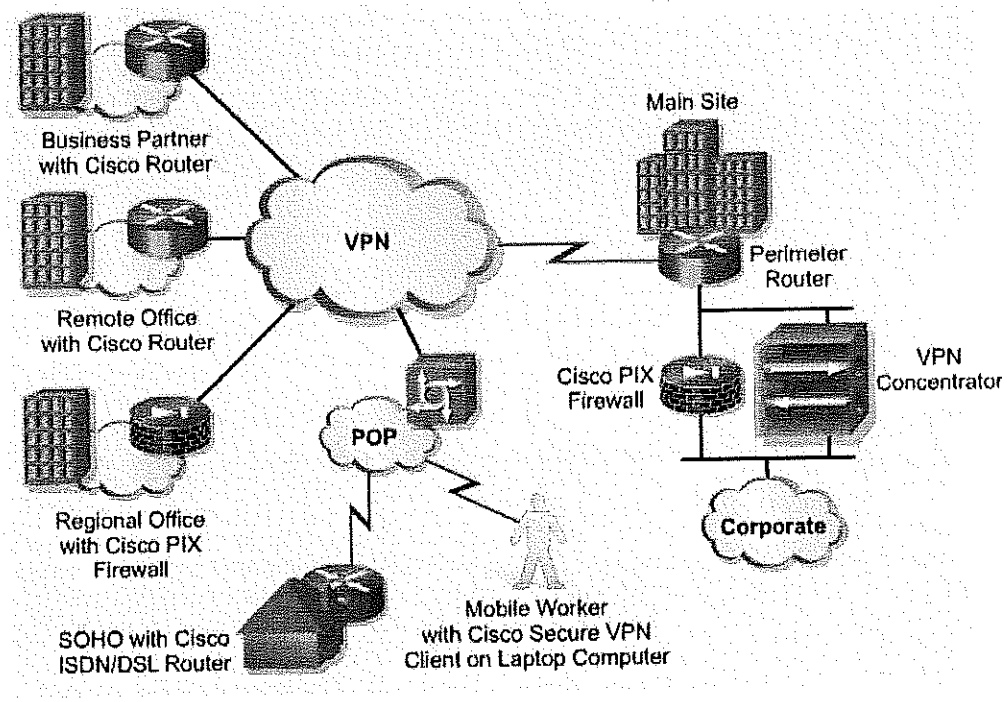
VI.2.Mạng riêng ảo (VPN) trong đề tài:

VPN là một mạng riêng được kiến tạo bên trong một hạ tầng mạng công cộng (ví dụ như Internet), sử dụng VPN một người làm việc tại nhà qua mạng (telecommuter) có thể truy xuất vào mạng của công ty thông qua internet bằng cách xây dựng một đường hầm bí mật (secure tunnel) giữa máy PC của họ và một VPN router đặt tại đại bản doanh của công ty hay trường học. Ở đây hiệu trưởng có thể kết nối đến PC ở trường từ một vị trí rất xa (ở nhà hoặc đang đi công tác) giống như đang làm việc trong mạng Lan ở trường vậy.



Hình 6.2: Vpn kết nối đến một máy tính trong trường

Lợi ích: là một dịch vụ cung ứng kết nối tin cậy, an toàn qua một hạ tầng mạng công cộng vốn được chia sẻ (ví dụ internet). VPN duy trì các chính sách quản lý và bảo mật như một mạng riêng. Chúng là phương thức rẻ tiền nhất để thiết lập một cầu nối điểm điểm giữa người dùng ở xa với một mạng khách hàng của doanh nghiệp hay trường học.



Hình 6.3: Các kết nối VPN

VI.3.Tiến trình đóng gói chi tiết:

Đóng gói tiến hành gói dữ liệu với thông tin giao thức cần thiết trước khi chuyển lên mạng. khi đóng gói dữ liệu di chuyển xuống các lớp của mô hình OSI, nó tiếp nhận các header, các trailer và các thông tin khác (hình 6.4). Một khi dữ liệu được truyền từ một nguồn, nó di chuyển xuyên qua lớp ứng dụng đến các lớp bên dưới. Việc gói và luồng dữ liệu thay đổi khi các lớp thực hiện các dịch vụ của chúng cho các user đầu cuối. Mạng thực hiện 5 bước chuyển đổi sau để đóng gói dữ liệu:

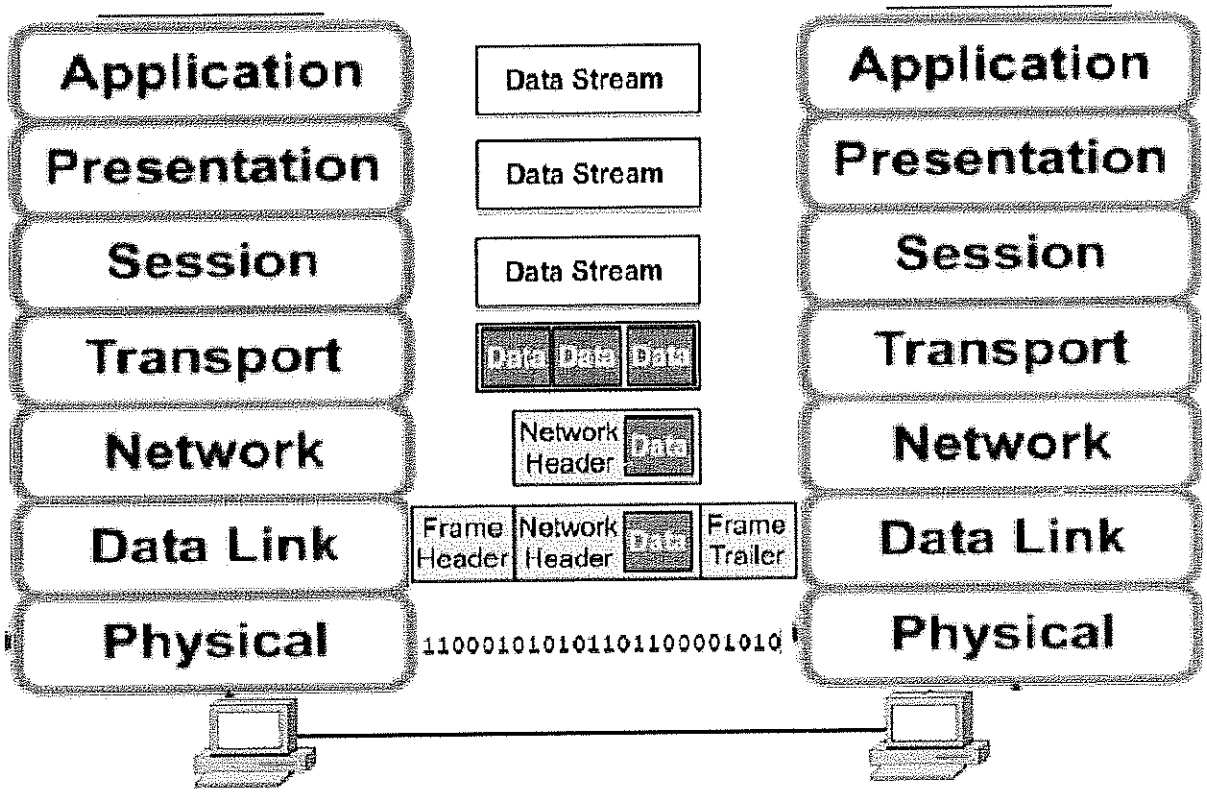
1.Xây dựng dữ liệu: khi user gửi một thông điệp e-mail, các kí tự của nó được chuyển đổi thành dữ liệu có thể di chuyển qua lớp liên mạng.

2.Gói dữ liệu để vận chuyển từ đầu cuối đến đầu cuối. Dữ liệu được đóng gói cho vận chuyển liên mạng. Bằng cách dùng các segment, chức năng vận chuyển đảm bảo rằng thông điệp được tiếp nhận tại cả hai đầu của hệ thống có thể truyền thông tin cậy.

3.Bổ sung địa chỉ IP vào header. Dữ liệu được đặt vào trong một gói hay datagram có chứa một header với các địa chỉ luận lý nguồn và đích. Các địa chỉ này giúp các thiết bị mạng truyền các gói xuyên qua mạng dọc theo một đường dẫn đã chọn.

4.Bổ sung header và trailer lớp liên kết dữ liệu. Mỗi thiết bị mạng phải đặt gói vào trong frame.Frame cho phép kết nối đến thiết bị mạng được gắn trực tiếp trên lien kết. mỗi thiết bị trên đường dẫn mạng đã chọn yêu cầu thao tác frame để nó kết nối được đến thiết bị kế tiếp.

5.Chuyển thành các bit để truyền dẫn, Frame phải được chuyển sang mẫu các bit 1 và 0 để truyền lên môi trường. Chức năng đồng bộ (clocking) cho phép các thiết bị phân tích các bit này khi chúng di chuyển xuyên qua môi trường. Môi trường trên liên mạng vật lý có thể thay đổi dọc theo đường dẫn được dùng (ví dụ: bắt đầu từ LAN, xuyên qua Wan rồi lại trở về LAN) cho đến khi đến được đích cần đến.

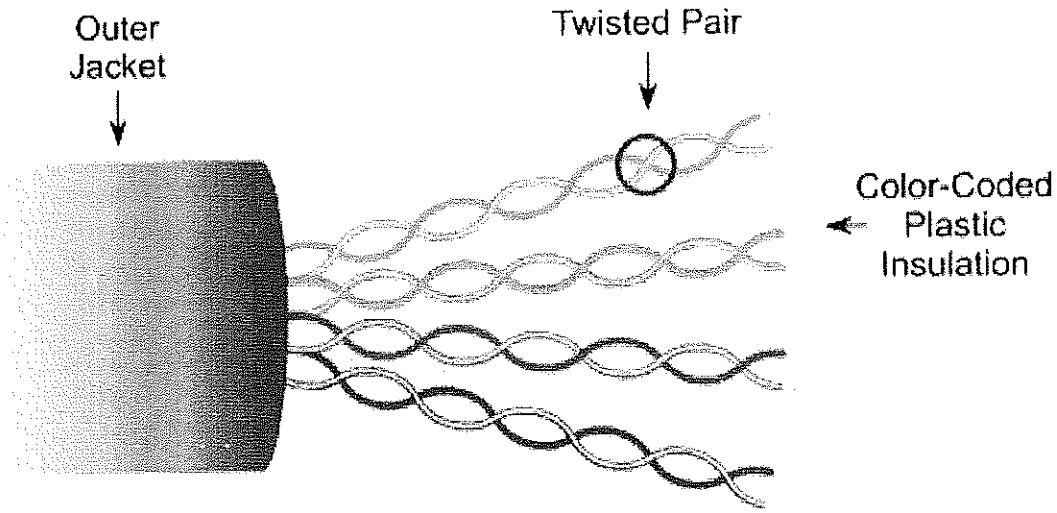


Hình 6.4: Tiến trình đóng gói chi tiết

VII. Cáp:

VII.1 Loại cáp sử dụng:

Đồ án là thiết kế mạng LAN nên dùng chủ yếu là cáp cặp xoắn (Twisted-Pair). Ở đây dùng cáp UTP.

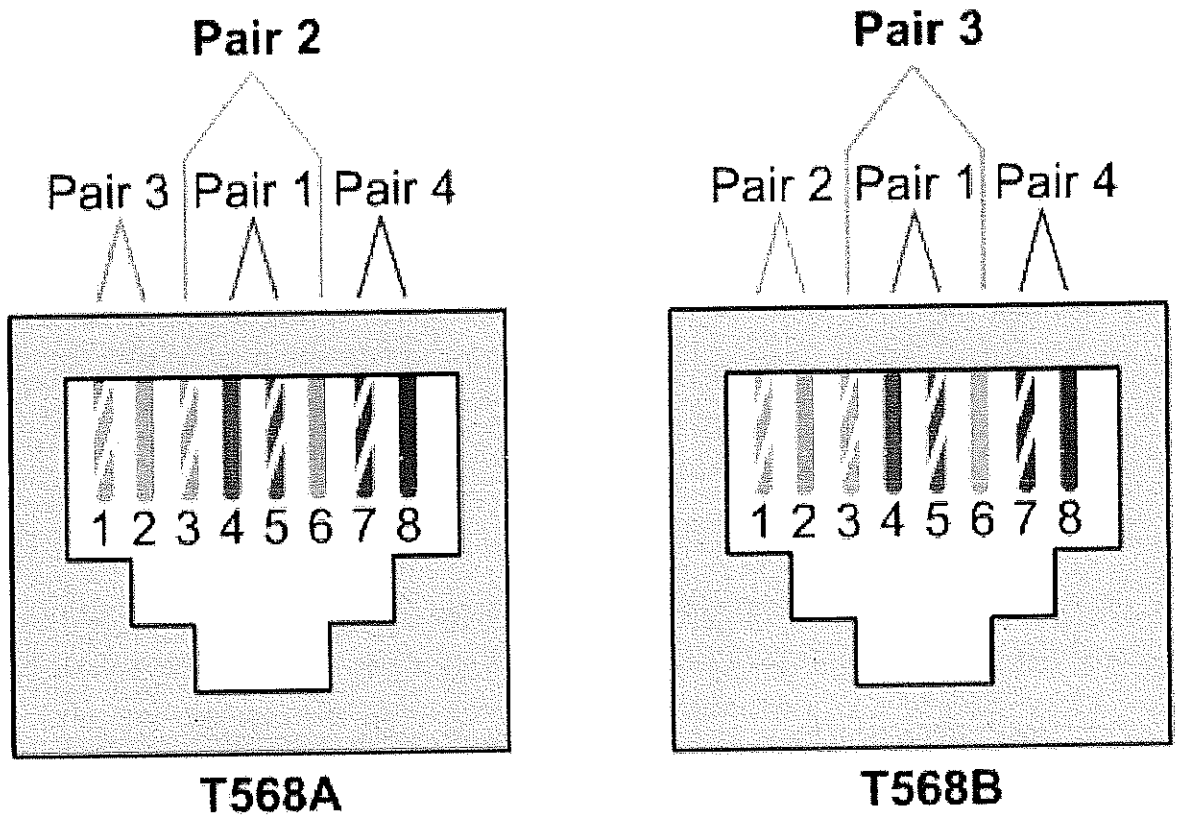


Hình 7.1: Cáp UTP

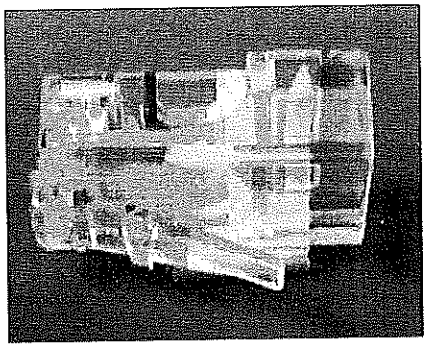
Cáp UTP: mỗi một dây trong 8 dây đồng tách biệt trong cáp UTP được bọc cách điện. Thêm vào đó là mỗi cặp hai dây được xoắn vào nhau. Loại cáp này chỉ dựa vào hiệu qủa triệt nhiễu duy nhất bởi sự xoắn dây để hạn chế suy thoái tín hiệu.

Cáp UTP có nhiều ưu điểm, trước hết là dễ dàng lắp đặt và rẻ tiền hơn so với các loại đường truyền khác.chi phí trên mỗi mét cáp thấp hơn bất kì loại cáp mạng LAN nào.tuy nhiên ưu điểm thực sự là kích thước của nó. Bởi có một kích thước bề ngoài nhỏ nên UTP không làm đầy các đường ống dẫn ngay tức thời như các loại cáp khác. Ngoài ra, cáp UTP sử dụng các đầu RJ45, các nguồn nhiễu mạnh được giảm đáng kể và một kết nối chắc chắn được đảm bảo. Tuy nhiên, cáp UTP dễ bị ảnh hưởng bởi tạp âm và xuyên nhiễu hơn các loại cáp khác và khoảng cách giữa các đoạn mang tín hiệu ngắn hơn so với cáp đồng trục hay cáp quang.

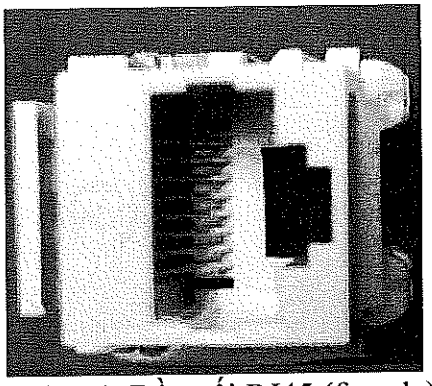
UTP từng được coi là loại đường truyền số liệu tốc độ thấp hơn các loại cáp khác. Nhưng với sự phát triển, UTP ngày nay đã được xem như đường truyền cáp đồng tốc độ cao.



Hình 7.2 Chuẩn kết nối T568A và T568B



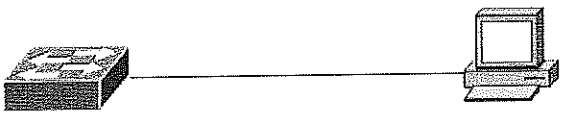
Hình7.3: Đầu nối RJ45 (male)



Hình 7.4: Đầu nối RJ45 (female)

VII.2.Nối cáp:

- Nối cáp thẳng (Straight-through cable): các pin được đấu với nhau đúng theo thứ tự. Đây là cách nối cáp dùng chủ yếu trong đề tài, thực hiện kết nối giữa PC và Switch, Switch và Router.



Pin 1	Pin 1
Pin 2	Pin 2
Pin 3	Pin 3
Pin 4	Pin 4
Pin 5	Pin 5
Pin 6	Pin 6
Pin 7	Pin 7
Pin 8	Pin 8

Hình 7.5: Sơ đồ nối cáp thẳng

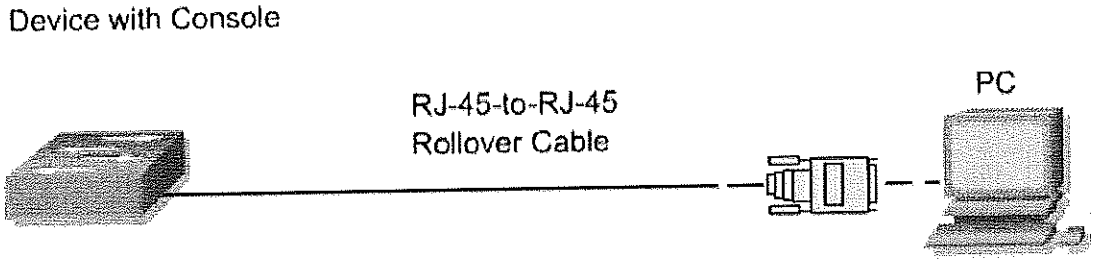
- Nối cáp chéo (crossover-cable): có sự thay đổi hai cặp pin 1-3 và 2-6. Dùng để kết nối giữa Switch của các phòng ban với Switch trung tâm lại



Pin 1	Pin 3
Pin 2	Pin 6
Pin 3	Pin 1
Pin 4	Pin 4
Pin 5	Pin 5
Pin 6	Pin 2
Pin 7	Pin 7
Pin 8	Pin 8

Hình 7.6: Sơ đồ nối cáp chéo

- Nối cáp đảo (rollover cable): Các Pin được đấu ngược thứ tự với nhau. Dùng để bấm cáp console cấu hình cho Switch và Router.

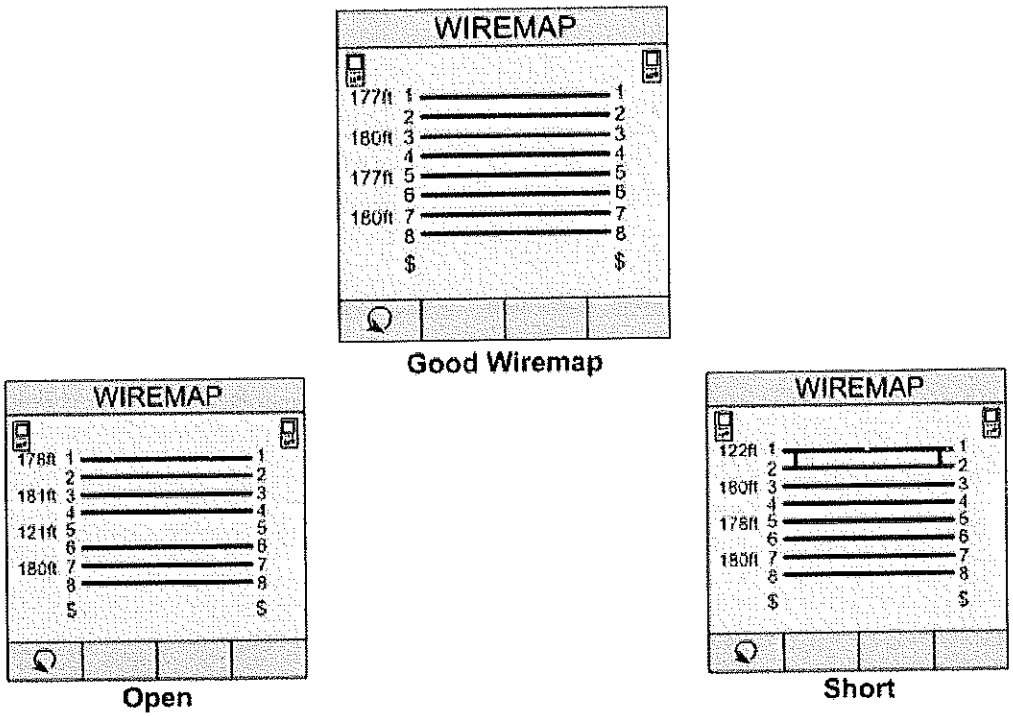


Pin 1	Pin 8
Pin 2	Pin 7
Pin 3	Pin 6
Pin 4	Pin 5
Pin 5	Pin 4
Pin 6	Pin 3
Pin 7	Pin 2
Pin 8	Pin 1

RJ-45-to-DB-9 Adapter
labeled TERMINAL

Hình 7.7: Sơ đồ nối cáp đảo

VII.3 Kiểm tra cáp: Sau khi bấm cáp xong, ta cần phải kiểm tra kết nối về mặt vật lý và kĩ thuật bấm có thành công hay không.



Hình 7.8: Chuẩn kiểm thử cáp

VIII. Ethernet Switching:

Để dễ hiểu hơn về hoạt động của Switch, em sẽ trình bày hoạt động chuyển mạch lớp 2 của bridge trước. Vì switch là một Bridge multi-port. Mỗi port sở hữu một đoạn mạng LAN, riêng biệt với các port khác. Việc chuyển tiếp frame dựa vào địa chỉ MAC chứa trong mỗi frame, switch không thể chuyển các frame mà không biết được địa chỉ đích. Hiểu được bridge sẽ dễ dàng hơn khi tiếp cận với Switch.

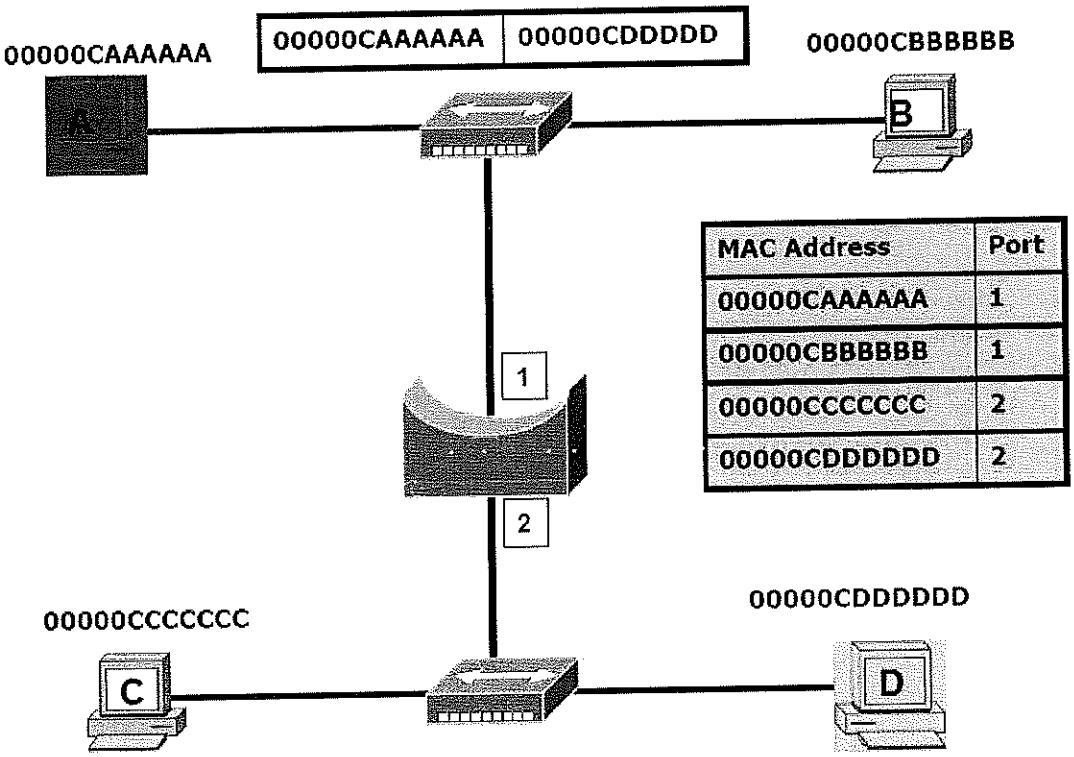
VIII.1 Bắc cầu ở lớp 2:

Vì Ethernet là một môi trường chia sẻ nên việc thêm nhiều node làm tăng nhu cầu về băng thông khả dụng và đặt các tải bổ sung vào môi trường. Tăng số lượng node trên một segment, xác suất đụng độ tăng, dẫn đến kết quả có nhiều hoạt dộng truyền lại hơn. Vì vậy ta phải chia segment lớn thành các phần và tách nó thành các miền đụng độ độc lập.

Để thực hiện điều này, Bridge sẽ giữ một bảng địa chỉ MAC và các port liên hệ. Sau đó Bridge chuyển hay loại bỏ frame căn cứ vào các mục trên bảng này. Các bước sau đây mô tả hoạt động của một Bridge:

- Một Bridge được khởi động với bảng bắc cầu là rỗng. Bridge chỉ đợi lưu lượng trên segment. Khi lưu lượng được phát hiện, nó được xử lý bởi Bridge này.

- Host A đang ping đến host B. Vì số liệu được truyền trên toàn bộ collision domain segment, nên cả Bridge và host B đều xử lý gói.
- Bridge thêm địa chỉ nguồn của frame vào bảng của nó. Vì địa chỉ này ở trong field địa chỉ nguồn và frame được nhận trên port 1, nên frame phải được liên hệ với port 1 trong bảng.
- Địa chỉ đích của frame được kiểm tra dựa vào bảng. Vì địa chỉ không ở trong bảng, mặc dù nó ở trên cùng một miền đụng độ, frame được chuyển đến segment khác. Địa chỉ của host B chưa được ghi vì chỉ có địa chỉ nguồn của frame là được ghi.
- Host B xử lý yêu cầu ping và truyền một đáp ứng ping trở lại host A. Số liệu được truyền qua toàn bộ miền đụng độ. Cả host A và Bridge đều nhận được frame và xử lý nó.
- Bridge thêm địa chỉ nguồn của frame vào bảng. Vì địa chỉ nguồn không có trong bảng và đã nhận được trên port 1, địa chỉ nguồn của frame phải được liên hệ với port 1 trong bảng. Địa chỉ đích của frame được kiểm tra dựa vào bảng để xem nó có một mục nào ở đây không. Vì địa chỉ này có trong bảng nên việc gán port được kiểm tra. Địa chỉ của host A được liên kết với port mà frame đến, vì vậy frame không được chuyển đi.
- Bây giờ host A tiến hành ping host C. Vì số liệu đang được truyền trên toàn bộ collision domain segment nên cả Bridge và Host B đều xử lý frame này. Host B loại bỏ frame vì nó không phải gửi đến nó.
- Bridge thêm địa chỉ nguồn cuả frame vào bảng. Vì địa chỉ này đã có trong bảng nên mục này chỉ được làm tươi lại.
- Địa chỉ đích của frame được kiểm tra dựa vào bảng để xem nó có mục nào ở đây không. Vì địa chỉ này chưa có trong bảng nên frame được chuyển đến segment khác. Địa chỉ của host C chưa được ghi vì chỉ có địa chỉ nguồn của frame được ghi.
- Host C xử lý yêu cầu Ping và truyền lại một đáp ứng cho host A. Số liệu được truyền qua toàn bộ miền đụng độ. Cả host D và Bridge đều nhận được frame và xử lý nó. Host D loại bỏ frame vì không phải gửi cho nó.
- Bridge thêm địa chỉ nguồn của frame vào bảng của nó. Vì địa chỉ ở trong field địa chỉ nguồn và frame được tiếp nhận trên port 2 nên frame này phải được liên kết với port 2 trong bảng.
- Địa chỉ đích của frame được kiểm tra căn cứ vào bảng để xem nó có mục nào không. Địa chỉ này có trong bảng nhưng nó được liên kết với port 1. Vì vậy frame được chuyển đến segment khác.
- Khi host D truyền số liệu, địa chỉ MAC của nó cũng sẽ được ghi lại trong bảng. Đây là cách Bridge điều khiển lưu lượng giữa các miền đụng độ.

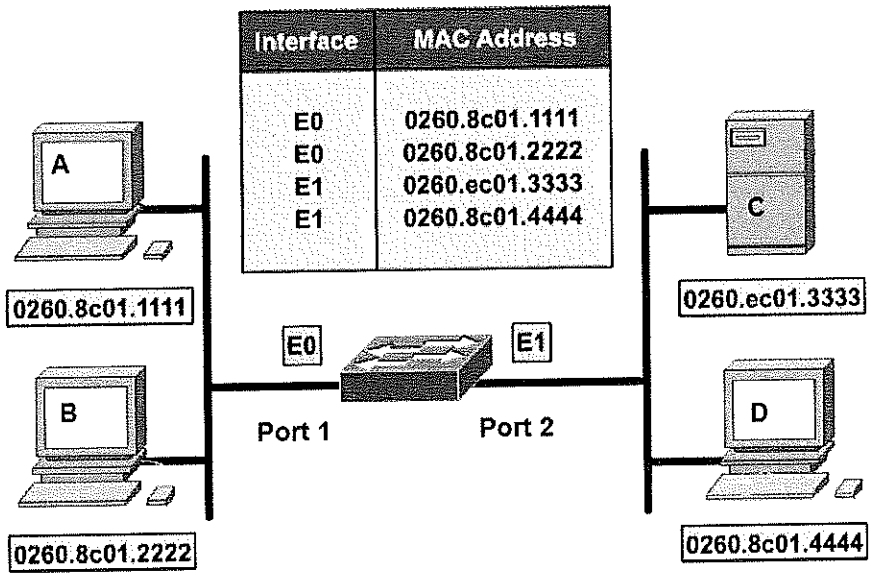


Hình 8.1: Hoạt động của Bridge

VIII.2 Chuyển mạch ở lớp 2:

Vì Brige chỉ có hai port nên miền đụng độ được hia thành hai phần. Tất cả các quyết định được đưa ra bởi Bridge đều dựa trên địa chỉ MAC hay địa chỉ lớp 2 và không ảnh hưởng đến địa chỉ luận lý hay địa chỉ lớp 3. Do đó một Bridge chia miền đụng độ nhưng không ảnh hưởng đến miền quảng bá. Có bao nhiêu Bridge trong mạng là không thành vấn đề, trừ phi có một thiết bị như router làm việc trên lược đồ địa chỉ lớp 3, đề tài sử dụng 2 router để đi ra internet. Toàn bộ mạng sẽ chia sẻ cùng không gian địa chỉ quảng bá. Một Bridge sẽ tạo nhiều miền đụng độ hơn nhưng sẽ không thêm các miền quảng bá.

Một switch về cơ bản là một Bridge nhiều port tốc độ cao hơn, nó có thể chứa đến hàng tá port. Thay vì tạo ra hai miền đụng độ, mỗi port tạo ra miền đụng độ riêng của nó. Trong một mạng có hai mươi node, hai mươi miền đụng độ tồn tại nếu mỗi node được nối vào port trên switch. Một switch thiết lập động và duy trì một bảng CAM (Content-Addressable Memory), lưu giữ tất cả thông tin MAC cho mỗi port



Hình 8.2: Hoạt động của Switch

VIII.3 Giới thiệu về luồng dữ liệu (data flow):

Data flow trong ngữ cảnh của collision domain và broadcast domain tập trung vào cách thức các frame di chuyển xuyên qua một mạng. Nó đề cập đến sự di chuyển của số liệu đi qua các thiết bị lớp 1,lớp 2 và lớp 3 và số liệu phải được đóng khối như thế nào để chúng có một hành trình hiệu quả. Số liệu được đóng gói tại lớp mạng với một địa chỉ IP nguồn và địa chỉ IP đích và tại lớp liên kết số liệu (lớp 2) thì với một địa chỉ MAC nguồn và địa chỉ MAC đích.

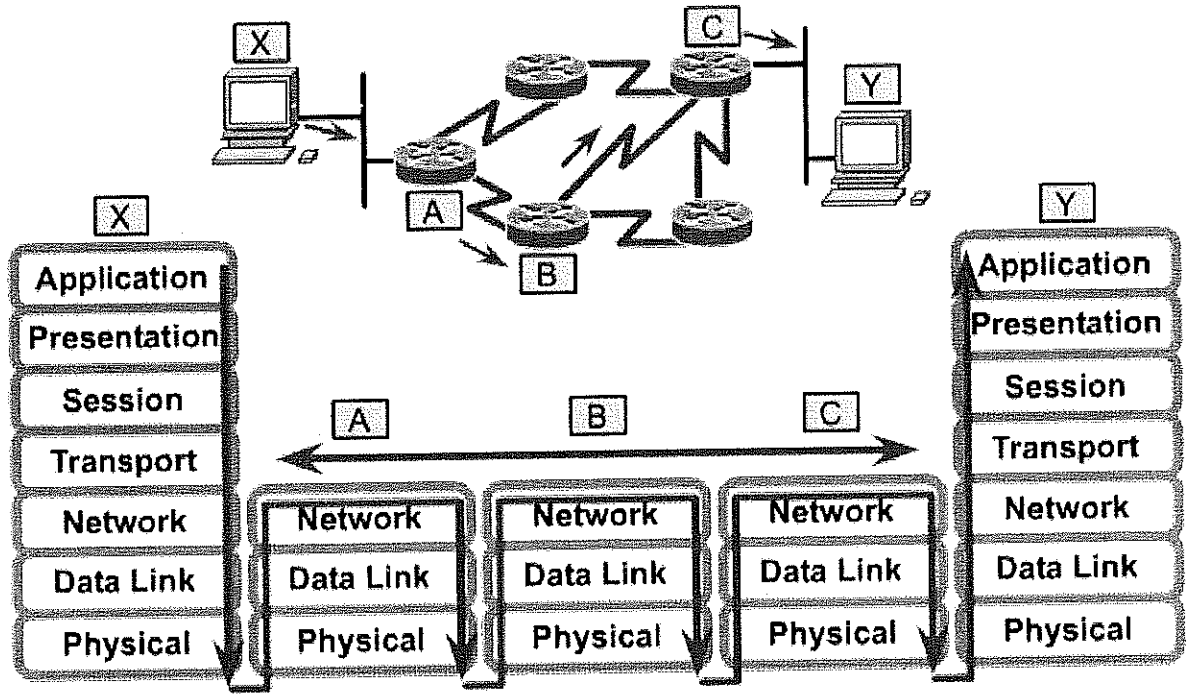
Một nguyên tắc tốt cho data flow là một thiết bị lớp 1 luôn chuyển frame đi, khi một thiết bị lớp 2 muốn chuyển qua frame này. Nói cách khác, một thiết bị lớp 2 sẽ chuyển frame qua trừ khi có vài yếu tố ngăn cản nó làm điều đó. Một thiết bị lớp 3 sẽ không chuyển qua một frame trừ khi nó bị buộc phải làm điều này. Sử dụng nguyên tắc này sẽ giúp nhận biết được các luồng số liệu xuyên qua một mạng như thế nào.

Các thiết bị lớp 1 không có chức năng thanh lọc, vì vậy mọi thứ mà chúng nhận được đều được chuyển qua sang segment kia. Frame được tái sinh, được định thời lại và do đó frame quay trở lại với chất lượng truyền ban đầu. Bất kì segment nào được kết nối bởi các thiết bị lớp 1 đều là thành phần của cùng một domain, cả đụng độ và quảng bá.

Các thiết bị lớp 2 lọc các frame số liệu căn cứ vào địa chỉ lớp 2(MAC address) của đích. Một frame được chuyển qua nếu nó đang đi đến một đích không thể nhận biết bên ngoài miền đụng độ. Frame cũng sẽ được chuyển qua nếu như nó là một broadcast, một multicast hay một unicast hướng ra bên ngoài của một miền đụng độ cục bộ. Chỉ có một trường hợp frame không chuyển qua đó là lúc thiết bị lớp 2 phát hiện host truyền frame và host nhận frame cùng ở trên một miền đụng độ. Một thiết bị lớp 2, như Bridge, tạo nhiều miền đụng độ nhưng chỉ duy trì một miền quảng bá.

Các thiết bị lớp 3 lọc các gói đưa vào địa chỉ IP đích. Chỉ có một cách duy nhất để một gói có thể được chuyển qua là nếu địa chỉ IP đích là nằm bên ngoài broadcast domain và router với một vị trí xác định để chuyển gói đi. Một thiết bị lớp 3 tạo ra nhiều collision domain và nhiều broadcast domain.

Data flow đi qua một mạng cậy vào IP được định tuyến liên quan đến số liệu di chuyển ngang qua các thiết bị quản lí lưu lượng tại lớp 1, lớp 2, lớp 3 của mô hình OSI. Lớp 1 dùng để truyền xuyên qua môi trường vật lí, lớp 2 để quản lí collision domain và lớp 3 để quản lí broadcast domain..



Hình 8.3: Luồng dữ liệu xuyên qua một mạng

Các địa chỉ IP lớp A, B, C,D và E:

Để phù hợp với các mạng có kích thước khác nhau và hỗ trợ trong việc phân loại các mạng này, các địa chỉ IP được chia thành các nhóm gọi là các lớp. Điều này được gọi là địa chỉ phân hóa lớp. Mỗi địa chỉ IP 32 bit hoàn chỉnh được chia thành phần mạng và phần host. Một bit hay một tuần tự bit bắt đầu mỗi địa chỉ sẽ xác định lớp của địa chỉ này. Có năm lớp địa chỉ IP được đặt tên theo thứ tự là A,B,C,D,E.

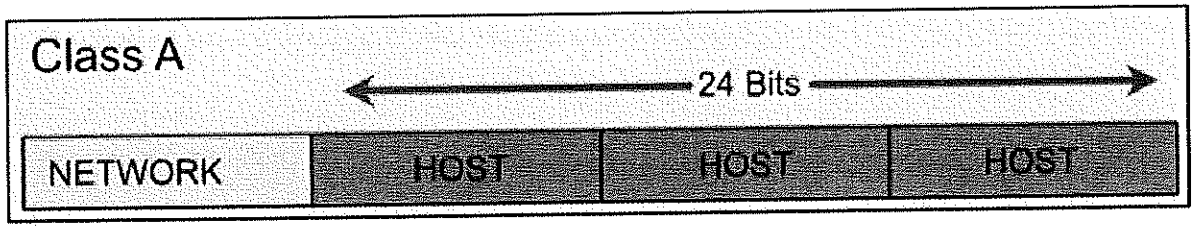
Địa chỉ lớp A được thiết kế cho các mạng cực kì lớn, với nhiều hơn 16 triệu địa chỉ có sẵn. Các địa chỉ lớp A chỉ dùng octet đầu tiên để chỉ địa chỉ mạng. Ba octet còn lại cung cấp địa chỉ host.

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

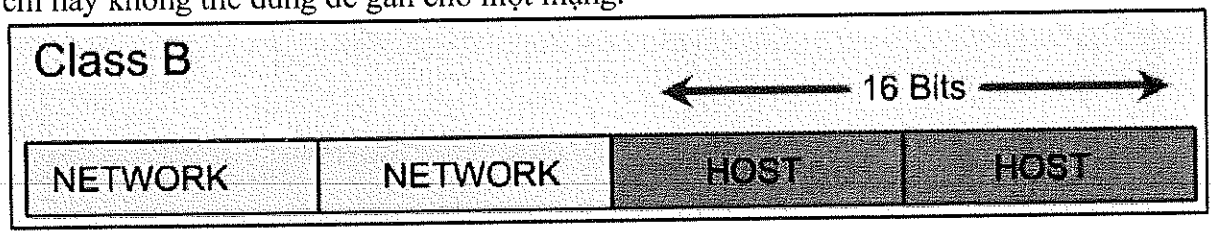
Hình 9.1: Các tiền tố lớp địa chỉ



Hình 9.2: Địa chỉ lớp A

Bit đầu tiên của địa chỉ lớp A luôn là 0. Với bit đầu tiên này là 0, số nhỏ nhất octet đầu tiên này có thể biểu diễn là 00000000, giá trị thập phân tương ứng là 0. Số lớn nhất nó có thể biểu diễn là 01111111, tương ứng với giá trị thập phân 127. Hai số 0 và 127 được dành riêng và không thể sử dụng như các địa chỉ mạng. Bất kì địa chỉ nào bắt đầu với giá trị giữa 1 và 126 ở octet đầu tiên là một địa chỉ lớp A.

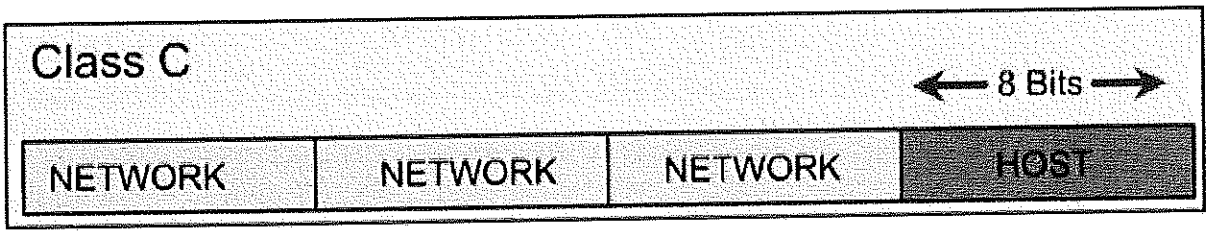
127.0.0.0 là địa chỉ dành riêng cho loopback testing. Các router hay các máy cục bộ có thể dùng địa chỉ này để truyền các gói vòng ngược trở lại chính chúng. Do đó địa chỉ này không thể dùng để gán cho một mạng.



Hình 9.2: Địa chỉ lớp B

Địa chỉ lớp B được thiết kế cho các nhu cầu mạng kích thước từ vừa phải đến lớn. Một địa chỉ lớp B dùng hai octet đầu để chỉ địa chỉ mạng. Hai octet kia chỉ địa chỉ host.

Hai bit đầu tiên của một địa chỉ lớp B luôn luôn là 10. Địa chỉ nào bắt đầu với một giá trị trong octet thứ nhất thuộc dải từ 128 đến 191 sẽ là một địa chỉ lớp B.



Hình 9.3: Địa chỉ lớp C

Không gian địa chỉ lớp C được dùng phổ biến trong các lớp địa chỉ IP. Không gian địa chỉ này hướng đến phục vụ cho các mạng nhỏ với tối đa 254 host, lớp C luôn bắt đầu bằng chuỗi 110. Nếu một địa chỉ chứa một số thuộc về dải từ 192 đến 223 trong octet thứ nhất thì đó là dịa chỉ lớp C. Đề tài sử dụng địa chỉ lớp C cho mạng 50 PCs.

Lớp địa chỉ D được tạo ra để cho phép mulicast cho địa chỉ IP. Một địa chỉ multicast là một địa chỉ mạng duy nhất hướng dẫn các gói đến một nhóm các địa chỉ IP, nhóm địa chỉ IP đó được định nghĩa trước là địa chỉ multicast này. Do đó, một trạm có thể truyền luồng số liệu đến nhiều đích một cách đồng thời.

Địa chỉ lớp E đã được định nghĩa. Tuy nhiên, IETF dành các địa chỉ này cho công việc nghiên cứu riêng. Do đó, không có các địa chỉ lớp E nào đã được cấp phát cho sử dụng trên mạng internet. Bốn bit đầu tiên của địa chỉ lớp E đều được cho là 1. Do đó, dải octet đầu tiên cho các địa chỉ lớp E là 11110000 đến 11111111, hay từ 240 đến 255.

Đề tài yêu cầu thiết kế 50 PC nên chỉ cần một octet cuối là có thể đáp ứng nhu cầu hệ thống cũng như dự phòng cho sự mở rộng mạng sau này. Địa chỉ được dùng là: 172.16.x1.x2/24

Trong đó: x1 là số của VLAN, x2 là số của PC.

Theo như thiết kế này thì các VLAN là không cùng một đường mạng vì subnetmask là 255.255.255.0. do đó đáp ứng được yêu cầu là các Vlan của các phòng ban khác nhau sẽ không thể trao đổi dữ liệu với nhau.

- **Các địa chỉ IP dành riêng:**

Địa chỉ mạng: được dùng để định danh chính mạng đó.

Địa chỉ broadcast: được dùng để quảng bá (broadcasting) các gói đến tất cả các thiết bị trên một mạng.

- **IP public va IP private:**

IP private : là các địa chỉ IP được dùng riêng cho các mạng LAN, không được thấy trên mạng Internet, được dùng để tiết kiệm địa chỉ IP. Các địa chỉ IP không phải private là địa chỉ IP public.

- Class A: 10.0.0.0.
- Class B: 172.16.0.0 - 172.31.0.0.
- Class C: 192.168.0.0 - 192.168.255.0

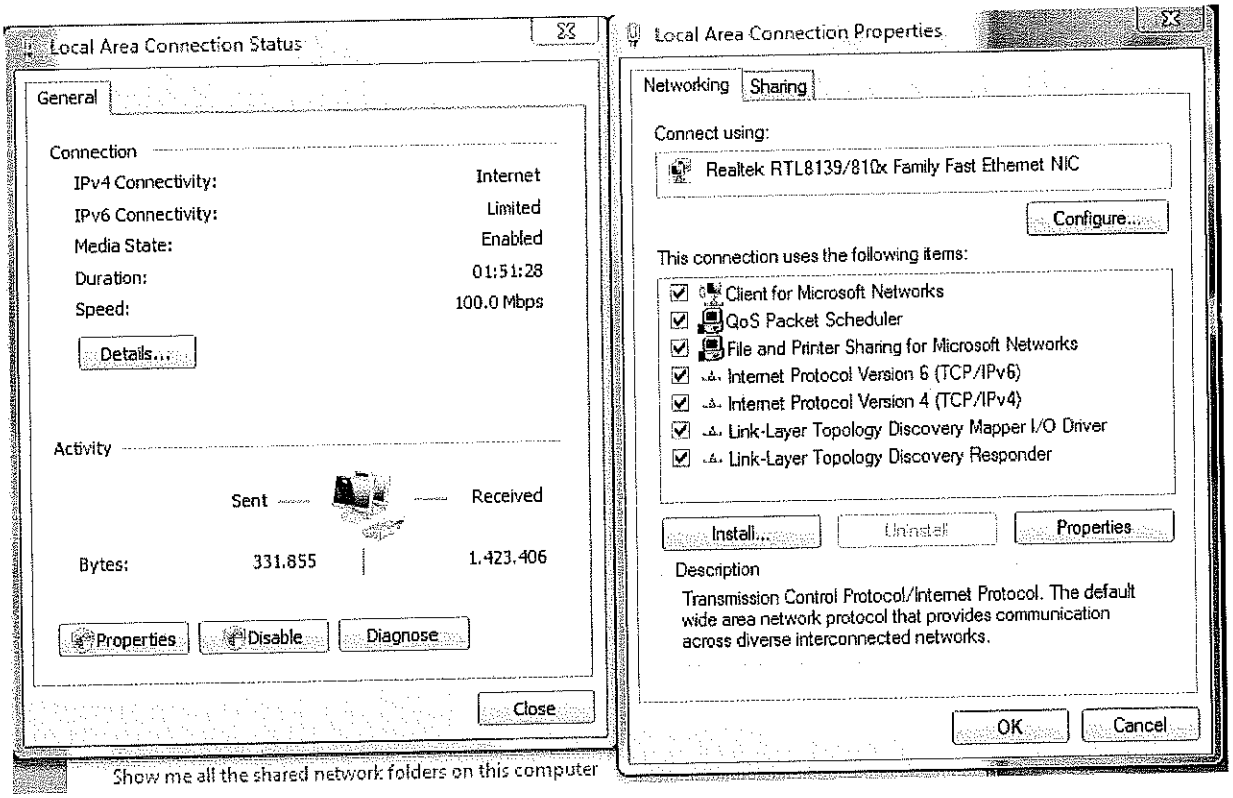
Hình 9.4: Các địa chỉ IP private

X. Sự gán tĩnh một địa chỉ IP:

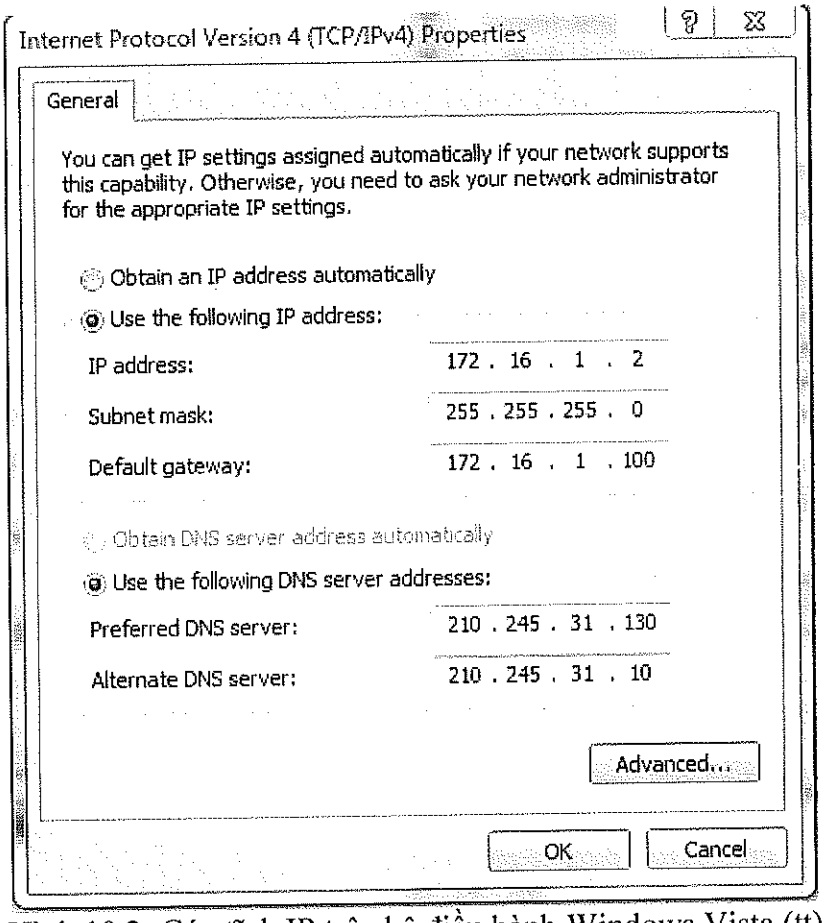
Gán tĩnh địa chỉ phù hợp cho các mạng nhỏ và ít thay đổi. người quản trị hệ thống gán bằng tay và theo dõi các địa chỉ IP trong mỗi máy tính, máy in hay server trên Intranet. Theo dõi tốt là điều quan trọng để ngăn các vấn đề phát sinh từ sự trùng lặp địa chỉ IP. Điều này chỉ có thể khi có một số lượng nhỏ các máy tính cần theo dõi. Ở đây ta chỉ thiết kế hệ thống có 50 PC nên việc gán tĩnh không có gì là trở ngại.

Các server sẽ được gán một địa chỉ IP tĩnh sao cho các máy trạm và các thiết bị khác luôn biết được cách thức truy xuất các dịch vụ cần thiết. Thử hình dung mức độ khó khăn như thế nào khi gọi điện thoại đến một doanh nghiệp mà số điện thoại luôn thay đổi hằng ngày.

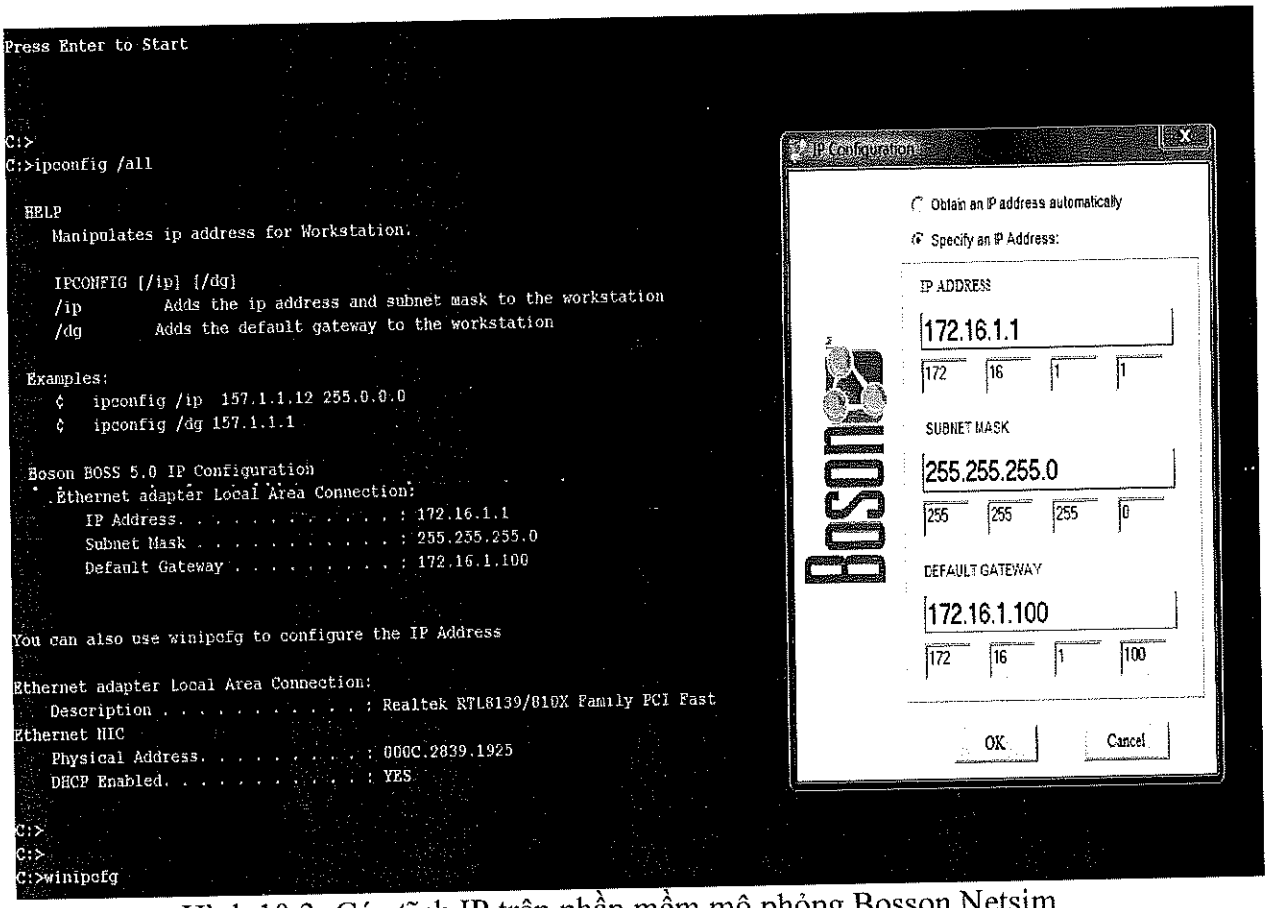
Các thiết bị khác được gán địa chỉ IP tĩnh là các máy in mạng, các server ứng dụng và các router.



Hình 10.1: Gán tĩnh IP trên hệ điều hành Windows Vista (PC)



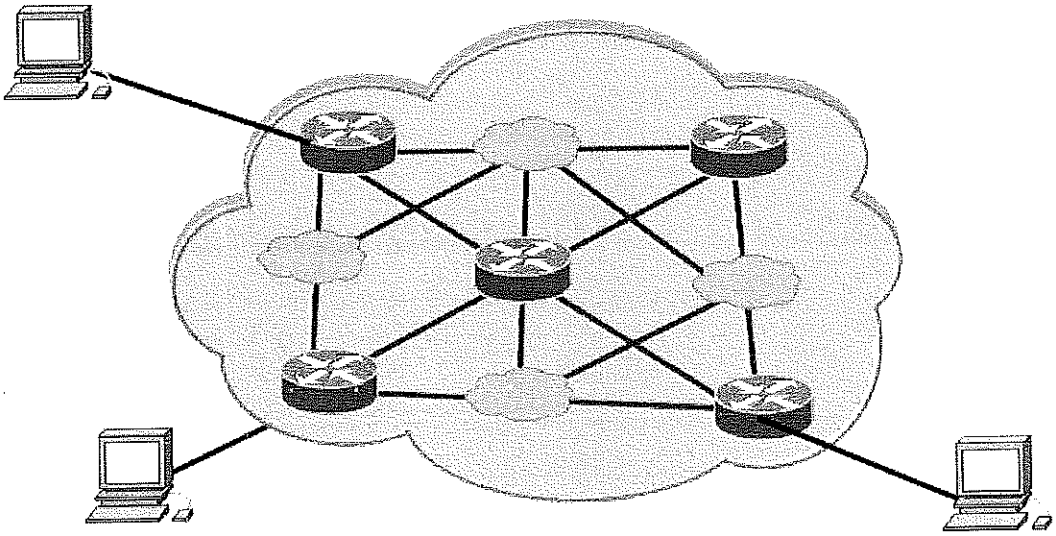
Hình 10.2: Gán tĩnh IP trên hệ điều hành Windows Vista (tt)



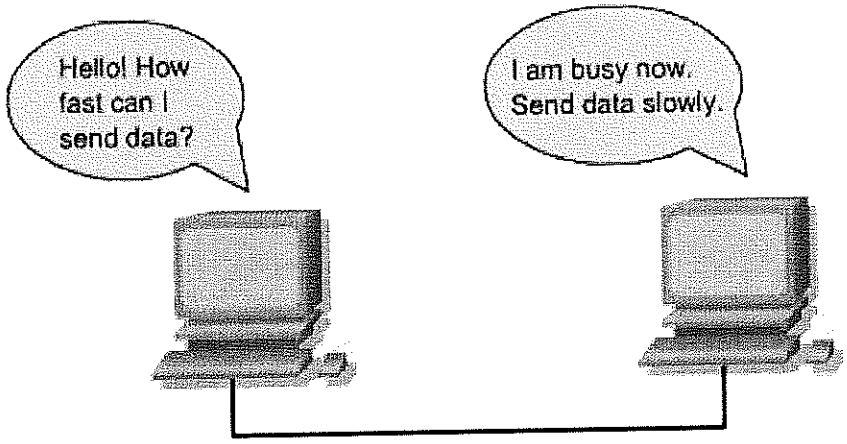
Hình 10.3: Gán tĩnh IP trên phần mềm mô phỏng Bosson Netsim

XI. Các thuật toán định tuyến và các metric:

Một thuật toán định tuyến là một lời giải chi tiết cho một bài toán. Trong trường hợp định tuyến các gói, các giao thức định tuyến khác nhau dùng các thuật toán định tuyến khác nhau để quyết định port nào mà một gói đến sẽ được chuyển đi tiếp.



Hình 11.1: Định tuyến đi qua mạng



Hình 11.2: Điều khiển tốc độ

XII. Phân chia Vlan trong hệ thống mạng:

XII.1 Vlan:

a) Khái niệm:

VLAN là cụm từ viết tắt của *virtual local area network* (hay *virtual* LAN) hay còn được gọi là mạng LAN ảo. VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ (giữa các khoa trong một trường học, giữa các cục trong một công ty,...) giúp giảm thiểu vùng quảng bá (*broadcast domain*) cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. VLAN tương đương như mạng con.

b) Phân loại VLAN

- ***Port - based VLAN*:** là cách cấu hình VLAN đơn giản và phổ biến. Đề tài sử dụng cách cấu hình này. Mỗi cổng của Switch được gắn với một VLAN xác định (mặc định là VLAN 1), do vậy bất cứ thiết bị host nào gắn vào cổng đó đều thuộc một VLAN nào đó.
- ***MAC address based VLAN:*** Cách cấu hình này ít được sử dụng do có nhiều bất tiện trong việc quản lý. Mỗi địa chỉ MAC được đánh dấu với một VLAN xác định.
- ***Protocol – based VLAN:*** Cách cấu hình này gần giống như MAC Address based, nhưng sử dụng một địa chỉ logic hay địa chỉ IP thay thế cho địa chỉ MAC. Cách cấu hình không còn thông dụng nhờ sử dụng giao thức DHCP.

c) Lợi ích của VLAN

- ***Tiết kiệm băng thông của hệ thống mạng:***

  VLAN chia mạng LAN thành nhiều đoạn (*segment*) nhỏ, mỗi đoạn đó là một vùng quảng bá (*broadcast domain)*. Khi có gói tin quảng bá (*broadcast*), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng.

- ***Tăng khả năng bảo mật:***

  Do các thiết bị ở các VLAN khác nhau không thể truy nhập vào nhau (trừ khi ta sử dụng router nối giữa các VLAN).

- ***Dễ dàng thêm hay bớt máy tính vào VLAN:***

Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn.

- ***Giúp mạng có tính linh động cao:***

  VLAN có thể dễ dàng di chuyển các thiết bị. Giả sử sau một thời gian sử dụng,nhà trường quyết định để mỗi bộ phận ở một tầng riêng biệt. Với VLAN, ta chỉ cần cấu hình lại các cổng switch rồi đặt chúng vào các VLAN theo yêu cầu.

VLAN có thể được cấu hình tĩnh hay động. Trong cấu hình tĩnh, ta phải cấu hình cho từng cổng của mỗi switch. Sau đó, gán cho nó vào một VLAN nào đó. Trong cấu hình động mỗi cổng của switch có thể tự cấu hình VLAN cho mình dựa vào địa chỉ MAC của thiết bị được kết nối vào.

XII.2 Khái niệm, hoạt động của mạch nối (trunk):

Thuật ngữ Trunking bắt nguồn từ công nghệ Radio và công nghệ điện thoại. Trong công nghệ radio, một đường Trunk là một đường dây truyền thông mà trên đó truyền tải nhiều kênh tín hiệu radio.

Trong công nghiệp điện thoại, khái niệm thuật ngữ Trunking là kết hợp giữa đường truyền thông điện thoại hoặc các kênh điện thoại giữa hai điểm. Một trong các điểm có thể là một tổng đài

Ngày nay, nguyên lý trunking được chấp nhận sử dụng trong công nghệ mạng chuyển mạch. Một đường Trunk là kết nối vật lý và logic giữa 2 switch.

a) Khái niệm:

Trong khuôn khổ môi trường chuyển mạch VLAN, một đường Trunk là một kết nối point-to-point để hỗ trợ các VLAN trên các switch liên kết với nhau. Một đường được cấu hình Trunk sẽ gộp nhiều liên kết ảo trên một liên kết vật lý để chuyển tín hiệu từ các VLAN trên các switch với nhau dựa trên một đường cáp vật lý.

b) Hoạt động của Trunking:

Giao thức Trunking được phát triển để nâng cao hiệu quả quản lý việc lưu chuyển các Frame từ các VLAN khác nhau trên một đường truyền vật lý. Giao thức trunking thiết lập các thoả thuận cho việc sắp sếp các Frame vào các cổng được liên kết với nhau ở hai đầu đường trunk.

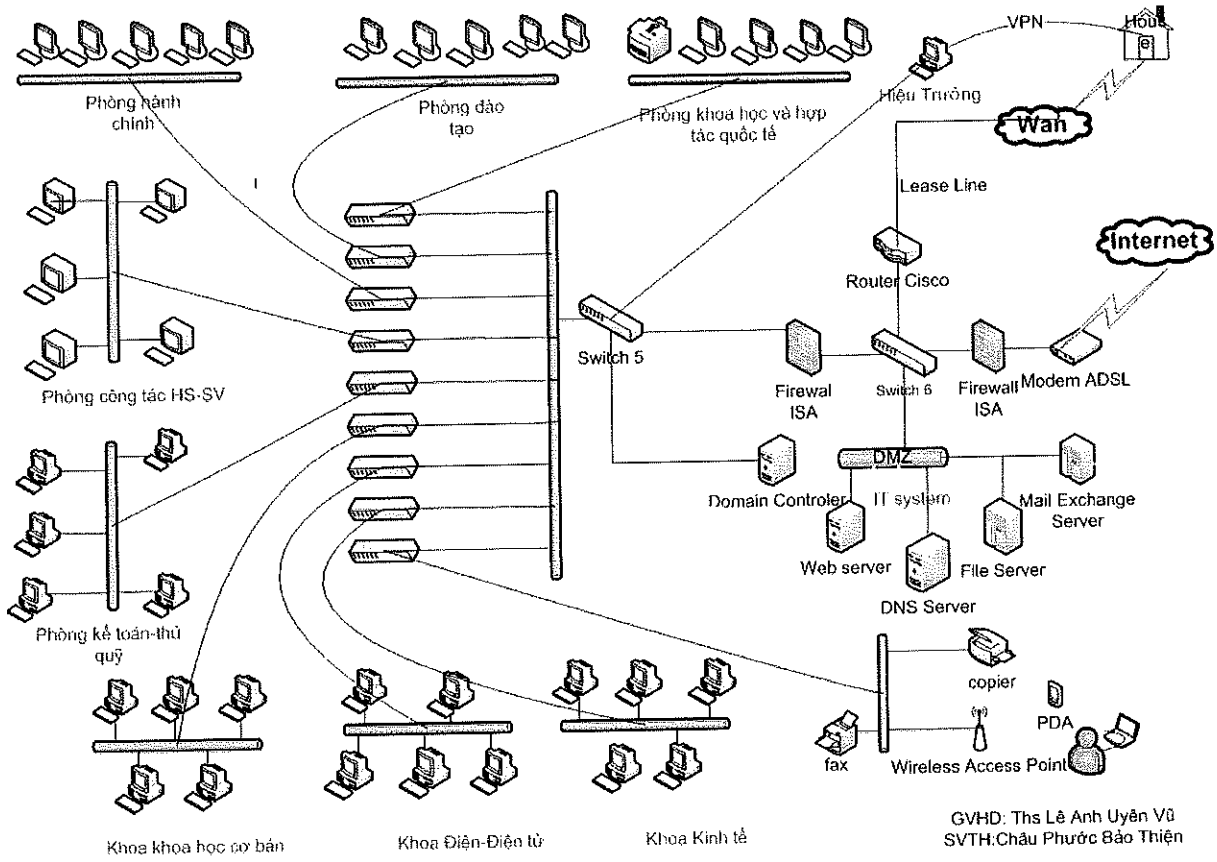
Hiện tại có 2 kỹ thuật Trunking là Frame Filtering và Frame Tagging. Trong khuôn khổ của luận văn này chỉ đề cập đến kỹ thuật Frame Tagging.

Giao thức Trunking sử dụng kỹ thuật Frame Tagging để phân biệt các Frame và để dễ dàng quản lý và phân phát các Frame nhanh hơn. Các tag được thêm vào trên đường gói tin đi ra vào đường trunk và được bỏ đi khi ra khỏi đường trunk. Các gói tin có gắn tag không phải là gói tin Broadcast.

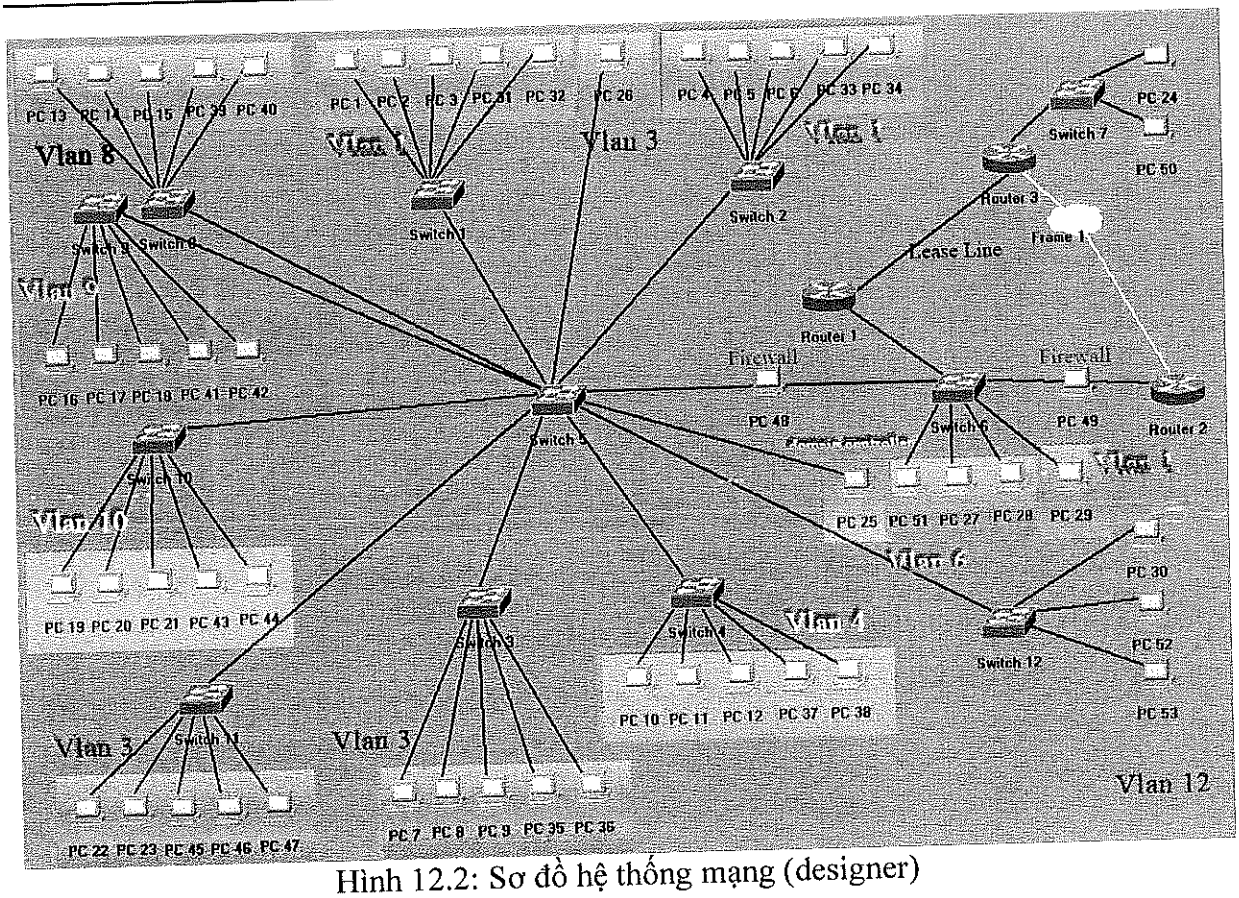
Một đường vật lý duy nhất kết nối giữa hai switch thì có thể truyền tải cho mọi VLAN. Để lưu trữ, mỗi Frame được gắn tag để nhận dạng trước khi gửi đi, Frame của VLAN nào thì đi về VLAN đó.

c) Cấu hình một cổng là Trunk trên switch

```
Switch_A(config)# interface fastethernet 0/1
Switch_A(config-if)# switchport mode trunk
Switch_A(config-if)# switchport trunk encapsulation dot1q
Hoặc
Switch_A(config-if)# switchport trunk encapsulation isl
Switch_A(config-if)# end
```



Hình 12.1: Sơ đồ hệ thống mạng (Visio)

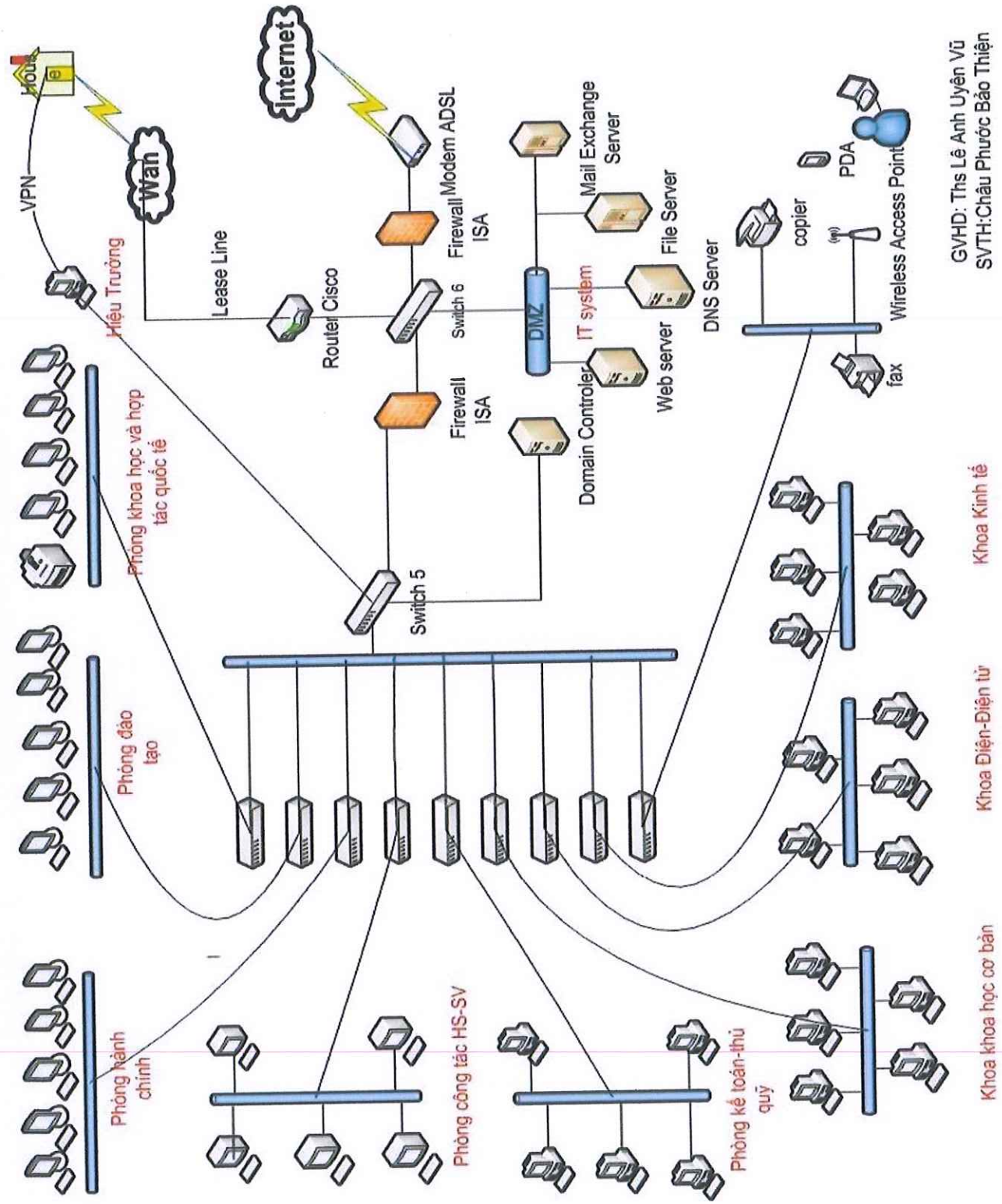


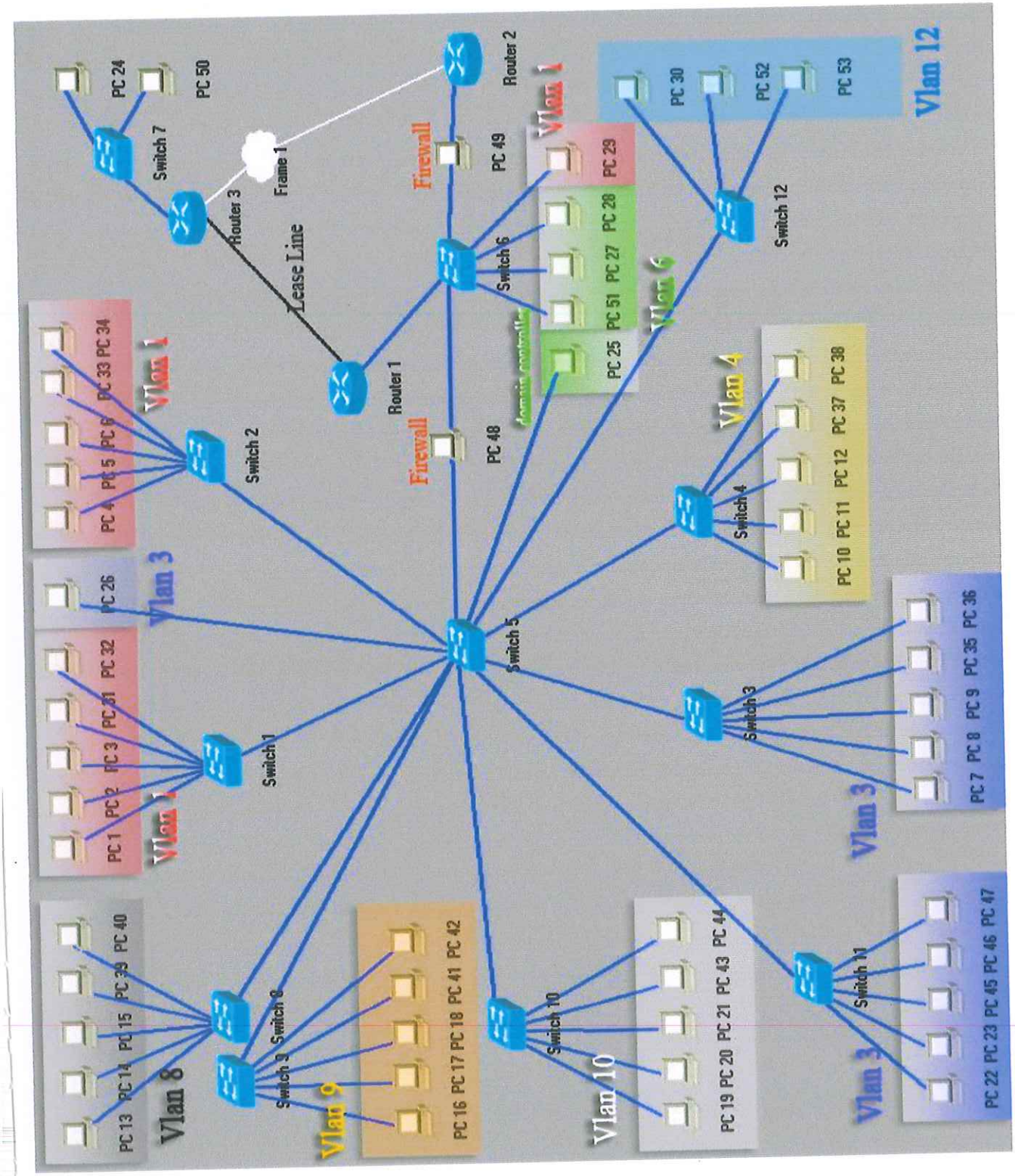
Hình 12.2: Sơ đồ hệ thống mạng (designer)

Mạng Lan được chia thành 7 Vlan theo các Switch như sau:
1) vlan 1 : gồm các PC thuộc switch 1(phòng đào tạo),switch 2(phòng khoa học và hợp tác quốc tế),PC 29
2) vlan 3 : gồm các PC thuộc switch 11 (khoa khoa học cơ bản),switch 3 (khoa điện-điện tử), PC26 (hiệu trưởng)
3) vlan 4 : gồm các PC thuộc switch 4 (khoa kinh tế)
4) vlan 6 : gồm các PC thuộc switch 6 (trừ PC29),PC25 (domain controller)
5) vlan 8 : gồm các PC thuộc switch 8 (phòng hành chính)
6) vlan 9 : gồm các PC thuộc switch 9 (phòng công tác học sinh-sinh viên)
7) vlan 10 : gồm các PC thuộc switch 10 (phòng kế toán thủ quỹ)

Thống kê		
Luận văn tốt nghiệp		
Biểu tượng	Số lượng	Thiết bị
	1	Modem
	21	PC
	1	PDA
	11	Switch
	11	Ethernet
	5	Terminal
	1	User
	3	Server
	2	Comm-link
	1	Multi-function device
	14	New iMac
	1	Laptop computer
	1	Copier
	1	Router
	2	Firewall
	1	Wireless access point
	1	Printer
	2	Mainframe

Bảng 12.3: Thống kê các thiết bị được sử dụng


Internet
Wan
VPN
Lease Line
Router Cisco
Modem ADSL
Firewall ISA
Switch 6
Firewall ISA
Switch 5
DMZ
Mail Exchange Server
File Server
IT system
Web server
Domain Controler
DNS Server
copier
PDA
Wireless Access Point
fax
Hiệu Trưởng
Phòng khoa học và hợp tác quốc tế
Phòng đào tạo
Phòng hành chính
Phòng công tác HS-SV
Phòng kế toán-thủ quỹ
Khoa Kinh tế
Khoa Điện-Điện tử
Khoa khoa học cơ bản
GVHD: Ths Lê Anh Uyên Vũ
SVTH:Châu Phước Bảo Thiện


Router 1
Router 2
Router 3
Frame 1
Lease Line
Firewall
Firewall
Switch 1
Switch 2
Switch 3
Switch 4
Switch 5
Switch 6
Switch 7
Switch 8
Switch 9
Switch 10
Switch 11
Switch 12
Vlan 1
Vlan 3
Vlan 4
Vlan 6
Vlan 8
Vlan 9
Vlan 10
Vlan 12
PC 1
PC 2
PC 3
PC 4
PC 5
PC 6
PC 7
PC 8
PC 9
PC 10
PC 11
PC 12
PC 13
PC 14
PC 15
PC 16
PC 17
PC 18
PC 19
PC 20
PC 21
PC 22
PC 23
PC 24
PC 25
PC 26
PC 27
PC 28
PC 29
PC 30
PC 31
PC 32
PC 33
PC 34
PC 35
PC 36
PC 37
PC 38
PC 39
PC 40
PC 41
PC 42
PC 43
PC 44
PC 45
PC 46
PC 47
PC 48
PC 49
PC 50
PC 51
PC 52
PC 53

XIII.Bức tường lửa (*firewall*):

Là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

Tường lửa là một thiết bị phần cứng và/hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các tòa nhà.

XIII.1.Chức năng

FireWall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong, và cả những dịch vụ nào bên ngoài được phép truy cập bởi những người bên trong.

XIII.2 Cấu trúc của FireWall

FireWall bao gồm :

Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.

Các phần mềm quản lí an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

Các thành phần của FireWall:

Một FireWall bao gồm một hay nhiều thành phần sau :

+ Bộ lọc packet (packet- filtering router).
+ Cổng ứng dụng (Application-level gateway hay proxy server).
+ Cổng mạch (Circuite level gateway).

FireWall bảo vệ cái gì ?

Nhiệm vụ cơ bản của FireWall là bảo vệ những vấn đề sau :

+ Dữ liệu : Những thông tin cần được bảo vệ do những yêu cầu sau:
  - Bảo mât.
  - Tính toàn vẹn.
  - Tính kịp thời.
+ Tài nguyên hệ thống.
+ Danh tiếng của công ty sở hữu các thông tin cần bảo vệ.

FireWall bảo vệ chống lại cái gì ?

FireWall bảo vệ chống lại những sự tấn công từ bên ngoài.

+ Tấn công trực tiếp:

Cách thứ nhất là dùng phương pháp dò mật khẩu trực tiếp. Thông qua các chương trình dò tìm mật khẩu với một số thông tin về người sử dụng như ngày sinh, tuổi, địa chỉ v.v...và kết hợp với thư viện do người dùng tạo ra, kẻ tấn công có thể dò được mật khẩu của bạn. Trong một số trường hợp khả năng thành công có thể lên tới 30%. Ví dụ như chương trình dò tìm mật khẩu chạy trên hệ điều hành Unix có tên là Crack.

Cách thứ hai là sử dụng lỗi của các chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được để chiếm quyền truy cập (có được quyền của người quản trị hệ thống).

+ Nghe trộm: Có thể biết được tên, mật khẩu, các thông tin chuyền qua mạng thông qua các chương trình cho phép đưa vi giao tiếp mạng (NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền qua mạng.

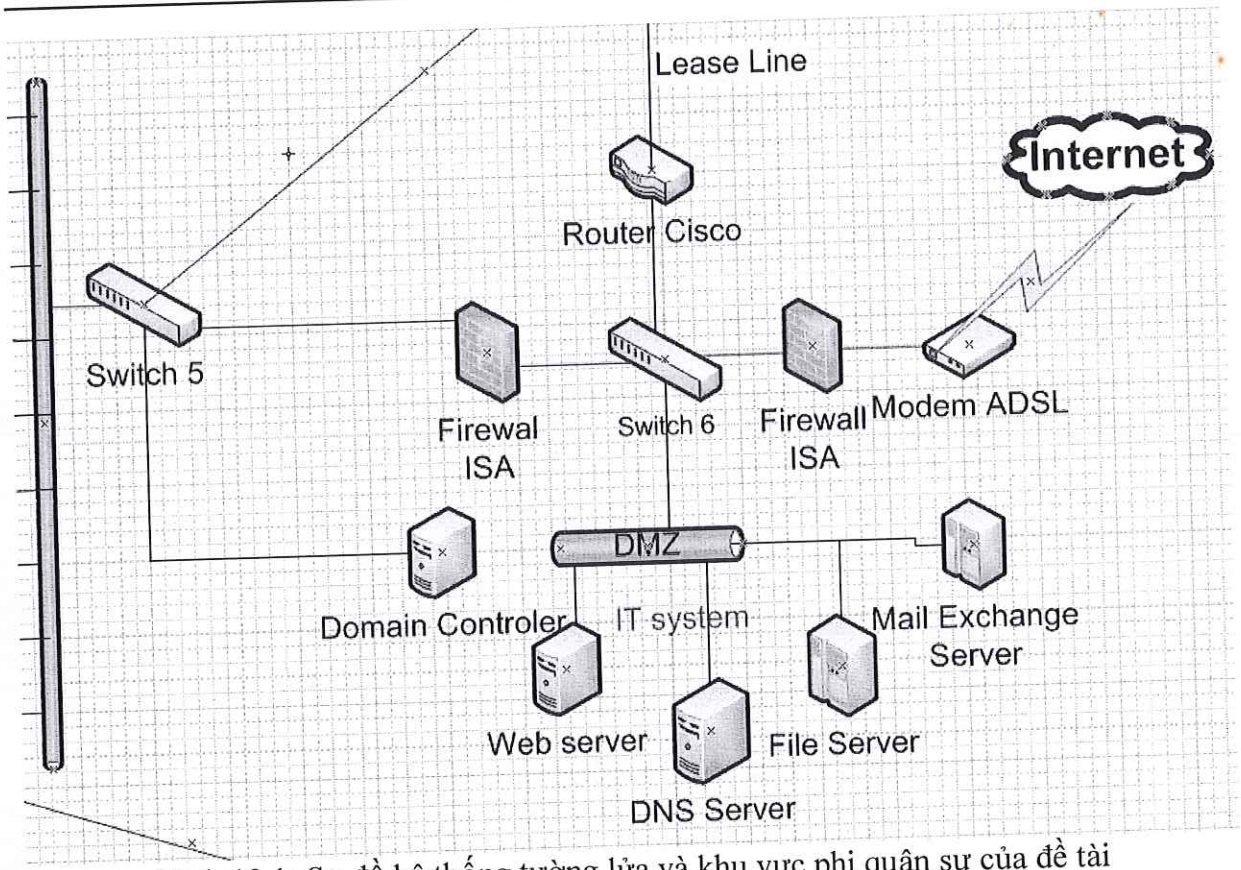
+ Giả mạo địa chỉ IP.

+ Vô hiệu hoá các chức năng của hệ thống (deny service). Đây là kiểu tấn công nhằm làm tê liệt toàn bộ hệ thống không cho nó thực hiện các chức năng mà nó được thiết kế. Kiểu tấn công này không thể ngăn chặn được do những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

+ Lỗi người quản trị hệ thống.

+ Yếu tố con người với những tính cách chủ quan và không hiểu rõ tầm quan trọng của việc bảo mật hệ thống nên dễ dàng để lộ các thông tin quan trọng cho hacker.

Ngày nay, trình độ của các hacker ngày càng giỏi hơn, trong khi đó các hệ thống mạng vẫn còn chậm chạp trong việc xử lý các lỗ hổng của mình. Điều này đòi hỏi người quản trị mạng phải có kiến thức tốt về bảo mật mạng để có thể giữ vững an toàn cho thông tin của hệ thống. Đối với người dùng cá nhân, họ không thể biết hết các thủ thuật để tự xây dựng cho mình một Firewall, nhưng cũng nên hiểu rõ tầm quan trọng của bảo mật thông tin cho mỗi cá nhân, qua đó tự tìm hiểu để biết một số cách phòng tránh những sự tấn công đơn giản của các hacker. Vấn đề là ý thức, khi đã có ý thức để phòng tránh thì khả năng an toàn sẽ cao hơn.



Hình 13.1: Sơ đồ hệ thống tường lửa và khu vực phi quân sự của đề tài theo mô hình Screened-Subnet

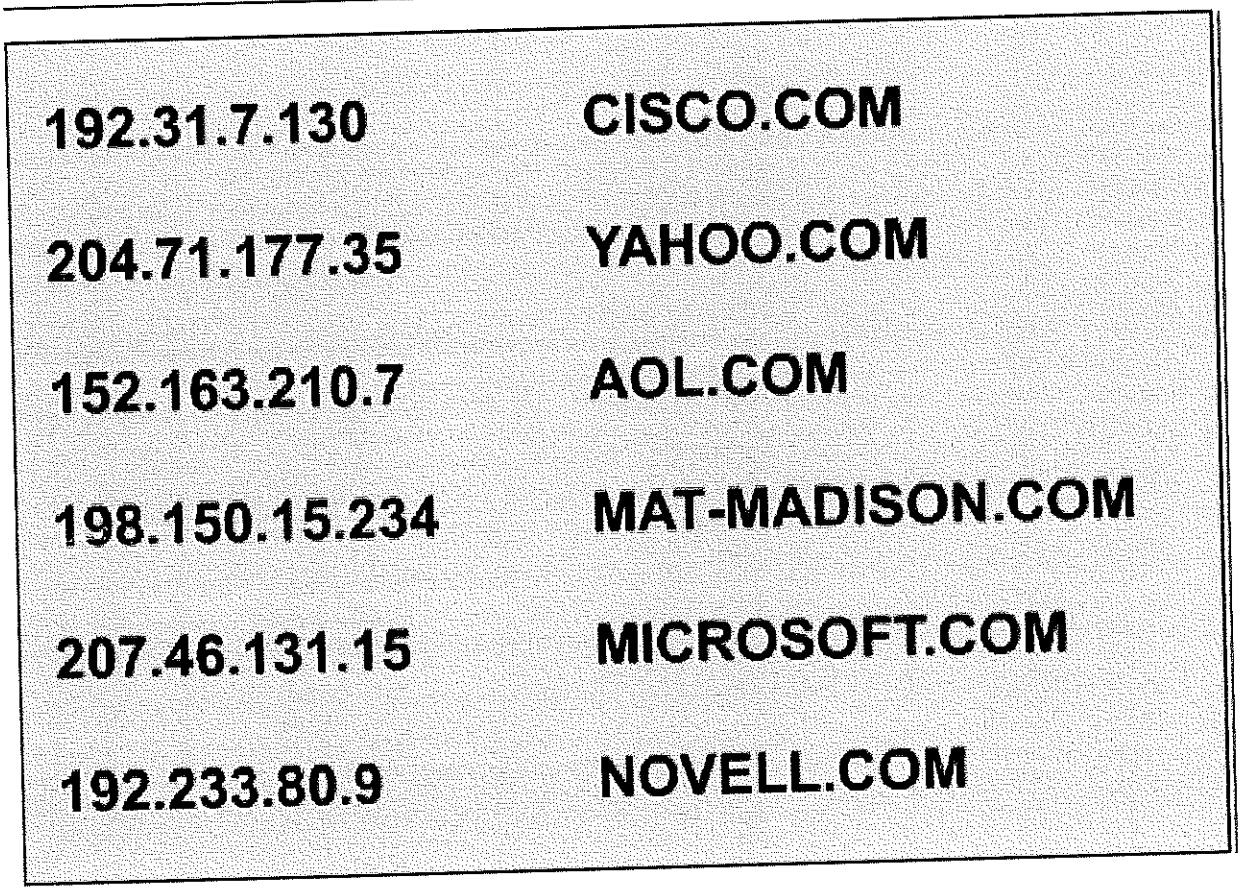
* Screened-Subnet Firewall:

Ưu điểm:

· Kẻ tấn công cần phá vỡ ba tầng bảo vệ: router ngoài, bastion host và router trong.

· Bởi vì router ngoài chỉ quảng cáo DMZ network tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã đợc chọn ra trên DMZ là được biết đến bởi Internet qua routing table và DNS information exchange (Domain Name Server).

· Bởi vì router trong chỉ quảng cáo DMZ network tới mạng nội bộ, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều nay đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ proxy.



Hình 13.2: Các địa chỉ IP của một số server hay dùng.

XIV. Domain Controller:

Một trong những khái niệm quan trọng nhất của mạng Windows là domain (tức miền hay vùng). Một domain là tập hợp các tài khoản người dùng và tài khoản máy tính được nhóm lại với nhau để quản lý một cách tập trung. Và công việc quản lý là dành cho domain controller (bộ điều khiển miền) nhằm giúp việc khai thác tài nguyên trở nên dễ dàng hơn.

Trong mạng, bất kỳ máy trạm nào đang chạy hệ điều hành Windows XP hoặc Vista cũng có một nhóm tài khoản người dùng tạo sẵn nào đó. Windows XP, Vista thậm chí còn cho phép ta tạo một số tài khoản bổ sung nếu thấy cần thiết. Nếu máy trạm có chức năng như một hệ thống độc lập hoặc là một phần của mạng ngang hàng thì tài khoản người dùng mức máy trạm (được gọi là tài khoản người dùng cục bộ) không thể điều

khiển truy cập tài nguyên mạng. Chúng chỉ được dùng để điều chỉnh truy cập máy cục bộ và hoạt động như với chức năng đảm bảo cho quản trị viên có thể thực hiện công việc bảo dưỡng, duy trì máy trạm, không cho phép người dùng cuối khả năng can thiệp vào các thiết lập trên máy trạm.

Lý do vì sao tài khoản người dùng cục bộ trên một máy trạm nhất định không được phép điều khiển truy cập tài nguyên nằm ngoài máy trạm đó là nó tăng thêm gánh nặng quản lý rất lớn. Tài khoản người dùng cục bộ chỉ nằm trên các máy trạm riêng rẽ. Nếu một tài khoản là có chức năng bảo mật chính trong mạng, quản trị viên sẽ phải di chuyển vật lý tới máy tính có tài khoản đó bất kỳ khi nào phải thực hiện thay đổi quyền hạn cho tài khoản. Vấn đề này không gây ra tác động gì lớn trong mạng nhỏ, nhưng sẽ trở nên cực kỳ nặng nề với ở mạng lớn hay khi cần áp dụng thay đổi rộng cho tất cả mọi tài khoản.

Một lý do khác nữa là không ai muốn phải chuyển tài khoản người dùng từ máy này sang máy khác. Chẳng hạn, nếu máy tính của một người dùng bị phá hoại, người đó không thể đăng nhập vào máy tính khác để làm việc vì tài khoản họ tạo chỉ có tác dụng trên máy cũ. Nếu muốn làm được việc người đó sẽ phải tạo tài khoản mới trên máy khác. Chỉ là một trong số rất nhiều lý do khiến việc sử dụng tài khoản người dùng cục bộ cho việc truy cập an toàn tài nguyên mạng là không thực tế. Thậm chí nếu ta muốn triển khai kiểu bảo mật này, Windows cũng không cho phép. Tài khoản người dùng cục bộ chỉ có thể dùng tài nguyên cục bộ trên một máy trạm nhất định.

Domain có nhiệm vụ giải quyết các vấn đề vừa nêu và một số vấn đề khác nữa. Chúng sẽ tập trung hoá tài khoản người dùng (hay cấu hình khác, các đối tượng liên quan đến bảo mật). Điều này giúp việc quản trị dễ dàng hơn và cho phép người dùng đăng nhập từ bất kỳ máy tính nào có trên mạng (trừ khi ta giới hạn quyền truy cập người dùng).

Toàn bộ công việc chúng ta phải làm với domain là gì? Khi máy chủ Windows sử dụng Windows 2000 Server, Windows Server 2003 hay Windows Server 2008, công việc của domain controller (bộ điều khiển miền) là chạy dịch vụ Active Directory. Active Directory hoạt động như một nơi lưu trữ các đối tượng thư mục, trong đó có tài khoản người dùng (user account). Và một trong các công việc chính của bộ điều khiển tên miền là cung cấp dịch vụ thẩm định.

Domain controller cung cấp dịch vụ thẩm định (authentication) chứ không phải là dịch vụ cấp phép (authorization). Khi một người dùng nào đó đăng nhập vào mạng, một bộ điều khiển miền sẽ kiểm tra tính hợp lệ của username và password họ nhập vào có

chính xác và khớp với dữ liệu lưu trong máy chủ hay không. Nhưng domain controller không nói với người dùng họ có quyền truy cập tài nguyên nào.

Tài nguyên trên mạng Windows được bảo vệ bởi các Danh sách điều khiển truy cập (ACL). Một ACL là danh sách chỉ rõ ai có quyền làm gì. Khi người dùng cố gắng truy cập tài nguyên, họ đưa ra nhân dạng của mình cho máy chủ chứa tài nguyên đó. Máy chủ sẽ kiểm tra để chắc chắn rằng nhận dạng người dùng này đã được thẩm định, sau đó tham chiếu chéo đến ACL để xem người dùng có quyền làm gì.

XV. Cấu trúc tổng quát các lệnh thiết yếu sử dụng trong đề tài:

XV.1.Các lệnh trên Switch:

Lệnh tạo Virtual Location Area Network(VLAN):

Switch# configure terminal ; vào chế độ cấu hình Switch
Switch(config)# vlan <n> ; vlan n được tạo trên Switch
Switch(config) # interface <name of interface> ;
Switch(config-if)# switchport access vlan <n>; vlan n được cấu hình cho port

Lệnh cấu hình chế độ trunk và access:

Mode access:

Switch# configure terminal
Switch(config)# interface <name of interface>
Switch(config)#switchport mode access : gán chế độ access cho port
Switch(config)#switchport access vlan <n>

Mode trunk:

Switch# configure terminal
Switch(config)# interface <name of interface>
Switch(config)#switchport mode trunk : gán chế độ trunk cho port
Switch(config)#switchport trunk encapsulation dot1q : đóng gói theo định dạng dot1q
Switch(config)#switchport trunk allowed vlan all ; cho phép tất cả các vlan được tạo đi qua trunk port này

XV.2.Các lệnh trên router:

Router#configure terminal
Router(config)# interface <name of interface>
Router(config-if)#no shutdown : mở port
Router(config-if)# exit
Router(config)# interface <name of interface>.<subinterface number>; trong đề tài subinterface được sử dụng là Vlan number.

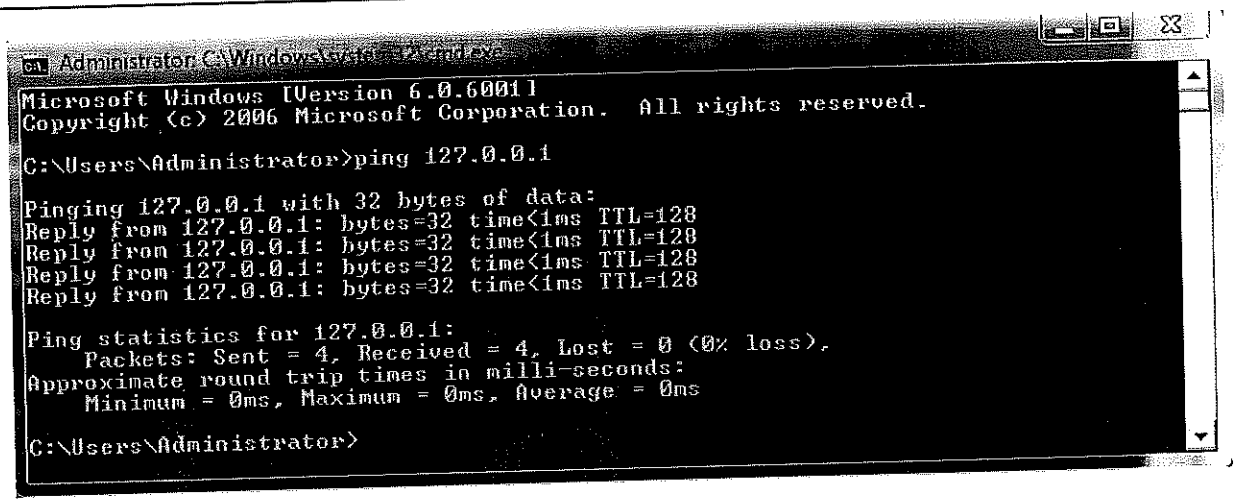
Router(config-if)#encapsulation dot1q <vlan number>
Router(config-if)#ip address <ip address> <subnet mask>

XVI. Kiểm tra tính kết nối bằng lệnh Ping:

Vì TCP/IP là một tập giao thức hay thể lệ được phát triển để cho phép các máy tính chia sẻ tài nguyên qua một mạng nên để cho phép TCP/IP trên một máy trạm, ta cần phải cấu hình thông qua các công cụ của hệ điều hành. Trong đồ án này, em sử dụng hệ điều hành trên nền tảng Microsoft là chủ yếu.

Ping là một tiện ích được dùng để xác thực kết nối Internet. Nó được đặt tên sau khi hoạt động định vị bằng sóng siêu âm được dùng để xác định khoảng cách đến các vật thể chì trong nước. Lệnh Ping làm việc bằng cách truyền đi nhiều gói ip đến một đích xác định. Mỗi gói truyền đi là một yêu cầu phúc đáp.Kết quả của một lệnh ping cho biết tỉ lệ thành công và thời gian hành trình đến đích. Từ thông tin này có thể xác định có một kết nối từ đây đến đích hay không. Lệnh ping được dùng để kiểm tra chức năng truyền nhận của NIC, cấu hình TCP/IP và tính kết nối của mạng. Các loại kiểm thử phổ biến dùng trong mạng với lệnh Ping:

- Ping 127.0.0.1-ping này là duy nhất và được gọi là kiểm thử vòng bên trong.Nó xác định hoạt động của TCP/IP và chức năng truyền/nhận của NIC
- Ping <địa chỉ IP của máy host cục bộ > đến host PC đẻ xác thực cấu hinh fđịa chỉ TCP/IP cho host cục bộ và tính kết nối đến host này.
- Ping<địa chỉ IP của default-gateway>-ping đến gateway mặc định xác định xem có đến router kết nối mạng cục bộ đến các mạng khác hay không.
- Ping <địa chỉ ip của đích ở xa>-Ping đến máy ở xa xem có kết nối được đến host đó không.



Hình15.1: Lệnh Ping

XVI.1 Ping thành công: Lệnh Ping thành công nếu ta nhận được trả lời từ thiết bị được ping tới như dưới đây:

Trên PC1, vào chế độ command line, gõ như sau:
C:>ping 172.16.1.29 →kiểm tra kết nối đến PC 29.
Pinging 172.16.1.29 with 32 bytes of data:

Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241

Ping statistics for 172.16.1.29: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

XVI.2 Ping tới gateway:
Từ PC1, vào chế độ command line, gõ như sau:
C:>ping 172.16.1.100→ kiểm tra kết nối đến gateway
Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=60ms TTL=241
Reply from 172.16.1.100: bytes=32 time=60ms TTL=241

Reply from 172.16.1.100: bytes=32 time=60ms TTL=241
Reply from 172.16.1.100: bytes=32 time=60ms TTL=241
Reply from 172.16.1.100: bytes=32 time=60ms TTL=241

Ping statistics for 172.16.1.100: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms
Ping to pc26 (hieu truong): di qua gateway (qua subinterfaces)

Tiếp tục từ PC1, vào chế độ command line, gõ:
C:>ping 172.16.3.26
Pinging 172.16.3.26 with 32 bytes of data:

Reply from 172.16.3.26: bytes=32 time=60ms TTL=241
Reply from 172.16.3.26: bytes=32 time=60ms TTL=241
Reply from 172.16.3.26: bytes=32 time=60ms TTL=241
Reply from 172.16.3.26: bytes=32 time=60ms TTL=241
Reply from 172.16.3.26: bytes=32 time=60ms TTL=241

Ping statistics for 172.16.3.26: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

XVI.3 Ping tới Vlan khác:

Ví dụ PC26 ping PC16 thuộc vlan 9: lệnh ping không thành công, kết nối giữa PC26 và PC16 không tồn tại vì khác VLAN với nhau.
Trên PC26, command line:
C:>ping 172.16.9.16
Pinging 172.16.9.16 with 32 bytes of data:

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

Ping statistics for 172.16.9.16:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),

Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Tương tự như vậy, một PC thuộc VLAN 1 chỉ kết nối được với PC thuộc VLAN của mình mà không thể kết nối với VLAN 3.(hình 15.2)

```
You can also use winipcfg to configure the IP Address

Ethernet adapter Local Area Connection:
    Description . . . . . . . . . . . : Realtek RTL8139/810X Family PCI Fast
Ethernet NIC
    Physical Address. . . . . . . . . : 000C.2839.1925
    DHCP Enabled. . . . . . . . . . . : YES

C:>
C:>
C:>winipcfg
C:>ping 172.16.1.29
Pinging 172.16.1.29 with 32 bytes of data:

Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241
Reply from 172.16.1.29: bytes=32 time=60ms TTL=241

Ping statistics for 172.16.1.29:     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum =  60ms, Average =  55ms

C:>ping 172.16.3.7
Pinging 172.16.3.7 with 32 bytes of data:

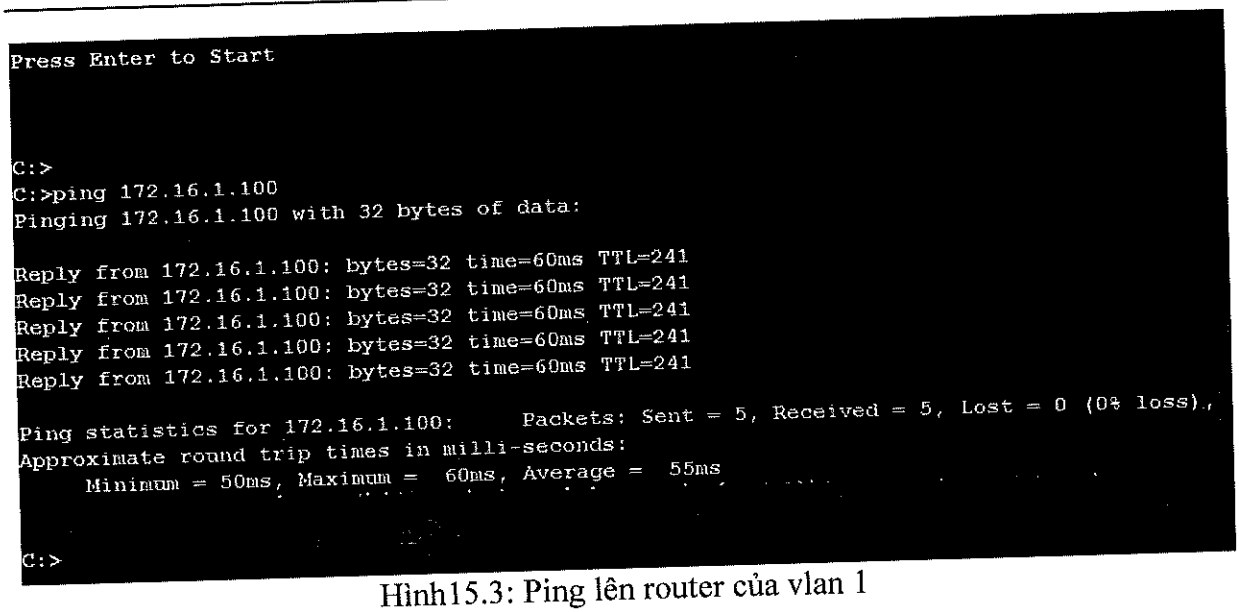
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.3.7:
    Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms


C:>
```

Hình 15.2: Ping cùng VLAN và khác VLAN.

PC 1 ping lên gateway của VLAN1 cho kết quả như hình 15.3:



Hình15.3: Ping lên router của vlan 1

Phần 3
Phụ Lục

Các cấu hình được thực hiện trên Router 1, Switch 1 và Switch 5:

Router1#show run
Building configuration...
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
!
!
ip subnet-zero
!
!
!
!
!
!
!
!
!
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet0/0
 ip address 172.16.100.100 255.255.255.0
 no ip directed-broadcast
!

```
interface FastEthernet0/0.2
 encapsulation dot1q 2
 ip address 172.16.2.100 255.255.255.0
!
!
interface FastEthernet0/0.1
 encapsulation dot1q 1
 ip address 172.16.1.100 255.255.255.0
!
!
interface FastEthernet0/0.6
 encapsulation dot1q 6
 ip address 172.16.6.100 255.255.255.0
!
!
interface FastEthernet0/0.5
 encapsulation dot1q 50
 ip address 172.16.129.101 255.255.255.0
!
!
interface FastEthernet0/0.12
 encapsulation dot1q 12
 ip address 172.16.12.100 255.255.255.0
!
!
interface FastEthernet0/0.3
 encapsulation dot1q 3
 ip address 172.16.3.100 255.255.255.0
!
!
interface FastEthernet0/0.4
 encapsulation dot1q 4
 ip address 172.16.4.100 255.255.255.0
!
!
interface FastEthernet0/0.8
 encapsulation dot1q 8
 ip address 172.16.8.100 255.255.255.0
!
```

```
!
interface FastEthernet0/0.9
 encapsulation dot1q 9
 ip address 172.16.9.100 255.255.255.0
!
!
interface FastEthernet0/0.10
 encapsulation dot1q 10
 ip address 172.16.10.100 255.255.255.0
!
!
interface FastEthernet0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
!
!
ip classless
no ip http server
!
!
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

Switch1#show run

```
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch1
!
!
!
ip subnet-zero
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/1
 switchport mode access
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 50
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport mode access
```

```
 switchport trunk encapsulation dot1q
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
 vtp Server
 vtp domain bigdomain
!
interface Vlan 1
 no ip address
 no ip route-cache
!
vlan 50 name vlan0050
vlan 2 name VLAN0002
!
!
!
ip classless
no ip http server
!
!
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end
```

Switch5#show run

```
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch5
!
!
!
ip subnet-zero
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
interface FastEthernet0/1
 switchport mode access
 switchport trunk allowed vlan 1-1005
 switchport trunk encapsulation dot1q
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport mode access
 switchport trunk allowed vlan 1-1005
 switchport trunk encapsulation dot1q
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 3
```

```
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 4
!
interface FastEthernet0/5
 switchport mode trunk
 switchport trunk allowed vlan 1-1005
 switchport trunk encapsulation dot1q
!
interface FastEthernet0/6
 switchport mode access
 switchport access vlan 3
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 6
!
interface FastEthernet0/8
 switchport mode access
 switchport access vlan 8
!
interface FastEthernet0/9
 switchport mode access
 switchport access vlan 9
!
interface FastEthernet0/10
 switchport mode access
 switchport access vlan 10
!
interface FastEthernet0/11
 switchport mode access
 switchport access vlan 3
!
interface FastEthernet0/12
 switchport mode access
 switchport access vlan 12
 switchport trunk allowed vlan 1-1005
 switchport trunk encapsulation dot1q
```

```
 vtp Server
 vtp domain bigdomain
!
interface Vlan 1
 no ip address
 no ip route-cache
!
vlan 3 name vlan0003
vlan 4 name vlan0004
vlan 6 name 6
vlan 8 name vlan0008
vlan 9 name 9
vlan 10 name 10
vlan 12 name vlan0012
vlan 2 name VLAN0002
vlan 5 name VLAN0005
!
!
!
ip classless
no ip http server
!
!
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end
```

Tài liệu tham khảo:

1. CCNA: Cisco Certified Network Associate Study Guide 5th Edition-Todd Lammle
2. Giáo trình hệ thống mạng máy tính-Nguyễn Hồng Sơn (chủ biên)
3. Giáo trình hệ thống máy tính CCNA 2- MKpub
4. Các tài liệu giảng dạy nội bộ của các trung tâm điện tử-tin học

Và một số tài liệu tham khảo trên internet : www.**wikipedia**.org,...

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TPHCM
KHOA ĐIỆN - ĐIỆN TỬ VIỄN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc
- - - o O o - - -

Ngày tháng năm

PHIẾU CHẤM ĐỒ ÁN TỐT NGHIỆP

(Dành cho người hướng dẫn)

1. Họ và tên SV: ..... MSSV: .....
   Ngày sinh: ..... Lớp: .....
2. Tên đề tài ĐATN: .....
   .....
3. Người hướng dẫn: .....
4. Tổng quát về bản thuyết minh :
   Số trang: ..... Số chương: .....
   Số bảng số liệu: ..... Số hình vẽ: .....
   Số tài liệu tham khảo: ..... Phần mềm tính toán:.....
   Hiện vật (sản phẩm nếu có): .....
5. Tổng quát về các bản vẽ:
   Số bảng vẽ: ..... bảng A1 ..... bảng A2 ..... khổ khác
   Số bảng vẽ tay: ..... Số bản vẽ trên máy tính: .....
6. Những ưu điểm chính của ĐATN:
   .....
   .....
   .....
   .....
   .....
7. Những thiếu sót chính của ĐATN:
   .....
   .....
   .....
   .....
   .....
8. Đề nghị: Được bảo vệ ☐ Bổ sung thêm để bảo vệ ☐ Không được bảo vệ ☐
9. 3 câu hỏi SV phải trả lời trước Hội đồng :
   a. .....
   .....
   b. .....
   .....
   c. .....
   .....
10. Đánh giá chung (bằng chữ: giỏi, khá, TB): Điểm ...../10

Ký tên (ghi rõ họ tên)

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TPHCM
KHOA ĐIỆN - ĐIỆN TỬ VIỄN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc
- - - o O o - - -

Ngày tháng năm

PHIẾU CHẤM ĐỒ ÁN TỐT NGHIỆP

(Dành cho người phản biện)

1. Họ và tên SV: ..... MSSV: .....
   Ngày sinh: ..... Lớp: .....
2. Tên đề tài ĐATN: .....
   .....
3. Người hướng dẫn: .....
4. Người phản biện: .....
5. Tổng quát về bản thuyết minh :
   Số trang: ..... Số chương: .....
   Số bảng số liệu: ..... Số hình vẽ: .....
   Số tài liệu tham khảo: ..... Phần mềm tính toán:.....
   Hiện vật (sản phẩm nếu có): .....
6. Tổng quát về các bản vẽ:
   Số bảng vẽ: ..... bảng A1 ..... bảng A2 ..... khổ khác
   Số bảng vẽ tay: ..... Số bản vẽ trên máy tính: .....
7. Những ưu điểm chính của ĐATN:
   .....
   .....
   .....
   .....
   .....
8. Những thiếu sót chính của ĐATN:
   .....
   .....
   .....
   .....
   .....
9. Đề nghị: Được bảo vệ ☐ Bổ sung thêm để bảo vệ ☐ Không được bảo vệ ☐
10. 3 câu hỏi SV phải trả lời trước Hội đồng :
    a. .....
    .....
    b. .....
    .....
    c. .....
    .....
11. Đánh giá chung (bằng chữ: giỏi, khá, TB): Điểm ...../10

Ký tên (ghi rõ họ tên)