

Giáo trình Quản trị mạng và Thiết bị mạng



LỜI NÓI ĐẦU	5
PHẦN I: KHÁI QUÁT VỀ CÔNG NGHỆ MẠNG	6
CHƯƠNG 1: TỔNG QUAN VỀ CÔNG NGHỆ MẠNG MÁY TÍNH VÀ MẠNG CỤC BỘ.....	6
MỤC 1: MẠNG MÁY TÍNH	6
1. GIỚI THIỆU MẠNG MÁY TÍNH.....	6
1.1. Định nghĩa mạng máy tính và mục đích của việc kết nối mạng	6
1.1.1. Nhu cầu của việc kết nối mạng máy tính.....	6
1.1.2. Định nghĩa mạng máy tính.....	6
1.2. Đặc trưng kỹ thuật của mạng máy tính.....	7
1.2.1. Đường truyền.....	7
1.2.2. Kỹ thuật chuyển mạch	7
1.2.3. Kiến trúc mạng.....	7
1.2.4. Hệ điều hành mạng	8
1.3. Phân loại mạng máy tính.....	8
1.3.1. Phân loại mạng theo khoảng cách địa lý :.....	8
1.3.2. Phân loại theo kỹ thuật chuyển mạch:	8
1.3.3. Phân loại theo kiến trúc mạng sử dụng.....	9
1.3.4. Phân loại theo hệ điều hành mạng	9
1.4. Các mạng máy tính thông dụng nhất	9
1.4.1. Mạng cục bộ.....	9
1.4.2. Mạng diện rộng với kết nối LAN to LAN	9
1.4.3. Liên mạng INTERNET.....	10
1.4.4. Mạng INTRANET	10
2. MẠNG CỤC BỘ, KIẾN TRÚC MẠNG CỤC BỘ	10
2.1. Mạng cục bộ.....	10
2.2. Kiến trúc mạng cục bộ	10
2.2.1. Đồ hình mạng (Network Topology)	10
2.3. Các phương pháp truy cập đường truyền vật lý.....	12
3. CHUẨN HOÁ MẠNG MÁY TÍNH.....	13
3.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng.....	13
3.2. Mô hình tham chiếu OSI 7 lớp.....	13
3.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X.....	14
MỤC 2: CÁC THIẾT BỊ MẠNG THÔNG DỤNG VÀ CÁC CHUẨN KẾT NỐI VẬT LÝ	15
1. CÁC THIẾT BỊ MẠNG THÔNG DỤNG	15
1.1. Các loại cáp truyền.....	15
1.1.1. Cáp đôi dây xoắn (Twisted pair cable)	15
1.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở	15
1.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable).....	16
1.1.4. Cáp quang	16
1.2. Các thiết bị ghép nối	17
1.2.1. Card giao tiếp mạng (Network Interface Card - NIC).....	17
1.2.2. Bộ chuyển tiếp (REPEATER)	17
1.2.3. Các bộ tập trung (Concentrator hay HUB)	17
1.2.4. Switching Hub (hay còn gọi tắt là switch).....	17
1.2.5. Modem	18
1.2.6. Multiplexor - Demultiplexor.....	18
1.2.7. Router.....	18
2. MỘT SỐ KIỂU NỐI MẠNG THÔNG DỤNG VÀ CÁC CHUẨN	19

2.1. Các thành phần thông thường trên một mạng cục bộ	18
2.2. Kiểu 10BASE5.....	19
2.3. Kiểu 10BASE2.....	19
2.4. Kiểu 10BASE-T.....	20
2.5. Kiểu 10BASE-F.....	20
CHƯƠNG 2: GIỚI THIỆU GIAO THỨC TCP/IP.....	22
1. GIAO THỨC IP.....	
1.1. Họ giao thức TCP/IP.....	21
1.2. Chức năng chính của - Giao thức liên mạng IP(v4)	23
1.3. Địa chỉ IP	23
1.4. Cấu trúc gói dữ liệu IP	24
1.5. Phân mảnh và hợp nhất các gói IP.....	25
1.6. Định tuyến IP	25
2. MỘT SỐ GIAO THỨC ĐIỀU KHIỂN	26
2.1. Giao thức ICMP.....	26
2.2. Giao thức ARP và giao thức RARP.....	26
3.1. Giao thức TCP	27
3.1.1 Cấu trúc gói dữ liệu TCP	27
3.1.2 Thiết lập và kết thúc kết nối TCP	28
PHẦN II: QUẢN TRỊ MẠNG.....	30
CHƯƠNG 3: TỔNG QUAN VỀ BỘ ĐỊNH TUYẾN	33
1. LÝ THUYẾT VỀ BỘ ĐỊNH TUYẾN.....	33
1.1. Tổng quan về bộ định tuyến.....	32
1.2. Các chức năng chính của bộ định tuyến, tham chiếu mô hình OSI	32
1.3. Cấu hình cơ bản và chức năng của các bộ phận của bộ định tuyến.....	34
2. GIỚI THIỆU VỀ BỘ ĐỊNH TUYẾN CISCO.....	35
2.1. Giới thiệu bộ định tuyến Cisco	35
2.2. Một số tính năng ưu việt của bộ định tuyến Cisco	36
2.3. Một số bộ định tuyến Cisco thông dụng.....	36
2.4. Các giao tiếp của bộ định tuyến Cisco.....	40
2.5. Kiến trúc module của bộ định tuyến Cisco.....	41
3. CÁCH SỬ DỤNG LỆNH CẤU HÌNH BỘ ĐỊNH TUYẾN	47
3.1. Giới thiệu giao tiếp dòng lệnh của bộ định tuyến Cisco.....	47
3.2. Làm quen với các chế độ cấu hình.....	50
3.3. Làm quen với các lệnh cấu hình cơ bản.....	53
3.4. Cách khắc phục một số lỗi thường gặp.....	60
4. CẤU HÌNH BỘ ĐỊNH TUYẾN CISCO	61
4.1. Cấu hình leased-line.....	61
4.2. Cấu hình X.25 & Frame Relay	65
4.3. Cấu hình Dial-up.....	80
4.4. Định tuyến tĩnh và động.....	83
5. BỘ CHUYỂN MẠCH LỚP 3	89
5.1. Tổng quan và kiến trúc bộ chuyển mạch lớp 3	89
5.2. Định tuyến trên bộ chuyển mạch lớp 3	91
5.3. Sơ lược về các bộ chuyển mạch lớp 3 thông dụng của Cisco.....	92
6. BÀI TẬP THỰC HÀNH SỬ DỤNG BỘ ĐỊNH TUYẾN CISCO.....	95
Bài 1: Thực hành nhận diện thiết bị, đầu nối thiết bị.....	94
Bài 2: Thực hành các lệnh cơ bản.....	94
Bài 3: Cấu hình bộ định tuyến với mô hình đầu nối leased-line.....	94
Bài 4: Cấu hình bộ định tuyến với Dial-up.....	94

Thiết bị phòng lab	95
CHƯƠNG 4: Hệ THỐNG TÊN MIỀN DNS	96
1. GIỚI THIỆU	96
1.1. Lịch sử hình thành của DNS	96
1.2. Mục đích của hệ thống DNS	96
2. DNS SERVER VÀ CẤU TRÚC CƠ SỞ DỮ LIỆU TÊN MIỀN	98
2.1. Cấu trúc cơ sở dữ liệu	98
2.2. Phân loại DNS server và đồng bộ dữ liệu giữa các DNS server	101
3. HOẠT ĐỘNG CỦA HỆ THỐNG DNS	105
4. BÀI TẬP THỰC HÀNH	109
Bài 1: Cài đặt DNS Server cho Window 2000	109
Bài 2: Cài đặt, cấu hình DNS cho Linux	118
CHƯƠNG 5: DỊCH VỤ TRUY CẬP TỪ XA VÀ DỊCH VỤ PROXY	128
MỤC 1: DỊCH VỤ TRUY CẬP TỪ XA (REMOTE ACCESS)	128
1. CÁC KHÁI NIỆM VÀ CÁC GIAO THỨC	128
1.1. Tổng quan về dịch vụ truy cập từ xa	128
1.2. Kết nối truy cập từ xa và các giao thức sử dụng trong truy cập từ xa	129
1.3. Modem và các phương thức kết nối vật lý	133
2. AN TOÀN TRONG TRUY CẬP TỪ XA	135
2.1. Các phương thức xác thực kết nối	135
2.2. Các phương thức mã hóa dữ liệu	137
3. TRIỂN KHAI DỊCH VỤ TRUY CẬP TỪ XA	138
3.1. Kết nối gọi vào và kết nối gọi ra	138
3.2. Kết nối sử dụng đa luồng (Multilink)	139
3.3. Các chính sách thiết lập cho dịch vụ truy nhập từ xa	140
3.4. Sử dụng dịch vụ gán địa chỉ động DHCP cho truy cập từ xa	141
3.5. Sử dụng RadiusServer để xác thực kết nối cho truy cập từ xa	142
3.6. Mạng riêng ảo và kết nối dùng dịch vụ truy cập từ xa	144
3.7. Sử dụng Network and Dial-up Connection	145
3.8. Một số vấn đề xử lý sự cố trong truy cập từ xa	146
4. BÀI TẬP THỰC HÀNH	147
Bài 1: Thiết lập dialup networking để tạo ra kết nối Internet, truy cập Internet và giới thiệu các dịch vụ cơ bản	147
Bài 2: Cài đặt và cấu hình dịch vụ truy cập từ xa cho phép người dùng từ xa truy cập vào mạng trên hệ điều hành Windows 2000 server	148
Bài 3: Cấu hình VPN server và thiết lập VPN Client, kiểm tra kết nối từ VPN Client tới VPN server	151
MỤC 2 : DỊCH VỤ PROXY - GIẢI PHÁP CHO VIỆC KẾT NỐI MẠNG DÙNG RIÊNG RA INTERNET	152
1. CÁC KHÁI NIỆM	152
1.1. Mô hình client server và một số khả năng ứng dụng	152
1.2. Socket	153
1.3. Phương thức hoạt động và đặc điểm của dịch vụ Proxy	155
1.4. Cache và các phương thức cache	157
2. TRIỂN KHAI DỊCH VỤ PROXY	159
2.1. Các mô hình kết nối mạng	159
2.2. Thiết lập chính sách truy cập và các qui tắc	162
2.3. Proxy client và các phương thức nhận thực	165
2.4. NAT và proxy server	169
3. CÁC TÍNH NĂNG CỦA PHẦN MỀM MICROSOFT ISA SERVER 2000	171

3.1. Các phiên bản.....	171
3.2. Lợi ích.....	171
3.3. Các chế độ cài đặt.....	172
3.4. Các tính năng của mỗi chế độ cài đặt.....	173
4. BÀI TẬP THỰC HÀNH.....	174
Bài 1: Các bước cài đặt cơ bản phần mềm ISA server 2000.....	174
Bài 2: Cấu hình ISA Server 2000 cho phép một mạng nội bộ có thể truy cập, sử dụng các dịch vụ cơ bản trên Internet qua 01 modem kết nối qua mạng PSTN.....	176
Bài 3: Thiết đặt các chính sách cho các yêu cầu truy cập và sử dụng các dịch vụ trên mạng internet.....	178
CHƯƠNG 6: BẢO MẬT HỆ THỐNG VÀ FIREWALL.....	185
1. BẢO MẬT HỆ THỐNG.....	182
1.1. Các vấn đề chung về bảo mật hệ thống và mạng.....	182
1.1.1. Một số khái niệm và lịch sử bảo mật hệ thống.....	182
1.1.2. Các lỗ hổng và phương thức tấn công mạng chủ yếu.....	184
1.1.3. Một số điểm yếu của hệ thống.....	194
1.1.4. Các mức bảo vệ an toàn mạng.....	195
1.2. Các biện pháp bảo vệ mạng máy tính.....	196
1.2.1. Kiểm soát hệ thống qua logfile.....	196
1.2.2. Thiết lập chính sách bảo mật hệ thống.....	204
2. TỔNG QUAN VỀ HỆ THỐNG FIREWALL.....	211
2.1. Giới thiệu về Firewall.....	208
2.1.1. Khái niệm Firewall.....	208
2.1.2. Các chức năng cơ bản của Firewall.....	208
2.1.3. Mô hình mạng sử dụng Firewall.....	208
2.1.4. Phân loại Firewall.....	210
2.2. Một số phần mềm Firewall thông dụng.....	214
2.2.1. Packet filtering.....	214
2.2.2. Application-proxy firewall.....	215
2.3. Thực hành cài đặt và cấu hình firewall Check Point v4.0 for Windows.....	215
2.3.1. Yêu cầu phần cứng:.....	215
2.3.2. Các bước chuẩn bị trước khi cài đặt:.....	216
2.3.3. Tiến hành cài đặt.....	217
2.3.4. Thiết lập cấu hình.....	228
TÀI LIỆU THAM KHẢO.....	229

Lời nói đầu

Giáo trình “**Quản trị mạng và các thiết bị mạng**” được biên soạn với mục tiêu cung cấp các kiến thức lý thuyết và thực hành quản trị chủ yếu cho các hệ thống thiết bị quan trọng nền tảng của mạng máy tính hiện đại. Giáo trình gồm 2 phần :

Phần 1. Khái quát về mạng máy tính : Bao gồm những khái niệm định nghĩa cơ bản nhất về mạng máy tính, phân loại mạng máy tính, giới thiệu các giao thức mạng, đặc biệt là giao thức TCP/IP. Các cơ sở lý thuyết đưa ra trong chương này đòi hỏi học viên phải nắm vững để có thể tiếp thu được các nội dung trong phần 2. **Tuy vậy, nếu học viên đã tự trang bị các kiến thức cơ bản trên hoặc đã được đào tạo theo giáo trình “Thiết kế và xây dựng mạng LAN và WAN” của đề án 112 có thể bỏ qua nội dung của phần một và học vào nội dung của phần 2 giáo trình**

Phần 2. Quản trị mạng : Đây là phần nội dung chính của giáo trình “Quản trị mạng và các thiết bị mạng” bao gồm 4 chương cung cấp các kiến thức lý thuyết và kỹ năng quản trị cơ bản với các thành phần trọng yếu của mạng bao gồm bộ định tuyến, bộ chuyển mạch, hệ thống tên miền, hệ thống truy cập từ xa, hệ thống proxy, hệ thống bức tường lửa (firewall). Các nội dung biên soạn về kỹ năng thực hành quản trị giúp học viên có đủ các kiến thức thực tế để có thể bắt tay vào công tác quản trị mạng cho đơn vị.

Do phạm vi rộng của công tác quản trị mạng, giáo trình này không bao gồm hết được mọi nội dung của công tác quản trị mạng. Học viên có nhu cầu nên tham khảo thêm các giáo trình khác của đề án 112 như :

- Thiết kế và xây dựng mạng LAN và WAN
- Quản trị Windows 2000-NT
- Tổng quan về Lotus Notes Domino
- Thiết kế và quản trị website, portal
- Thiết lập và quản trị hệ thống thư điện tử

Giáo trình được biên soạn lần đầu tiên nên không tránh khỏi có những thiếu sót. Nhóm biên soạn rất mong nhận được các góp ý từ phía các học viên, bạn đọc để có thể hoàn thiện nội dung giáo trình tốt hơn.

PHẦN I: KHÁI QUÁT VỀ CÔNG NGHỆ MẠNG

Chương 1

Tổng quan về công nghệ mạng máy tính và mạng cục bộ

Mục 1: Mạng máy tính

1. Giới thiệu mạng máy tính

1.1. Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

1.1.1. Nhu cầu của việc kết nối mạng máy tính

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan vì :

- Có rất nhiều công việc về bản chất là phân tán hoặc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.
- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm (ổ cứng, máy in, ổ CD ROM . . .)
- Nhu cầu liên lạc, trao đổi thông tin nhờ phương tiện máy tính.
- Các ứng dụng phần mềm đòi hỏi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

1.1.2. Định nghĩa mạng máy tính

Nói một cách ngắn gọn thì mạng máy tính là tập hợp các máy tính độc lập được kết nối với nhau thông qua các đường truyền vật lý và tuân theo các quy ước truyền thông nào đó.

Khái niệm máy tính độc lập được hiểu là các máy tính không có máy nào có khả năng khởi động hoặc đình chỉ một máy khác.

Các đường truyền vật lý được hiểu là các môi trường truyền tín hiệu vật lý (có thể là hữu tuyến hoặc vô tuyến).

Các quy ước truyền thông chính là cơ sở để các máy tính có thể "nói chuyện" được với nhau và là một yếu tố quan trọng hàng đầu khi nói về công nghệ mạng máy tính.

1.2. Đặc trưng kỹ thuật của mạng máy tính

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

1.2.1. Đường truyền

Là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điện tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON-OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tùy theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

Thông thường người ta hay phân loại đường truyền theo hai loại:

- Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây dẫn tín hiệu).
- Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyến với các thiết bị điều chế/giải điều chế ở các đầu nút.

1.2.2. Kỹ thuật chuyển mạch

Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các kỹ thuật chuyển mạch như sau:

- Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.
- Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo
- Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng quy định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gửi đi qua mạng tới đích theo nhiều con đường khác nhau.

1.2.3. Kiến trúc mạng

Kiến trúc mạng máy tính (network architecture) thể hiện cách nối các máy tính với nhau và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt.

Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

- Network Topology: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Các giao thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, . . .

1.2.4. Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:

- Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:

+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này

+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng

- Quản lý người dùng và các công việc trên hệ thống.

Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.

- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung ...)

Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

1.3. Phân loại mạng máy tính

Có nhiều cách phân loại mạng khác nhau tùy thuộc vào yếu tố chính được chọn dùng để làm chỉ tiêu phân loại, thông thường người ta phân loại mạng theo các tiêu chí như sau

- Khoảng cách địa lý của mạng
- Kỹ thuật chuyển mạch mà mạng áp dụng
- Kiến trúc mạng
- Hệ điều hành mạng sử dụng ...

Tuy nhiên trong thực tế người ta thường chỉ phân loại theo hai tiêu chí đầu tiên

1.3.1. Phân loại mạng theo khoảng cách địa lý

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ (LAN), mạng đô thị (MAN), mạng diện rộng (WAN), mạng toàn cầu.

1.3.2. Phân loại theo kỹ thuật chuyển mạch

Nếu lấy kỹ thuật chuyển mạch làm yếu tố chính để phân loại sẽ có: mạng chuyển mạch kênh, mạng chuyển mạch thông báo và mạng chuyển mạch gói.

Mạch chuyển mạch kênh (circuit switched network) : hai thực thể thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc.

Mạng chuyển mạch thông báo (message switched network) : Thông báo là một đơn vị dữ liệu qui ước được gửi qua mạng đến điểm đích mà không thiết lập kênh truyền cố định. Căn cứ vào thông tin tiêu đề mà các nút mạng có thể xử lý được việc gửi thông báo đến đích

Mạng chuyển mạch gói (packet switched network) : ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gửi đi qua mạng tới đích theo nhiều con đường khác nhau.

1.3.3. Phân loại theo kiến trúc mạng sử dụng

Kiến trúc của mạng bao gồm hai vấn đề: hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

Hình trạng mạng: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Giao thức mạng: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

Phân loại theo giao thức mà mạng sử dụng người ta phân loại thành mạng : TCP/IP, mạng NETBIOS . . .

Tuy nhiên các cách phân loại trên không phổ biến và chỉ áp dụng cho các mạng cục bộ.

1.3.4. Phân loại theo hệ điều hành mạng

Nếu phân loại theo hệ điều hành mạng người ta chia ra theo mô hình mạng ngang hàng, mạng khách/chủ hoặc phân loại theo tên hệ điều hành mà mạng sử dụng: Windows NT, Unix, Novell . . .

1.4. Các mạng máy tính thông dụng nhất

1.4.1. Mạng cục bộ

Một mạng cục bộ là sự kết nối một nhóm máy tính và các thiết bị kết nối mạng được lắp đặt trên một phạm vi địa lý giới hạn, thường trong một toà nhà hoặc một khu công sở nào đó. Mạng có tốc độ cao

1.4.2. Mạng diện rộng với kết nối LAN to LAN

Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu. Mạng có tốc độ truyền dữ liệu không cao, phạm vi địa lý không giới hạn

1.4.3. Liên mạng INTERNET

Với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng INTERNET. Mạng Internet là sở hữu của nhân loại, là sự kết hợp của rất nhiều mạng dữ liệu khác chạy trên nền tảng giao thức TCP/IP

1.4.4. Mạng INTRANET

Thực sự là một mạng INTERNET thu nhỏ vào trong một cơ quan/công ty/tổ chức hay một bộ/ngành . . ., giới hạn phạm vi người sử dụng, có sử dụng các công nghệ kiểm soát truy cập và bảo mật thông tin .

Được phát triển từ các mạng LAN, WAN dùng công nghệ INTERNET

2. Mạng cục bộ, kiến trúc mạng cục bộ

2.1. Mạng cục bộ

Tên gọi “mạng cục bộ” được xem xét từ quy mô của mạng. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng. Sau đây là một số đặc điểm của mạng cục bộ:

Đặc điểm của mạng cục bộ

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km.
- Mạng cục bộ thường là sở hữu của một tổ chức. Thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả.
- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đạt vài trăm Kbit/s đến Mb/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100 Mbit/s và tới nay với Gigabit Ethernet.

2.2. Kiến trúc mạng cục bộ

2.2.1. Đồ hình mạng (Network Topology)

* Định nghĩa Topo mạng:

Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng. Có hai kiểu nối mạng chủ yếu đó là :

- Nối kiểu điểm - điểm (point - to - point): các đường truyền nối từng cặp nút với nhau, mỗi nút “lưu và chuyển tiếp” dữ liệu

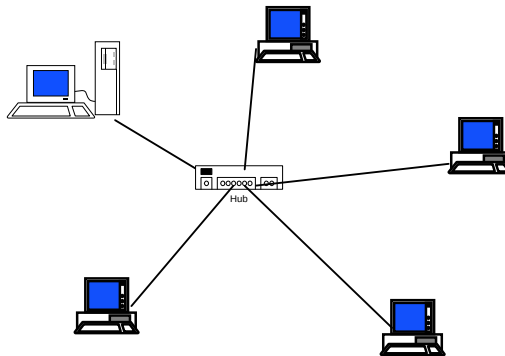
- Nối kiểu điểm - nhiều điểm (point - to - multipoint hay broadcast) : tất cả các nút phân chia nhau một đường truyền vật lý, gửi dữ liệu đến nhiều nút một lúc và kiểm tra gói tin theo địa chỉ

* Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.

Tô pô của mạng diện rộng thông thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router) và kênh viễn thông. Khi nói tới tô pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

- **Mạng hình sao:** Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích

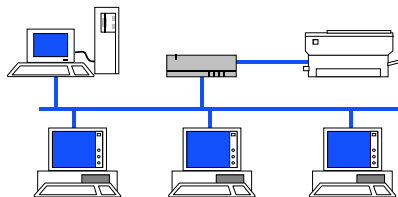
Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100m, với công nghệ hiện nay).



Hình 1.1: Kết nối hình sao

- **Mạng trục tuyến tính (Bus):**

Trong mạng trục tất cả các trạm phân chia một đường truyền chung (bus). Đường truyền chính được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver).

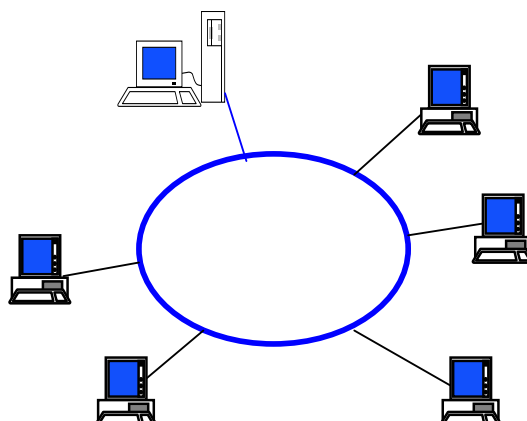


Hình 1.2. Kết nối kiểu bus

- **Mạng hình vòng**

Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng mạng cho trạm có nhu cầu.

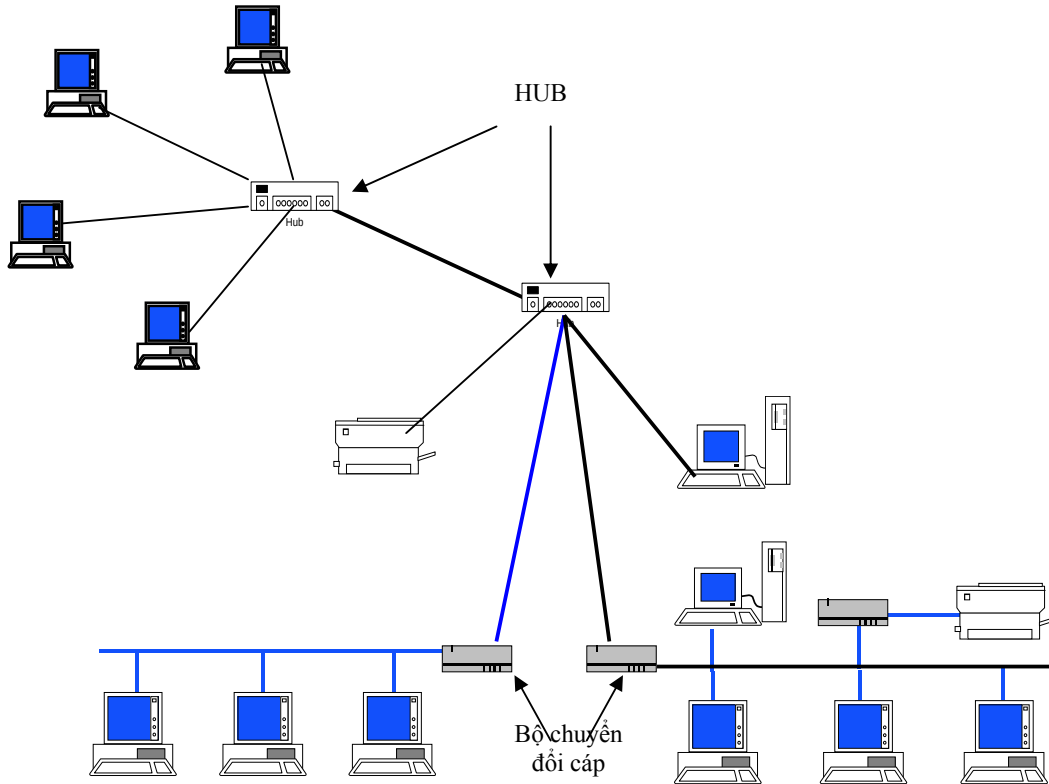
Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.



Hình 1.3. Kết nối kiểu vòng

d) Kết nối hỗn hợp

Là sự phối hợp các kiểu kết nối khác nhau,



Hình 1.4. Một kết nối hỗn hợp

2.3. Các phương pháp truy cập đường truyền vật lý

Trong mạng cục bộ, tất cả các trạm kết nối trực tiếp vào đường truyền chung. Nếu nhiều trạm cùng gửi tín hiệu lên đường truyền đồng thời thì tín hiệu sẽ chồng lên nhau và bị hỏng. Vì vậy cần phải có một phương pháp tổ chức chia sẻ đường truyền để việc truyền thông được đúng đắn.

Có hai phương pháp chia sẻ đường truyền chung thường được dùng trong các mạng cục bộ:

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đương nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tín dẫn đến tín hiệu bị trùm lên nhau thì phải truyền lại. Diễn hình của phương pháp này là giao thức truy cập CSMA/CD

- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột. Diễn hình phương pháp này là giao thức truy cập Tokenring

3. Chuẩn hoá mạng máy tính

3.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

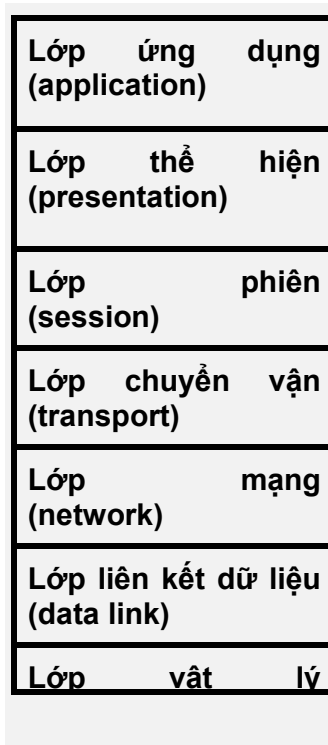
Khi thiết kế các giao thức mạng, các nhà thiết kế tự do lựa chọn kiến trúc cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Vấn đề không tương thích đó làm trở ngại cho sự tương tác giữa những giao thức mạng khác nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng.

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (International Organization for Standardization) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

3.2. Mô hình tham chiếu OSI 7 lớp

Mô hình OSI được biểu diễn theo hình dưới đây:

Mô hình OSI phân chia thành 7 lớp bao gồm các lớp ứng dụng, lớp thể hiện, lớp phiên, lớp vận chuyển, lớp mạng, lớp liên kết và lớp vật lý. Mô hình OSI cũng định nghĩa phần tiêu đề (header) của đơn vị dữ liệu và mối liên kết giữa các lớp, việc gắn thêm phần mào đầu (header) để chuyển dữ liệu từ các lớp trên xuống lớp dưới và mở gói là chức năng gỡ bỏ phần mào đầu để chuyển dữ liệu lên lớp trên.



Hình 1.5. Mô hình OSI 7 lớp

(physical link)

Chức năng cụ thể của từng lớp theo mô hình OSI có thể tham khảo chi tiết thêm trong giáo trình “Thiết kế và xây dựng mạng LAN và WAN”

3.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

Bên cạnh việc chuẩn hoá cho mạng nói chung dẫn đến kết quả cơ bản nhất là mô hình tham chiếu OSI như đã giới thiệu, người ta cũng chuẩn hóa các giao thức mạng cục bộ LAN.

- Các chuẩn IEEE 802.x và ISO 8802.x

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hoá mạng cục bộ với đề án IEEE 802 với kết quả là một loạt các chuẩn thuộc họ IEEE 802.x ra đời. Cuối những năm 80, tổ chức ISO đã tiếp nhận họ chuẩn này và ban hành thành chuẩn quốc tế dưới mã hiệu tương ứng là ISO 8802.x.

IEEE 802.: là chuẩn đặc tả kiến trúc mạng, kết nối giữa các mạng và việc quản trị mạng đối với mạng cục bộ.

IEEE 802.2: là chuẩn đặc tả tầng dịch vụ giao thức của mạng cục bộ.

IEEE 802.3: là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng của Digital, Intel và Xerox hợp tác xây dựng từ năm 1980. Các chuẩn qui định vật lý như 10BASE5, 10BASE2, 10BASE-F,

IEEE 802.5: là chuẩn đặc tả mạng cục bộ với topo mạng dạng vòng (ring) dùng thẻ bài để điều việc truy nhập đường truyền.

IEEE 802.11: là chuẩn đặc tả mạng cục bộ không dây (Wireless LAN) hiện đang được tiếp tục phát triển.

Ngoài ra trong họ chuẩn 802.x còn có các chuẩn IEEE 802.4, 802.6, 802.9, 802.10 và 802.12

Mục 2: Các thiết bị mạng thông dụng và các chuẩn kết nối vật lý

1. Các thiết bị mạng thông dụng

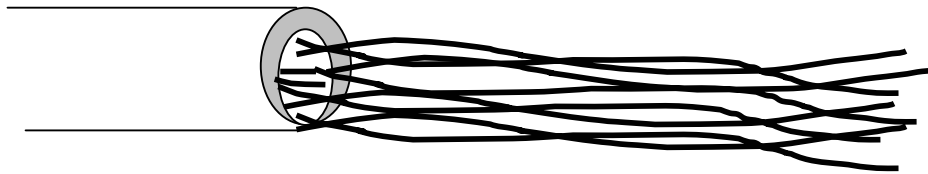
1.1. Các loại cáp truyền

1.1.1. Cáp đôi dây xoắn (Twisted pair cable)

Cáp đôi dây xoắn là cáp gồm hai dây đồng xoắn để tránh gây nhiễu cho các đôi dây khác, có thể kéo dài tới vài km mà không cần khuếch đại. Giải tần trên cáp dây xoắn đạt khoảng 300–4000Hz, tốc độ truyền đạt vài kbps đến vài Mbps. Cáp xoắn có hai loại:

- Loại có bọc kim loại để tăng cường chống nhiễu gọi là STP (Shield Twisted Pair). Loại này trong vỏ bọc kim có thể có nhiều đôi dây. Về lý thuyết thì tốc độ truyền có thể đạt 500 Mb/s nhưng thực tế thấp hơn rất nhiều (chỉ đạt 155 Mbps với cáp dài 100 m)

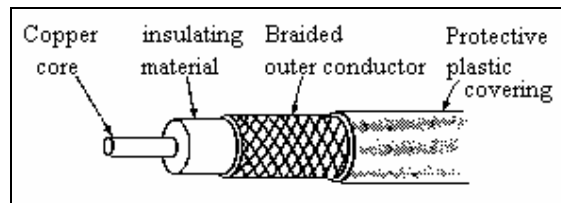
- Loại không bọc kim gọi là UTP (UnShield Twisted Pair), chất lượng kém hơn STP nhưng rất rẻ. Cáp UTP được chia làm 5 hạng tùy theo tốc độ truyền. Cáp loại 3 dùng cho điện thoại. Cáp loại 5 có thể truyền với tốc độ 100Mb/s rất hay dùng trong các mạng cục bộ vì vừa rẻ vừa tiện sử dụng. Cáp này có 4 đôi dây xoắn nằm trong cùng một vỏ bọc



Hình 1.6. Cáp UTP Cat. 5

1.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở

Là cáp mà hai dây của nó có lõi lồng nhau, lõi ngoài là lưới kim loại. Khả năng chống nhiễu rất tốt nên có thể sử dụng với chiều dài từ vài trăm mét đến vài km. Có hai loại được dùng nhiều là loại có trở kháng 50 ohm và loại có trở kháng 75 ohm.



Hình 1.7. Cáp đồng trục

Dải thông của cáp này còn phụ thuộc vào chiều dài của cáp. Với khoảng cách 1 km có thể đạt tốc độ truyền từ 1– 2 Gbps. Cáp đồng trục băng tần cơ sở thường dùng cho các mạng cục bộ. Có thể nối cáp bằng các đầu nối theo chuẩn BNC có hình chữ T. ở VN người ta hay gọi cáp này là cáp gậy do dịch từ tên trong tiếng Anh là ‘Thick Ethernet’.

Một loại cáp khác có tên là “Thick Ethernet” mà ta gọi là cáp béo. Loại này thường có màu vàng. Người ta không nối cáp bằng các đầu nối chữ T như cáp gậy mà nối qua các kẹp bấm vào dây. Cự 2m5 lại có đánh dấu để nối dây (nếu cần). Từ kẹp đó người ta gắn các tranceiver rồi nối vào máy tính.

1.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable)

Đây là loại cáp theo tiêu chuẩn truyền hình (thường dùng trong truyền hình cáp) có dải thông từ 4 – 300 KHz trên chiều dài 100 km. Thuật ngữ “băng rộng” vốn là thuật ngữ của ngành truyền hình còn trong ngành truyền số liệu điều này chỉ có nghĩa là cáp loại này cho phép truyền thông tin tương tự (analog) mà thôi. Các hệ thống dựa trên cáp đồng trục băng rộng có thể truyền song song nhiều kênh. Việc khuếch đại tín hiệu chống suy hao có thể làm theo kiểu khuếch đại tín hiệu tương tự (analog). Để truyền thông cho máy tính cần chuyển tín hiệu số thành tín hiệu tương tự.

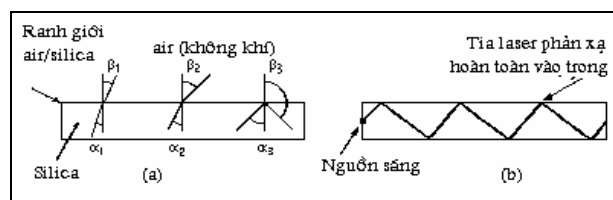
1.1.4. Cáp quang

Dùng để truyền các xung ánh sáng trong lòng một sợi thủy tinh phản xạ toàn phần. Môi trường cáp quang rất lý tưởng vì

- Xung ánh sáng có thể đi hàng trăm km mà không giảm cường độ sáng.
- Dải thông rất cao vì tần số ánh sáng dùng đối với cáp quang cỡ khoảng 10¹⁴ – 10¹⁶

- An toàn và bí mật, không bị nhiễu điện từ

Chỉ có hai nhược điểm là khó nối dây và giá thành cao.



Hình 1.8. Truyền tín hiệu bằng cáp quang

Cáp quang cũng có hai loại

- Loại đa mode (multimode fiber): khi góc tới thành dây dẫn lớn đến một mức nào đó thì có hiện tượng phản xạ toàn phần. Các cáp đa mode có đường kính khoảng 50 μ

- Loại đơn mode (singlemode fiber): khi đường kính dây dẫn bằng bước sóng thì cáp quang giống như một ống dẫn sóng, không có hiện tượng phản xạ nhưng chỉ cho một tia đi. Loại này có đường kính khoảng 8 μ m và phải dùng

diode laser. Cáp quang đa mode có thể cho phép truyền xa tới hàng trăm km mà không cần phải khuếch đại.

1.2. Các thiết bị ghép nối

1.2.1. Card giao tiếp mạng (Network Interface Card - NIC)

Đó là một card được cắm trực tiếp vào máy tính trên khe cắm mở rộng ISA hoặc PCI hoặc tích hợp vào bo mạch chủ PC. Trên đó có các mạch điện giúp cho việc tiếp nhận (receiver) hoặc/và phát (transmitter) tín hiệu lên mạng. Người ta thường dùng từ transceiver để chỉ thiết bị (mạch) có cả hai chức năng thu và phát.

1.2.2. Bộ chuyển tiếp (REPEATER)

Nhiệm vụ của các repeater là hồi phục tín hiệu để có thể truyền tiếp cho các trạm khác bao gồm cả công tác khuếch đại tín hiệu, điều chỉnh tín hiệu.

1.2.3. Các bộ tập trung (Concentrator hay HUB)

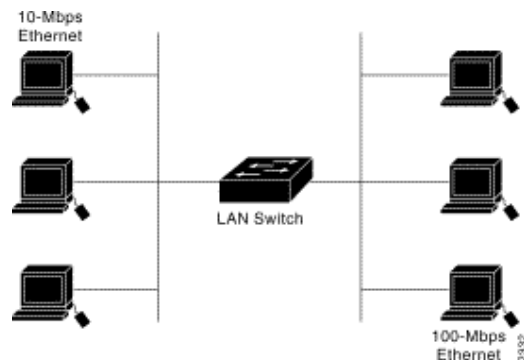
HUB là một loại thiết bị có nhiều đầu cắm các đầu cáp mạng. Người ta sử dụng HUB để nối mạng theo kiểu hình sao. Ưu điểm của kiểu nối này là tăng độ độc lập của các máy khi một máy bị sự cố dây dẫn.

Có loại HUB thụ động (passive HUB) là HUB chỉ đảm bảo chức năng kết nối hoàn toàn không xử lý lại tín hiệu. HUB chủ động (active HUB) là HUB có chức năng khuếch đại tín hiệu để chống suy hao.

HUB thông minh (intelligent HUB) là HUB chủ động nhưng có khả năng tạo ra các gói tin mạng tin tức về hoạt động của mình và gửi lên mạng để người quản trị mạng có thể thực hiện quản trị tự động

1.2.4. Switching Hub (hay còn gọi tắt là switch)

Là các bộ chuyển mạch thực sự. Khác với HUB thông thường, thay vì chuyển một tín hiệu đến từ một cổng cho tất cả các cổng, nó chỉ chuyển tín hiệu đến cổng có trạm đích. Do vậy Switch là một thiết bị quan trọng trong các mạng cục bộ lớn dùng để phân đoạn mạng. Nhờ có switch mà độ trễ trên mạng giảm hẳn. Ngày nay switch là các thiết bị mạng quan trọng cho phép tùy biến trên mạng chẳng hạn lập mạng ảo VLAN.



Hình 1.9. LAN Switch nối hai Segment mạng

1.2.5. Modem

Là tên viết tắt từ hai từ điều chế (MODulation) và giải điều chế (DEMODulation) là thiết bị cho phép điều chế để biến đổi tín hiệu số sang tín hiệu tương tự để có thể gửi theo đường thoại và khi nhận tín hiệu từ đường thoại có thể biến đổi ngược lại thành tín hiệu số.

1.2.6. Multiplexor - Demultiplexor

Bộ dồn kênh có chức năng tổ hợp nhiều tín hiệu để cùng gửi trên một đường truyền. Bộ tách kênh có chức năng ngược lại ở nơi nhận tín hiệu

1.2.7. Router

Router là một thiết bị dùng để ghép nối các mạng cục bộ với nhau thành mạng rộng. Router thực sự là một máy tính làm nhiệm vụ chọn đường cho các gói tin hướng ra ngoài. Router độc lập về phần cứng và có thể dùng trên các mạng chạy giao thức khác nhau

2. Một số kiểu nối mạng thông dụng và các chuẩn

2.1. Các thành phần thông thường trên một mạng cục bộ

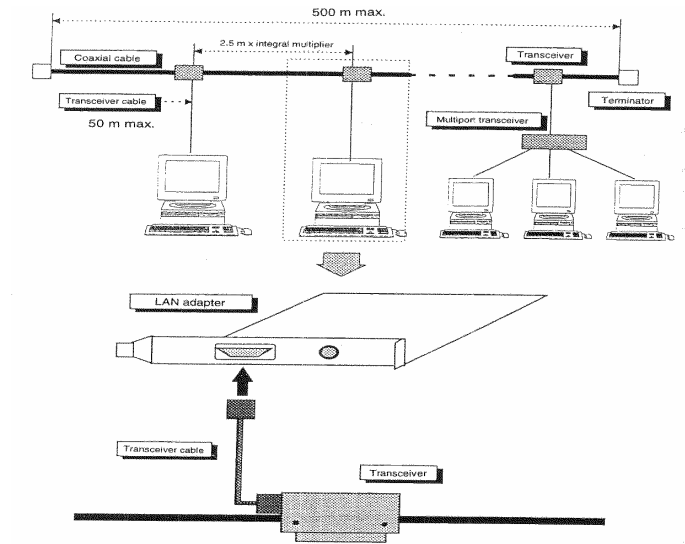
- Các máy chủ cung cấp dịch vụ (server)
- Các máy trạm cho người làm việc (workstation)
- Đường truyền (cáp nối)
- Card giao tiếp giữa máy tính và đường truyền (network interface card)
- Các thiết bị nối (connection device)

Hai yếu tố được quan tâm hàng đầu khi kết nối mạng cục bộ là tốc độ trong mạng và bán kính mạng. Tên các kiểu mạng dùng theo giao thức CSMA/CD cũng thể hiện điều này. Sau đây là một số kiểu kết nối đó với tốc độ 10 Mb/s khá thông dụng trong thời gian qua và một số thông số kỹ thuật:

Chuẩn	IEEE 802.3		
Kiểu	10BASE5	10BASE2	10BASE-T
Kiểu cáp	Cáp đồng trục	Cáp đồng trục	Cáp UTP
Tốc độ	10 Mb/s		
Độ dài cáp tối đa	500 m/segment	185 m/segment	100 m kể từ HUB
Số các thực thể truyền thông	100 host /segment	30 host / segment	Số cổng của HUB

2.2. Kiểu 10BASE5

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 500 m. Kiểu này dùng cáp đồng trục loại thick ethernet (cáp đồng trục béo) với transceiver. Có thể kết nối vào mạng khoảng 100 máy

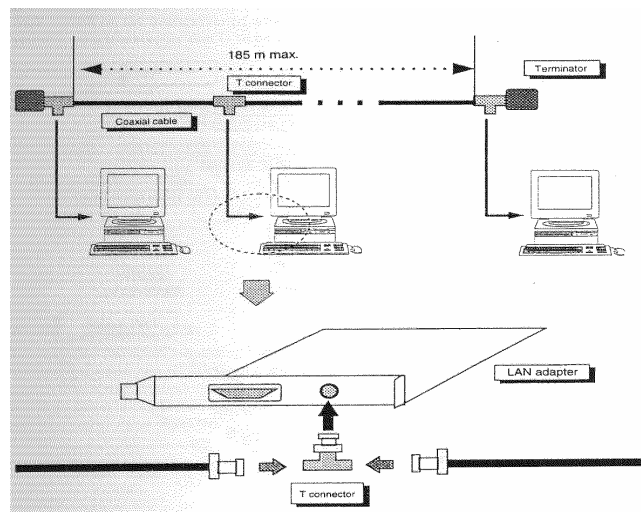


Hình 1.10. Kết nối theo chuẩn 10BASE5

Transceiver: Thiết bị nối giữa card mạng và đường truyền, đóng vai trò là bộ thu-phát.

2.3. Kiểu 10BASE2

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 200 m. Kiểu này dùng cáp đồng trục loại thin ethernet với đầu nối BNC. Có thể kết nối vào mạng khoảng 30 máy

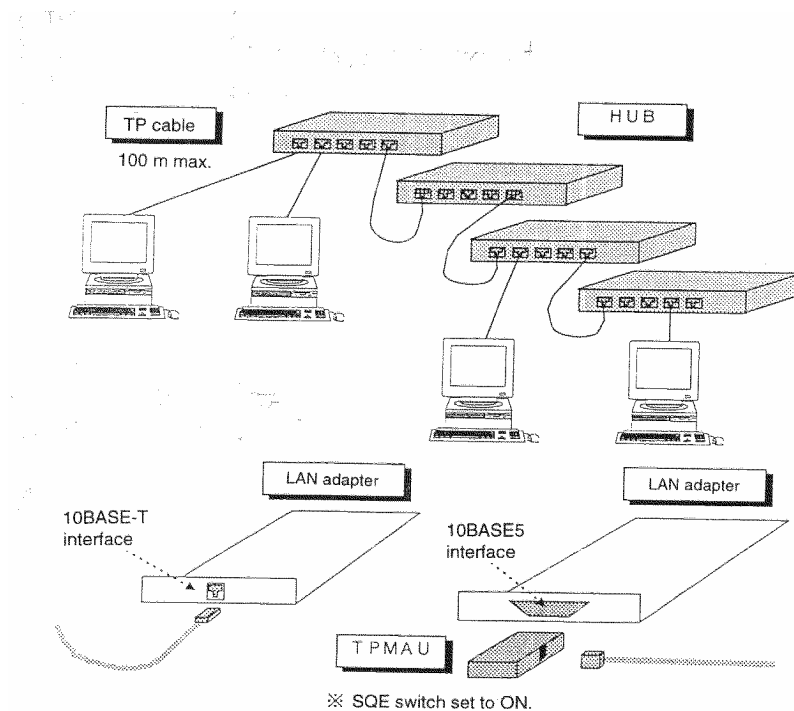


Hình 1.11: Nối theo chuẩn 10BASE2 với cáp đồng trục và đầu nối BNC

2.4. Kiểu 10BASE-T

Là kiểu nối dùng HUB có các ổ nối kiểu RJ45 cho các cáp UTP. Ta có thể mở rộng mạng bằng cách tăng số HUB, nhưng cũng không được tăng quá nhiều tầng vì hoạt động của mạng sẽ kém hiệu quả nếu độ trễ quá lớn.

Hiện nay mô hình phiên bản 100BASE-T, 1000BASE-T bắt đầu được sử dụng nhiều, tốc độ đạt tới 100 Mbps, 1000Mbps



Hình 1.12: Nối mạng theo kiểu 10BASE-T với cáp UTP và HUB

2.5. Kiểu 10BASE-F

Dùng cáp quang (Fiber cab), chủ yếu dùng nối các thiết bị xa nhau, tạo dựng đường trục xương sống (backbone) để nối các mạng LAN xa nhau (2-10 km). Hiện nay cũng đã có các phiên bản 100BASE-F và 1000BASE-F với tốc độ truyền dữ liệu cao hơn 10 và 100 lần

Chương 2

Giới thiệu giao thức TCP/IP

1. Giao thức IP

1.1. Họ giao thức TCP/IP

Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng **ARPAnet** (**A**dvanced **R**esearch **P**rojects **A**gency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở của nó. Hai giao thức được dùng chủ yếu ở đây là **TCP** (**T**ransmission **C**ontrol **P**rotocol) và **IP** (**I**nternet **P**rotocol). Chúng đã nhanh chóng được đón nhận và phát triển bởi nhiều nhà nghiên cứu và các hãng công nghiệp máy tính với mục đích xây dựng và phát triển một mạng truyền thông mở rộng khắp thế giới mà ngày nay chúng ta gọi là Internet.

Đến năm 1981, TCP/IP phiên bản 4 mới hoàn tất và được phổ biến rộng rãi cho toàn bộ những máy tính sử dụng hệ điều hành UNIX. Sau này Microsoft cũng đã đưa TCP/IP trở thành một trong những giao thức căn bản của hệ điều hành Windows 9x mà hiện nay đang sử dụng.

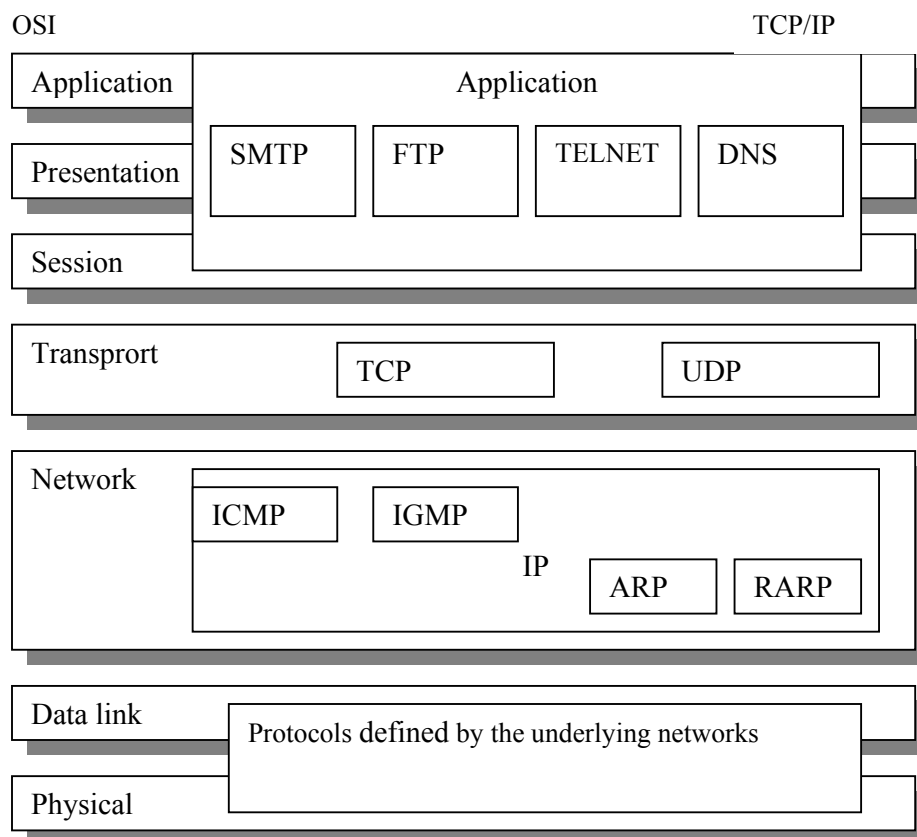
Đến năm 1994, một bản thảo của phiên bản IPv6 được hình thành với sự cộng tác của nhiều nhà khoa học thuộc các tổ chức Internet trên thế giới để cải tiến những hạn chế của IPv4.

Khác với mô hình ISO/OSI tầng liên mạng sử dụng giao thức kết nối mạng "không liên kết" (connectionless) IP, tạo thành hạt nhân hoạt động của Internet. Cùng với các thuật toán định tuyến RIP, OSPF, BGP, tầng liên mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring, X.25...

Giao thức trao đổi dữ liệu "có liên kết" (connection - oriented) TCP được sử dụng ở tầng vận chuyển để đảm bảo tính chính xác và tin cậy việc trao đổi dữ liệu dựa trên kiến trúc kết nối "không liên kết" ở tầng liên mạng IP.

Các giao thức hỗ trợ ứng dụng phổ biến như truy nhập từ xa (telnet), chuyển tệp (FTP), dịch vụ World Wide Web (HTTP), thư điện tử (SMTP), dịch vụ tên miền (DNS) ngày càng được cài đặt phổ biến như những bộ phận cấu thành của các hệ điều hành thông dụng như UNIX (và các hệ điều hành chuyên dụng cùng họ của các nhà cung cấp thiết bị tính toán như AIX của IBM, SINIX của Siemens, Digital UNIX của DEC), Windows9x/NT, Novell Netware,...

1.2. Chức năng chính của giao thức liên mạng IP (v4)



Hình 2.1 Mô hình OSI và mô hình kiến trúc của TCP/IP

Trong cấu trúc bốn lớp của TCP/IP, khi dữ liệu truyền từ lớp ứng dụng cho đến lớp vật lý, mỗi lớp đều cộng thêm vào phần điều khiển của mình để đảm bảo cho việc truyền dữ liệu được chính xác. Mỗi thông tin điều khiển này được gọi là một *header* và được đặt ở trước phần dữ liệu được truyền. Mỗi lớp xem tất cả các thông tin mà nó nhận được từ lớp trên là dữ liệu, và đặt phần thông tin điều khiển *header* của nó vào trước phần thông tin này. Việc cộng thêm vào các *header* ở mỗi lớp trong quá trình truyền tin được gọi là *encapsulation*. Quá trình nhận dữ liệu diễn ra theo chiều ngược lại: mỗi lớp sẽ tách ra phần *header* trước khi truyền dữ liệu lên lớp trên.

Mỗi lớp có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở lớp trên hay lớp dưới của nó. Sau đây là giải thích một số khái niệm thường gặp.

Stream là dòng số liệu được truyền trên cơ sở đơn vị số liệu là Byte.

Số liệu được trao đổi giữa các ứng dụng dùng TCP được gọi là *stream*, trong khi dùng UDP, chúng được gọi là *message*.

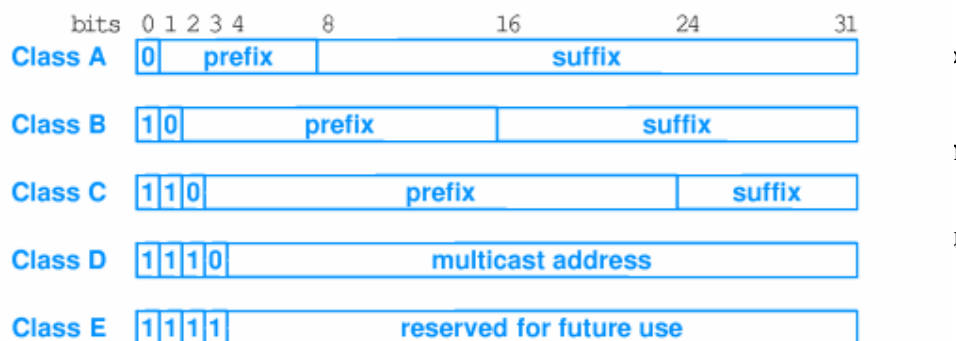
Mỗi gói số liệu TCP được gọi là *segment* còn UDP định nghĩa cấu trúc dữ liệu của nó là *packet*.

Lớp Internet xem tất cả các dữ liệu như là các khối và gọi là *datagram*. Bộ giao thức TCP/IP có thể dùng nhiều kiểu khác nhau của lớp mạng dưới cùng, mỗi loại có thể có một thuật ngữ khác nhau để truyền dữ liệu.

Phần lớn các mạng kết cấu phần dữ liệu truyền đi dưới dạng các *packets* hay là các *frames*.

Application	Stream
Transport	Segment/datagram
Internet	Datagram
Network Access	Frame

Hình 2.2: Cấu trúc dữ liệu tại các lớp của TCP/IP



Hình 2.3: Cách đánh địa chỉ TCP/IP

- Thực hiện việc phân mảnh và hợp nhất (fragmentation -reassembly) các gói dữ liệu và nhúng / tách chúng trong các gói dữ liệu ở tầng liên kết.

1.3. Địa chỉ IP

Mỗi địa chỉ IP có độ dài 32 bits (đối với IP4) được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu thị dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm để tách giữa các vùng. Địa chỉ IP là để định danh duy nhất cho một host bất kỳ trên liên mạng.

Khuôn dạng địa chỉ IP: mỗi host trên mạng TCP/IP được định danh duy nhất bởi một địa chỉ có khuôn dạng

<Network Number, Host number>

Do tổ chức và độ lớn của các mạng con của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp ký hiệu A,B,C, D, E. Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0-lớp A; 10 lớp B; 110 lớp C; 1110 lớp D; 11110 lớp E).

Subneting

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với 3 lớp A, B, C như sau:

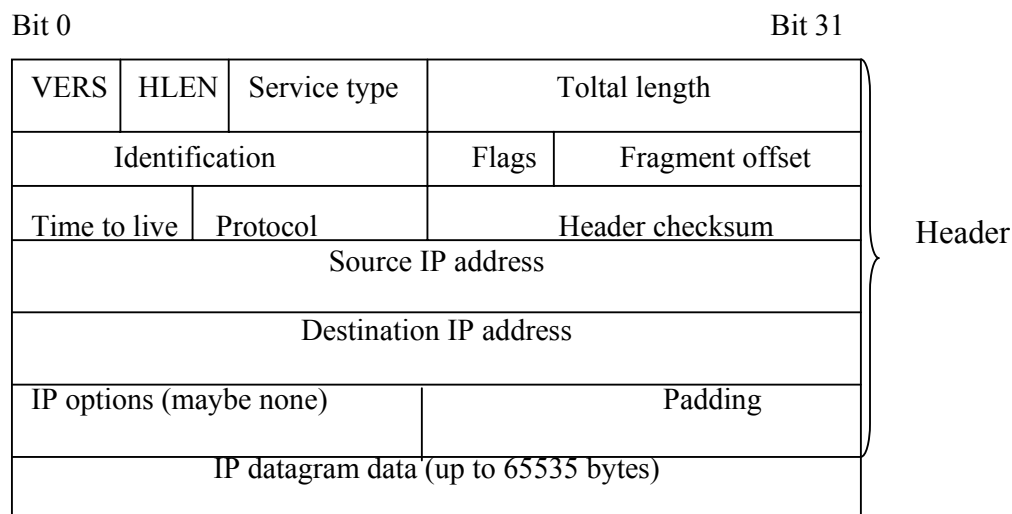
Netid	Subnetid	hostid	Lớp A
0	7 8	15 16 23 24 31	
Netid	Subnetid	hostid	Lớp B
0	7 8	15 16 23 24 26 27 31	
Netid	Subnetid	hostid	Lớp C

Hình 2.4: Bổ sung vùng subnetid

Tham khảo chi tiết thêm trong giáo trình “Thiết kế và xây dựng mạng LAN và WAN”

1.4. Cấu trúc gói dữ liệu IP

IP là giao thức cung cấp dịch vụ truyền thông theo kiểu “không liên kết” (connectionless). Các gói dữ liệu IP được định nghĩa là các datagram. Mỗi datagram có phần tiêu đề (header) chứa các thông tin cần thiết để chuyển dữ liệu (ví dụ địa chỉ IP của trạm đích). Nếu địa chỉ IP đích là địa chỉ của một trạm nằm trên cùng một mạng IP với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích; nếu địa chỉ IP đích không nằm trên cùng một mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển, IP gateway để chuyển tiếp. IP gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau.



Hình 2.5: Cấu trúc gói dữ liệu TCPIP

1.5. Phân mảnh và hợp nhất các gói IP

Một gói dữ liệu IP có độ dài tối đa 65536 byte, trong khi hầu hết các tầng liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất MTU của một khung dữ liệu Ethernet là 1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi thu đối với các gói dữ liệu IP.

Original IP packet	1. fragment	2.fragment																																																																																																																																																
<table><tr><td colspan="4">04 05 00</td><td colspan="4">2000</td></tr><tr><td colspan="4">1 1 1 1</td><td>0</td><td colspan="3">0 0 0</td></tr><tr><td colspan="2">05</td><td colspan="2">06</td><td colspan="4">checksum</td></tr><tr><td colspan="8">128.82.24.12</td></tr><tr><td colspan="8">192.12.2.5</td></tr><tr><td colspan="8">Data 1980 byte</td></tr></table>	04 05 00				2000				1 1 1 1				0	0 0 0			05		06		checksum				128.82.24.12								192.12.2.5								Data 1980 byte								<table><tr><td colspan="4">04 05 00</td><td colspan="4">1500</td></tr><tr><td colspan="4">1 1 1 1</td><td>1</td><td colspan="3">0 0 0</td></tr><tr><td colspan="2">05</td><td colspan="2">06</td><td colspan="4">checksum</td></tr><tr><td colspan="8">128.82.24.12</td></tr><tr><td colspan="8">192.12.2.5</td></tr><tr><td colspan="8">Data 1480 byte</td></tr></table>	04 05 00				1500				1 1 1 1				1	0 0 0			05		06		checksum				128.82.24.12								192.12.2.5								Data 1480 byte								<table><tr><td colspan="4">04 05 00</td><td colspan="4">520</td></tr><tr><td colspan="4">1 1 1 1</td><td>0</td><td colspan="3">0 0 0</td></tr><tr><td colspan="2">05</td><td colspan="2">06</td><td colspan="4">checksum</td></tr><tr><td colspan="8">128.82.24.12</td></tr><tr><td colspan="8">192.12.2.5</td></tr><tr><td colspan="8">Data 500 byte</td></tr></table>	04 05 00				520				1 1 1 1				0	0 0 0			05		06		checksum				128.82.24.12								192.12.2.5								Data 500 byte							
04 05 00				2000																																																																																																																																														
1 1 1 1				0	0 0 0																																																																																																																																													
05		06		checksum																																																																																																																																														
128.82.24.12																																																																																																																																																		
192.12.2.5																																																																																																																																																		
Data 1980 byte																																																																																																																																																		
04 05 00				1500																																																																																																																																														
1 1 1 1				1	0 0 0																																																																																																																																													
05		06		checksum																																																																																																																																														
128.82.24.12																																																																																																																																																		
192.12.2.5																																																																																																																																																		
Data 1480 byte																																																																																																																																																		
04 05 00				520																																																																																																																																														
1 1 1 1				0	0 0 0																																																																																																																																													
05		06		checksum																																																																																																																																														
128.82.24.12																																																																																																																																																		
192.12.2.5																																																																																																																																																		
Data 500 byte																																																																																																																																																		

Hình 2.6: Nguyên tắc phân mảnh gói dữ liệu

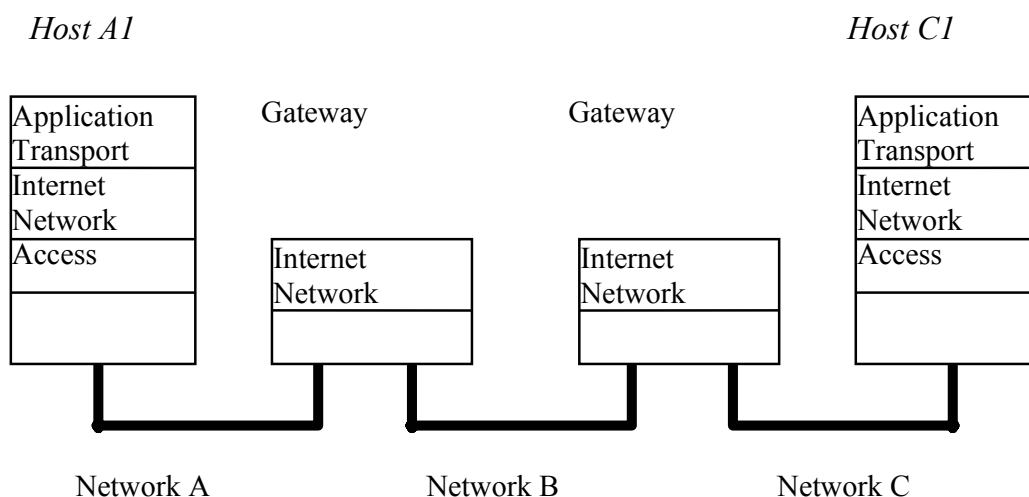
P dùng cờ MF (3 bit thấp của trường Flags trong phần đầu của gói IP) và trường Fragment offset của gói IP (đã bị phân đoạn) để định danh gói IP đó là một phân đoạn và vị trí của phân đoạn này trong gói IP gốc. Các gói cùng trong chuỗi phân mảnh đều có trường này giống nhau. Cờ MF bằng 1 nếu là gói đầu của chuỗi phân mảnh và 0 nếu là gói cuối của gói đã được phân mảnh.

1.6. Định tuyến IP

Có hai loại định tuyến:

- Định tuyến trực tiếp: Định tuyến trực tiếp là việc xác định đường nối giữa hai trạm làm việc trong cùng một mạng vật lý.
- Định tuyến không trực tiếp. Định tuyến không trực tiếp là việc xác định đường nối giữa hai trạm làm việc không nằm trong cùng một mạng vật lý và vì vậy, việc truyền tin giữa chúng phải được thực hiện thông qua các trạm trung gian là các gateway.

Để kiểm tra xem trạm đích có nằm trên cùng mạng vật lý với trạm nguồn hay không, người gửi phải tách lấy phần địa chỉ mạng trong phần địa chỉ IP. Nếu hai địa chỉ này có địa chỉ mạng giống nhau thì datagram sẽ được truyền đi trực tiếp; ngược lại phải xác định một gateway, thông qua gateway này chuyển tiếp các datagram.



Hình 2.7: Định tuyến giữa hai hệ thống

2. Một số giao thức điều khiển

2.1. Giao thức ICMP

ICMP ((Internet Control Message Protocol) là một giao thức điều khiển của mức IP, được dùng để trao đổi các thông tin điều khiển dòng số liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP. Ví dụ:

- Điều khiển lưu lượng dữ liệu (Flow control).
- Thông báo lỗi : ví dụ "Destination Unreachable".
- Định hướng lại các tuyến đường: gói tin redirect
- Kiểm tra các trạm ở xa: gói tin echo

Ví dụ khuôn dạng của thông điệp ICMP redirect như sau:

0	7 8	15 16	31
type (5)		Code(0-3)	Checksum
Địa chỉ IP của Router mặc định			
IP header (gồm option) và 8 bytes đầu của gói dữ liệu IP nguồn			

2.2. Giao thức ARP và giao thức RARP

Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao thức RARP (Reverse Address

Resolution Protocol) được dùng để chuyển đổi địa chỉ vật lý sang địa chỉ IP. Các giao thức ARP và RARP không phải là bộ phận của IP mà IP sẽ dùng đến chúng khi cần.

3. Giao thức lớp chuyển tải (Transport Layer)

3.1. Giao thức TCP

TCP (Transmission Control Protocol) là một giao thức “có liên kết” (connection - oriented), nghĩa là cần thiết lập liên kết (logic), giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các máy trạm trong hệ thống các mạng. Nó cung cấp thêm các chức năng nhằm kiểm tra tính chính xác của dữ liệu khi đến và bao gồm cả việc gửi lại dữ liệu khi có lỗi xảy ra. TCP cung cấp các chức năng chính sau:

1. Thiết lập, duy trì, kết thúc liên kết giữa hai quá trình.
2. Phân phát gói tin một cách tin cậy.
3. Đánh số thứ tự (sequencing) các gói dữ liệu nhằm truyền dữ liệu một cách tin cậy.
4. Cho phép điều khiển lỗi.
5. Cung cấp khả năng đa kết nối với các quá trình khác nhau giữa trạm nguồn và trạm đích nhất định thông qua việc sử dụng các cổng.
6. Truyền dữ liệu sử dụng cơ chế song công (full-duplex).

3.1.1 Cấu trúc gói dữ liệu TCP

0				31							
Source port				Destination port							
Sequence number											
Acknowledgment number											
Data	Resersed	U	A	P	R	S	F	Window			
Offset		R	C	S	S	Y	I				
		G	K	H	T	N	N				
Checksum				Urgent pointer							
Options				Padding							
TCP data											

Có thể tham khảo nội dung chi tiết các trường trong giáo trình “Thiết kế và xây dựng mạng LAN và WAN”

Một tiến trình ứng dụng trong một host truy nhập vào các dịch vụ của TCP cung cấp thông qua một cổng (port) như sau:

Một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng. Cũng giống như ở các giao thức khác, các thực thể ở tầng trên sử dụng TCP thông qua các hàm dịch vụ nguyên thủy (service primitives), hay còn gọi là các lời gọi hàm (function call).

3.1.2 Thiết lập và kết thúc kết nối TCP

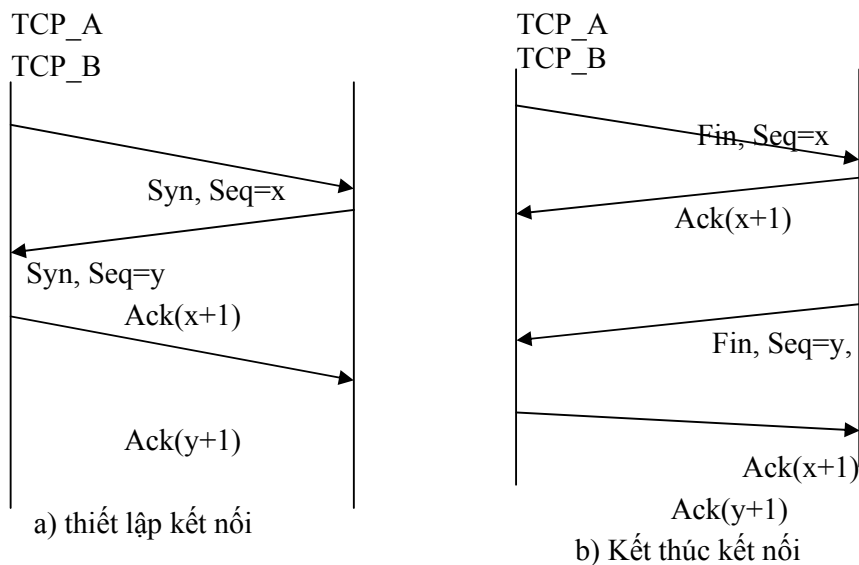
Thiết lập kết nối

Thiết lập kết nối TCP được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree - way Handsake) hình sau. Yêu cầu kết nối luôn được tiến trình trạm khởi tạo, bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi tạo số tuần tự ISN của client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi kết nối được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 2^{32}). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn kết nối (bước 1).

Mỗi thực thể kết nối TCP đều có một giá trị ISN mới số này được tăng theo thời gian. Vì một kết nối TCP có cùng số hiệu cổng và cùng địa chỉ IP được dùng lại nhiều lần, do đó việc thay đổi giá trị INS ngăn không cho các kết nối dùng lại các dữ liệu đã cũ (stale) vẫn còn được truyền từ một kết nối cũ và có cùng một địa chỉ kết nối.

Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận kết nối. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự thu để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm (bước 2).

Tiến trình trạm trả lời lại gói SYN của thực thể dịch vụ bằng một thông báo trả lời ACK cuối cùng. Bằng cách này, các thực thể TCP trao đổi một cách tin cậy các giá trị ISN của nhau và có thể bắt đầu trao đổi dữ liệu. Không có thông điệp nào trong ba bước trên chứa bất kỳ dữ liệu gì; tất cả thông tin trao đổi đều nằm trong phần tiêu đề của thông điệp TCP (bước 3).



Hình 2.8: Quá trình kết nối theo 3 bước

Kết thúc kết nối

Khi có nhu cầu kết thúc kết nối, thực thể TCP, ví dụ cụ thể A gửi yêu cầu kết thúc kết nối với $FIN=1$. Vì kết nối TCP là song công (full-duplex) nên mặc dù nhận được yêu cầu kết thúc kết nối của A (A thông báo hết số liệu gửi) thực thể B vẫn có thể tiếp tục truyền số liệu cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc kết nối với $FIN=1$ của mình. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của chính mình, kết nối TCP thực sự kết thúc.

PHẦN II : QUẢN TRỊ MẠNG

Quản trị mạng lưới (network administration) được định nghĩa là các công việc quản lý mạng lưới bao gồm cung cấp các dịch vụ hỗ trợ, đảm bảo mạng lưới hoạt động hiệu quả, đảm bảo chất lượng mạng lưới cung cấp đúng như chỉ tiêu định ra.

Quản trị hệ thống (system administration) được định nghĩa là các công việc cung cấp các dịch vụ hỗ trợ, đảm bảo sự tin cậy, nâng cao hiệu quả hoạt động của hệ thống, và đảm bảo chất lượng dịch vụ cung cấp trên hệ thống đúng như chỉ tiêu định ra.

Một định nghĩa khái quát về công tác quản trị mạng là rất khó vì tính bao hàm rộng của nó. Quản trị mạng theo nghĩa mạng máy tính có thể được hiểu khái quát là tập bao gồm của các công tác quản trị mạng lưới và quản trị hệ thống.

Có thể khái quát công tác quản trị mạng bao gồm các công việc sau:

Quản trị cấu hình, tài nguyên mạng : Bao gồm các công tác quản lý kiểm soát cấu hình, quản lý các tài nguyên cấp phát cho các đối tượng sử dụng khác nhau. Có thể tham khảo các công việc quản trị cụ thể trong các tài liệu, giáo trình về quản trị hệ thống windows, linux, novell netware ...

Quản trị người dùng, dịch vụ mạng: Bao gồm các công tác quản lý người sử dụng trên hệ thống, trên mạng lưới và đảm bảo dịch vụ cung cấp có độ tin cậy cao, chất lượng đảm bảo theo đúng các chỉ tiêu đề ra. Có thể tham khảo các tài liệu, giáo trình quản trị hệ thống windows, novell netware, linux, unix, quản trị dịch vụ cơ bản thư tín điện tử, DNS...

Quản trị hiệu năng, hoạt động mạng : Bao gồm các công tác quản lý, giám sát hoạt động mạng lưới, đảm bảo các thiết bị, hệ thống, dịch vụ trên mạng hoạt động ổn định, hiệu quả. Các công tác quản lý, giám sát hoạt động của mạng lưới cho phép người quản trị tổng hợp, dự báo sự phát triển mạng lưới, dịch vụ, các điểm yếu, điểm mạnh của toàn mạng, các hệ thống và dịch vụ đồng thời giúp khai thác toàn bộ hệ thống mạng với hiệu suất cao nhất. Có thể tham khảo các tài liệu, giáo trình về các hệ thống quản trị mạng NMS, HP Openview, Sunet Manager, hay các giáo trình nâng cao hiệu năng hoạt động của hệ thống (performance tuning).

Quản trị an ninh, an toàn mạng: Bao gồm các công tác quản lý, giám sát mạng lưới, các hệ thống để đảm bảo phòng tránh các truy nhập trái phép, có tính phá hoại các hệ thống, dịch vụ, hoặc mục tiêu đánh cắp thông tin quan trọng của các tổ chức, công ty hay thay đổi nội dung cung cấp lên mạng với dụng ý xấu. Việc phòng chống, ngăn chặn sự lây lan của các loại virus máy tính, các phương thức tấn công ví dụ như DoS làm tê liệt hoạt động mạng hay

dịch vụ cũng là một phần cực kỳ quan trọng của công tác quản trị an ninh, an toàn mạng. Đặc biệt, hiện nay khi nhu cầu kết nối ra mạng Internet trở nên thiết yếu thì các công tác đảm bảo an ninh, an toàn được đặt lên hàng đầu, đặc biệt là với các cơ quan cần bảo mật nội dung thông tin cao độ (nhà băng, các cơ quan lưu trữ, các các báo điện tử, tập đoàn kinh tế mũi nhọn...).

Trong phần 2 của giáo trình này sẽ tập trung nghiên cứu sâu về một số kiến thức, kỹ năng cơ bản và thông dụng nhất về quản trị mạng. Tuy nhiên, các nội dung trình bày tại phần 2 sẽ không bao hàm hết được các nội dung đã khái quát ở trên do sự phức tạp phong phú của bản thân mỗi nội dung cũng như giới hạn về thời gian biên soạn. Với mục tiêu cung cấp các kỹ năng phổ biến nhất giúp cho các học viên tiếp cận nhanh chóng vào công tác quản trị mạng để đảm đương được nhiệm vụ cơ quan, công ty giao cho. Phần 2 của giáo trình sẽ bao gồm :

- Tổng quan về bộ định tuyến trên mạng
- Hệ thống tên miền DNS
- Dịch vụ truy cập từ xa và dịch vụ proxy
- Firewall và bảo mật hệ thống

Học viên cũng có thể tham khảo bổ sung thêm kiến thức về quản trị mạng với các giáo trình về mạng cục bộ, giáo trình về thư tín điện tử, giáo trình về các hệ điều hành Windows, Linux, Unix là các nội dung biên soạn trong bộ các giáo trình phục vụ đào tạo cho đề án 112.

Chương 3

Tổng quan về bộ định tuyến

Chương ba cung cấp các kiến thức cơ bản về bộ định tuyến trên mạng và các bộ chuyển mạch lớp 3. Các thiết bị này là một phần thiết yếu của mạng máy tính hiện đại và là các thiết bị hạ tầng cốt lõi. Các minh họa tường tận về cấu trúc của các sản phẩm hãng Cisco sẽ giúp học viên nắm vững các lý thuyết hệ thống đặc biệt là lý thuyết định tuyến. Phần nội dung cũng bổ sung các kỹ năng cấu hình hoạt động của thiết bị trên các giao thức mạng WAN khác nhau như Frame Relay, X.25...

Chương ba đòi hỏi các học viên cần có các kiến thức sơ khởi về các giao thức trên mạng diện rộng như Frame Relay, X.25..., các kiến thức về địa chỉ lớp 2, lớp 3.

1. Lý thuyết về bộ định tuyến

1.1. Tổng quan về bộ định tuyến

Bộ định tuyến là thiết bị được sử dụng trên mạng để thực thi các hoạt động xử lý truyền tải thông tin trên mạng. Có thể xem bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng của nó và do đó nó cũng bao gồm các CPU, trái tim của mọi hoạt động, bộ nhớ ROM, RAM, các giao tiếp, các bus dữ liệu, hệ điều hành v.v...

Chức năng của bộ định tuyến là định hướng cho các gói tin được truyền tải qua bộ định tuyến. Trên cơ sở các thuật toán định tuyến, thông tin cấu hình và chuyển giao, các bộ định tuyến sẽ quyết định hướng đi tốt nhất cho các gói tin được truyền tải qua nó. Bộ định tuyến còn có vai trò để xử lý các nhu cầu truyền tải và chuyển đổi giao thức khác.

Vai trò của bộ định tuyến trên mạng là đảm bảo các kết nối liên thông giữa các mạng với nhau, tính toán và trao đổi các thông tin liên mạng làm căn cứ cho các bộ định tuyến ra các quyết định truyền tải thông tin phù hợp với cấu hình thực tế của mạng. Bộ định tuyến làm việc với nhiều công nghệ đầu nối mạng diện rộng khác nhau như FRAME RELAY, X.25, ATM, SONET, ISDN, xDSL... đảm bảo các nhu cầu kết nối mạng theo nhiều các công nghệ và độ chuẩn mực khác nhau mà nếu thiếu vai trò của bộ định tuyến thì không thể thực hiện được.

1.2. Các chức năng chính của bộ định tuyến, tham chiếu mô hình OSI

Mô hình OSI đã được học ở chương 1 gồm 7 lớp trong đó bao gồm:

- 3 lớp thuộc về các lớp ứng dụng
- o lớp ứng dụng

- o lớp trình bày
- o lớp phiên
- 4 lớp thuộc về các lớp truyền thông
- o lớp vận chuyển
- o lớp mạng
- o lớp liên kết dữ liệu
- o lớp vật lý

Đối với các lớp truyền thông:

- Lớp vận chuyển: phân chia / tái thiết dữ liệu thành các dòng chảy dữ liệu. Các chức năng chính bao gồm điều khiển dòng dữ liệu, đa truy nhập, quản lý các mạch ảo, phát hiện và sửa lỗi. TCP, UDP là hai giao thức thuộc họ giao thức Internet (TCP/IP) thuộc về lớp vận chuyển này.

- Lớp mạng: cung cấp hoạt động định tuyến và các chức năng liên quan khác cho phép kết hợp các môi trường liên kết dữ liệu khác nhau lại với nhau cùng tạo nên mạng thống nhất. Các giao thức định tuyến hoạt động trong lớp mạng này.

- Lớp liên kết dữ liệu: cung cấp khả năng truyền tải dữ liệu từ qua môi trường truyền dẫn vật lý. Mỗi đặc tả khác nhau của lớp liên kết dữ liệu sẽ có các định nghĩa khác nhau về giao thức và các chuẩn mực kết nối đảm bảo truyền tải dữ liệu.

- Lớp vật lý: định nghĩa các thuộc tính điện, các chức năng, thường trình dùng để kết nối các thiết bị mạng ở mức vật lý. Một số các thuộc tính được định nghĩa như mức điện áp, đồng bộ, tốc độ truyền tải vật lý, khoảng cách truyền tải cho phép...

Trong môi trường truyền thông, các thiết bị truyền thông giao tiếp với nhau thông qua các họ giao thức truyền thông khác nhau được xây dựng dựa trên các mô hình chuẩn OSI nhằm đảm bảo tính tương thích và mở rộng. Các giao thức truyền thông thường được chia vào một trong bốn nhóm: các giao thức mạng cục bộ, các giao thức mạng diện rộng, giao thức mạng và các giao thức định tuyến. *Giao thức mạng cục bộ* hoạt động trên lớp vật lý và lớp liên kết dữ liệu. *Giao thức mạng diện rộng* hoạt động trên 3 lớp dưới cùng trong mô hình OSI. *Giao thức định tuyến* là giao thức lớp mạng và đảm bảo cho các hoạt động định tuyến và truyền tải dữ liệu. *Giao thức mạng* là các họ các giao thức cho phép giao tiếp với lớp ứng dụng.

Vai trò của bộ định tuyến trong môi trường truyền thông là đảm bảo cho các kết nối giữa các mạng khác nhau với nhiều giao thức mạng, sử dụng các công nghệ truyền dẫn khác nhau.

Chức năng chính của bộ định tuyến là:

- Định tuyến (routing)
- Chuyển mạch các gói tin (packet switching)

Định tuyến là chức năng đảm bảo gói tin được chuyển chính xác tới địa chỉ cần đến. **Chuyển mạch các gói tin** là chức năng chuyển mạch số liệu, truyền tải các gói tin theo hướng đã định trên cơ sở các định tuyến được đặt ra. Như vậy, trên mỗi bộ định tuyến, ta phải xây dựng một bảng định tuyến, trên đó chỉ rõ địa chỉ cần đến và đường đi cho nó. Bộ định tuyến dựa vào địa chỉ của gói tin kết hợp với bảng định tuyến để chuyển gói tin đi đúng đến đích. Các gói tin không có đúng địa chỉ đích trên bảng định tuyến sẽ bị hủy.

Chức năng đầu tiên của bộ định tuyến là chức năng định tuyến như tên gọi của nó cũng là chức năng chính của bộ định tuyến làm việc với các *giao thức định tuyến*. Bộ định tuyến được xếp vào các thiết bị mạng làm việc ở lớp 3, lớp mạng.

Bảng 3-1: Tương đương chức năng thiết bị trong mô hình OSI

Lớp 3	Lớp mạng	
Lớp 2	Lớp liên kết dữ liệu	  
Lớp 1	Lớp vật lý	 

Chức năng khác của bộ định tuyến là cho phép sử dụng các phương thức truyền thông khác nhau để đầu nối diện rộng. Chức năng kết nối diện rộng WAN của bộ định tuyến là không thể thiếu để đảm bảo vai trò kết nối truyền thông giữa các mạng với nhau. Chức năng kết nối mạng cục bộ, bất kỳ bộ định tuyến nào cũng cần có chức năng này để đảm bảo kết nối đến vùng dịch vụ của mạng. Bộ định tuyến còn có các chức năng đảm bảo hoạt động cho các giao thức mạng mà nó quản lý.

1.3. Cấu hình cơ bản và chức năng của các bộ phận của bộ định tuyến

Như đã nói ở phần trước, bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng. Nó được thiết kế bao gồm các phần tử không thể thiếu như CPU, bộ nhớ ROM, RAM, các bus dữ liệu, hệ điều hành. Các phần tử khác tùy theo nhu cầu sử dụng có thể có hoặc không bao gồm các giao tiếp, các module và các tính năng đặc biệt của hệ điều hành.

CPU: điều khiển mọi hoạt động của bộ định tuyến trên cơ sở các hệ thống chương trình thực thi của hệ điều hành.

ROM: chứa các chương trình tự động kiểm tra và có thể có thành phần cơ bản nhất sao cho bộ định tuyến có thể thực thi được một số hoạt động tối thiểu ngay cả khi không có hệ điều hành hay hệ điều hành bị hỏng.

RAM: giữ các bảng định tuyến, các vùng đệm, tập tin cấu hình khi chạy, các thông số đảm bảo hoạt động của bộ định tuyến khác.

Flash: là thiết bị nhớ / lưu trữ có khả năng xóa và ghi được, không mất dữ liệu khi cắt nguồn. Hệ điều hành của bộ định tuyến được chứa ở đây. Tùy thuộc các bộ định tuyến khác nhau, hệ điều hành sẽ được chạy trực tiếp từ

Flash hay được gắn ra RAM trước khi chạy. Tập tin cấu hình cũng có thể được lưu trữ trong Flash.

Hệ điều hành: đảm đương hoạt động của bộ định tuyến. Hệ điều hành của các bộ định tuyến khác nhau có các chức năng khác nhau và thường được thiết kế khác nhau. Mỗi bộ định tuyến có thể chạy rất nhiều hệ điều hành khác nhau tùy thuộc vào nhu cầu sử dụng cụ thể, các chức năng cần thiết phải có của bộ định tuyến và các thành phần phần cứng có trong bộ định tuyến. Các thành phần phần cứng mới yêu cầu có sự nâng cấp về hệ điều hành. Các tính năng đặc biệt được cung cấp trong các bản nâng cấp riêng của hệ điều hành.

Các giao tiếp: bộ định tuyến có nhiều các giao tiếp trong đó chủ yếu bao gồm:

- Giao tiếp WAN: đảm bảo cho các kết nối diện rộng thông qua các phương thức truyền thông khác nhau như leased-line, Frame Relay, X.25, ISDN, ATM, xDSL ... Các giao tiếp WAN cho phép bộ định tuyến kết nối theo nhiều các giao diện và tốc độ khác nhau: V.35, X.21, G.703, E1, E3, cáp quang v.v...
- Giao tiếp LAN: đảm bảo cho các kết nối mạng cục bộ, kết nối đến các vùng cung cấp dịch vụ trên mạng. Các giao tiếp LAN thông dụng: Ethernet, FastEthernet, GigaEthernet, cáp quang.

2. Giới thiệu về bộ định tuyến Cisco

2.1. Giới thiệu bộ định tuyến Cisco

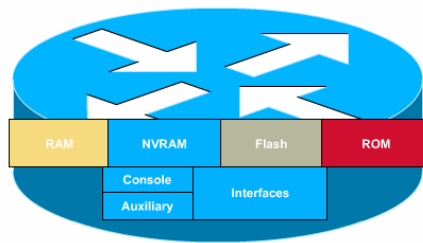
Sơ lược về bộ định tuyến

Bộ định tuyến Cisco bao gồm nhiều nền tảng phần cứng khác nhau được thiết kế xây dựng cho phù hợp với nhu cầu và mục đích sử dụng của các giải pháp khác nhau.

Các chức năng xử lý hoạt động của bộ định tuyến Cisco dựa trên nền tảng cốt lõi là hệ điều hành IOS.

Tùy theo các nhu cầu cụ thể mà một bộ định tuyến Cisco sẽ cần một IOS có các tính năng phù hợp. IOS có nhiều phiên bản khác nhau, một số loại phần cứng mới được phát triển chỉ có thể được hỗ trợ bởi các IOS phiên bản mới nhất.

Các thành phần cấu thành bộ định tuyến



Hình 3.1: Các thành phần của bộ định tuyến Cisco

- RAM: Giữ bảng định tuyến, ARP Cache, fast-switching cache, packet buffer, và là nơi chạy các file cấu hình cho bộ định tuyến. Đây chính là nơi lưu giữ file Running-Config, chứa cấu hình đang hoạt động của Router. Khi ngừng cấp nguồn cho bộ định tuyến, bộ nhớ này sẽ tự động giải phóng. Tất cả các thông tin trong file Running-Config sẽ bị mất hoàn toàn.

- NVRAM: non-volatile RAM, là nơi giữ startup/backup configure, không bị mất thông tin khi mất nguồn vào. File Startup-Config được lưu trong này để đảm bảo khi khởi động lại, cấu hình của bộ định tuyến sẽ được tự động đưa về trạng thái đã lưu giữ trong file. Vì vậy, phải thường xuyên lưu file Running-Config thành file Startup-Config.

- Flash: Là ROM có khả năng xóa, và ghi đọc. Là nơi chứa hệ điều hành IOS của bộ định tuyến. Khi khởi động, bộ định tuyến sẽ tự đọc ROM để nạp IOS trước khi nạp file Startup-Config trong NVRAM.

- ROM: Chứa các chương trình tự động kiểm tra.

- Cổng Console: Được sử dụng để cấu hình trực tiếp bộ định tuyến. Tốc độ dữ liệu dùng cho cấu hình bằng máy tính qua cổng COM là 9600b/s. Giao diện ra của cổng này là RJ45 female.

- Cổng AUX: Được sử dụng để quản lý và cấu hình cho bộ định tuyến thông qua modem dự phòng cho cổng Console. Giao diện ra của cổng này cũng là RJ45 female.

- Các giao diện:

- o Cổng Ethernet / Fast Ethernet
- o Cổng Serial
- o Cổng ASYNC ...

2.2. Một số tính năng ưu việt của bộ định tuyến Cisco

- Có khả năng tích hợp nhiều chức năng xử lý trên cùng một sản phẩm với việc sử dụng các module chức năng thích hợp và IOS thích hợp.

- Dễ dàng trong việc nâng cấp bộ định tuyến Cisco cả về phần mềm lẫn phần cứng do đó dễ dàng đáp ứng các nhu cầu thay đổi, mở rộng mạng, đáp ứng các nhu cầu phát triển và ứng dụng công nghệ mới.

- Tương thích và dễ dàng mở rộng cho các nhu cầu về đa dịch vụ ngày càng gia tăng trên.

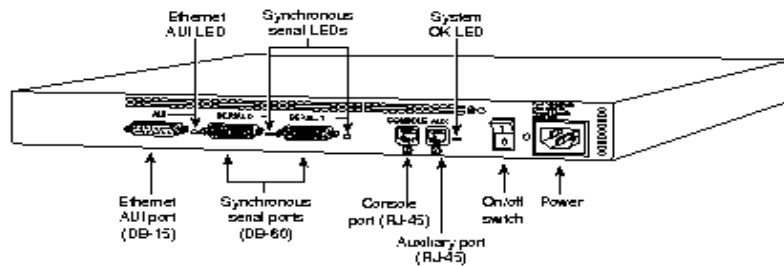
- Tính bền vững, an toàn và bảo mật.

2.3. Một số bộ định tuyến Cisco thông dụng

Bộ định tuyến Cisco 2500

- Bộ định tuyến Cisco 2509
- 01 cổng console, 01 AUX
- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...

- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường.

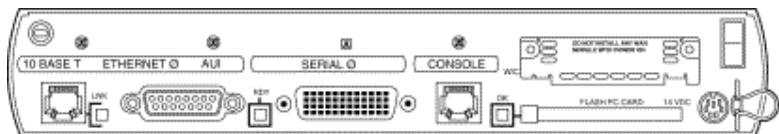


Hình 3.2: Bộ định tuyến Cisco 2501

- 01 cổng Async cho phép kết nối đến 08 modem V34/V90. Sử dụng một cáp kết nối Octal để kết nối các modem đến bộ định tuyến.
- Bộ định tuyến Cisco 2501
- 01 cổng console, 01 AUX
- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...
- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường

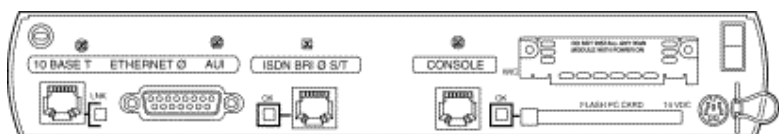
Cisco đã ngừng sản xuất các bộ định tuyến Cisco dòng 2500.

Bộ định tuyến Cisco 1600



Hình 3.3: Bộ định tuyến Cisco 1601

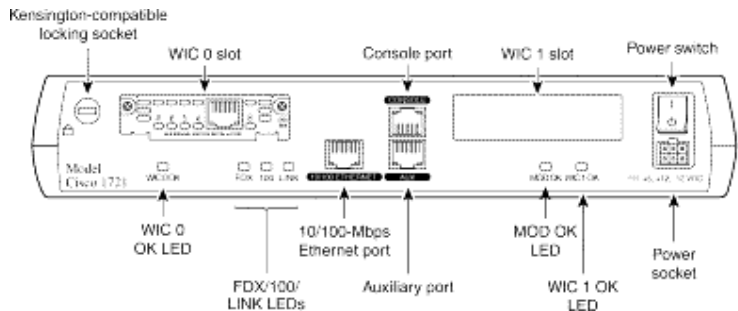
- Bộ định tuyến Cisco 1601
- 01 cổng console
- 01 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...
- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)
- 01 serial slot: có thể sử dụng cho cổng Serial thứ 2, card ISDN BRI



Hình 3.4: Bộ định tuyến Cisco 1603

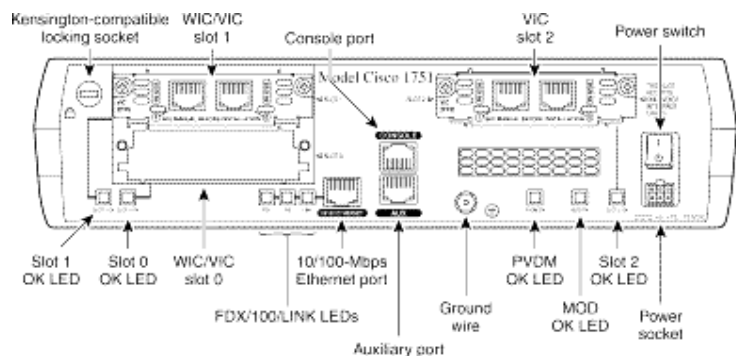
- Bộ định tuyến Cisco 1603
- 01 cổng console
- 01 cổng ISDN BRI giao diện S/T: kết nối ISDN tốc độ 2B+D, khi sử dụng ở Việt nam cần có thêm một bộ tiếp hợp NT1 để đấu nối vào mạng ISDN.
- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)
- 01 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI

Bộ định tuyến Cisco 1700



Hình 3.5: Bộ định tuyến Cisco 1721

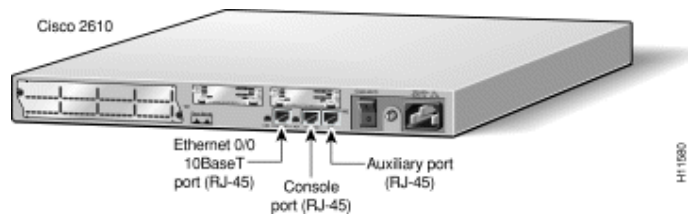
- Bộ định tuyến Cisco 1721
- 01 cổng console, 01 AUX
- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...



Hình 3.6: Bộ định tuyến Cisco 1751

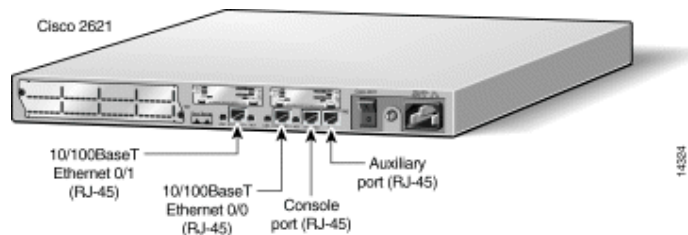
- Bộ định tuyến Cisco 1751
- 01 cổng console, 01 AUX
- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...
- 01 Voice slot: chỉ cho phép cắm các card voice

Bộ định tuyến Cisco 2600



Hình 3.7: Bộ định tuyến Cisco 2610

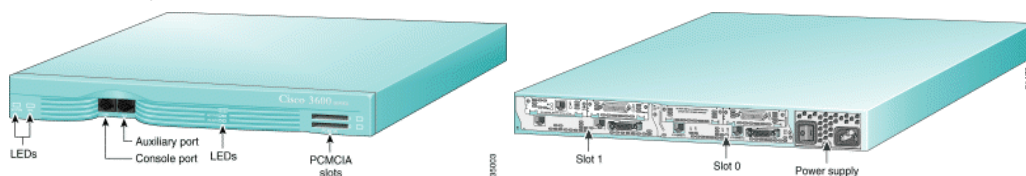
- Bộ định tuyến Cisco 2610
- 01 cổng console, 01AUX
- 01 Ethernet tốc độ 10Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...



Hình 3.8: Bộ định tuyến Cisco 2621

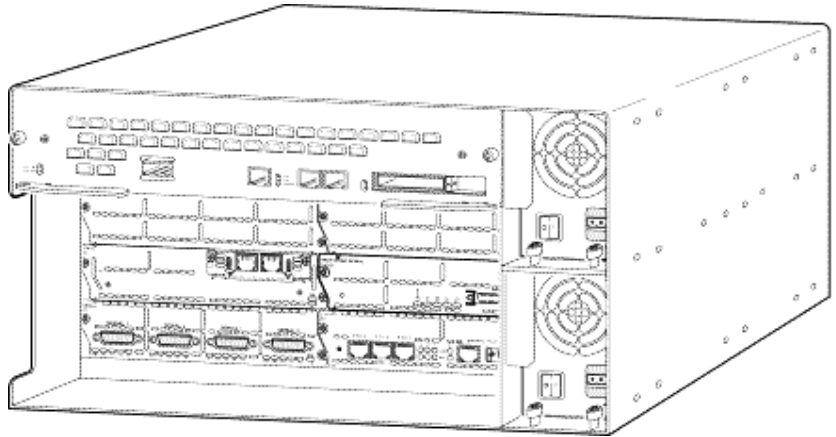
- Bộ định tuyến Cisco 2621
- 01 cổng console, 01AUX
- 02 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...

Bộ định tuyến Cisco 3600



Hình 3.9: Bộ định tuyến Cisco 3620

- Bộ định tuyến 3620
- 01 cổng console, 01AUX
- PCMCIA slot
- 02 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- Khi kết nối với mạng LAN cần thiết có một Network module có cổng Ethernet/FastEthernet



Hình 3.10: Bộ định tuyến Cisco 3661

- Bộ định tuyến 3661
- 01 cổng console, 01AUX
- PCMCIA slot
- 01 FastEthernet tốc độ 100Mbps
- 06 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- 02 module nguồn, hỗ trợ và dự phòng lẫn nhau, đảm bảo về mặt cung cấp nguồn điện cho bộ định tuyến. Có thể thay thế module nguồn mà không cần phải tắt điện toàn bộ bộ định tuyến.

2.4. Các giao tiếp của bộ định tuyến Cisco

- Cổng Console
 - o Tốc độ có thể 11500Bps, làm việc ở tốc độ 9600Bps
 - o Dùng cho cấu hình cho bộ định tuyến Cisco
 - o Sử dụng cáp Console để kết nối
- Cổng AUX
 - o Tốc độ 11500Bps
 - o Sử dụng cho quản trị/cấu hình từ xa qua modem V34/V90
 - o Có thể sử dụng để cấu hình trực tiếp sử dụng cáp Console
 - o Chỉ làm việc sau khi bộ định tuyến Cisco đã khởi động hoàn toàn

- o Có thể cấu hình để AUX làm việc như một đường kết nối dự phòng

- Ethernet/FastEthernet

- o Tốc độ 10Mbps/100Mbps giao diện AUI hoặc RJ45
- o Dùng cho đầu nối trực tiếp vào mạng LAN
- o Tuân theo các chuẩn của IEEE802.3

- Serial

- o Tốc độ kết nối tới 2Mbps
- o Dùng cho kết nối mạng WAN
- o Có khả năng kết nối theo nhiều chuẩn giao diện khác nhau V35, V24, X21, EIA530... bằng việc sử dụng các cáp nối

- ISDN

- o Tốc độ 2B+D
- o Dùng cho kết nối mạng ISDN sử dụng cho Dialup Server hoặc kết nối dự phòng
- o Có các giao diện U hoặc S/T, giao diện S/T cần thiết có thiết bị NT1 để kết nối vào mạng

- Async

- o Giao diện truyền số liệu không đồng bộ
- o Dùng cho kết nối với các hệ thống modem V34/V90
- o Sử dụng cáp kết nối Async (Octal Cable) để nối tới 08 modem. Octal cable thường có giao diện RJ45 và cần có chuyển đổi RJ45-DB25 để phù hợp với giao diện của modem

2.5. Kiến trúc module của bộ định tuyến Cisco

Các bộ định tuyến có kiến trúc module

Các bộ định tuyến Cisco thông dụng được giới thiệu ở phần trước hầu hết là có kiến trúc module trừ bộ định tuyến 2500 đã không được tiếp tục sản xuất.

Ngoài các bộ định tuyến có kiến trúc module đã được biết, còn có các bộ định tuyến khác:

- **1600:** 1601, 1602, 1603, 1604, 1605
- **1700:** 1710, 1720, 1721, 1750, 1751, 1760
- **2600:** 2610, 2160XM, 2611, 2611XM, 2612, 2613, 2620, 2620XM, 2621, 2621XM, 2650, 2650XM, 2651, 2651XM, 2691
- **3600:** 3620, 3631, 3640, 3661, 3662
- **3700:** 3725, 3745

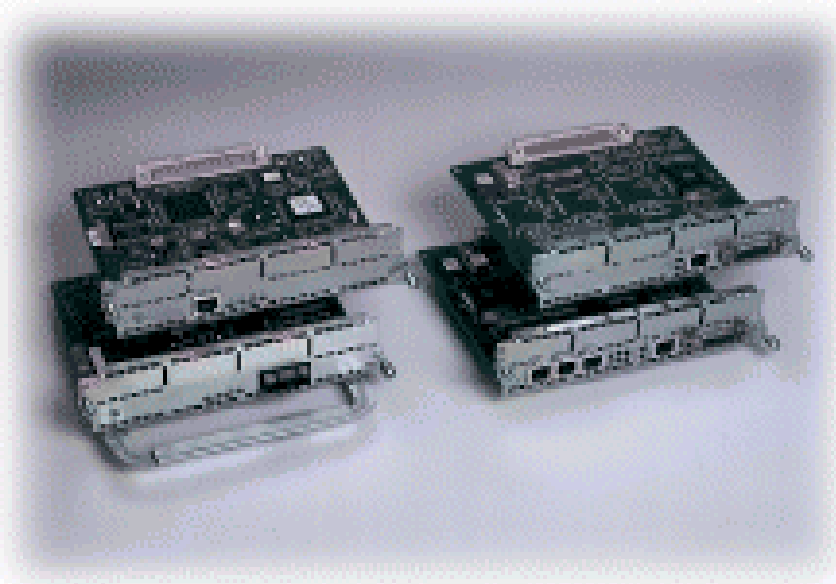
Tính tương thích dùng lẫn và thay thế

Các bộ định tuyến có kiến trúc module của Cisco được thiết kế để sử dụng chung một kho các card giao tiếp và module chức năng khác nhau.

Các card giao tiếp được sử dụng cho bất kỳ một bộ định tuyến nào có khe cắm tương thích. Tương thích phổ biến nhất là card giao tiếp Serial. Card giao tiếp serial có thể sử dụng trên bất kỳ bộ định tuyến nào. Một số card giao tiếp khác như card voice sẽ yêu cầu về cấu hình phần cứng và phần mềm tối thiểu. Các card giao tiếp được sử dụng cho các bộ định tuyến 1600, 1700 có thể sử dụng cho các bộ định tuyến 2600, 3600.

Bộ định tuyến 2600, 3600, 3700 cho phép sử dụng các module chức năng khác nhau. Một module chức năng có thể chỉ bao gồm một chức năng như module Async, module Serial, cũng có thể bao gồm nhiều chức năng hay bao gồm các khe cắm cho card giao tiếp khác như module NM-1E- có 01 cổng Ethernet và 02 khe cắm cho bất kỳ một loại card tương thích nào. Việc lựa chọn module tùy thuộc vào nhu cầu sử dụng cụ thể. Các module cùng được sử dụng giữa các bộ định tuyến. Một số module yêu cầu cấu hình tối thiểu về phần cứng và phần mềm. Bộ định tuyến 1600 và 1700 không cho phép sử dụng các module như các bộ định tuyến 2600, 3600.

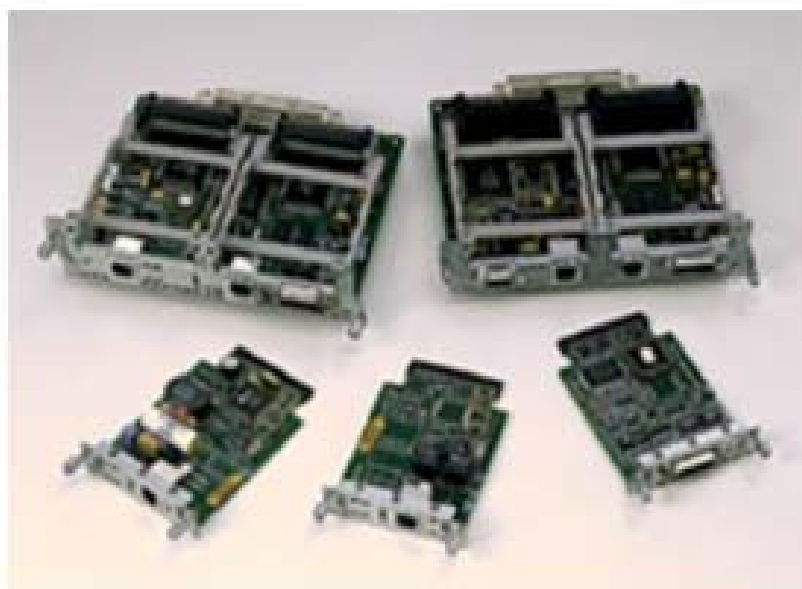
Một số module thường gặp



Hình 3.11: Module Ethernet/FastEthernet

Bảng 3-2: Một số loại module Ethernet/FastEthernet

Loại module	Số cổng LAN	Số khe cắm WAN
Single-Port Ethernet	1	None
Four-Port Ethernet	4	None
Single-Port Ethernet Mixed Media	1	Two WAN interface card slots
Dual-Port Ethernet Mixed Media	2	Two WAN interface card slots
Single-Port Ethernet and Single-Port Token Ring	1/1	Two WAN interface card slots
Single Port Fast Ethernet	1	None



Hình 3.12: Module Ethernet có khe cắm WAN

Bảng 3-3: Một số loại module có khe cắm WAN

Tên module	Loại module
NM-1FE2W/NM-1FE2W-V2	1 10/100 Ethernet, 2 khe cắm WAN
NM-2FE2W/NM-2FE2W-V2	2 10/100 Ethernet, 2 khe cắm WAN
NM-1FE1R2W	1 10/100 Ethernet, 1 4/16 Token Ring,

	2 khe cắm WAN
NM-2W	2 khe cắm WAN

Bảng 3-4: Giới hạn số lượng module trên các bộ định tuyến

	2600	2691	3620	3631	3640	3660	3725	3745
NM-1FE2W/NM-1FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-2FE2W/NM-2FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-1FE1R2W	N/A	1	2	N/A	4	6	2	4
NM-2W	1	1	1	N/A	3	6	2	4



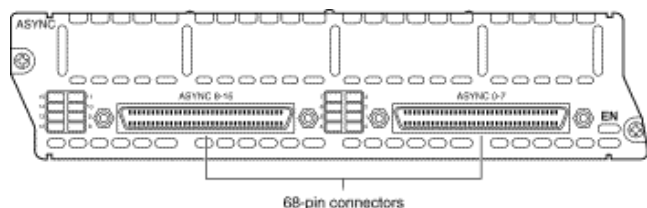
Hình 3.13: Module 4 cổng serial

- Module 4 cổng serial
- Hỗ trợ tổng lưu lượng 8Mbps: có thể sử dụng tốc độ tối đa 8Mbps trên một cổng hoặc mỗi 2Mbps cho 4 cổng.
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đầu nối leased-line, Frame Relay, X.25 ...



Hình 3.14: Module 8 cổng Sync/Async

- Module 8 cổng Sync/Async
- Tốc độ kết nối trên mỗi cổng thấp (tối đa 128Kbps)
- Có thể sử dụng ở hai chế độ đồng bộ và không đồng bộ. Có thể sử dụng cho modem quay số.
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đầu nối leased-line, Frame Relay, X.25, modem quay số...



Hình 3.15: Module 16 cổng Async

- Module 16 cổng Async
- Kết nối không đồng bộ sử dụng cho modem quay số.
- Kết nối với modem theo các chuẩn EIA/TIA-232 sử dụng cáp Octal



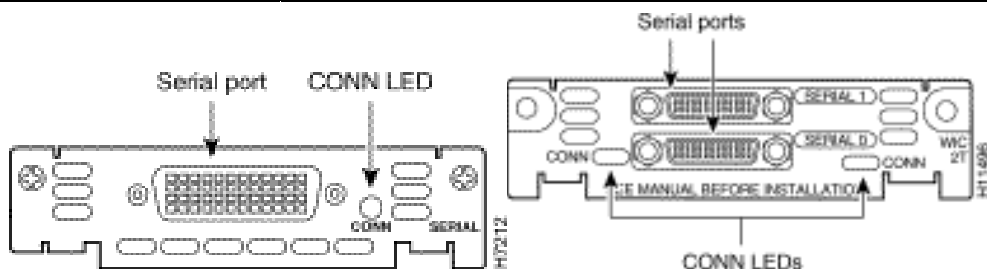
Hình 3.16: Module và card ISDN BRI

Bảng 3-5: Một số loại module ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại module	Mô tả
NM-4B-S/T	4 cổng ISDN BRI giao diện S/T
NM-4B-U	4 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)
NM-8B-S/T	8 cổng ISDN BRI giao diện S/T
NM-8B-U	8 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

Bảng 3-6: Một số loại card giao tiếp ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại card	Mô tả
WIC-1B-S/T-V2	1 cổng ISDN BRI giao diện S/T
WIC 1B-U-V2	1 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)



Hình 3.17: Card giao tiếp Serial

- Card một và hai cổng giao tiếp Serial
- Kết nối đồng bộ tốc độ đến 2Mbps
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đầu nối leased-line, Frame Relay, X.25, modem quay số...

3. Cách sử dụng lệnh cấu hình bộ định tuyến

3.1. Giới thiệu giao tiếp dòng lệnh của bộ định tuyến Cisco

Giao tiếp dòng lệnh

Giao tiếp dòng lệnh CLI (Command Line Interface) khác với các giao tiếp đồ họa GUI (Graphic User Interface) là giao tiếp đặc biệt được Cisco thiết kế cho phép người dùng, người quản trị làm việc với các thiết bị của Cisco thông qua các dòng lệnh trực tiếp.

Với giao tiếp dòng lệnh, người dùng, người quản trị có thể trực tiếp xem, cấu hình các thiết bị của Cisco thông qua các lệnh phù hợp. Để có thể sử dụng được giao tiếp dòng lệnh, người dùng phải nắm vững được các lệnh, các tham số lệnh và cách sử dụng các lệnh.

Mỗi thiết bị của Cisco đều có rất nhiều các lệnh, các bộ lệnh đi kèm tuy nhiên người sử dụng, người quản trị không nhất thiết phải hiểu hết toàn bộ các lệnh trong mỗi thiết bị mà chỉ cần hiểu, nắm vững một số lệnh cần thiết cho các mục đích sử dụng cụ thể.

Giao tiếp dòng lệnh của Cisco cung cấp cho người dùng khả năng sử dụng trợ giúp trực tuyến. Điều đó có nghĩa là trong quá trình làm việc với thiết bị thông qua giao tiếp dòng lệnh, người dùng có thể liệt kê các lệnh, xem lại ý nghĩa sử dụng của nó hay thậm chí xem các thông số lệnh.

Lưu ý: khi sử dụng giao tiếp dòng lệnh để cấu hình thiết bị, sau khi lệnh được thực thi (ấn phím Enter) các hoạt động của bộ định tuyến sẽ ảnh hưởng ngay lập tức bởi lệnh thực thi đó. Một cho những ví dụ là khi đang thực hiện cấu hình từ xa thông qua telnet, nếu thay đổi địa chỉ của bộ định tuyến, sẽ lập tức mất kết nối đến bộ định tuyến và chỉ có thể thực hiện cấu hình bộ định tuyến trực tiếp từ cổng console. Điều này có nghĩa cần thiết phải rất cẩn thận và chắc chắn cũng như thực hiện đúng trình tự mỗi khi thực hiện cấu hình bộ định tuyến.

Ví dụ về giao tiếp dòng lệnh như sau:

```
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
```

Các khả năng thực hiện cấu hình bộ định tuyến Cisco

- Cấu hình bộ định tuyến trực tiếp từ cổng console: là phương pháp sử dụng một cáp console thông qua một phần mềm kết nối trực tiếp cổng COM như HyperTerminal của WINDOWS để truy nhập vào bộ định tuyến sau đó cấu hình bộ định tuyến theo giao thức dòng lệnh. Phương pháp cấu hình này được sử dụng nhiều nhất và trong hầu hết các trường hợp. Các bộ định tuyến sử dụng lần đầu cũng phải được cấu hình bằng phương pháp này.

- Cấu hình bộ định tuyến thông qua truy nhập từ xa telnet: truy nhập từ xa tới bộ định tuyến với telnet chỉ có thể thực hiện được khi bộ định tuyến đã được cấu hình với ít nhất một địa chỉ mạng, có mật khẩu bảo vệ và máy tính sử dụng để cấu hình bộ định tuyến phải có khả năng kết nối được với bộ định tuyến thông qua môi trường mạng. Sau khi kết nối được tới bộ định tuyến, sử dụng giao diện dòng lệnh để cấu hình bộ định tuyến.

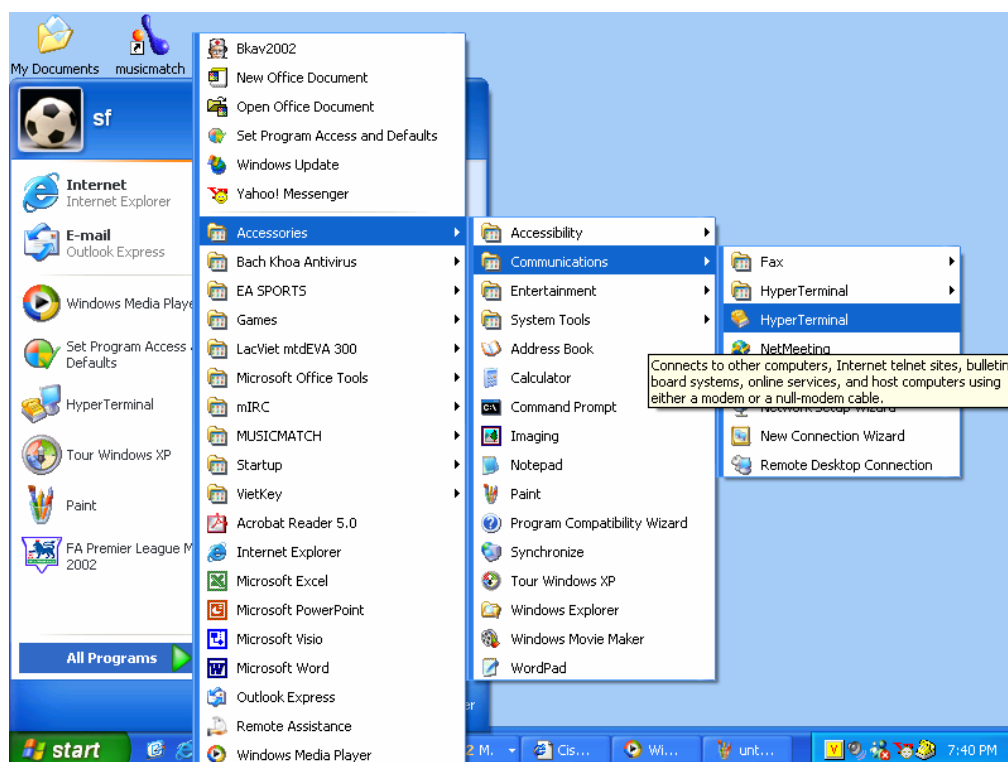
- Cấu hình bộ định tuyến sử dụng tập tin cấu hình lưu trữ trên máy chủ TFTP: trong một số trường hợp, tập tin cấu hình cho bộ định tuyến có thể được lưu trữ trên máy chủ TFTP, bộ định tuyến được cấu hình sao cho sau khi khởi động sẽ tìm kiếm tập tin cấu hình trên máy chủ TFTP thay vì sử dụng tập tin cấu hình lưu trữ trong NVRAM. Có thể sử dụng lệnh copy để tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Cấu hình bộ định tuyến thông qua giao diện WEB: chỉ thực hiện được sau khi bộ định tuyến đã được cấu hình với địa chỉ IP và cho phép cấu hình qua giao thức http.

Sử dụng giao tiếp dòng lệnh

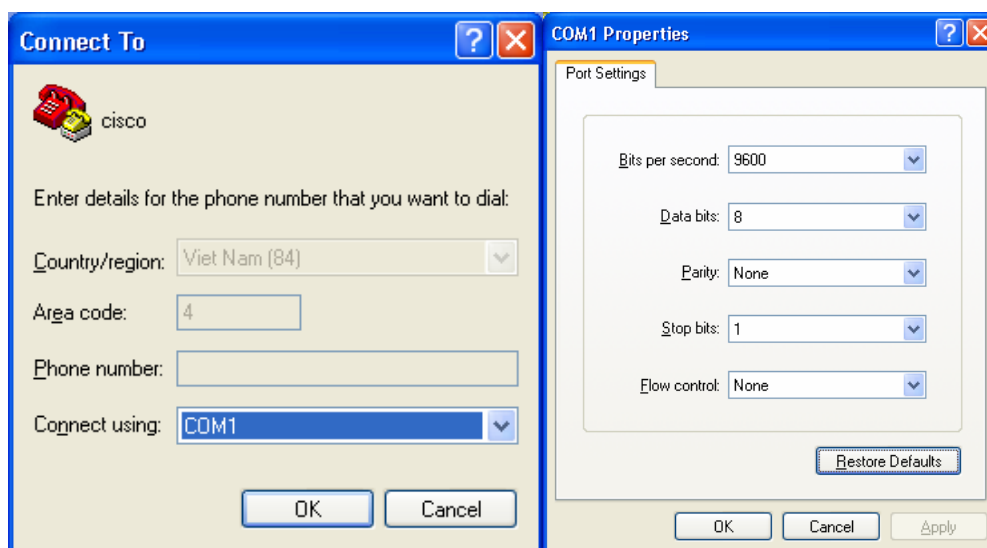
Để thực hiện việc kết nối máy tính với bộ định tuyến, người ta dùng cáp console của Cisco, một đầu cắm trực tiếp vào cổng CONSOLE của bộ định tuyến, đầu kia cắm vào cổng COM của máy tính, có thể sử dụng các đầu chuyển đổi DB9/RJ45 hoặc DB25/RJ45 khi cần thiết.

Phần mềm giao tiếp giữa máy tính và bộ định tuyến thông dụng nhất là HyperTerminal được cài đặt sẵn trong các phiên bản WINDOWS.

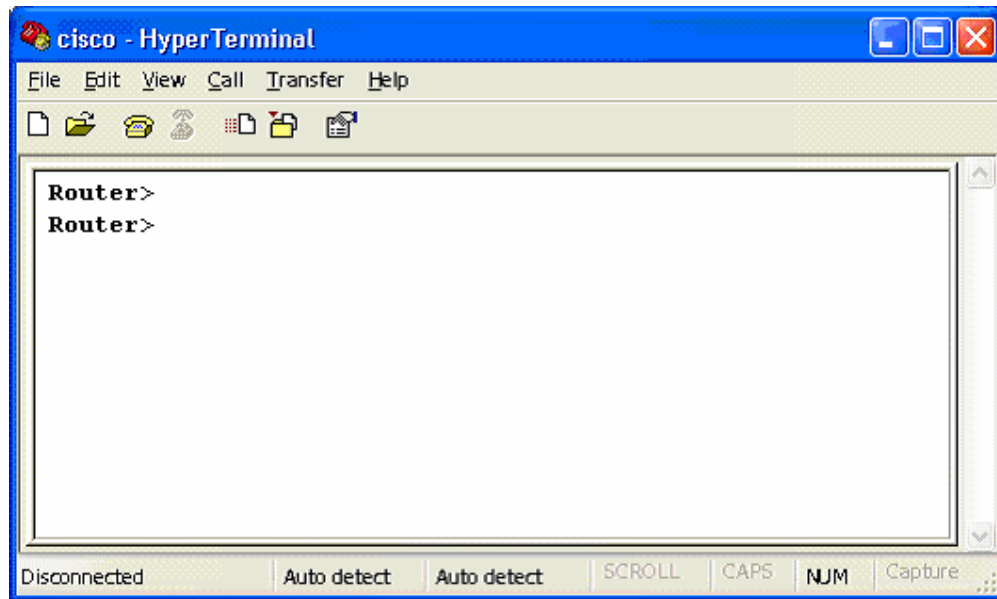


Hình 3.18: Sử dụng HyperTerminal để kết nối đến bộ định tuyến

Chọn đúng cổng COM kết nối với cáp console để tiến hành cài đặt các thông số làm việc. Tốc độ kết nối thông qua cổng COM của máy tính và cổng CONSOLE của bộ định tuyến là 9600b/s (hình 3.19). Chọn OK, bấm phím Enter, cửa sổ làm việc xuất hiện dấu lớn hơn ">" sau tên của của bộ định tuyến, nghĩa là việc kết nối đã hoàn tất (hình 3-20).



Hình 3.19: Xác lập các tham số cho kết nối



Hình 3.20: Kết nối tới bộ định tuyến thành công

Sau khi đã kết nối thành công, sử dụng các lệnh của bộ định tuyến để xem, kiểm tra, cấu hình và bắt lỗi các hoạt động của bộ định tuyến.

Sử dụng dấu ? để truy cập thông tin trợ giúp

- Đánh dấu ? ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiển thị các lệnh có thể bắt đầu từ các từ chưa hoàn chỉnh đã gõ
- Đánh dấu ? sau câu lệnh một ký tự trắng sẽ hiển thị các tham số có thể của câu lệnh
- Khi câu lệnh không có sẽ hiển thị một báo lỗi

Sử dụng TAB ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiển thị câu lệnh hoàn chỉnh

3.2. Làm quen với các chế độ cấu hình

Chế độ người dùng

Bao gồm các tác vụ phổ biến chủ yếu gồm những lệnh kiểm tra trạng thái hoạt động của bộ định tuyến, trạng thái các giao tiếp, các bảng định tuyến v.v... và một số lệnh để kiểm tra kết nối mạng như ping, traceroute, telnet v.v.... Ở chế độ này không được phép thay đổi các cấu hình bộ định tuyến. Chế độ người dùng không cho phép xem xét sâu đến các hoạt động của bộ định tuyến mà trong quá trình khai thác, vận hành, người quản trị phải cần thiết sử dụng chế độ quản trị để thực hiện. Biểu hiện của chế độ người dùng là dấu lớn hơn, >, sau tên bộ định tuyến:

Router>

Router>?

Exec commands:

<1-99>

Session number to resume

access-enable	Create a temporary Access-List entry
access-profile	Apply user-profile to interface
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
----- các lệnh đã được bỏ bớt -----	
ping	Send echo messages
ppp	Start IETF Point-to-Point Protocol (PPP)
resume	Resume an active network connection
rlogin	Open an rlogin connection
show	Show running system information
slip	Start Serial-line IP (SLIP)
systat	Display information about terminal lines
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
tunnel	Open a tunnel connection
udptn	Open an udptn connection
where	List active connections
x28	Become an X.28 PAD
x3	Set X.3 parameters on PAD

Chế độ quản trị

Bao gồm hầu hết các lệnh của chế độ người dùng và các lệnh chỉ dành cho người quản trị. Chỉ có thể cấu hình bộ định tuyến ở chế độ này. Trong quá trình khai thác, vận hành, để hiểu rõ hoặc khi có sự cố xảy ra, người quản trị có thể sử dụng các lệnh debug để làm rõ thêm thông tin cần thiết. Đặc trưng cho chế độ quản trị là biểu hiện của dấu thăng, #.

Router>en

Password:

Router#

Router#?

Exec commands:

<1-99>	Session number to resume
access-enable	Create a temporary Access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary Access-List entry
archive	manage archive files
bfe	For manual emergency modes setting
cd	Change current directory

clear	Reset functions
clock	Manage the system clock
configure	Enter configuration mode
connect	Open a terminal connection
copy	Copy from one file to another
debug	Debugging functions (see also 'undebug')
----- các lệnh đã được bỏ bớt -----	
traceroute	Trace route to destination
tunnel	Open a tunnel connection
udptn	Open an udptn connection
undebug	Disable debugging functions (see also 'debug')
upgrade	Upgrade firmware
verify	Verify a file
where	List active connections
write	Write running configuration to memory, network, or terminal
x28	Become an X.28 PAD
x3	Set X.3 parameters on PAD

Chế độ cấu hình toàn cục

Là chế độ cấu hình các tham số toàn cục cho bộ định tuyến.

Có rất nhiều các cấu hình toàn cục như cấu hình tên bộ định tuyến, cấu hình tên và mật khẩu người dùng, cấu hình định tuyến toàn cục, cấu hình danh sách truy nhập v.v... Biểu hiện của chế độ cấu hình toàn cục như sau:

```
Router#  
Router#config terminal  
Router(config)#hostname RouterA
```

Chế độ cấu hình giao tiếp

Chế độ cấu hình giao tiếp là chế độ cấu hình cho các giao tiếp của bộ định tuyến như giao tiếp Serial, giao tiếp Ethernet, giao tiếp Async...

Chế độ cấu hình giao tiếp cho phép người quản trị mạng thiết lập các tham số hoạt động cho mỗi giao tiếp như các giao thức mạng được sử dụng trên giao tiếp, địa chỉ mạng của giao tiếp, gán các danh sách truy nhập cho giao tiếp v.v... Một ví dụ về chế độ cấu hình giao tiếp như sau:

```
Router#  
Router#config terminal  
Router(config)#interface s0/0  
Router(config-if)#encapsulation ppp  
Router(config-if)#ip address 192.168.100.5 255.255.255.0  
Router(config-if)#
```

Chế độ cấu hình định tuyến

Là chế độ cấu hình các tham số cho các giao thức định tuyến. Các giao thức định tuyến được cấu hình độc lập với nhau và đều được thực hiện ở chế độ cấu hình định tuyến như ví dụ sau:

```
Router#
Router#config terminal
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-if)#
```

Chế độ cấu hình đường kết nối

Chế độ cấu hình đường kết nối là một chế độ cấu hình đặc biệt sử dụng để thiết lập các tham số mức thấp cho giao tiếp logic trong đó điển hình là các tham số thiết lập cho các kết nối modem quay số.

```
Router#config terminal
Router(config)#line 33 48
Router(config-line)#modem inout
Router(config-line)#modem autoconfig discovery
Router(config-line)#
```

Bảng 3-7: Một số chế độ cấu hình và thể hiện

Chế độ cấu hình	Thể hiện
Global	Router(config)#
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)#
Route-map	Router(config-route-map)#

3.3. Làm quen với các lệnh cấu hình cơ bản

Enable: dùng để vào chế độ quản trị. Sau khi thực hiện lệnh enable, người dùng phải cung cấp mật khẩu quản trị đúng để thực sự được làm việc ở chế độ quản trị, mật khẩu không được phép nhập sai quá 3 lần.

```
Router>
Router>en
Password:
Password:
Password:
% Bad secrets
Router>en
Password:
Router#
Router#
Router#disa
Router>
```

Disable: thoát khỏi chế độ quản trị về chế độ người dùng.

Setup: thực hiện khởi tạo lại cấu hình của bộ định tuyến ở chế độ cấu hình hội thoại. Sau đây là một ví dụ về sử dụng lệnh setup. Chế độ hội thoại này cũng được thực hiện tự động đối với các bộ định tuyến chưa hề có tập tin cấu hình hay nói cách khác có NVRAM không chứa thông tin.

```
Router#setup
    --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: n
First, would you like to see the current interface summary? [yes]: n
Configuring global parameters:
Enter host name [Router]:
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret [<Use current secret>]:
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password []:123456
```

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: 654321
Configure SNMP Network Management? [yes]:
  Community string [public]:
Configure IP? [yes]:
  Configure IGRP routing? [yes]: n
  Configure RIP routing? [no]:
Configure bridging? [no]:
Async lines accept incoming modems calls. If you will have
users dialing in via modems, configure these lines.
  Configure Async lines? [yes]: n
Configuring interface parameters:
Do you want to configure FastEthernet0/0 interface? [yes]: n
Do you want to configure Serial0/0 interface? [yes]: n
Do you want to configure Serial0/1 interface? [no]: y
  Some supported encapsulations are
    ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
  Choose encapsulation type [hdlc]: ppp
  No serial cable seen.
  Choose mode from (dce/dte) [dte]:
Configure IP on this interface? [no]: y
  IP address for this interface: 192.168.100.5
  Subnet mask for this interface [255.255.255.0] :
  Class C network is 192.168.100.0, 24 subnet bits; mask is /24
The following configuration command script was created:
hostname Router
enable secret 5 $1$EuXV$Yhj/OYkz/U1R5VABqXsMC0
enable password 7 123456
line vty 0 4
password 7 654321
snmp-server community public
!
ip routing
no bridge 1
!
interface FastEthernet0/0
shutdown
no ip address
!
interface Serial0/0
shutdown
no ip address
```



```
!  
interface Serial0/1  
no shutdown  
encapsulation ppp  
ip address 192.168.100.5 255.255.255.0  
dialer-list 1 protocol ip permit  
dialer-list 1 protocol ipx permit  
!  
end  
[0] Go to the IOS command prompt without saving this config.  
[1] Return back to the setup without saving this config.  
[2] Save this configuration to nvram and exit.
```

Config: cho phép thực hiện các lệnh cấu hình bộ định tuyến. Sau lệnh config, quản trị mạng mới có thể thực hiện các lệnh cấu hình bộ định tuyến.

Trình tự thực hiện cấu hình cho một bộ định tuyến có thể được thể hiện như sau

- Đặt tên cho bộ định tuyến

```
Router#config terminal  
Router(config)#  
Router(config)#hostname RouterABC  
RouterABC(config)#
```

- Đặt tên mật khẩu bí mật dành cho người quản trị

```
RouterABC(config)#enable secret matkhaubimat  
RouterABC(config)#
```

- Đặt tên mật khẩu cho chế độ quản trị. Mật khẩu này chỉ sử dụng khi cấu hình bộ định tuyến không có mật khẩu bí mật dành cho quản trị.

```
RouterABC(config)#enable password matkhau  
RouterABC(config)#
```

- Cấu hình cho phép người dùng truy cập từ xa đến bộ định tuyến

```
RouterABC(config)#line vty 0 4  
RouterABC(config-line)#login  
RouterABC(config-line)#password telnet  
RouterABC(config-line)#
```

- Cấu hình các giao tiếp

```
RouterABC(config)#interface ethernet 0  
RouterABC(config-if)#ip address 192.168.2.1 255.255.255.0  
RouterABC(config-if)#no shutdown  
RouterABC(config-if)#
```

- Cấu hình định tuyến

```
RouterABC(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2  
RouterABC(config)#
```

Copy: lệnh copy cho phép thực hiện các sao chép cấu hình của bộ định tuyến đi/đến máy chủ TFTP, sao chép, lưu trữ, nâng cấp các tập tin IOS của bộ định tuyến từ / tới máy chủ TFTP.

Để có thể lưu bản sao cấu hình hiện hành lên máy chủ TFTP, sử dụng lệnh *copy running-config tftp* như được trình bày ở dưới. Tiếp theo là tiến trình ngược lại với việc tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Nhập lệnh *copy running-config tftp*
- Nhập địa chỉ IP của máy chủ TFTP nơi dùng để lưu tập tin cấu hình
- Nhập tên ấn định cho tập tin cấu hình
- Xác nhận chọn lựa với trả lời yes

Lệnh copy dùng để lưu tập tin cấu hình lên máy chủ:

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Name of configuration file to write [Router-config]? cisco.cfg
Write file cisco.cfg to 192.168.1.5? [confirm] y
Writing cisco.cfg !!!!! [OK]
Router#
```

Lệnh copy dùng để tải tập tin cấu hình từ máy chủ:

```
Router#copy tftp running-config
Address or name of remote host []? 192.168.1.5
Source filename []? cisco.cfg
Destination filename [running-config]?
```

Show: là lệnh được dùng nhiều và phổ biến nhất.

Lệnh show dùng để xác định trạng thái hiện hành của bộ định tuyến. Các lệnh này giúp cho phép có được các thông tin quan trọng cần biết khi kiểm tra và điều chỉnh các hoạt động của bộ định tuyến.

- show version: hiển thị cấu hình phần cứng hệ thống, phiên bản phần mềm, tên và nguồn của các tập tin cấu hình, và ảnh chương trình khởi động.
- show processes: hiển thị thông tin các quá trình hoạt động của bộ định tuyến.
- show protocols: hiển thị các giao thức được cấu hình.
- show memory: thống kê về bộ nhớ của bộ định tuyến.
- show stacks: giám sát việc sử dụng stack của các quá trình, các thủ tục ngắt và hiển thị nguyên nhân khởi động lại hệ thống lần cuối cùng.
- show buffers: cung cấp thống kê về các vùng bộ đệm trên bộ định tuyến.

- show flash: thể hiện thông tin về bộ nhớ Flash.
- show running-config: hiển thị tập tin cấu hình đang hoạt động của bộ định tuyến.
- show startup-config: hiển thị tập tin cấu hình được lưu trữ trên NVRAM và được đưa vào bộ nhớ để hoạt động khi bật nguồn bộ định tuyến. Thông thường running-config và startup-config là giống nhau. Khi thực hiện các lệnh cấu hình, running-config và startup-config sẽ không còn giống nhau, cấu hình hoạt động (running-config) cần phải được ghi trở lại NVRAM sau khi kết thúc cấu hình bộ định tuyến.
- show interfaces: thống kê các giao tiếp của bộ định tuyến. Đây là một trong các lệnh được sử dụng nhiều nhất cho biết trạng thái hoạt động của các giao tiếp, số liệu thống kê lưu lượng, số lượng các gói tin lỗi v.v...

<pre>Router#sh run Building configuration... ! Version 12.1 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Router ! interface Ethernet0 no ip address no ip directed-broadcast shutdown</pre>	<pre>Router#sh startup-config Current configuration : 677 bytes ! Version 12.1 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Router ! interface Ethernet0 no ip address no ip directed-broadcast</pre>
--	--

Hình 3.21: Lệnh show

```
Router#show interface s0/0
```

```
Serial0/0 is up, line protocol is up
```

```
Hardware is PowerQUICC Serial
Description: 2M link to the Internet
Internet address is 192.168.100.5/24
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
    reliability 255/255, txload 248/255, rxload 84/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/12/0 (size/max/drops/flushes); Total output
drops: 2383688
Queueing strategy: weighted fair
Output queue: 24/1000/64/2383671 (size/max total/threshold/drops)
Conversations 5/184/256 (active/max active/max total)
```

```
Reserved Conversations 0/0 (allocated/max allocated)

5 minute input rate 677000 bits/sec, 161 packets/sec
5 minute output rate 1996000 bits/sec, 395 packets/sec

106754998 packets input, 2930909441 bytes, 0 no buffer
Received 68850 broadcasts, 0 runts, 0 giants, 0 throttles

51143 input errors, 30726 CRC, 20248 frame, 0 overrun, 0
ignored, 169 abort

319791176 packets output, 1669977392 bytes, 0 underruns
0 output errors, 0 collisions, 125 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions

DCD=up DSR=up DTR=up RTS=up CTS=up
```

Hình 3.22: Lệnh show interface

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(2), RELEASE
SOFTWARE (fc1)

Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 09-May-00 23:34 by linda
Image text-base: 0x80008088, data-base: 0x807D2544

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 1 week, 1 day, 1 minute

System returned to ROM by power-on at 13:29:57 Hanoi Thu Jul 31 2003
System restarted at 20:24:22 Hanoi Tue Sep 2 2003
System image file is "flash:c2600-i-mz.121-2.bin"

cisco 2620 (MPC860) processor (revision 0x102) with 26624K/6144K
bytes of memory

.

Processor board ID JAD04340ID8 (2733840160)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.

1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Hình 3.23: Lệnh show version

Write: lệnh write sử dụng để ghi lại cấu hình hiện đang chạy của bộ định tuyến. Nhất thiết phải dùng lệnh *write memory* để ghi lại cấu hình của bộ định tuyến vào NVRAM mỗi khi có thay đổi về cấu hình.

```
Router#write ?
      erase      Erase NV memory
      memory    Write to NV memory
      network    Write to network TFTP server
      terminal   Write to terminal
      <cr>
```

3.4. Cách khắc phục một số lỗi thường gặp

Lỗi kết nối đến cổng console sử dụng Hyper Terminal

- Kiểm tra lại xem đã sử dụng chính xác loại cáp dùng để cấu hình bộ định tuyến chưa. Cáp console dùng để cấu hình bộ định tuyến là cáp 8 sợi có hai đầu RJ45 có sơ đồ đầu nối như bảng 3-8 và sử dụng đầu chuyển đổi DB9/RJ45 được cung cấp kèm theo bộ định tuyến.
- Kiểm tra xem đã sử dụng đúng cổng kết nối COM của máy tính để nối tới bộ định tuyến.

Bảng 3-8: Sơ đồ đầu nối cáp console

Console	Cáp console		DB9/RJ45	COM
Tín hiệu	RJ45	RJ45	DB9	Tín hiệu
RTS	1	8	8	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8	1	7	RTS

- Kiểm tra các tham số kết nối. Tốc độ kết nối phải là 9600 cho kết nối qua cổng console.

Lỗi kết nối sử dụng telnet

Khi sử dụng telnet để cấu hình từ xa bộ định tuyến, người dùng có thể không kết nối được đến bộ định tuyến. Một trong các lỗi sau cần được kiểm tra:

- Máy tính dùng để cấu hình bộ định tuyến không có kết nối mạng với bộ định tuyến. Kiểm tra lại khả năng kết nối mạng từ máy tính đến bộ định tuyến. Có thể dùng lệnh *ping* để kiểm tra.

- Khi cấu hình bộ định tuyến lần đầu, người quản trị mạng đã quên không thiết lập mật khẩu cho truy nhập từ xa. Khi cố gắng truy nhập từ xa, người dùng sẽ nhận được thông báo về việc mật khẩu truy nhập chưa được thiết lập. Trường hợp này cần sử dụng cấp console để thiết lập mật khẩu theo trình tự như trình bày dưới đây:

```
Router#config terminal
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password 123456
Router(config-line)#end
Router#write memory
```

- Kiểm tra về việc có hay không có các hạn chế telnet sử dụng các danh sách kiểm soát truy nhập (access-list).

4. Cấu hình bộ định tuyến Cisco

4.1. Cấu hình leased-line

Giới thiệu leased-line

Leased-line, hay còn được gọi là kênh thuê riêng, là một hình thức kết nối trực tiếp giữa các node mạng sử dụng kênh truyền dẫn số liệu thuê riêng.

Kênh truyền dẫn số liệu thuê riêng thông thường cung cấp cho người sử dụng sự lựa chọn trong suốt về giao thức đầu nối hay nói cách khác, có thể sử dụng các giao thức khác nhau trên kênh thuê riêng như PPP, HDLC, LAPB v.v...

Về mặt hình thức, kênh thuê riêng có thể là các đường cáp đồng trực tiếp kết nối giữa hai điểm hoặc có thể bao gồm các tuyến cáp đồng và các mạng truyền dẫn khác nhau. Khi kênh thuê riêng phải đi qua các mạng truyền dẫn khác nhau, các quy định về giao tiếp với mạng truyền dẫn sẽ được quy định bởi nhà cung cấp dịch vụ. Do đó, các thiết bị đầu cuối CSU/DSU cần thiết để kết nối kênh thuê riêng sẽ phụ thuộc và nhà cung cấp dịch vụ. Một số các chuẩn kết nối chính được sử dụng là HDSL, G703, 2B1Q v.v...

Khi sử dụng kênh thuê riêng, người sử dụng cần thiết phải có đủ các giao tiếp trên các bộ định tuyến sao cho có một giao tiếp kết nối WAN cho mỗi một kết nối kênh thuê riêng tại mỗi node. Điều đó có nghĩa là, tại điểm node có kết nối kênh thuê riêng đến 10 điểm khác nhất thiết phải có đủ 10 giao tiếp WAN để phục vụ cho các kết nối kênh thuê riêng. Đây là một vấn đề hạn chế về đầu tư thiết bị ban đầu, không linh hoạt trong mở rộng, phát triển, phức tạp

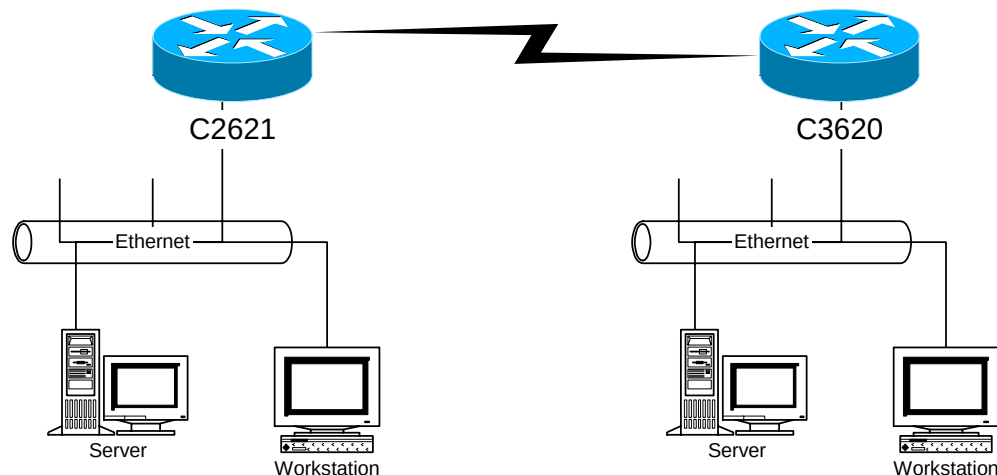
trong quản lý, đặc biệt là chi phí thuê kênh lớn đối với các yêu cầu kết nối xa về khoảng cách địa lý.

Các giao thức sử dụng với đường lease-line

Hai giao thức sử dụng với leased-line là HDLC, PPP và LAPB. Trong đó:

- HDLC: là giao thức được sử dụng với họ các bộ định tuyến Cisco hay nói cách khác chỉ có thể sử dụng HDLC khi cả hai phía của kết nối leased-line đều là bộ định tuyến Cisco.
- PPP: là giao thức chuẩn quốc tế, tương thích với tất cả các bộ định tuyến của các hãng sản xuất khác nhau. Khi đầu nối kênh leased-line giữa một phía là thiết bị của Cisco và một phía là thiết bị của hãng thứ 3 thì nhất thiết phải dùng giao thức đầu nối này. PPP là giao thức lớp 2 cho phép nhiều giao thức mạng khác nhau có thể chạy trên nó do vậy nó được sử dụng phổ biến.
- LAPB: là giao thức truyền thông lớp hai tương tự như giao thức mạng X.25 với đầy đủ các thủ tục, quá trình kiểm soát truyền dẫn, phát hiện và sửa lỗi. LAPB ít được sử dụng.

Mô hình kết nối lease-line



Cấu hình kết nối lease-line cơ bản

- Phân định địa chỉ

o Việc phân định địa chỉ cho các mạng và cho các kết nối giữa các bộ định tuyến là rất quan trọng, đảm bảo cho việc liên lạc thông suốt giữa các mạng, đảm bảo cho vấn đề qui hoạch địa chỉ, nhóm gọn các định tuyến ...

o Khi thực hiện xây dựng một mạng dùng riêng, điều cần thiết phải ghi nhớ là chỉ được dùng các địa chỉ trong nhóm các địa chỉ dành cho mạng dùng riêng: 10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x

o Để đảm bảo không bị trùng lặp và giảm thiểu các vấn đề phát sinh, các kết nối mạng WAN theo kiểu leased-line cần được sắp xếp trên lớp mạng nhỏ nhất. Các kết nối mạng WAN trong trường hợp này được thực hiện trên các lớp mạng gồm 4 địa chỉ.

o Các lớp mạng khác tùy theo yêu cầu cụ thể và số lượng các địa chỉ có thể mà phân chia cho phù hợp.

- Để bắt đầu cấu hình mạng:

```
o Router> enable ↵
o Password: ***** ↵
o Router# config terminal ↵
o Router(config)#
```

- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện

- Cấu hình

```
o Router2621(config)# interface serial 0 ↵
```

- Lựa chọn giao thức sử dụng

```
o Router2621(config-if)# encapsulation HDLC ↵
```

- Đặt địa chỉ IP cho giao tiếp kết nối leased-line

```
o Router2621(config-if)# ip address 192.168.113.5
255.255.255.252 ↵
```

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

```
o Router2621(config-if)# no shutdown ↵
o Router2621(config-if)# interface serial 1 ↵
```

- Lựa chọn giao thức PPP sử dụng cho một giao tiếp khác

```
o Router2621(config-if)# encapsulation PPP ↵
o Router2621(config-if)# ip address 192.168.113.9
255.255.255.252 ↵
```

```
o Router2621(config-if)# no shutdown ↵
o Router2621(config-if)# exit ↵
```

- Sử dụng định tuyến tĩnh với cú pháp: ip route [địa chỉ mạng đích] [netmask] [địa chỉ next hop]

```
o Router2621(config)# ip route 0.0.0.0 0.0.0.0
192.168.113.6 ↵
```

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

```
o Router2621# write memory ↵
```

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

o Dùng lệnh **show interface** để kiểm tra trạng thái của giao tiếp

o **show interface**: xem trạng thái tất cả các giao tiếp

o **show interface serial 0**: xem trạng thái cổng serial 0

o *Serial 0 is administrative down line protocole is down*: thể hiện trạng thái đang bị cấu hình là không làm việc, sử dụng lệnh no shutdown trong Interface mode để đưa giao tiếp serial 0 vào làm việc

o *Serial 0 is down line protocole is down*: kiểm tra lại đường truyền

o *Serial 0 is up line protocole is down*: kiểm tra lại các giao thức được sử dụng tại hai phía

o *Serial 0 is up line protocole is up*: là trạng thái làm việc

Cấu hình bộ định tuyến 2621

```
!  
hostname 2621  
!  
!  
interface FastEthernet0/0  
  ip address 10.0.5.1 255.255.255.0  
!  
!  
interface Serial0/0  
  ip address 192.168.113.5 255.255.255.252  
  encapsulation ppp  
!  
!  
ip route 0.0.0.0 0.0.0.0 192.168.113.6  
!  
!  
line con 0  
  exec-timeout 0 0  
  transport input none  
line aux 0  
line vty 0 4  
  login  
!  
end
```

Hình 3.24: Cấu hình của bộ định tuyến 2621

Cấu hình bộ định tuyến 3620

```
!  
hostname 3620  
!  
!  
interface FastEthernet0/0  
  ip address 10.0.6.1 255.255.255.0  
!  
!  
interface Serial1/0
```

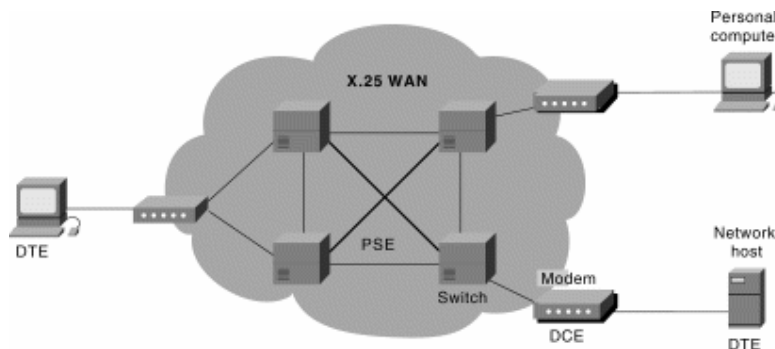
```
ip address 192.168.113.6 255.255.255.252
encapsulation ppp
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.5
!
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line vty 0 4
  login
!
end
```

Hình 3.25: Cấu hình của bộ định tuyến 3620

4.2. Cấu hình X.25 & Frame Relay

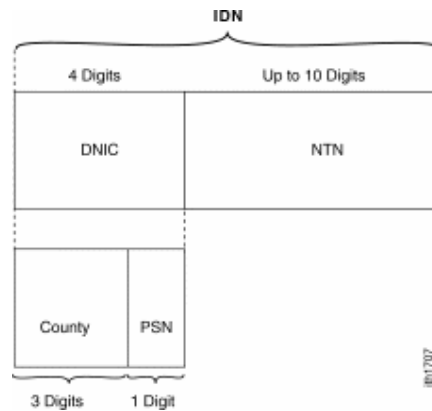
Giới thiệu X.25 và Frame Relay

X.25: Năm 1978 ISO thay đổi thêm HDLC và CCITT thêm một số thông số để sinh ra LAPB “Link Access Procedure – Balanced Mode”. LAPB định nghĩa một số quy luật cho mức Frame của X.25 như các loại khung đặc biệt như RR (Receive Ready), REJ (Reject) . . .



Hình 3.26: Chuyển mạch gói X.25

X.25 cung cấp các kết nối diện rộng thông qua môi trường chuyển mạch gói. Mỗi thuê bao X.25 có một địa chỉ xác định duy nhất được đánh số gồm các phần mã quốc gia, nhà cung cấp dịch vụ và địa chỉ của thuê bao trực thuộc nhà cung cấp dịch vụ.



Hình 3.27: Cấu trúc địa chỉ X.25

Khi có nhu cầu kết nối truyền dữ liệu, các thiết bị đầu cuối X.25 sẽ phát khởi tạo một VC (virtual circuit) tới địa chỉ đích. Sau khi VC được thiết lập, dữ liệu sẽ được truyền tải giữa hai điểm thông qua VC đó. Nếu nhu cầu dữ liệu lớn hơn, thiết bị đầu cuối sẽ khởi tạo thêm các VC mới. Khi hết giữ liệu, các VC sẽ được giải phóng cho các nhu cầu truyền tải khác.

X.25 qui định một số tham số xác định bao gồm:

- Độ lớn gói tin (ips/ops): là giá trị kích thước gói tin được quy định bởi nhà cung cấp dịch vụ.

- Độ lớn cửa sổ điều khiển luồng (win/wout): X.25 sử dụng cơ chế điều khiển luồng bằng cửa sổ để đảm bảo tốc độ gửi nhận tin phù hợp không làm mất mát thông tin. Với tham số cửa sổ bằng 7, X.25 cho phép gửi tối đa 7 gói tin khi chưa nhận được phúc đáp.

- Số lượng kênh VC tối đa cho chiều đến/hai chiều/chiều đi (hic/htc/hoc): Số lượng kênh VC được cung cấp cho mỗi thuê bao X.25 đã được xác định bởi nhà cung cấp. Thuê bao chỉ có thể truyền tải dữ liệu với số lượng các VC tối đa cho phép đã được xác định. Không thể thực hiện được yêu cầu truyền tải nếu có yêu cầu truyền tải tới các điểm mới khi số lượng VC đã hết. Khi các thiết bị đầu cuối X.25 thực hiện truyền tải dữ liệu nó phải tuân theo các quy tắc:

- o Cuộc gọi ra được thực hiện từ VC lớn nhất còn trống. Điều đó có nghĩa là, nếu chưa hề có cuộc gọi nào và số VC được cung cấp cho một thuê bao là 16 thì cuộc gọi ra đầu tiên sẽ khởi tạo VC số 16 để thực hiện yêu cầu kết nối. Trong trường hợp đã dùng hết 3 VC gọi ra thì cuộc gọi ra thứ 4 sẽ sử dụng VC số 13 để thực hiện.

- o Cuộc gọi tới được thực hiện từ VC nhỏ nhất còn trống. Tương tự như cuộc gọi ra, cuộc gọi vào đầu tiên sẽ nhận được trên VC số 1 và cuộc gọi vào thứ 10 sẽ nhận được trên VC số 10.

- o Quá trình khởi tạo VC sẽ dừng lại khi không còn VC trống.

- o Với các quy tắc này, yêu cầu cần thiết phải xác lập một cách chính xác các tham số cho thiết bị đầu cuối X.25 thì mới có thể thực hiện được các kết nối truyền tải dữ liệu.

Về đặc điểm của X.25

- Tốc độ truyền tải hạn chế, tại Việt Nam tốc độ cung cấp tối đa là 128Kbps.
- Độ trễ lớn, không phù hợp cho các ứng dụng có yêu cầu cao về độ trễ.
- Khả năng mở rộng dễ dàng, chi phí không cao.
- An toàn và bảo mật, vẫn được sử dụng trong các giao dịch ngân hàng.

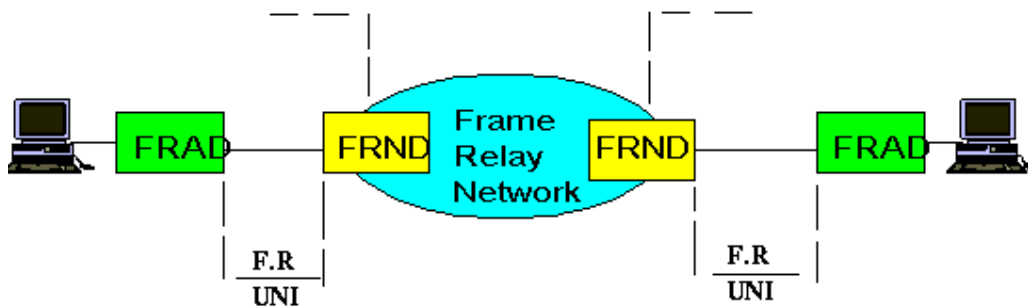
Frame Relay: Frame Relay ra đời trên nền tảng hạ tầng viễn thông ngày càng được cải thiện, không cần có quá nhiều các thủ tục phát hiện và sửa lỗi như X.25. Frame relay có thể chuyển nhận các khung lớn tới 4096 byte trong khi đó gói tiêu chuẩn của X.25 khuyến cáo dùng là 128 byte. Frame Relay rất thích hợp cho truyền số liệu tốc độ cao và cho kết nối LAN to LAN và cả cho âm thanh, nhưng điều kiện tiên quyết để sử dụng công nghệ Frame relay là chất lượng mạng truyền dẫn phải cao.

Bảng 3-9: So sánh giữa X.25 và Frame Relay

TT	Chức năng của mạng	X25	Frame relay
1	Phúc đáp khung thông tin nhận được	√	
2	Phúc đáp gói tin nhận được	√	
3	Dịch địa chỉ của gói tin	√	√
4	Cất giữ gói tin vào vùng đệm để chờ phúc đáp	√	
5	Phát hiện gói tin sai thứ tự	√	
6	Hủy gói tin bị lỗi	√	√
7	Đảm bảo khung tin có giá trị N(s) là hợp lệ	√	
8	Thiết lập và hủy bỏ kết nối logical	√	
9	Thiết lập và hủy bỏ kênh ảo	√	
10	Điền các bit cờ vào giữa các khung	√	
11	Điều khiển luồng dữ liệu ở lớp liên kết logic	√	
12	Tạo và kiểm tra FCS	√	√
13	Tạo và nhận dạng bit cờ	√	√
14	Tạo ra khung báo chưa sẵn sàng	√	
15	Tạo ra khung báo đã sẵn sàng	√	

√16	Tạo ra khung báo khung bị từ chối	√	
17	Quản lý các bit D, M, Q trong gói tin	√	
18	Quản lý các khung ở mức liên kết dữ liệu	√	
19	Quản lý các bộ định thời ở mức 3	√	
20	Quản lý các bit Poll/Final trong khung	√	
21	Quản lý các bộ đếm số thứ tự của khung và gói tin	√	
22	Ghép các kênh logic	√	
23	Quản lý các thủ tục khởi động ở mức 2 và 3	√	
24	Nhận dạng các khung không hợp lệ	√	√
25	Trả lời các khung và gói tin báo chưa sẵn sàng	√	
26	Trả lời các khung và gói tin báo đã sẵn sàng	√	
27	Trả lời các khung và gói tin báo từ chối khung	√	
28	Đánh dấu số lần phải truyền lại	√	
29	Chèn thêm và bỏ các bit 0 vào số liệu	√	√

Bảng chức năng trên cho thấy Frame relay đã giảm rất nhiều các công việc không cần thiết cho thiết bị chuyển mạch do đó giảm gánh nặng cũng như thời gian xử lý công việc cho các nút mạng, nhờ vậy mà làm giảm thời gian trễ cho các khung thông tin khi truyền trên mạng.



Hình 3.28: Mô hình mạng Frame Relay

Cơ sở để tạo được mạng Frame relay là các thiết bị truy nhập mạng FRAD (Frame Relay Access Device), các thiết bị mạng FRND (Frame Relay Network Device), đường nối giữa các thiết bị và mạng trực Frame Relay.

Thiết bị FRAD có thể là các LAN bridge, LAN Router v.v...

Thiết bị FRND có thể là các Tổng đài chuyển mạch khung (Frame) hay tổng đài chuyển mạch tế bào (Cell Relay - chuyển tải tổng hợp các tế bào của các dịch vụ khác nhau như âm thanh, truyền số liệu, video v.v..., mỗi tế bào độ dài 53 byte, đây là phương thức của công nghệ ATM). Đường kết nối giữa các thiết bị là giao diện chung cho FRAD và FRND, giao thức người dùng và mạng hay gọi F.R UNI (Frame Relay User Network Interface). Mạng trực Frame Relay cũng tương tự như các mạng viễn thông khác có nhiều tổng đài kết nối với nhau trên mạng truyền dẫn, theo thủ tục riêng của mình.

Công nghệ Frame Relay có một ưu điểm đặc trưng rất lớn là cho phép người sử dụng dùng tốc độ cao hơn mức họ đăng ký trong một khoảng thời gian nhất định, có nghĩa là Frame Relay không cố định độ rộng băng cho từng cuộc gọi một mà phân phối băng thông một cách linh hoạt điều mà X.25 và thuê kênh riêng không có. Ví dụ người sử dụng hợp đồng sử dụng với tốc độ 64Kbps, khi họ chuyển đi một lượng thông tin quá lớn, Frame Relay cho phép truyền chúng ở tốc độ cao hơn 64Kbps. Hiện tượng này được gọi là bùng nổ Bursting.

Các đặc điểm của Frame Relay:

- Cung cấp các kết nối thông qua các kênh ảo cố định PVC. Khi có nhu cầu kết nối giữa 2 điểm, nhà cung cấp dịch vụ sẽ thiết lập các thông số trên các node Frame Relay tạo ra các kênh ảo cố định giữa 2 điểm. Không như X.25, hướng kết nối Frame Relay là cố định và không thể khởi tạo bởi người dùng. Khi có nhu cầu kết nối đến điểm đích khác, khách hàng phải thuê mới PVC đến điểm đích mới đó.

- CIR (Committed Information Rate): là tốc độ truyền dữ liệu mà nhà cung cấp dịch vụ cam kết sẽ đảm bảo cho khách hàng, điều đó có nghĩa là khách hàng sẽ được đảm bảo cung cấp đường truyền với đúng tốc độ yêu cầu. CIR được gắn liền với các PVC và độc lập giữa các PVC khác nhau. Nếu tắc nghẽn xảy ra thì khách hàng vẫn truyền được với tốc độ yêu cầu khi ký kết hợp đồng.

- Frame Relay hỗ trợ truyền số liệu khi có bùng nổ số liệu hay còn gọi là “bursty”, có nghĩa là lượng thông tin được gửi đi trong thời gian ngắn và với dung lượng lớn hơn dung lượng bình thường. Nói cách khác, khi có một nhu cầu truyền tải khối lượng dữ liệu lớn, mạng Frame Relay cho phép được thực hiện truyền tải dữ liệu với tốc độ lớn hơn tốc độ CIR đã mua của nhà cung cấp dịch vụ. Điều này đảm bảo cho khách hàng tiết kiệm được chi phí mà vẫn đảm bảo truyền dữ liệu với khối lượng lớn trong những điều kiện cần thiết đảm bảo lưu thông thông tin. Truyền dữ liệu bursty chỉ thực hiện được khi không có tắc nghẽn trên mạng.

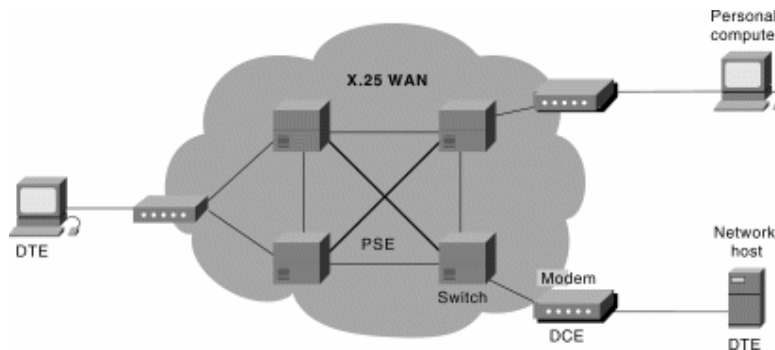
- Frame Relay không sử dụng địa chỉ định danh như X.25. Để phân biệt các PVC, Frame Relay sử dụng DLCI, mỗi một PVC được gắn liền với một DLCI. DLCI chỉ có tính chất cục bộ có nghĩa là chỉ có ý nghĩa quản lý trên cùng một chuyển mạch. Nói cách khác số DLCI chỉ cần là duy nhất cho mỗi PVC trên một chuyển mạch còn có thể có cùng số DLCI đó trên một chuyển mạch khác.

- Frame Relay sử dụng giao thức LMI (Local Management Interface) là giao thức quản lý và trao đổi thông tin quản trị giữa các thiết bị mạng FRND và các thiết bị kết nối FRAD.

- Cũng như X.25, Frame Relay là môi trường mạng đa truy nhập không quảng bá (multiaccess nonbroadcast media). Vấn đề này cần được chú ý khi sử dụng với các giao thức định tuyến.

Các mô hình kết nối của X.25 và Frame Relay

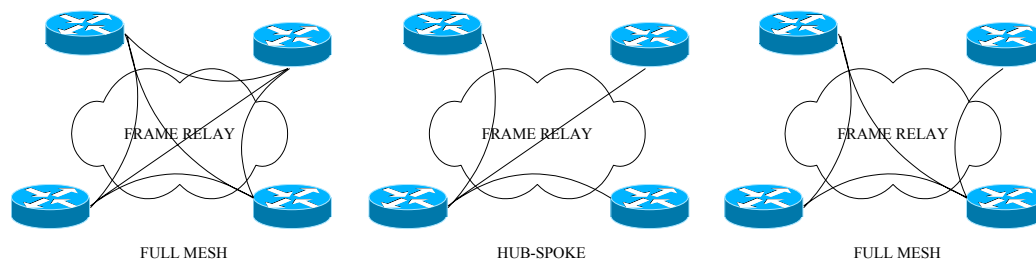
Khi sử dụng phương thức truyền thông X.25, mô hình kết nối cơ bản là điểm-đa điểm (point-to-multipoint) dựa trên tính chất cơ bản của X.25 là sử dụng các VC cho các nhu cầu truyền tải dữ liệu.



Hình 3.29: Mô hình kết nối X.25

Frame Relay đa dạng hơn về các mô hình kết nối. Frame Relay sử dụng các PVC định trước để thực hiện truyền tải dữ liệu giữa hai điểm, người ta chia Frame Relay thành các cấu hình kết nối mạng. Trong đó:

- Full mesh: là mô hình kết nối mà trong đó bất cứ hai node mạng nào cũng có một PVC liên kết giữa chúng. Mô hình này đảm bảo tính sẵn sàng cho toàn bộ hệ thống mạng, nếu có một hoặc một vài PVC có sự cố, các PVC còn lại vẫn có thể đảm bảo cho kết nối mạng giữa các node mạng. Yếu điểm của mô hình mạng này là chi phí thuê các PVC quá lớn.



Hình 3.30: Mô hình kết nối Frame Relay

- Hub-Spoke: là mô hình có một điểm tập trung mọi kết nối Frame Relay tới các điểm khác, các trao đổi dữ liệu giữa 2 điểm bất kỳ đều phải đi qua điểm tập trung. Mô hình này có chi phí giảm thiểu nhất nhưng có yếu điểm về việc tập trung mọi gánh nặng lên điểm tập trung và nếu có bất kỳ sự cố trên một PVC nào thì sẽ mất khả năng truyền tải dữ liệu với điểm thuộc về PVC bị sự cố đó.

- Partial mesh: là mô hình được sử dụng nhiều nhất, nó là sự lai ghép giữa hai mô hình trên, đảm bảo chi phí và dự phòng cho các điểm thiết yếu.

Cấu hình X.25 cơ bản

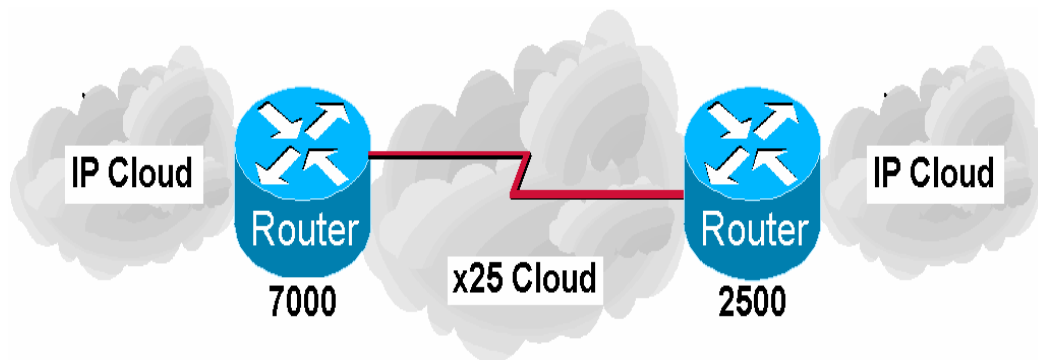
Các lưu ý trong cấu hình X.25

- X.25 là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động

- X.25 làm việc với sự khởi tạo các VC do đó khi thực hiện cấu hình phải thực hiện các thủ tục liên kết (map) và định tuyến theo địa chỉ

- Các tham số cần lưu ý

- o Độ lớn gói tin (ips/ops)
- o Độ lớn cửa sổ điều khiển luồng (win/wout)
- o Số lượng kênh VC tối đa cho chiều đến / hai chiều / chiều đi (hic/htc/hoc)
- o Số lượng VC dành cho một kết nối (nvc). Nên hạn chế số lượng VC cho phép kết nối đến một điểm trong giới hạn hợp lý để tổng số VC cần thiết không vượt quá số VC tối đa hiện có (HTC)
- o Khi thực hiện các liên kết (map) phải thực hiện map địa chỉ IP của phía đối phương tới địa chỉ X25 của họ
- o Khi thực hiện định tuyến, phải thực hiện định tuyến với địa chỉ IP next hop
- o Cấu hình mạng đầu nối X25 là cấu hình đa điểm, địa chỉ đầu nối phải nằm trong lớp mạng con đủ cho số lượng các điểm



Hình 3.31: Mô hình kết nối X.25 cơ bản

Cấu hình bộ định tuyến 7000

```
!  
interface Serial1/1  
 ip address 10.1.1.2 255.255.255.0  
 encapsulation x25  
 no ip mroute-cache
```



```
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
x25 address 4522973407000
!--- Các dòng lệnh dưới là các tham số X.25
x25 ips 256
x25 ops 256
x25 htc 16
x25 win 7
x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 2500 với
!địa chỉ X.121 của nó
x25 map ip 10.1.1.1 4522973402500
!
!
```

Hình 3.32: Cấu hình của bộ định tuyến 7000

```
Cấu hình bộ định tuyến 2500
!
hostname 2500
!
interface Serial0
 ip address 10.1.1.1 255.255.255.0
 no ip mroute-cache
 encapsulation x25
 bandwidth 56
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
x25 address 4522973402500
!--- Các dòng lệnh dưới là các tham số X.25
x25 ips 256
x25 ops 256
x25 htc 16
x25 win 7
x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 7000 với
!địa chỉ X.121 của nó
x25 map ip 10.1.1.1 4522973407000!
```

Hình 3.33: Cấu hình của bộ định tuyến 2500

- Giám sát:

- o Show interfaces serial 0: dùng để kiểm tra trạng thái
- o Show x25 vc: hiển thị thông tin kết nối X.25
- o Show x25 map: hiển thị các liên kết hiện có của FR

Cấu hình Frame Relay cơ bản

Các lưu ý trong cấu hình Frame Relay:

- Frame Relay là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động
- Khi sử dụng định tuyến động giao thức định tuyến vector như RIP, IGRP phải để ý đến luật Split Horizon. Luật Split Horizon là luật không cho phép các thông tin định tuyến vừa đi vào một giao tiếp đi trở ra chính giao tiếp đó để tránh việc cập nhật sai các thông tin về định tuyến dẫn đến việc vòng đi vòng lại của các thông tin định tuyến. Vấn đề này được đặt ra do có nhiều PVC cùng chạy trên một giao tiếp vật lý.
- Giám sát:
 - o `Show interfaces serial 0`: dùng để kiểm tra DLCI, LMI
 - o `Show frame-relay lmi`: hiển thị thông tin tổng hợp về LMI
 - o `Show frame-relay map`: hiển thị các liên kết hiện có của FR
 - o `Show frame-relay pvc`: hiển thị các thông số của PVC
 - o `Show frame-relay traffic`: hiển thị traffic



Hình 3.34: Mô hình kết nối Frame Relay cơ bản

- Để bắt đầu cấu hình mạng:
 - o Router> `enable` ↵
 - o Password: `*****` ↵
 - o Router# `config terminal` ↵
 - o Router(config)#
- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện
- Cấu hình
 - o Spicey(config)# `interface serial 0` ↵
- Lựa chọn giao thức sử dụng
 - o Spicey(config-if)# `encapsulation frame-relay` ↵
- Xác định giao thức quản trị LMI. Giao thức quản trị LMI nhất thiết phải có để đảm bảo việc trao đổi thông tin hai chiều giữa thiết bị đầu cuối và thiết bị mạng Frame Relay. LMI hoạt động như một thông báo keepalive.

- 0 Spicey(config-if)# frame-relay lmi-type cisco ↵
- Gán DLCI được cấp cho giao tiếp.
 - 0 Spicey(config-if)# frame-relay interface-dlci 140 ↵
- Đặt địa chỉ IP cho giao tiếp kết nối leased-line
 - 0 Spicey(config-if)# ip address 3.1.3.1 255.255.255.0 ↵
- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown
 - 0 Spicey(config-if)# no shutdown ↵
 - 0 Spicey(config-if)# exit ↵
- Sử dụng định tuyến động RIP
 - 0 Spicey(config)# router rip ↵
 - 0 Spicey(config-router)# network 3.0.0.0 ↵
 - 0 Spicey(config-router)# network 124.0.0.0 ↵
 - 0 Spicey(config-router)# end ↵
- Luôn phải ghi lại cấu hình khi đã cấu hình xong
 - 0 Spicey# write memory ↵
- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

```
Current configuration : 1705 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
interface Serial0
 ip address 3.1.3.1 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 140
!
!
router rip
 network 3.0.0.0
 network 124.0.0.0
```

```
!  
line con 0  
    exec-timeout 0 0  
    transport input none  
line aux 0  
line vty 0 4  
    login  
!  
end
```

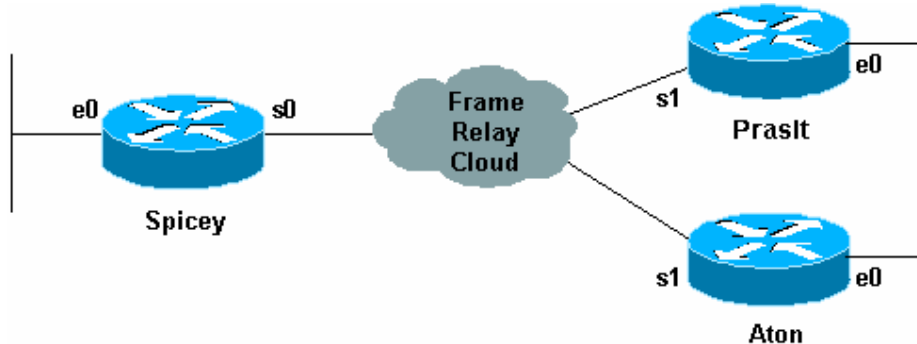
Hình 3.35: Cấu hình của bộ định tuyến Spicey

Cấu hình bộ định tuyến Prasit

```
Current configuration : 1499 bytes  
!  
version 12.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Prasit  
!  
!  
!  
interface Ethernet0  
    ip address 123.123.123.1 255.255.255.0  
!  
!  
interface Serial1  
    ip address 3.1.3.2 255.255.255.0  
    encapsulation frame-relay  
    frame-relay interface-dlci 150  
!  
!  
router rip  
    network 3.0.0.0  
    network 123.0.0.0  
!  
!  
line con 0  
    exec-timeout 0 0  
    transport input none
```

```
line aux 0
line vty 0 4
  login
!
end
```

Hình 3.36: Cấu hình của bộ định tuyến Prasit



Hình 3.37: Mô hình kết nối Frame Relay Hub-Spoke

- Cấu hình

```
0 Spicey(config)# interface serial 0 ↵
```

- Lựa chọn giao thức sử dụng

```
0 Spicey(config-if)# encapsulation frame-relay ↵
```

- Xác định giao thức quản trị LMI. Lưu ý trong ví dụ này có sử dụng một chuẩn kết nối LMI khác. Chuẩn kết nối LMI không có giá trị toàn cục mà chỉ có giá trị tại giao tiếp của thiết bị đầu cuối với mạng Frame Relay. Trong cấu hình của các bộ định tuyến khác vẫn sử dụng LMI chuẩn cisco.

```
0 Spicey(config-if)# frame-relay lmi-type ansi ↵
```

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

```
0 Spicey(config-if)# no shutdown ↵
```

- Trong ví dụ này, sử dụng giao tiếp con, subinterface, nên không đặt địa chỉ cho giao tiếp thực, physical interface.

- Cấu hình giao tiếp con. Giao tiếp con phải sử dụng một trong hai lựa chọn là point-to-point hoặc multipoint, ở đây sử dụng point-to-point cho giao tiếp con s0.1 và multipoint cho giao tiếp con s0.2.

```
0 Spicey(config-if)# interface serial 0.1 point-to-point ↵
```

- Hoặc

```
0 Spicey(config-if)# exit ↵
```

```
0 Spicey(config)# interface serial 0.1 point-to-point ↵
```

- Gán DLCI được cấp cho giao tiếp. DLCI 140 là DLCI gắn với PVC nối giữa Spicey và Prasit, còn DLCI 130 gắn với PVC nối tới Aton.

```
0 Spicey(config-if)# frame-relay interface-dlci 140 ↵
```

- Xác lập địa chỉ IP cho giao tiếp con thứ nhất

```
0 Spicey(config-subif)# ip address 4.0.1.1 255.255.255.0 ↵
```

```
0 Spicey(config-subif)# exit ↵
```

- Cấu hình giao tiếp con thứ hai tới Aton

```
0 Spicey(config)# interface serial 0.2 multipoint ↵
```

- Gán DLCI được cấp cho giao tiếp là DLCI 130

```
0 Spicey(config-if)# frame-relay interface-dlci 130 ↵
```

- Xác lập địa chỉ IP cho giao tiếp con thứ 2

```
0 Spicey(config-subif)# ip address 3.1.3.1 255.255.255.0 ↵
```

```
0 Spicey(config-subif)# exit ↵
```

- Sử dụng định tuyến động RIP

```
0 Spicey(config)# router rip ↵
```

```
0 Spicey(config-router)# network 3.0.0.0 ↵
```

```
0 Spicey(config-router)# network 4.0.0.0 ↵
```

```
0 Spicey(config-router)# network 124.0.0.0 ↵
```

```
0 Spicey(config-router)# end ↵
```

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

```
0 Spicey# write memory ↵
```

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

```
Spicey#show running-config
Building configuration...
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
```

```
interface Serial0
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
  ip address 4.0.1.1 255.255.255.0
  frame-relay interface-dlci 140
!
interface Serial0.2 multipoint
  ip address 3.1.3.1 255.255.255.0
  frame-relay interface-dlci 130
!
router igrp 2
  network 3.0.0.0
  network 4.0.0.0
  network 124.0.0.0
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line vty 0 4
  login
!
end
```

Hình 3.38: Cấu hình của bộ định tuyến Spicey

Cấu hình bộ định tuyến Prasit

```
Prasit#show running-config
Building configuration...

version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
interface Ethernet0
  ip address 123.123.123.1 255.255.255.0
```

```
!  
interface Serial1  
  no ip address  
  encapsulation frame-relay  
!  
!--- LMI cisco là mặc định nên không thể hiện trong cấu hình  
!--- Prasit và Spicey đã sử dụng 2 kiểu LMI khác nhau  
!--- Bộ định tuyến tại Prasit sử dụng giao tiếp con point-to-point  
interface Serial1.1 point-to-point  
  ip address 4.0.1.2 255.255.255.0  
  frame-relay interface-dlci 150  
!  
router igrp 2  
  network 4.0.0.0  
  network 123.0.0.0  
!  
!  
line con 0  
  exec-timeout 0 0  
  transport input none  
line aux 0  
line vty 0 4  
  login  
!  
end
```

Hình 3.39: Cấu hình của bộ định tuyến Prasit

Cấu hình bộ định tuyến Aton

```
Aton#show running-config  
Building configuration...  
  
Current configuration:  
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
!  
hostname Aton  
!  
!  
!
```



```
interface Ethernet0
 ip address 122.122.122.1 255.255.255.0
!
interface Serial1
 ip address 3.1.3.3 255.255.255.0
 encapsulation frame-relay
 frame-relay lmi-type q933a
!--- Aton có kiểu LMI khác hai bộ định tuyến kia
!--- Aton không sử dụng giao tiếp con. Giao tiếp con cần xác định
!là point-to-point hay multipoint ở bộ định tuyến trung tâm
!còn ở các bộ định tuyến còn lại có thể dùng giao tiếp con
!point-to-point hay giao tiếp thực, physical interface
 frame-relay interface-dlci 160
!
router igrp 2
 network 3.0.0.0
 network 122.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.40: Cấu hình của bộ định tuyến Aton

4.3. Cấu hình Dial-up

Giới thiệu quay số

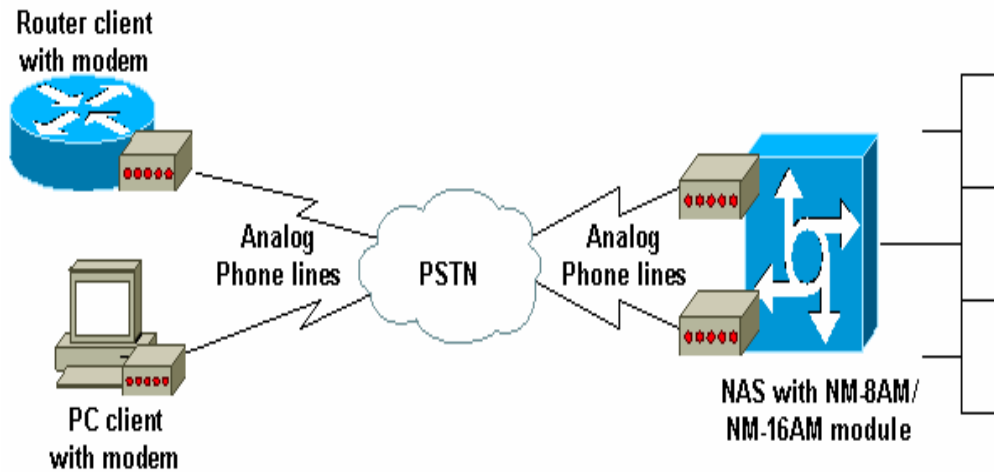
Kết nối quay số cho phép sử dụng đường điện thoại để kết nối trao đổi dữ liệu. Tốc độ của kết nối quay số là không cao và chỉ có thể đáp ứng được cho các ứng dụng không yêu cầu về băng thông cũng như thời gian trễ.

Kết nối quay số sử dụng modem V34, V90 là phổ biến. Tốc độ truyền dữ liệu lên mạng và tải dữ liệu về tối đa là 33,6Kbps. Để có thể thực hiện tải về với tốc độ lớn hơn, tới 56Kbps, bộ định tuyến đóng vai trò điểm truy nhập phải có kết nối thuê bao dạng số và dùng modem số.

Đối với các doanh nghiệp nhỏ, việc xác thực người dùng có thể thực hiện bằng cách khai báo dữ liệu trực tiếp trên bộ định tuyến. Cách sử dụng này không thích hợp cho các doanh nghiệp vừa và lớn hay các doanh nghiệp cần có sự quản lý chặt chẽ người dùng một cách hệ thống. Lúc này cần thiết có các hệ

thống quản lý người dùng. Các bộ định tuyến của Cisco cho phép sử dụng hai chuẩn xác thực TACACS+ và RADIUS.

Mô hình sử dụng quay số



Hình 3.41: Cấu hình của bộ định tuyến Aton

Cấu hình quay số cơ bản

Danh mục công việc:

- Cấu hình giao tiếp không đồng bộ Async
- Cấu hình giao tiếp điều khiển modem
- Cấu hình xác thực
- Giám sát

```
0 Router#show interface Async 1
0 Router#show line 1
0 Router#debug ppp authentication
```

Cấu hình quay số cơ bản

```
Current configuration : 1251 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname cisco3640
!
boot system flash:c3640-i-mz.122-8.T
```

```
enable secret 5 <đã xóa>
!
! --- Tên truy nhập cho xác thực người dùng cục bộ
username abc password 0 abc
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
!
! --- Xác định địa chỉ máy chủ DNS cho các máy trạm quay số
async-bootp DNS-server 5.5.5.1 5.5.5.2
!
!
interface Loopback0
    ip address 1.1.1.1 255.255.255.0
!
interface Ethernet2/0
    ip address 20.20.20.1 255.255.255.0
    half-duplex
!
! <<--các giao tiếp không dùng được bỏ đi
!
!--- Giao tiếp Group-Async1 cấu hình cho tất cả các các modem
!--- không cần cấu hình riêng rẽ từng modem
interface Group-Async1
    ip unnumbered Loopback0
    encapsulation ppp
    dialer in-band
!--- Xác lập thời gian không sử dụng là 10 phút
!--- sau thời gian này, bộ định tuyến sẽ tự động cắt kết nối
    dialer idle-timeout 600
!--- Định nghĩa các loại hình dữ liệu được dùng
!--- thông qua cấu hình dialer-group và dialer-list
    dialer-group 1
!--- Chế độ interactive cho phép người dùng sử dụng nhiều giao thức
!--- để không cho phép người dùng thiết lập các kết nối đến bộ định
tuyến sử dụng chế độ dedicated
    async mode interactive
!--- Các máy trạm khi quay số vào sẽ được cấp địa chỉ IP
!--- được qui định trong DIALIN
    peer default ip address pool DIALIN
    ppp authentication chap
```

```
!--- Xác lập các modem từ line 1 đến line 8 thuộc về nhóm này
group-range 1 8
!
ip local pool DIALIN 10.1.1.1 10.1.1.10
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.100
ip http server
ip pim bidir-enable
!
!--- Dòng lệnh sau cho phép giao thức IP là giao thức hoạt động
!--- nếu không có các dữ liệu IP đi qua sau khoảng thời gian 10 phút
!--- đường kết nối sẽ bị cắt
dialer-list 1 protocol ip permit
!
line con 0
  password abc
line 1 8
!--- Dòng lệnh dưới cho phép modem quay vào và quay ra
  modem InOut
  transport input all
  autoselect ppp
  flowcontrol hardware
line aux 0
line vty 0 4
  login
!
!
end
```

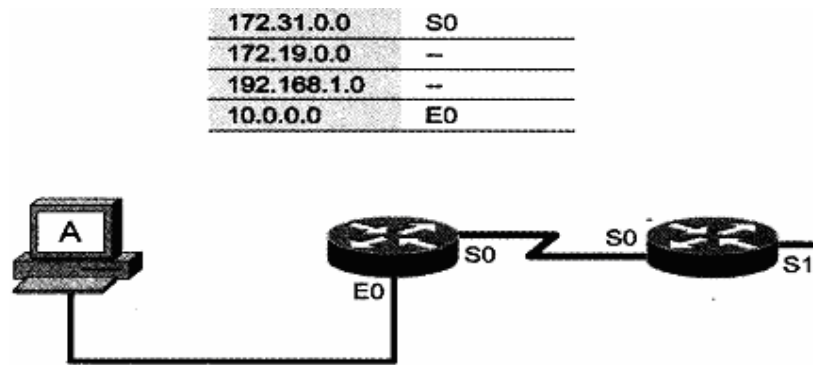
Hình 3.42: Cấu hình quay số cơ bản

4.4. Định tuyến tĩnh và động

Sơ lược về định tuyến

Chức năng xác định đường dẫn cho phép bộ định tuyến ước lượng các đường dẫn khả thi để đến đích và thiết lập sự kiểm soát các gói tin. Bộ định tuyến sử dụng các cấu hình mạng để đánh giá các đường dẫn mạng. Thông tin này có thể được cấu hình bởi người quản trị mạng hay được thu thập thông qua quá trình xử lý động được thực thi trên mạng.

Lớp mạng dùng bảng định tuyến IP để gửi các gói tin từ mạng nguồn đến mạng đích. Bộ định tuyến dựa vào các thông tin được giữ trong bảng định tuyến để quyết định truyền tải các gói tin theo các giao tiếp thích hợp.



Hình 3.43: Sử dụng bảng định tuyến để truyền tải các gói tin

Một bảng định tuyến IP bao gồm các địa chỉ mạng đích, địa chỉ của điểm cần đi qua, giá trị định tuyến và giao tiếp để thực hiện việc truyền tải. Khi không có thông tin về mạng đích, bộ định tuyến sẽ gửi các gói tin theo một đường dẫn mặc định được cấu hình trên bộ định tuyến, nếu đường dẫn không tồn tại, bộ định tuyến tự động loại bỏ gói tin.

Có hai phương thức định tuyến là:

- Định tuyến tĩnh (static routing): là cách định tuyến không sử dụng các giao thức định tuyến. Các định tuyến đến một mạng đích sẽ được thực hiện một cách cố định không thay đổi trên mỗi bộ định tuyến. Mỗi khi thực hiện việc thêm hay bớt các mạng, phải thực hiện thay đổi cấu hình trên mỗi bộ định tuyến.

- Định tuyến động (dynamic routing): là việc sử dụng các giao thức định tuyến để thực hiện xây dựng nên các bảng định tuyến trên các bộ định tuyến. Các bộ định tuyến thông qua các giao thức định tuyến sẽ tự động trao đổi các thông tin định tuyến, các bảng định tuyến với nhau. Mỗi khi có sự thay đổi về mạng, chỉ cần khai báo thông tin mạng mới trên bộ định tuyến quản lý trực tiếp mạng mới đó mà không cần phải khai báo lại trên mỗi bộ định tuyến. Một số giao thức định tuyến động được sử dụng là RIP, RIPv2, OSPF, EIGRP v.v...

Giá trị định tuyến được xây dựng tùy theo các giao thức định tuyến khác nhau. Giá trị định tuyến của các kết nối trực tiếp và định tuyến tĩnh có giá trị nhỏ nhất bằng 0, đối với định tuyến động thì giá trị định tuyến được tính toán tùy thuộc và từng giao thức cụ thể. Giá trị định tuyến được thể hiện trong bảng định tuyến là giá trị định tuyến tốt nhất đã được bộ định tuyến tính toán và xây dựng nên trên cơ sở các giao thức định tuyến được cấu hình và giá trị định tuyến của từng giao thức.

Các giao thức định tuyến động được chia thành 2 nhóm chính:

- **Các giao thức định tuyến khoảng cách véc tơ** (distance-vecto, sau đây được gọi tắt là *định tuyến vector*): dựa vào các giải thuật định tuyến có cơ sở hoạt động là khoảng cách véc tơ.

Theo định kỳ các bộ định tuyến chuyển toàn bộ các thông tin có trong bảng định tuyến đến các bộ định tuyến láng giềng đầu nối trực tiếp với nó và

cũng theo định kỳ nhận các bảng định tuyến từ các bộ định tuyến láng giềng. Sau khi nhận được các bảng định tuyến từ các bộ định tuyến láng giềng, bộ định tuyến sẽ so sánh với bảng định tuyến hiện có và quyết định về việc xây dựng lại bảng định tuyến theo thuật toán của từng giao thức hay không. Trong trường hợp phải xây dựng lại, bộ định tuyến sau đó sẽ gửi bảng định tuyến mới cho các láng giềng và các láng giềng lại thực hiện các công việc tương tự. Các bộ định tuyến tự xác định các láng giềng trên cơ sở thuật toán và các thông tin thu lượm từ mạng.

Từ việc cần thiết phải gửi các bảng định tuyến mới lại cho các láng giềng và các láng giềng sau khi xây dựng lại bảng định tuyến lại gửi trở lại bảng định tuyến mới, định tuyến thành vòng có thể xảy ra nếu sự hội về trạng thái bền vững của mạng diễn ra chậm trên một cấu hình mới. Các bộ định tuyến sử dụng các kỹ thuật bộ đếm định thời để đảm bảo không nảy sinh việc xây dựng một bảng định tuyến sai. Có thể diễn giải điều đó như sau:

- o Khi một bộ định tuyến nhận một cập nhật từ một láng giềng chỉ rằng một mạng có thể truy xuất trước đây, nay không thể truy xuất được nữa, bộ định tuyến đánh dấu tuyến là không thể truy xuất và khởi động một bộ định thời.

- o Nếu tại bất cứ thời điểm nào mà trước khi bộ định thời hết hạn một cập nhật được tiếp nhận cũng từ láng giềng đó chỉ ra rằng mạng đã được truy xuất trở lại, bộ định tuyến đánh dấu là mạng có thể truy xuất và giải phóng bộ định thời.

- o Nếu một cập nhật đến từ một bộ định tuyến láng giềng khác với giá trị định tuyến tốt hơn giá trị định tuyến được ghi cho mạng này, bộ định tuyến đánh dấu mạng có thể truy xuất và giải phóng bộ định thời. Nếu giá trị định tuyến tồi hơn, cập nhật được bỏ qua.

- o Khi bộ định thời được đếm về 0, giá trị định tuyến mới được xác lập, bộ định tuyến có bảng định tuyến mới.

- **Các giao thức định tuyến trạng thái đường** (link-state, gọi tắt là *định tuyến trạng thái*): Giải thuật cơ bản thứ hai được dùng cho định tuyến là giải thuật link-state. Các giải thuật định tuyến trạng thái, cũng được gọi là SPF (shortest path first, *chọn đường dẫn ngắn nhất*), duy trì một cơ sở dữ liệu phức tạp chứa thông tin về cấu hình mạng.

- Trong khi giải thuật vector không có thông tin đặc biệt gì về các mạng ở xa và cũng không biết các bộ định tuyến ở xa, giải thuật định tuyến trạng thái biết được đầy đủ về các bộ định tuyến ở xa và biết được chúng liên kết với nhau như thế nào.

Giao thức định tuyến trạng thái sử dụng:

- o Các thông báo về trạng thái liên kết: LSA (Link State Advertisements).
- o Một cơ sở dữ liệu về cấu hình mạng.
- o Giải thuật SPF, và cây SPF sau cùng.
- o Một bảng định tuyến liên hệ các đường dẫn và các cổng đến từng mạng.

Hoạt động tìm hiểu khám phá mạng trong định tuyến trạng thái được thực hiện như sau:

- o Các bộ định tuyến trao đổi các LSA cho nhau. Mỗi bộ định tuyến bắt đầu với các mạng được kết nối trực tiếp để lấy thông tin.

- o Mỗi bộ định tuyến đồng thời với các bộ định tuyến khác tiến hành xây dựng một cơ sở dữ liệu về cấu hình mạng bao gồm tất cả các LSA đến từ liên mạng.

- o Giải thuật SPF tính toán mạng có thể đạt đến. Bộ định tuyến xây dựng cấu hình mạng luận lý này như một cây, tự nó là gốc, gồm tất cả các đường dẫn có thể đến mỗi mạng trong toàn bộ mạng đang chạy giao thức định tuyến trạng thái. Sau đó, nó sắp xếp các đường dẫn này theo chiến lược chọn đường dẫn ngắn nhất.

- o Bộ định tuyến liệt kê các đường dẫn tốt nhất của nó, và các cổng dẫn đến các mạng đích, trong bảng định tuyến của nó. Nó cũng duy trì các cơ sở dữ liệu khác về các phần tử cấu hình mạng và các chi tiết về hiện trạng của mạng.

Khi có thay đổi về cấu hình mạng, bộ định tuyến đầu tiên nhận biết được sự thay đổi này gửi thông tin đến các bộ định tuyến khác hay đến một bộ định tuyến định trước được gán là tham chiếu cho tất cả các bộ định tuyến trên mạng làm căn cứ cập nhật.

- o Theo dõi các láng giềng của nó, xem xét có hoạt động hay không, và giá trị định tuyến đến láng giềng đó.

- o Tạo một gói LSA trong đó liệt kê tên của tất cả các bộ định tuyến láng giềng và các giá trị định tuyến đối với các láng giềng mới, các thay đổi trong giá trị định tuyến, và các liên kết dẫn đến các láng giềng đã được ghi.

- o Gửi gói LSA này đi sao cho tất cả các bộ định tuyến đều nhận được.

- o Khi nhận một gói LSA, ghi gói LSA vào cơ sở dữ liệu để sao cho cập nhật gói LSA mới nhất được phát ra từ mỗi bộ định tuyến.

- o Hoàn thành bản đồ của liên mạng bằng cách dùng dữ liệu từ các gói LSA tích lũy được và sau đó tính toán các tuyến dẫn đến tất cả các mạng khác sử dụng thuật toán SPF.

Có hai vấn đề lưu ý đối với giao thức định tuyến trạng thái:

- o Hoạt động của các giao thức định tuyến trạng thái trong hầu hết các trường hợp đều yêu cầu các bộ định tuyến dùng nhiều bộ nhớ và thực thi nhiều hơn so với các giao thức định tuyến theo vector. Các yêu cầu này xuất phát từ việc cần thiết phải lưu trữ thông tin của tất cả các láng giềng, cơ sở dữ liệu mạng đến từ các nơi khác và việc thực thi các thuật toán định tuyến trạng thái. Người quản lý mạng phải đảm bảo rằng các bộ định tuyến mà họ chọn có khả năng cung cấp các tài nguyên cần thiết này.

- o Các nhu cầu về băng thông cần phải tiêu tốn để khởi động sự phát tán gói trạng thái. Trong khi khởi động quá trình khám phá, tất cả các bộ định tuyến dùng các giao thức định tuyến trạng thái để gửi các gói LSA đến tất cả

các bộ định tuyến khác. Hành động này làm tràn ngập mạng khi mà các bộ định tuyến đồng loạt yêu cầu bảng thông và tạm thời làm giảm lượng băng thông khả dụng dùng cho lưu lượng dữ liệu thực được định tuyến. Sau khởi động phát tán này, các giao thức định tuyến trạng thái thường chỉ yêu cầu một lượng băng thông tối thiểu để gửi các gói LSA kích hoạt sự kiện không thường xuyên nhằm phản ánh sự thay đổi của cấu hình mạng.

- **Và một nhóm giao thức thứ 3** là nhóm các giao thức định tuyến lai ghép giữa 2 nhóm trên hay nói cách khác có các tính chất của cả hai nhóm giao thức trên.

Các giao thức định tuyến

Bảng 3-10: Các giao thức định tuyến

Các đặc trưng	RIPv1	RIPv2	IRGP	EIGRP	OSPF
Khoảng cách vector	X	X	x	x	
Trạng thái đường					x
Tự động tóm tắt định tuyến	X	X	x	x	
Hỗ trợ VLSM ¹		X		x	x
Tương thích với sản phẩm thứ ba	X	X			X
Thích hợp	Nhỏ	Nhỏ	Vừa	Lớn	Lớn
Thời gian hội tụ về trạng thái cân bằng	Chậm	Chậm	Chậm	Nhanh	Nhanh
Giá trị định tuyến	hop count ²	hop count	~ BW ³ +D ⁴	~ BW+D	~ 10E8/BW
Giới hạn hop count	15	15	100	100	
Cân bằng tải cùng giá trị định tuyến	X	X	x	x	X

¹ VLSM (Vary Length Subnet Mask): hỗ trợ định tuyến cho các mạng con subnetmask có độ dài thay đổi hay nói cách khác thông tin về subnetmask bao gồm trong bảng định tuyến

² Hop count: được tính bằng số các điểm node mạng mà gói tin phải đi qua từ điểm này đến điểm kia hay chính bằng số các bộ định tuyến mà gói tin phải đi qua

³ BW (bandwidth): băng thông

⁴ D (delay): trễ

Cân bằng tải không cùng giá trị định tuyến			x	x	
Thuật toán	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra

Cấu hình định tuyến động cơ bản với RIP

Một số lưu ý khi cấu hình định tuyến động với RIP

- RIP gửi các thông tin cập nhật theo các chu kỳ định trước, giá trị mặc định là 30 giây, và khi có sự thay đổi bảng định tuyến.
- RIP sử dụng số đếm các node (hop count) để làm giá trị đánh giá chất lượng của định tuyến (metric). RIP chỉ giữ duy nhất định tuyến có giá trị định tuyến thấp nhất.
- Giá trị hop count tối đa cho phép là 15.
- RIP sử dụng các bộ đếm thời gian cho việc thực hiện gửi các thông tin cập nhật, xoá bỏ một định tuyến trong bảng cũng như để điều khiển các quá trình tạo lập bảng định tuyến, tránh loop vòng.
- RIPv1: Classfull: không có thông tin về subnetmask
- RIPv2: Classless: có thông tin về subnetmask

Cấu hình định tuyến với RIP:

- Cho phép giao thức định tuyến RIP hoạt động trên bộ định tuyến.

```
0 Router(config)#router rip
```
- Thiết lập các cấu hình mạng. Network là nhóm mạng tính theo lớp mạng cơ bản đang có các giao tiếp trực tiếp trên bộ định tuyến.

```
0 Router(config-router)#network 192.168.100.0
0 Router(config-router)#network 172.25.0.0
0 Router(config-router)#network 10.0.0.0
```
- Trong trường hợp sử dụng RIP với các mạng không phải là mạng broadcast như X.25, Frame Relay cần thiết cấu hình RIP với các địa chỉ Unicast là các địa chỉ mà RIP sẽ gửi tới các thông tin cập nhật

```
0 Router(config-router)#neighbor 192.168.113.1
0 Router(config-router)#neighbor 192.168.113.5
```
- Tuỳ theo điều kiện cụ thể về hạ tầng mạng có thể thay đổi chu kỳ cập nhật thông tin, các định nghĩa thời gian khác cho phù hợp.

```
0 Router(config-router)# timers basic update invalid holddown flush [sleeptime]
```
- Các thay đổi khác.

```
0 Router(config-router)# version {1 | 2}
0 Router(config-router)# ip rip authentication key-chain name-of-chain
0 Router(config-router)# ip rip authentication mode {text | md5}
```

- Giám sát.
- ```
0 show ip interfaces
0 show ip rip
```

**Cấu hình bộ định tuyến với RIP**

```
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
end
```

*Hình 3.44: Cấu hình của bộ định tuyến với RIP*

## 5. Bộ chuyển mạch lớp 3

### 5.1. Tổng quan và kiến trúc bộ chuyển mạch lớp 3

#### Tổng quan

Bộ chuyển mạch lớp 3 là một trong các thiết bị mạng được phát triển mới trên các công nghệ ngày càng tiên tiến. Bộ chuyển mạch lớp 3, như tên gọi của nó, bao gồm các chức năng xử lý gói tin hoạt động trên lớp 3, lớp mạng, trong mô hình 7 lớp OSI, thực hiện các chức năng định tuyến và xử lý gói tin tương tự bộ định tuyến đồng thời thực hiện chuyển mạch gói tin ở lớp 2 như các bộ chuyển

mạch lớp 2, khác hẳn với thể hệ trước đây của nó chỉ thực hiện các xử lý chuyển mạch gói tin ở lớp 2 căn cứ trên các địa chỉ MAC của gói tin.

Khi nhận được gói tin, bộ định tuyến sẽ thực hiện xem xét các thông tin lớp 3 của gói tin để lựa chọn đường đi cho gói tin còn bộ chuyển mạch thì chỉ căn cứ vào địa chỉ lớp 2, địa chỉ MAC, để thực hiện chuyển gói tin. Sự khác nhau cơ bản giữa bộ định tuyến và bộ chuyển mạch lớp 3 là bộ chuyển mạch lớp 3 được cấu thành từ các phần cứng chuyên dụng được thiết kế riêng cho bộ chuyển mạch cho phép thực hiện các chuyển mạch gói tin nhanh như các chuyển mạch lớp 2, điều không có ở các bộ định tuyến, trong khi vẫn có khả năng xử lý định tuyến các gói tin với chức năng tương tự như bộ định tuyến.

Trong môi trường LAN, bộ chuyển mạch lớp 3 được đánh giá là nhanh hơn so với bộ định tuyến và làm tăng năng lực hoạt động của mạng trên cơ sở năng lực chuyển mạch và định tuyến của nó. Tuy nhiên, bộ chuyển mạch lớp 3 không thể thay thế hoàn toàn cho bộ định tuyến do đặc trưng LAN của bộ chuyển mạch lớp 3 và không hoạt động trên môi trường đa giao thức như bộ định tuyến.

Chức năng và kiến trúc của bộ chuyển mạch lớp 3 cũng tương tự như bộ định tuyến và bao gồm:

- Chuyển mạch gói tin
- Các hoạt động định tuyến
- Tính năng mạng thông minh

### **Chuyển mạch gói tin**

Chuyển mạch gói tin là chức năng cơ bản chính của bộ chuyển mạch lớp 3. Điều khác nhau cơ bản giữa bộ định tuyến và bộ chuyển mạch lớp 3 chính là bộ định tuyến dùng bộ xử lý trung tâm để thực hiện các xử lý chuyển mạch gói tin còn bộ chuyển mạch lớp 3 dùng các thành phần phần cứng được thiết kế chuyên dụng ASIC (Application Specific Integrated Circuit).

Thành phần chức năng chuyển mạch gói tin của bộ chuyển mạch thực hiện các công việc kiểm tra địa chỉ gói tin, so sánh với thông tin lưu trữ và thực hiện truyền tải chúng theo hướng xác định. Chúng đồng thời cũng thực hiện các xử lý lớp dưới tương tự bộ định tuyến với việc gán lại các địa chỉ MAC, giảm số đếm TTL... Chức năng chuyển mạch gói tin cũng thực hiện phép so sánh đúng nhất để lựa chọn đường đi đúng khi có nhiều hơn một khả năng để lựa chọn.

### **Các hoạt động định tuyến**

Hoạt động định tuyến là một hoạt động độc lập khác so với hoạt động chuyển mạch gói tin. Bộ định tuyến cũng như bộ chuyển mạch lớp 3 quản lý và điều hành các thông tin định tuyến, xây dựng, cập nhật và trao đổi chúng thông qua các giao thức định tuyến mỗi khi có sự thay đổi về mạng như lỗi đường, thêm mới hay cập nhật thiết bị...

Cũng như các bộ định tuyến, bộ chuyển mạch lớp 3 hoạt động với hầu hết các giao thức định tuyến động hiện có.

### **Tính năng mạng thông minh**

Các tính năng quản trị, cấp phát động, các tính năng định tuyến thông minh, các tính năng bảo mật, xác thực cũng được thiết kế và xây dựng trên bộ định tuyến lớp 3 qua đó dễ dàng cho người quản trị thực hiện việc xây dựng, quản trị và phát triển mạng.

## 5.2. Định tuyến trên bộ chuyển mạch lớp 3

### VLAN

VLAN là khái niệm để chỉ một mạng LAN độc lập một cách logic với nhau. Về thực chất, tất cả các thiết bị mạng được đấu nối và hoạt động trên cùng một môi trường vật lý, hạ tầng mạng chung và hình thành một cách logic các mạng LAN trên môi trường đó dựa trên các thiết đặt nhận dạng độc lập với nhau đối với mỗi nhóm thành viên. Nói cách khác, mỗi cổng kết nối của các bộ chuyển mạch được định nghĩa thuộc về một nhóm làm việc (VLAN) nào đó và hình thành các khả năng độc lập tách rời của các nhóm làm việc đó với nhau. Các gói tin của một VLAN chỉ được lưu chuyển tới các cổng trong cùng VLAN mà không được lưu chuyển đến các cổng khác VLAN trừ cổng được định nghĩa là trung kế của các VLAN. Khác với LAN, VLAN không bị giới hạn về phạm vi địa lý cụ thể mà chỉ phụ thuộc vào nhu cầu và hình thức triển khai.

VLAN Trunking là khái niệm được dùng để chỉ việc kết nối giữa các bộ chuyển mạch với nhau mà qua đó cho phép các gói tin của tất cả các VLAN được truyền qua.

VLAN được cấu hình tại lớp 2 cho phép phân định các nhóm thiết bị máy tính độc lập logic với nhau, các nhu cầu trao đổi dữ liệu giữa các thiết bị khác VLAN phải được thực hiện bởi các thiết bị hoạt động ở lớp 3 như bộ chuyển mạch lớp 3 hay các bộ định tuyến.

Các giao thức và mô hình kết nối VLAN xin xem thêm trong các giáo trình về mạng nội bộ LAN.

### Cấu trúc xử lý định tuyến

Như đã nói ở phần trước, bộ chuyển mạch lớp 3 đồng thời thực hiện các chức năng chuyển mạch và chức năng định tuyến. Bộ chuyển mạch lớp 3 cho phép các thiết bị thuộc về các nhóm mạng khác nhau, các VLAN khác nhau có thể kết nối được với nhau.

Ở đây cần phân biệt các nhu cầu kết nối trao đổi dữ liệu khác nhau trong đó bao gồm:

- Các nhu cầu kết nối trao đổi dữ liệu trên các mạng sử dụng nhóm giao thức mạng định tuyến được như IP, IPX.
- Các nhu cầu kết nối trao đổi dữ liệu trên các mạng sử dụng nhóm giao thức mạng không định tuyến được như NetBEUI, AppleTalk.

Đối với nhóm giao thức không định tuyến được, bộ chuyển mạch xử lý chúng bằng nhóm các giao thức cầu nối (bridge). Các giao thức định tuyến được sẽ được xử lý tương tự như một bộ định tuyến. Bộ chuyển mạch lớp 3 hỗ trợ định

tuyến - cầu nối kết hợp, định tuyến giữa các VLAN, các chuyển mạch nhiều lớp.

### **Chuyển mạch và định tuyến kết hợp**

Cho phép bộ chuyển mạch chuyển các gói tin thuộc nhóm các giao thức không định tuyến được giữa các cổng được cấu hình ở chế độ cầu nối đồng thời cho phép chuyển các gói tin thuộc nhóm định tuyến được qua lại giữa các cổng thuộc về các VLAN sử dụng cho nhóm các giao thức định tuyến được. Giao thức chuyển mạch và định tuyến kết hợp chỉ thực hiện xử lý định hướng các gói tin trên cùng một thiết bị chuyển mạch.

### **Định tuyến giữa các VLAN**

Việc định tuyến giữa các VLAN được thực hiện trên các bộ chuyển mạch lớp 3, thông qua các module định tuyến lớp 3 hoặc thực hiện trên các bộ chuyển mạch. Bộ chuyển mạch lớp 3 hỗ trợ các giao thức định tuyến tĩnh, định tuyến động RIP, OSPF, IGRP, EIGRP.

## **5.3. Sơ lược về các bộ chuyển mạch lớp 3 thông dụng của Cisco**

### **Bộ chuyển mạch lớp 3 Cisco 2948G-L3**



*Hình 3.45: Bộ chuyển mạch lớp 3 Cisco 2948G-L3*

- 48 cổng 10/100 Ethernet, giao diện RJ45
- 02 cổng uplink Gigabit Ethernet hỗ trợ GBIC (Gigabit Interface Converter) cho phép lựa chọn các giao diện khác nhau phù hợp với nhu cầu sử dụng cổng kết nối Gigabit
- Tốc độ chuyển mạch lớp 3: 10.000 gói tin/giây
- Thông lượng: 22Gbit/giây
- Hỗ trợ IP, IPX, IP multicast
- Chức năng định tuyến lớp 3: RIP, OSPF, IGRP, EIGRP
- Chức năng chuyển đổi dự phòng, hỗ trợ trung chuyển giao thức cấp địa chỉ động
- Hỗ trợ QoS
- Chức năng an ninh mạng với danh sách truy nhập ACL

### **Bộ chuyển mạch lớp 3 Cisco 3550**



Hình 3.46: Các bộ chuyển mạch lớp 3 Cisco 3550

| Loại chuyển mạch            | Số cổng 10/100                                                                                  | Số cổng Gigabit                    |
|-----------------------------|-------------------------------------------------------------------------------------------------|------------------------------------|
| Catalyst 3550-24 Switch     | 24                                                                                              | 2 (GBIC)                           |
| Catalyst 3550-24 PWR Switch | 24 (cho phép cấp nguồn qua cáp mạng đến các thiết bị khác như thiết bị điểm truy cập không dây) | 2 (GBIC)                           |
| Catalyst 3550-24-DC Switch  | 24                                                                                              | 2 (GBIC)                           |
| Catalyst 3550-24-FX Switch  | 24 (cổng quang tốc độ 100Mbps)                                                                  | 2 (GBIC)                           |
| Catalyst 3550-48 Switch     | 48                                                                                              | 2 (GBIC)                           |
| Catalyst 3550-12G Switch    |                                                                                                 | 10 (GBIC)<br>2 (10/100/1000BASE-T) |
| Catalyst 3550-12T switch    |                                                                                                 | 10 (10/100/1000BASE-T)<br>2 (GBIC) |

- Năng lực xử lý cao:
  - o CEF: Cisco Express Forwarding
  - o Các giao thức định tuyến: RIP, OSPF, IGRP, EIGRP, BGPv4
  - o Inter-VLAN IP routing
  - o Các giao thức định tuyến multicast
  - o Các giao thức chuyển đổi dự phòng
- Tối ưu băng thông:
  - o 1,6 Gigabit cho cổng 10/100 và 16 Gigabit cho cổng Gigabit
  - o Chức năng làm việc với máy chủ cache theo giao thức WCCP
  - o Khả năng hạn chế tốc độ theo từng ứng dụng, nhóm người dùng

- Dễ dàng sử dụng và khai thác
- An toàn và bảo mật
  - o Xác thực người dùng với các hệ thống quản trị tập trung TACACS+, RADIUS
  - o Mã hóa SSH, Kerberos
  - o Các tính năng xác thực thiết bị
  - o VLAN
- Dễ dàng thực hiện QoS với các mức độ đa dạng và linh hoạt.
- Quản trị từ xa và tập trung. Tương thích với các hệ thống quản trị thông dụng.

Ngoài ra còn có các bộ chuyển mạch lớp 3 của Cisco với các dòng 4000, 6000..

## **6. Bài tập thực hành sử dụng bộ định tuyến Cisco**

### **Bài 1: Thực hành nhận diện thiết bị, đầu nối thiết bị**

Yêu cầu:

- Nhận diện đúng các chủng loại thiết bị
- Nhận diện các giao tiếp của bộ định tuyến, ý nghĩa và mục đích sử dụng
- Biết cách sử dụng các loại cáp với từng loại thiết bị, giao tiếp khác nhau
- Biết đầu nối bộ định tuyến với nhau và với các thiết bị modem khác
- Sử dụng phần mềm HyperTerminal kết nối với bộ định tuyến

### **Bài 2: Thực hành các lệnh cơ bản**

- Các lệnh show
- Lệnh config

Yêu cầu:

- Nắm vững ý và sử dụng thành thạo các lệnh kiểm tra và các lệnh cấu hình cơ bản

### **Bài 3: Cấu hình bộ định tuyến với mô hình đầu nối leased-line**

- Cấu hình Interface
- Cấu hình giao thức
- Cấu hình định tuyến

Yêu cầu:

- Sử dụng thiết bị phòng lab để cấu hình một kết nối leased-line cho phép kết nối 2 mạng với nhau.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

### **Bài 4: Cấu hình bộ định tuyến với Dial-up**

- Cấu hình line vật lý

- Cấu hình async interface
- Cấu hình định tuyến
- Cấu hình xác thực

Yêu cầu:

- Sử dụng thiết bị phòng lab để cấu hình một điểm truy nhập gián tiếp quay số qua thoại.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

### **Thiết bị phòng lab**

- 02 bộ định tuyến 2509 (leased-line và async) hoặc tương đương
- 02 modem leased-line CSU/DSU dùng cho kết nối leased-line
- 02 cáp V.35 DTE
- 04 modem dial-up 56kbps
- 02 cáp Async dùng cho kết nối modem 56kbps
- Phần mềm giả lập bộ định tuyến (router simulator)
- 02 máy tính dùng để cấu hình trực tiếp các bộ định tuyến
- các máy tính để thực hành trên phần mềm giả lập bộ định tuyến
- 04 đường điện thoại



## Chương 4

# Hệ thống tên miền DNS

Chương 4 sẽ tập trung nghiên cứu về hệ thống tên miền là một hệ thống định danh phổ biến trên mạng TCP/IP nói chung và đặc biệt là mạng Internet. Hệ thống tên miền tối quan trọng cho sự phát triển của các ứng dụng phổ biến như thư tín điện tử, web... Cấu trúc hệ thống tên miền, cấu trúc và ý nghĩa của các trường tên miền cũng như các kỹ năng cơ bản được cung cấp sẽ giúp cho người quản trị có thể hoạch định được các nhu cầu liên quan đến tên miền cho mạng lưới, tiến hành thủ tục đăng ký chính xác (nếu đăng ký tên miền Internet) và đảm nhận được các công tác tạo mới, sửa đổi ... hay nói chung là các công việc quản trị hệ thống máy chủ tên miền DNS

Chương 4 đòi hỏi các học viên phải quen thuộc với địa chỉ IP, việc soạn thảo quản trị các tiến trình trên các hệ thống linux, unix, windows.

### 1. Giới thiệu

#### 1.1. Lịch sử hình thành của DNS

Vào những năm 1970 mạng ARPAnet của bộ quốc phòng Mỹ rất nhỏ và dễ dàng quản lý các liên kết vài trăm máy tính với nhau. Do đó mạng chỉ cần một file HOSTS.TXT chứa tất cả thông tin cần thiết về máy tính trong mạng và giúp các máy tính chuyển đổi được thông tin địa chỉ và tên mạng cho tất cả máy tính trong mạng ARPAnet một cách dễ dàng. Và đó chính là bước khởi đầu của hệ thống tên miền gọi tắt là DNS (Domain name system)

Như khi mạng máy tính ARPAnet ngày càng phát triển thì việc quản lý thông tin chỉ dựa vào một file HOSTS.TXT là rất khó khăn và không khả thi. Vì thông tin bổ xung và sửa đổi vào file HOSTS.TXT ngày càng nhiều và nhất là khi ARPAnet phát triển hệ thống máy tính dựa trên giao thức TCP/IP dẫn đến sự phát triển tăng vọt của mạng máy tính:

- Lưu lượng và trao đổi trên mạng tăng lên
- Tên miền trên mạng và địa chỉ ngày càng nhiều
- Mật độ máy tính ngày càng cao do đó đảm bảo phát triển ngày càng khó khăn

Đến năm 1984 Paul Mockpetris thuộc viện USC's Information Sciences Institute phát triển một hệ thống quản lý tên miền mới (miêu tả trong chuẩn RFC 882 - 883) gọi là DNS (Domain Name System) và ngày nay nó ngày càng được phát triển và hiệu chỉnh bổ xung tính năng để đảm bảo yêu cầu ngày càng cao của hệ thống (hiện nay DNS được tiêu chuẩn theo chuẩn RFC 1034 - 1035)

#### 1.2. Mục đích của hệ thống DNS

Máy tính khi kết nối vào mạng Internet thì được gán cho một địa chỉ IP xác định. Địa chỉ IP của mỗi máy là duy nhất và có thể giúp máy tính có thể xác định đường đi đến một máy tính khác một cách dễ dàng. Như đối với người dùng thì địa chỉ IP là rất khó nhớ. Do vậy cần phải sử dụng một hệ thống để giúp cho máy tính tính toán đường đi một cách dễ dàng và đồng thời cũng giúp người dùng dễ nhớ. Do vậy hệ thống DNS ra đời nhằm giúp cho người dùng có thể chuyển đổi từ địa chỉ IP khó nhớ mà máy tính sử dụng sang một tên dễ nhớ cho người sử dụng và đồng thời nó giúp cho hệ thống Internet dễ dàng sử dụng để liên lạc và ngày càng phát triển.

Hệ thống DNS sử dụng hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây do đó việc quản lý sẽ dễ dàng và cũng rất thuận tiện cho việc chuyển đổi từ tên miền sang địa chỉ IP và ngược lại. Cũng giống như mô hình quản lý cá nhân của một đất nước mỗi cá nhân sẽ có một tên xác định đồng thời cũng có địa chỉ chứng minh thư để giúp quản lý con người một cách dễ dàng hơn (nhưng khác là tên miền không được trùng nhau còn tên người thì vẫn có thể trùng nhau)

Mỗi cá nhân đều có một số căn cước để quản lý



Mỗi một địa chỉ IP tương ứng với một tên miền

Vậy tóm lại tên miền là (domain name) gì ? những tên gọi nhớ như home.vnn.vn hoặc www.cnn.com thì được gọi là tên miền (domain name hoặc DNS name). Nó giúp cho người sử dụng dễ dàng nhớ vì nó ở dạng chữ mà người bình thường có thể hiểu và sử dụng hàng ngày.

Hệ thống DNS đã giúp cho mạng Internet thân thiện hơn với người sử dụng do đó mạng internet phát triển bùng nổ một vài năm lại đây. Theo thống kê trên thế giới vào thời điểm tháng 7/2000 số lượng tên miền được đăng ký là 93.000.000

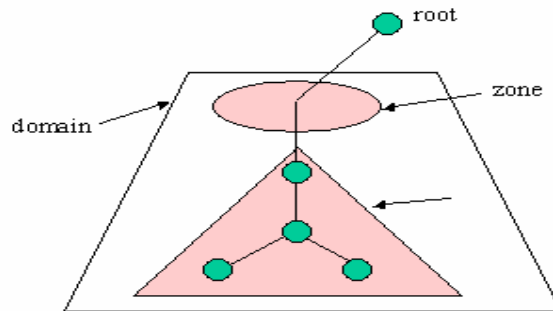
Tóm lại mục đích của hệ thống DNS là:

- Địa chỉ IP khó nhớ cho người sử dụng nhưng dễ dàng với máy tính
- Tên thì dễ nhớ với người sử dụng như không dùng được với máy tính
- Hệ thống DNS giúp chuyển đổi từ tên miền sang địa chỉ IP và ngược lại giúp người dùng dễ dàng sử dụng hệ thống máy tính

## 2. DNS server và cấu trúc cơ sở dữ liệu tên miền

### 2.1. Cấu trúc cơ sở dữ liệu

Cơ sở dữ liệu của hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây. Với .Root server là đỉnh của cây và sau đó các domain được phân nhánh dần xuống dưới và phân quyền quản lý. Khi một client truy vấn một tên miền nó sẽ lần lượt đi từ root phân cấp lần lượt xuống dưới để đến DNS quản lý domain cần truy vấn.



Cấu trúc của dữ liệu được phân cấp hình cây root quản lý toàn bộ sơ đồ và phân quyền quản lý xuống dưới và tiếp đó các tên miền lại được tiếp tục chuyển xuống cấp thấp hơn (delegate) xuống dưới.

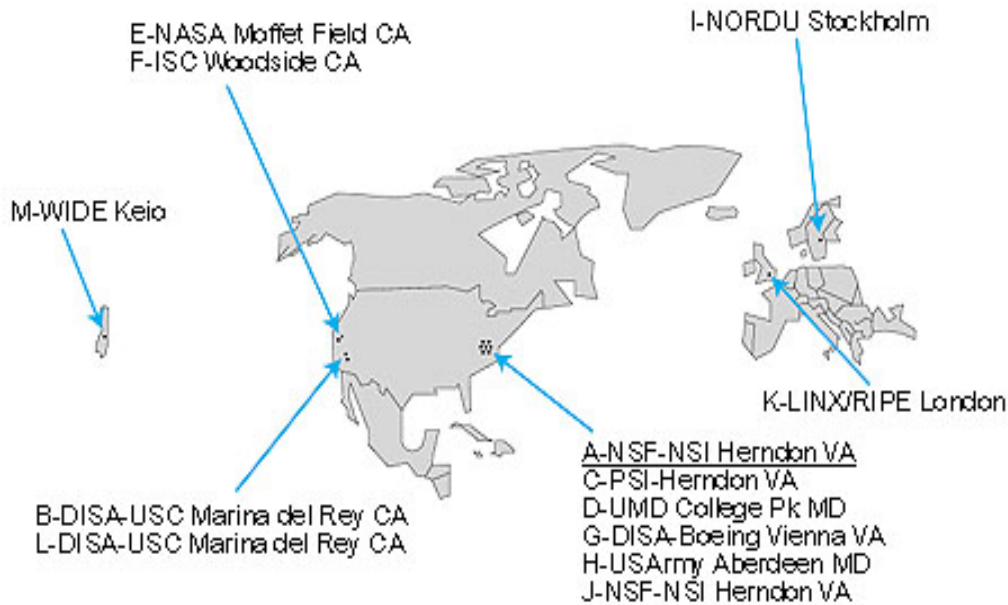
#### **Zone**

Hệ thống DNS cho phép phân chia tên miền để quản lý và nó chia hệ thống tên miền ra thành zone và trong zone quản lý tên miền được phân chia đó và nó chứa thông tin về domain cấp thấp hơn và có khả năng chia thành các zone cấp thấp hơn và phân quyền cho các DNS server khác quản lý.

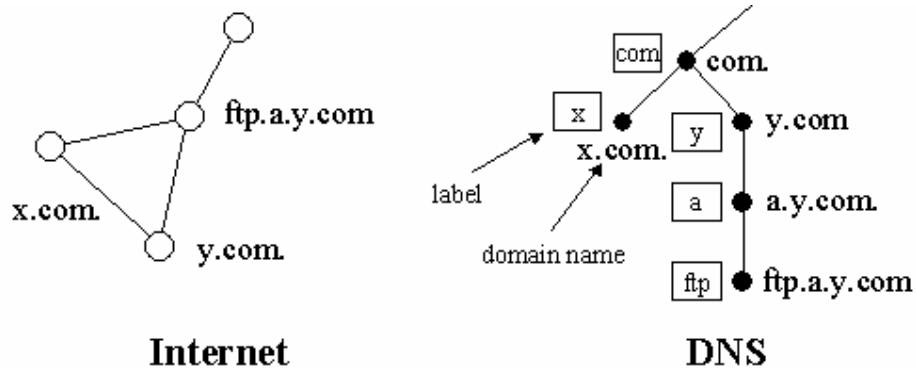
Ví dụ: zone “.com” thì DNS server quản lý zone “.com” chứa thông tin về các bản ghi có đuôi là “.com” và có khả năng chuyển quyền quản lý (delegate) các zone cấp thấp hơn cho các DNS khác quản lý như “.microsoft.com” là vùng (zone) do microsoft quản lý.

#### **Root Server**

- ✓ Là server quản lý toàn bộ cấu trúc của hệ thống DNS
- ✓ Root server không chứa dữ liệu thông tin về cấu trúc hệ thống DNS mà nó chỉ chuyển quyền (delegate) quản lý xuống cho các server cấp thấp hơn và do đó root server có khả năng xác định đường đến của một domain tại bất cứ đâu trên mạng
- ✓ Hiện nay trên thế giới có khoảng 13 root server quản lý toàn bộ hệ thống Internet (vị trí của root server như trên hình vẽ dưới)



Hệ thống cơ sở dữ liệu của DNS là hệ thống dữ liệu phân tán hình cây như cấu trúc đó là cấu trúc logic trên mạng Internet



Về mặt vật lý hệ thống DNS nằm trên mạng Internet không có cấu trúc hình cây nhưng nó được cấu hình phân cấp logic phân cấp hình cây phân quyền quản lý.

Một DNS server có thể nằm bất cứ vị trí nào trên mạng Internet nhưng được cấu hình logic để phân cấp chuyển tên miền cấp thấp hơn xuống cho các DNS server khác nằm bất cứ vị trí nào trên mạng Internet (về nguyên tắc ta có thể đặt DNS tại bất cứ vị trí nào trên mạng Internet. Nhưng tốt nhất là đặt DNS tại vị trí nào gần với các client để dễ dàng truy vấn đến đồng thời cũng gần với vị trí của DNS server cấp cao hơn trực tiếp của nó).

Mỗi một tên miền đều được quản lý bởi ít nhất một DNS server và trên đó ta khai các bản ghi của tên miền trên DNS server. Các bản ghi đó sẽ xác định địa chỉ IP của tên miền hoặc các dịch vụ xác định trên Internet như web, thư điện tử ...

**Sau đây là các bản ghi trên DNS**

| Tên trường | Tên đầy đủ         | Mục đích                                                                            |
|------------|--------------------|-------------------------------------------------------------------------------------|
| SOA        | Start of Authority | Xác định máy chủ DNS có thẩm quyền cung cấp thông tin về tên miền xác định trên DNS |
| NS         | Name Server        | Chuyển quyền quản lý tên miền xuống một DNS cấp thấp hơn                            |
| A          | Host               | Ánh xạ xác định địa chỉ IP của một host                                             |
| MX         | Mail Exchanger     | Xác định host có quyền quản lý thư điện tử cho một tên miền xác định                |
| PTR        | Pointer            | Xác định chuyển từ địa chỉ IP sang tên miền                                         |
| CNAME      | Canonical NAME     | Thường sử dụng xác định dịch vụ web hosting                                         |

**Cấu trúc của một tên miền**

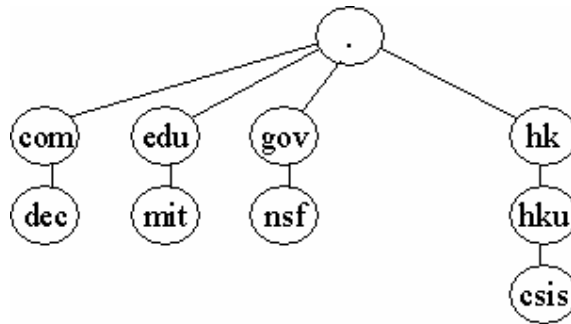
- Domain sẽ có dạng : lable.lable.label...lable
- Độ dài tối đa của một tên miền là 255 ký tự
- Mỗi một Lable tối đa là 63 ký tự
- Lable phải bắt đầu bằng chữ hoặc số và chỉ được phép chứa chữ, số, dấu trừ(-), dấu chấm (.) mà không được chứa các ký tự khác.

**Phân loại tên miền**

Hầu hết tên miền được chia thành các loại sau:

- *Arpa* : tên miền ngược (chuyển đổi từ địa chỉ IP sang tên miền reverse domain)
- *Com* : các tổ chức thương mại
- *Edu* : các cơ quan giáo dục
- *Gov* : các cơ quan chính phủ
- *Mil* : các tổ chức quân sự, quốc phòng
- *Net* : các trung tâm mạng lớn
- *Org* : các tổ chức khác
- *Int* : các tổ chức đa chính phủ (ít được sử dụng)

Ngoài ra hiện nay trên thế giới sử dụng loại tên miền có hai ký tự cuối để xác định tên miền thuộc quốc gia nào (được xác định trong chuẩn ISO3166)



| Loại tên                                  | Miêu tả                                                                                                                                                                                                    | Ví dụ                                                                                                                         |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Gốc<br>(domain root)                      | Nó là đỉnh của nhánh cây của tên miền. Nó xác định Đơn giản nó chỉ là dấu chấm (.) sử dụng kết thúc của domain (fully định tại cuối của tên ví như qualified domain names "example.microsoft.com." FQDNs). |                                                                                                                               |
| Tên miền cấp một<br>(Top-level domain)    | Là hai hoặc ba ký tự xác định nước/khu vực hoặc các tổ chức.                                                                                                                                               | ".com", xác định tên sử dụng trong xác định là tổ chức thương mại .                                                           |
| Tên miền cấp hai<br>(Second-level domain) | Nó rất đa dạng trên internet, nó có thể là tên của một công ty, một tổ chức hay một cá nhân .v.v. đăng ký trên internet.                                                                                   | "microsoft.com.", là tên miền cấp hai đăng ký là công ty Microsoft.                                                           |
| Tên miền cấp nhỏ hơn<br>(Subdomain)       | Chia nhỏ thêm ra của tên miền cấp hai xuống thường được sử dụng như chi nhánh, phong ban của một quản lý tài liệu ví dụ của microsoft cơ quan hay một chủ đề nào đó.                                       | "example.microsoft.com." là phần nhánh, phong ban của một quản lý tài liệu ví dụ của microsoft cơ quan hay một chủ đề nào đó. |

*Một số chú ý khi đặt tên miền:*

- Tên miền nên đặt giới hạn từ từ cấp 3 đến cấp 4 hoặc cấp 5 vì nếu nhiều hơn nữa việc quản trị là khó khăn.
- Sử dụng tên miền là phải duy nhất trong mạng internet
- Nên đặt tên đơn giản gợi nhớ và tránh đặt tên quá dài

## 2.2. Phân loại DNS server và đồng bộ dữ liệu giữa các DNS server

Có ba loại DNS server sau:

- *Primary server*

Nguồn xác thực thông tin chính thức cho các domain mà nó được phép quản lý quản lý

Thông tin về tên miền do nó được phân cấp quản lý thì được lưu trữ tại đây và sau đó có thể được chuyển sang cho các secondary server.

Các tên miền do primary server quản lý thì được tạo và sửa đổi tại primary server và sau đó được cập nhập đến các secondary server.

- *Secondary server*

DNS được khuyến nghị nên sử dụng ít nhất là hai DNS server để lưu cho mỗi một zone. Primary DNS server quản lý các zone và secondary server được sử dụng để lưu trữ dự phòng cho zone cho primary server. Secondary DNS server được khuyến nghị dùng nhưng không nhất thiết phải có. Secondary server được phép quản lý domain nhưng dữ liệu về domain không phải tạo tại secondary server mà nó được lấy về từ primary server.

Secondary server có thể cung cấp hoạt động ở chế độ không có tải trên mạng. Khi lượng truy vấn zone tăng cao tại primary server nó sẽ chuyển bớt tải sang secondary server hoặc khi primary server bị sự cố thì secondary sẽ hoạt động thay thế cho đến khi primary server hoạt động trở lại

Secondary server nên được sử dụng tại nơi gần với client để có thể phục vụ cho việc truy vấn tên miền một cách dễ dàng. Nhưng không nên cài đặt secondary server trên cùng một subnet hoặc cùng một kết nối với primary server. Vì điều đó sẽ là một giải pháp tốt để sử dụng secondary server để dự phòng cho primary server vì có thể kết nối đến primary server bị hỏng thì cũng không ảnh hưởng gì đến secondary server.

Primary server luôn luôn duy trì một lượng lớn dữ liệu và thường xuyên thay đổi hoặc thêm vào các zone. Do đó DNS server sử dụng một cơ chế cho phép chuyển các thông tin từ primary server sang secondary server và lưu giữ nó trên đĩa. Các thông tin nhận dữ liệu về các zone có thể sử dụng giải pháp lấy toàn bộ (full) hoặc lấy phần thay đổi (incremental)

Nhiều secondary DNS server sẽ tăng độ ổn định hoạt động của mạng và việc lưu trữ thông tin của tên miền một cách đảm bảo như một điều cần quan tâm là dữ liệu của zone được chuyển trên mạng từ primary server đến các secondary server sẽ làm tăng lưu lượng đường truyền và yêu cầu thời gian để đồng bộ dữ liệu trên các secondary server.

- *Caching-only server*

Mặc dù tất cả các DNS server đều có khả năng lưu trữ dữ liệu trên bộ nhớ cache của máy để trả lời truy vấn một cách nhanh chóng. Caching-only server là loại DNS server chỉ sử dụng cho việc truy vấn, lưu giữ câu trả lời dựa trên thông tin trên cache của máy và cho kết quả truy vấn. Chúng không hề quản lý một domain nào và thông tin mà nó chỉ giới hạn những gì được lưu trên cache của server.

Khi nào thì sử dụng caching-only server ?. Khi mà server bắt đầu chạy thì nó không có thông tin lưu trong cache. Thông tin sẽ được cập nhập theo thời gian khi các client server truy vấn dịch vụ DNS. Nếu bạn sử dụng kết nối mạng WAN tốc độ thấp thì việc sử dụng caching-only DNS server là một giải pháp tốt nó cho phép giảm lưu lượng thông tin truy vấn trên đường truyền.

#### *Chú ý*

- Caching-only DNS server không chứa zone nào và cũng không quyền quản lý bất kỳ domain nào. Nó sử dụng bộ nhớ cache của mình để lưu các truy vấn DNS của client. Thông tin sẽ được lưu trong cache để trả lời cho các truy vấn đến của client
- Caching-only DNS có khả năng trả lời các truy vấn như không quản lý hoặc tạo bất cứ zone hoặc domain nào
- DNS server nói chung được khuyến nghị là được cấu hình sử dụng TCP/IP và dùng địa chỉ IP tĩnh.

#### **Đồng bộ dữ liệu giữa các DNS server (zone transfer)**

##### *Truyền toàn bộ zone*

Bởi vì tầm quan trọng của hệ thống DNS và việc quản lý các domain thuộc zone phải được đảm bảo. Do đó thường một zone thì thường được đặt trên hơn một DNS server để tránh lỗi khi truy vấn tên miền thuộc zone đó. Nói cách khác nếu chỉ có một server quản lý zone và khi server không trả lời truy vấn thì các tên miền trong zone đó sẽ không được trả lời và không còn tồn tại trên Internet. Do đó ta cần có nhiều DNS server cùng quản lý một zone và có cơ chế để chuyển dữ liệu của các zone và đồng bộ nó từ một DNS server này đến các DNS server khác

Khi một DNS server mới được thêm vào mạng thì nó được cấu hình như một secondary server mới cho một zone đã tồn tại. Nó sẽ tiến hành nhận toàn bộ (full) zone từ DNS server khác. Như DNS server thế hệ đầu tiên thường dùng giải pháp lấy toàn bộ cơ sở dữ liệu về zone khi có các thay đổi trong zone.

##### *Truyền phần thay đổi (Incremental zone)*

Truyền chỉ những thay đổi (incremental zone transfer) của zone được miêu tả chi tiết trong tiêu chuẩn RFC 1995. Nó là phần bổ xung cho chuẩn sao chép DNS zone. Incremental transfer thì được hỗ trợ bởi cả DNS server là nguồn lấy thông tin và DNS server nhận thông tin về zone, nó cung cấp giải pháp hiệu quả cho việc đồng bộ nhưng thay đổi hoặc thêm bớt zone.

Giải pháp ban đầu cho DNS yêu cầu cho việc thay đổi dữ liệu về zone là truyền toàn bộ dữ liệu của zone sử dụng truy vấn AXFR. Với việc chỉ truyền các thay đổi (incremental transfer) sẽ sử dụng truy vấn (IXFR) được sử dụng thay thế cho AXFR. Nó cho phép secondary server chỉ lấy về như zone thay đổi để đồng bộ dữ liệu.

Với trao đổi IXFR zone, thì sự khác nhau giữa versions của nguồn dữ liệu và bản sao của nó. Nếu cả hai bản đều có cùng version ( xác định bởi số serial



trong khai báo tại phần đầu của zone SOA "start of authority") thì việc truyền dữ liệu của zone sẽ không được thực hiện.

Nếu số serial cho dữ liệu nguồn lớn hơn số serial của secondary server thì nó sẽ thực hiện chuyển những thay đổi với các bản ghi nguồn (Resource record - RR) của zone. Để truy vấn IXFR thực hiện thành công và các thay đổi được gửi thì tại DNS server nguồn của zone phải lưu giữ các phần thay đổi để sử dụng truyền đến nơi yêu cầu của truy vấn IXFR. Incremental sẽ cho phép lưu lượng truyền dữ liệu là ít và thực hiện nhanh hơn.

```
SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
32802 ; serial number
 ; refresh every 30 mins
 ; retry every hour
 ; expire after 24 hours
 ; minimum TTL 2 hours
```

```
NS vdc-hn01.vnn.vn.
NS hcm-server1.vnn.vn.
```

Zone transfer sẽ xảy ra khi có những hành động sau xảy ra:

- Khi quá trình làm mới của zone kết thúc (refresh expire)
- Khi secondary server được thông báo zone đã thay đổi tại server nguồn quản lý zone
- Khi dịch vụ DNS bắt đầu chạy tại secondary server
- Tại secondary server yêu cầu chuyển zone

Sau đây là các bước yêu cầu từ secondary server đến DNS server chứa zone để yêu cầu lấy dữ liệu về zone mà nó quản lý.

1. Trong khi cấu hình mới DNS server. Thì nó sẽ gửi truy vấn yêu cầu gửi toàn bộ zone ("all zone" transfer (AXFR) request) đến DNS server quản lý chính dữ liệu của zone

2. DNS server chính quản lý dữ liệu của zone sẽ trả lời và chuyển toàn bộ dữ liệu về zone đến secondary (destination) server mới cấu hình.

zone thì được chuyển đến DNS server yêu cầu căn cứ vào version được xác định bằng số Serial tại phần khai báo (start of authority SOA). Tại phần SOA cũng có chứa các thông số xác định thời gian làm mới lại zone ...

3. Khi thời gian làm mới (refresh interval) của zone hết, thì DNS server nhận dữ liệu sẽ truy vấn yêu cầu làm mới zone tới DNS server chính chứa dữ liệu zone.

4. DNS server chính quản lý dữ liệu sẽ trả lời truy vấn và gửi lại dữ liệu.

Trả lời sẽ bao gồm cả số serial của zone hiện tại tại DNS server chính.

5. DNS server nhận dữ liệu về zone sẽ kiểm tra số serial trong trả lời và quyết định sẽ làm thế nào với zone

Nếu giá trị của số serial bằng với số hiện tại tại DNS server nhận trả lời thì nó sẽ kết luận rằng sẽ không cần chuyển dữ liệu về zone đến. Và nó sẽ thiết lập lại với các thông số cũ và thời gian để làm mới lại bắt đầu.

Nếu giá trị của số serial tại DNS server chính lớn hơn giá trị hiện tại tại dữ liệu DNS nói nhận thì nó kết luận rằng zone cần phải được cập nhập và việc chuyển zone là cần thiết.

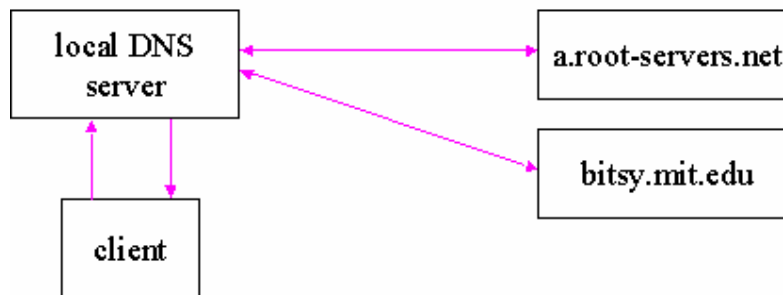
6. Nếu DNS server nơi nhận kết luận rằng zone cần phải thay đổi và nó sẽ gửi truy vấn IXFR tới DNS server chính để yêu cầu gửi zone

7. DNS server chính sẽ trả lời với việc gửi những thay đổi của zone hoặc toàn bộ zone

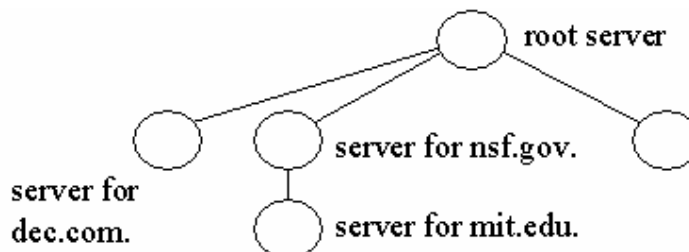
Nếu DNS server chính có hỗ trợ việc gửi những thay đổi của zone thì nó sẽ gửi những phần thay đổi (incremental zone transfer (IXFR) of the zone.). Nếu nó không hỗ trợ thì nó sẽ gửi toàn bộ zone (full AXFR transfer of the zone)

### 3. Hoạt động của hệ thống DNS

Hệ thống DNS hoạt động động tại lớp 4 của mô hình OSI nó sử dụng truy vấn bằng giao thức UDP và mặc định là sử dụng cổng 53 để trao đổi thông tin về tên miền.



Hoạt động của hệ thống DNS là chuyển đổi tên miền sang địa chỉ IP và ngược lại. Hệ thống cơ sở dữ liệu của DNS là hệ thống cơ sở dữ liệu phân tán, các DNS server được phân quyền quản lý các tên miền xác định và chúng liên kết với nhau để cho phép người dùng có thể truy vấn một tên miền bất kỳ (có tồn tại) tại bất cứ điểm nào trên mạng một cách nhanh nhất



Như đã trình bày các DNS server phải biết ít nhất một cách để đến được root server và ngược lại. Như trên hình vẽ muốn xác định được tên miền mit.edu thì root server phải biết DNS server nào được phân quyền quản lý tên miền mit.edu để chuyển truy vấn đến.

Nói tóm lại tất cả các DNS server đều được kết nối một cách logic với nhau:

- Tất cả các DNS server đều được cấu hình để biết ít nhất một cách đến root server
- Một máy tính kết nối vào mạng phải biết làm thế nào để liên lạc với ít nhất là một DNS server

### **Hoạt động của DNS**

Khi DNS client cần xác định cho một tên miền nó sẽ truy vấn DNS.

Truy vấn DNS và trả lời của hệ thống DNS cho client sử dụng thủ tục UDP cổng 53, UDP hoạt động ở mức thứ 3 (network) của mô hình OSI, UDP là thủ tục phi kết nối (connectionless), tương tự như dịch vụ gửi thư bình thường bạn cho thư vào thùng thư và hy vọng có thể chuyển đến nơi bạn cần gửi tới.

Mỗi một message truy vấn được gửi đi từ client bao gồm ba phần thông tin :

- Tên của miền cần truy vấn (tên đầy đủ FQDN)
- Xác định loại bản ghi là mail, web ...
- Lớp tên miền (phần này thường được xác định là IN internet, ở đây không đi sâu vào phần này)

Ví dụ : tên miền truy vấn đầy đủ như "hostname.example.microsoft.com.", và loại truy vấn là địa chỉ A. Client truy vấn DNS hỏi "Có bản ghi địa chỉ A cho máy tính có tên là "hostname.example.microsoft.com" khi client nhận được câu trả lời của DNS server nó sẽ xác định địa chỉ IP của bản ghi A.

Có một số giải pháp để trả lời các truy vấn DNS. Client có thể tự trả lời bằng cách sử dụng các thông tin đã được lưu trữ trong bộ nhớ cache của nó từ những truy vấn trước đó. DNS server có thể sử dụng các thông tin được lưu trữ trong cache của nó để trả lời hoặc DNS server có thể hỏi một DNS server khác lấy thông tin đó để trả lời lại client.

*Nói chung các bước của một truy vấn gồm có hai phần như sau:*

- Truy vấn sẽ bắt đầu ngay tại client computer để xác định câu trả lời
- Khi ngay tại client không có câu trả lời, câu hỏi sẽ được chuyển đến DNS server để tìm câu trả lời.

Tự tìm câu trả lời truy vấn

Bước đầu tiên của quá trình xử lý một truy vấn. Tên miền sử dụng một chương trình trên máy tính truy vấn để tìm câu trả lời cho truy vấn. Nếu truy vấn có câu trả lời thì quá trình truy vấn kết thúc

Ngay tại máy tính truy vấn thông tin được lấy từ hai nguồn sau:

- Trong file HOSTS được cấu hình ngay tại máy tính. Các thông tin ánh xạ từ tên miền sang địa chỉ được thiết lập ở file này được sử dụng đầu tiên. Nó được tải ngay lên bộ nhớ cache của máy khi bắt đầu chạy DNS client.

- Thông tin được lấy từ các câu trả lời của truy vấn trước đó. Theo thời gian các câu trả lời truy vấn được lưu giữ trong bộ nhớ cache của máy tính và nó được sử dụng khi có một truy vấn lặp lại một tên miền trước đó.

### Truy vấn DNS server

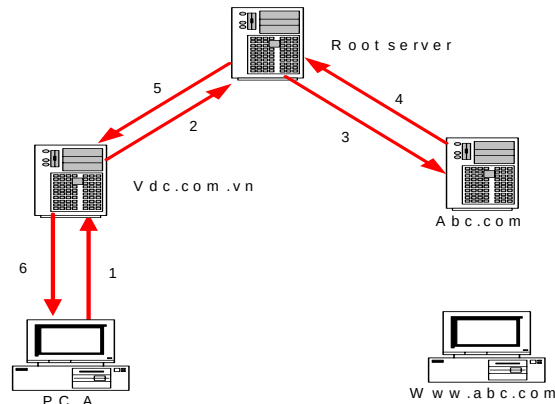
Khi DNS server nhận được một truy vấn. Đầu tiên nó sẽ kiểm tra câu trả lời liệu có phải là thông tin của bản ghi mà nó quản lý trong các zone của server. Nếu truy vấn phù hợp với bản ghi mà nó quản lý thì nó sẽ sử dụng thông tin đó để trả lời trả lời (authoritatively answer) và kết thúc truy vấn.

Nếu không có thông tin về zone của nó phù hợp với truy vấn. Nó sẽ kiểm tra các thông tin được lưu trong cache liệu có các truy vấn tương tự nào trước đó phù hợp không nếu có thông tin phù hợp nó sẽ sử dụng thông tin đó để trả lời và kết thúc truy vấn.

Nếu truy vấn không tìm thấy thông tin phù hợp để trả lời từ cả cache và zone mà DNS server quản lý thì truy vấn sẽ tiếp tục. Nó sẽ nhờ DNS server khác để trả lời truy vấn đến khi tìm được câu trả lời.

### Các cách để DNS server liên lạc với nhau xác định câu trả lời

*Trường hợp Root server kết nối trực tiếp với server tên miền cần truy vấn*



Hình 4.1: Root server kết nối trực tiếp với server tên miền cần truy vấn

Trong trường hợp root server biết được DNS server quản lý tên miền cần truy vấn. Thì các bước của truy vấn sẽ như sau:

Bước 1 : PC A truy vấn DNS server tên miền vdc.com.vn. (là local name server) tên miền www.abc.com.

Bước 2 : DNS server tên miền vdc.com.vn không quản lý tên miền www.abc.com do vậy nó sẽ chuyển truy vấn lên root server.

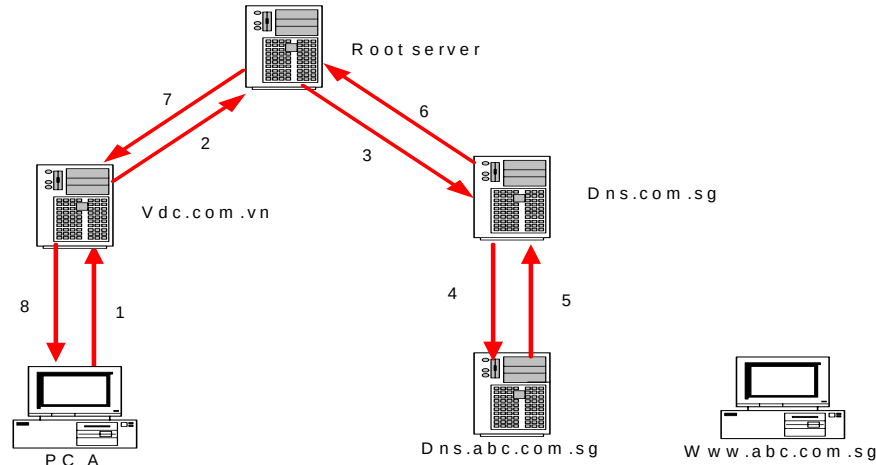
Bước 3 : Root server sẽ xác định được rằng DNS server quản lý tên miền www.abc.com là server DNS.abc.com và nó sẽ chuyển truy vấn đến DNS server DNS.abc.com để trả lời

Bước 4 : DNS server DNS.abc.com sẽ xác định bản ghi www.abc.com và trả lời lại root server

Bước 5 : Root server sẽ chuyển câu trả lời lại cho server vdc.com.vn

Bước 6 : DNS server vdc.com.vn sẽ chuyển câu trả lời về cho PC A và từ đó PC A có thể kết nối đến PC B (quản lý www.abc.com)

*Trường hợp root server không kết nối trực tiếp với server tên miền cần truy vấn*



Hình 4.2: Root server không kết nối trực tiếp với server tên miền cần truy vấn

Trong trường hợp không kết nối trực tiếp thì root server sẽ hỏi server trung gian (phân lớp theo hình cây) để xác định được đến server tên miền quản lý tên miền cần truy vấn

Bước 1 - PC A truy vấn DNS server vdc.com.vn (local name server) tên miền www.acb.com.sg.

Bước 2 - DNS server vdc.com.vn không quản lý tên miền www.abc.com.sg vậy nó sẽ chuyển lên root server.

Bước 3 - Root server sẽ không xác định được DNS server quản lý trực tiếp tên miền www.abc.com.sg nó sẽ căn cứ vào cấu trúc của hệ thống tên miền để chuyển đến DNS quản lý cấp cao hơn của tên miền abc.com.sg đó là com.sg và nó xác định được rằng DNS server DNS.com.sg quản lý tên miền com.sg.

Bước 4 - DNS.com.sg sau đó sẽ xác định được rằng DNS server DNS.abc.com.sg có quyền quản lý tên miền www.abc.com.sg.

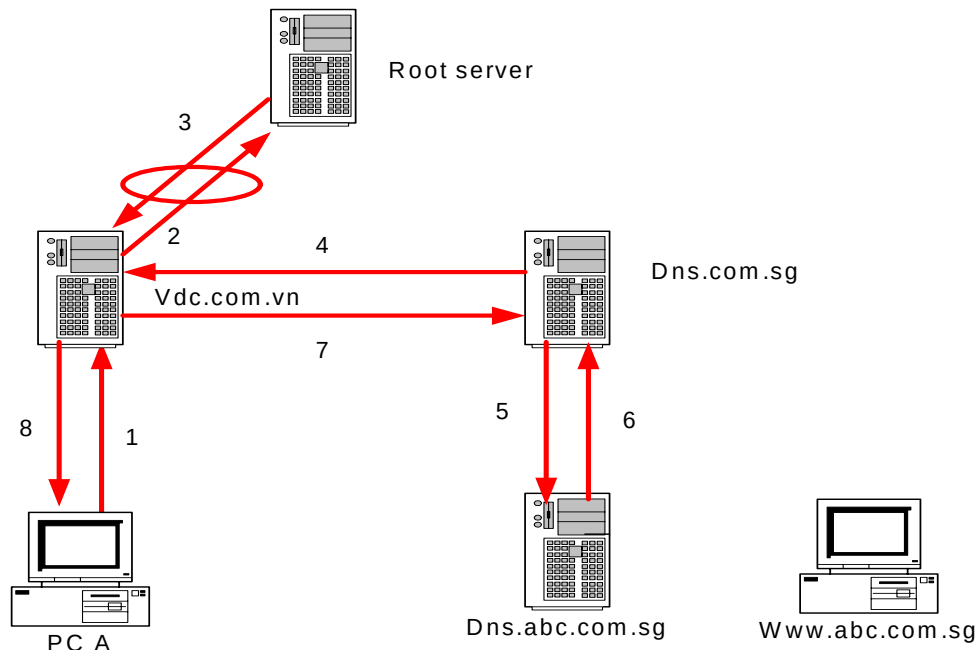
Bước 5 - DNS.abc.com.sg sẽ lấy bản ghi xác định cho tên miền www.abc.com.sg để trả lời DNS server DNS.com.sg.

Bước 6 - DNS.com.sg sẽ lại chuyển câu trả lời lên root server.

Bước 7 - Root server sẽ chuyển câu trả lời trở lại DNS server vdc.com.vn.

Bước 8 - Và DNS server vdc.com.vn sẽ trả lời về PC A câu trả lời và PC A đã kết nối được đến host quản lý tên miền www.abc.com.sg.

Khi các truy vấn lặp đi lặp lại thì hệ thống DNS có khả năng thiết lập chuyển quyền trả lời đến DNS trung gian mà không cần phải qua root server và nó cho phép thời gian truy vấn được giảm đi.



### Hoạt động của DNS cache

Khi DNS server xử lý các truy vấn của client và sử dụng các truy vấn lặp lại. Nó sẽ xác định và lưu lại các thông tin quan trọng của tên miền mà client truy vấn. Thông tin đó sẽ được ghi lại trong bộ nhớ cache của DNS server.

Cache lưu giữ thông tin là giải pháp hữu hiệu tăng tốc độ truy vấn thông tin cho các truy vấn thường xuyên của các tên miền hay được sử dụng và làm giảm lưu lượng thông tin truy vấn trên mạng.

DNS server khi thực hiện các truy vấn đệ quy cho client thì DNS server sẽ tạm thời lưu trong cache bản ghi thông tin ( resource record - RR) lấy được từ DNS server lưu trữ thông tin về truy vấn đó. Sau đó một client khác truy vấn yêu cầu thông tin của đúng bản ghi đó thì nó sẽ lấy thông tin bản ghi (RR) lưu trong cache để trả lời.

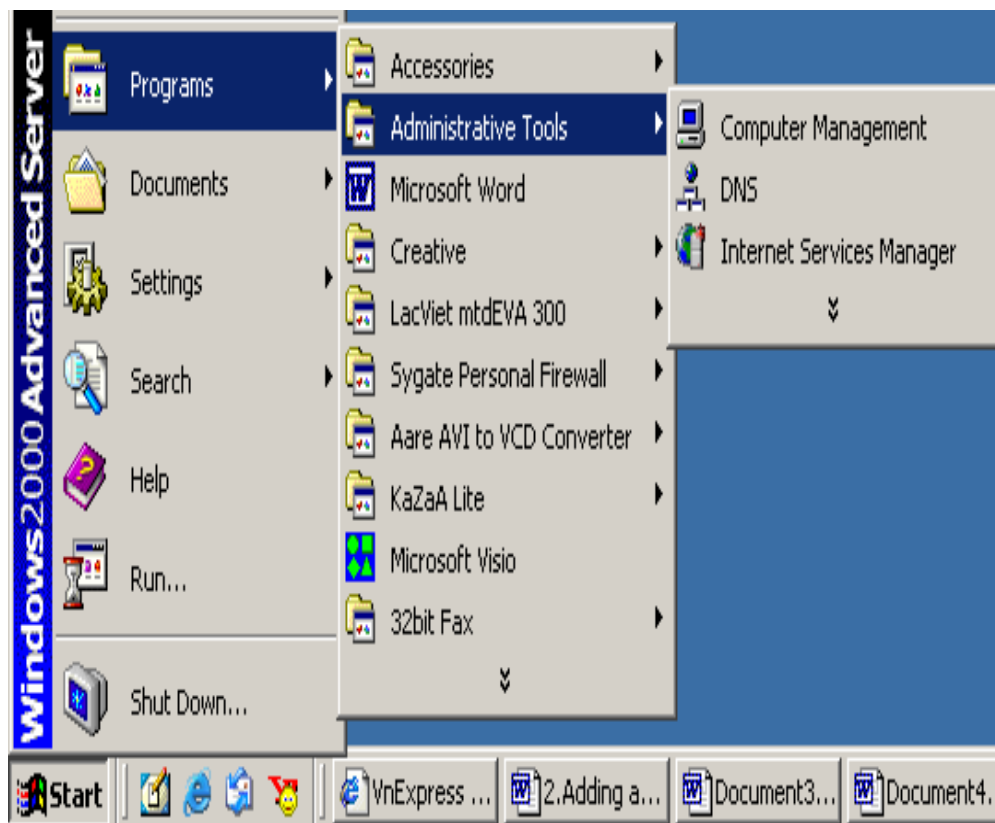
Khi thông tin được lưu trong cache. Thì các bản ghi RR được ghi trong cache sẽ được cung cấp thời gian sống (TTL - Time-To-Live). Thời gian sống của một bản ghi trong cache là thời gian mà nó tồn tại trong cache và được dùng để trả lời cho các truy vấn của client khi truy vấn tên miền trong bản ghi đó. Thời gian sống (TTL) được khai khi cấu hình cho các zone. Giá trị mặc định nhỏ nhất của thời gian sống (Minimum TTL) là 3600 giây (1 giờ) như giá trị này ta có thể thay đổi khi cấu hình zone. Hết thời gian sống bản ghi sẽ được xóa khỏi bộ nhớ cache.

## 4. Bài tập thực hành

### Bài 1: Cài đặt DNS Server cho Window 2000

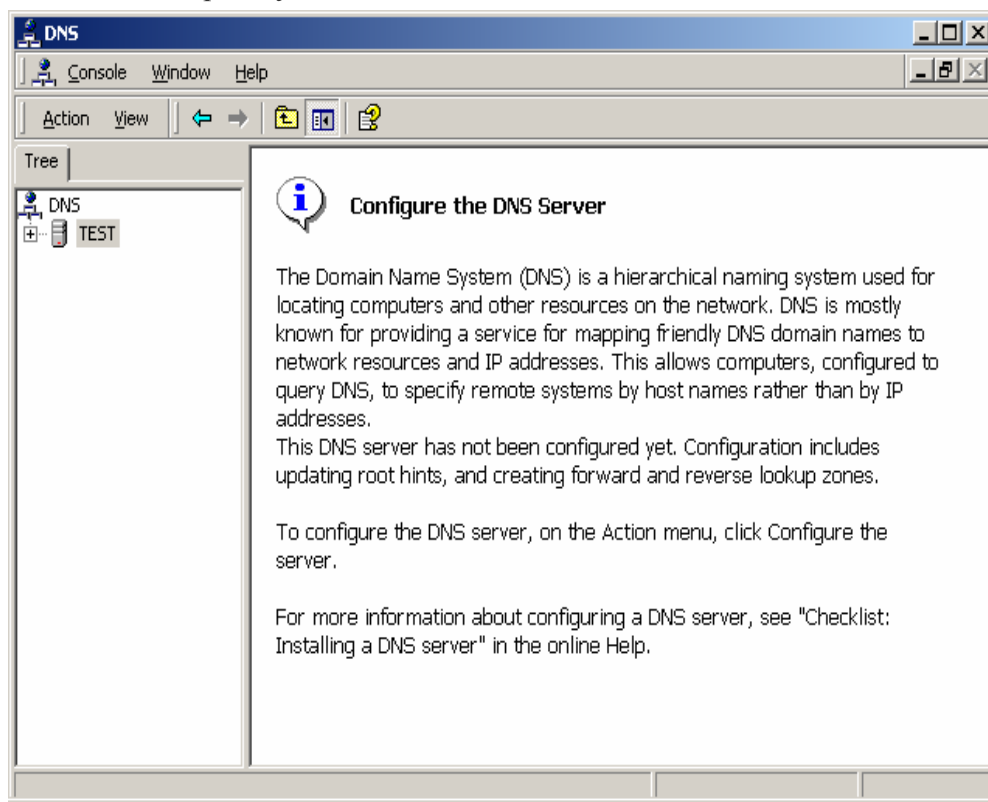
#### Mở cửa sổ quản lý DNS

**Bước 1:** Mở cửa sổ quản lý DNS



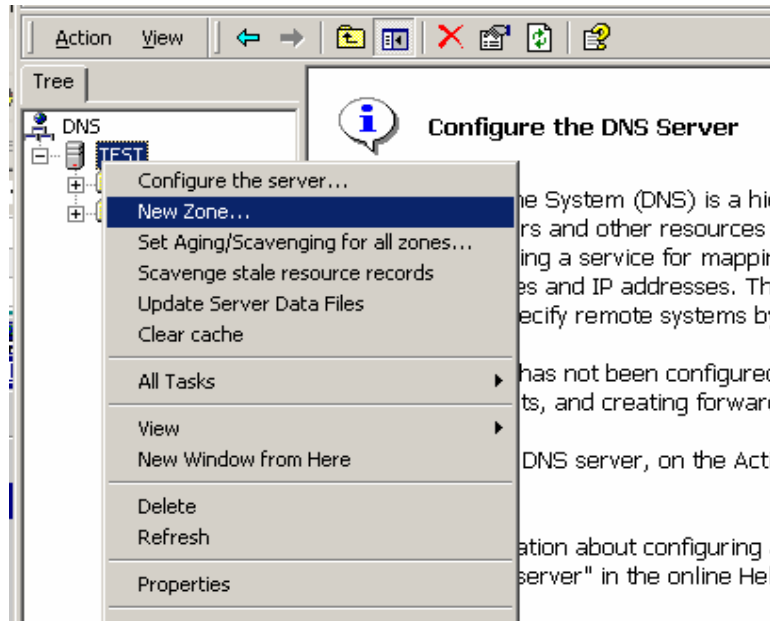
Bấm vào mune *Start* chọn *Programs* và sau đó là "*Administrative tools*" Chọn "*DNS Manager*"

**Bước 2:** Cửa sổ quản lý DNS server sẽ xuất hiện

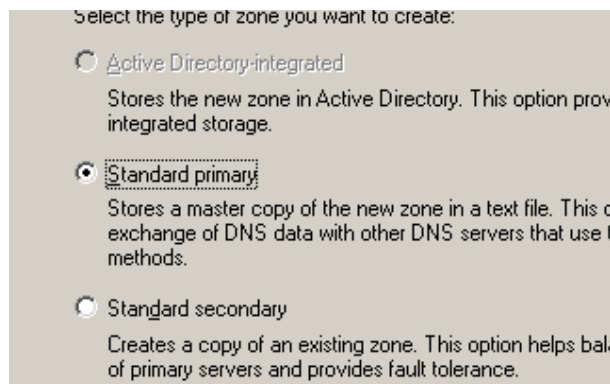


Tại cửa sổ quản lý DNS server bạn có thể khai báo các tính năng của DNS

### Thêm trường (zone)

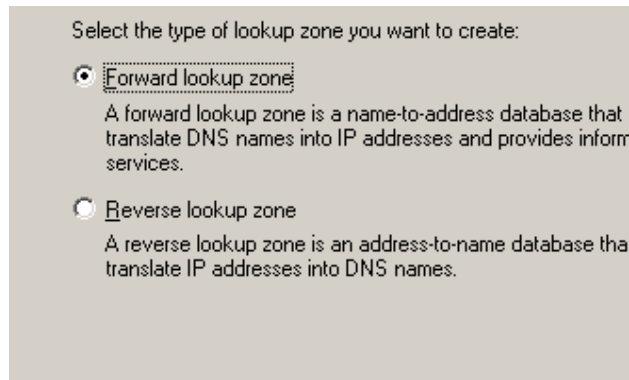


zone là tên miền (domain name) mà server quản lý. Tại cửa sổ quản lý DNS tại phần server quản lý bấm chuột phải để hiện menu và chọn "new zone" như hình trên



Bấm vào "new zone" sẽ hiện cửa sổ cho phép chọn kiểu dữ liệu mà zone quản lý. *Standard Primary* là loại dữ liệu của zone được khai báo và quản lý ngay tại server. Còn *Standard Secondary* là loại zone mà dữ liệu được lấy về từ *Standard Primary* và dữ liệu cũng nằm trên server. *Standard Primary* thường sử dụng để dự phòng cho các zone đã tồn tại. Bấm *Next* để tiếp tục



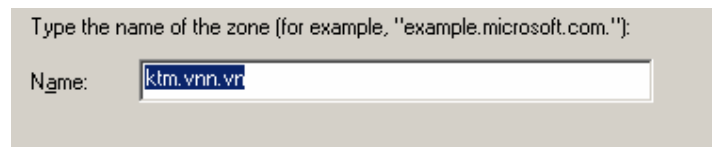


Select the type of lookup zone you want to create:

☒ **Forward lookup zone**  
A forward lookup zone is a name-to-address database that translate DNS names into IP addresses and provides inform services.

☐ **Reverse lookup zone**  
A reverse lookup zone is an address-to-name database tha translate IP addresses into DNS names.

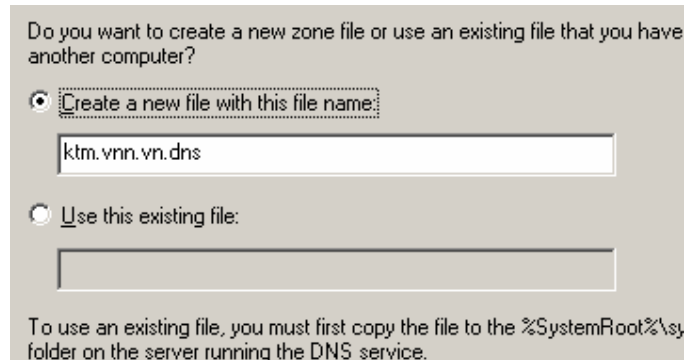
Sẽ xuất cửa sổ như trên. *Forward lookup zone* là loại zone quản lý việc chuyển đổi từ domain name sang địa chỉ IP. Còn phần *Reverse lookup zone* quản lý việc chuyển đổi từ IP sang Domain name. Bấm *Next* tiếp tục



Type the name of the zone (for example, "example.microsoft.com."):

Name:

Tại cửa sổ này điền zone (domain name) mà sẽ quản lý. Bấm *Next* tiếp tục



Do you want to create a new zone file or use an existing file that you have another computer?

☒ **Create a new file with this file name:**

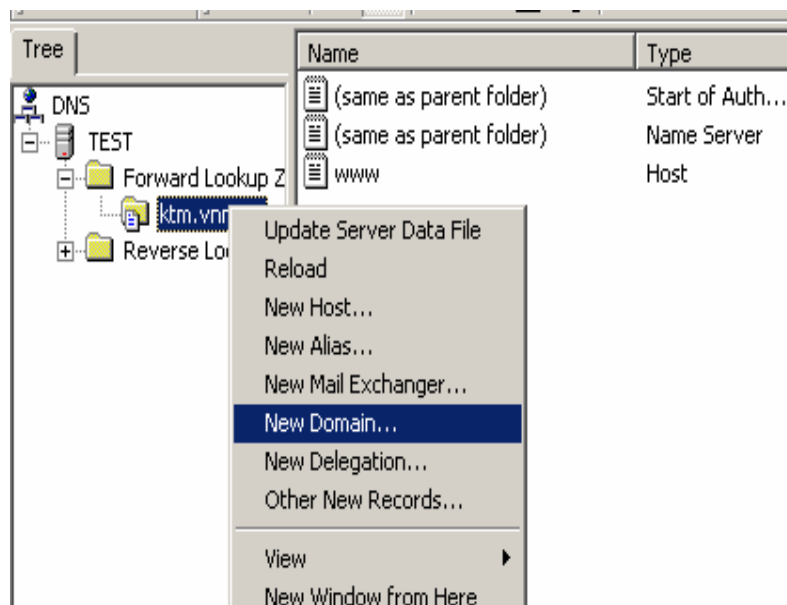
☐ **Use this existing file:**

To use an existing file, you must first copy the file to the %SystemRoot%\sys folder on the server running the DNS service.

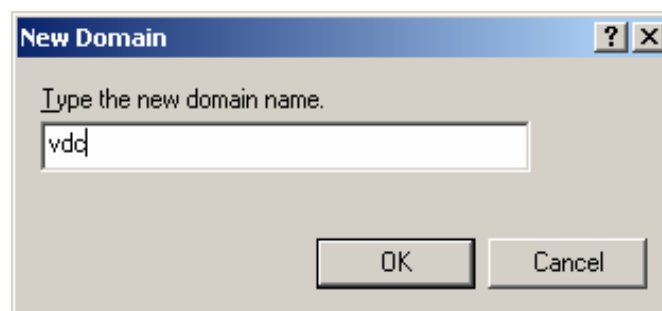
Điền tên của file để lưu trữ zone tại "*Create a new file with this file name*" hoặc sử dụng file có sẵn tại "*Use this existing file*" Và bấm *Next* cho đến khi xuất hiện nút *finish* để kết thúc tạo zone

### Thêm tên miền (domain name)

Tại cửa sổ quản lý domain chọn vào server và bấm chuột phải hiện lên menu và chọn "*New Domain...*" để điền một domain mới.

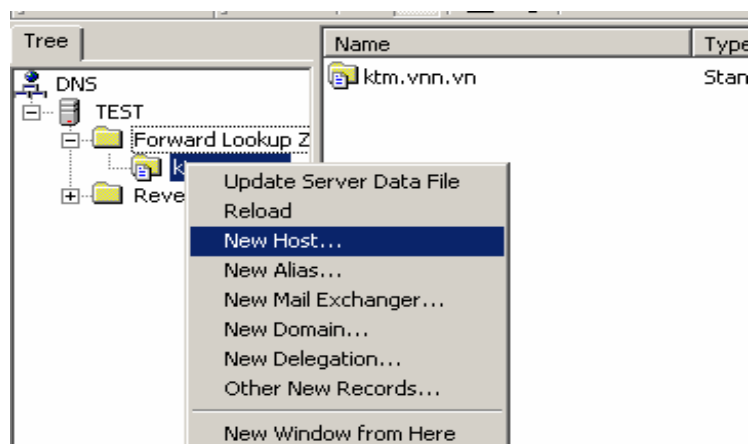


Sau khi bấm vào "New Domain" nó sẽ xuất hiện cửa sổ cho phép bạn điền tên miền mà server được phép quản lý. Sau khi điền bấm "OK" để kết thúc

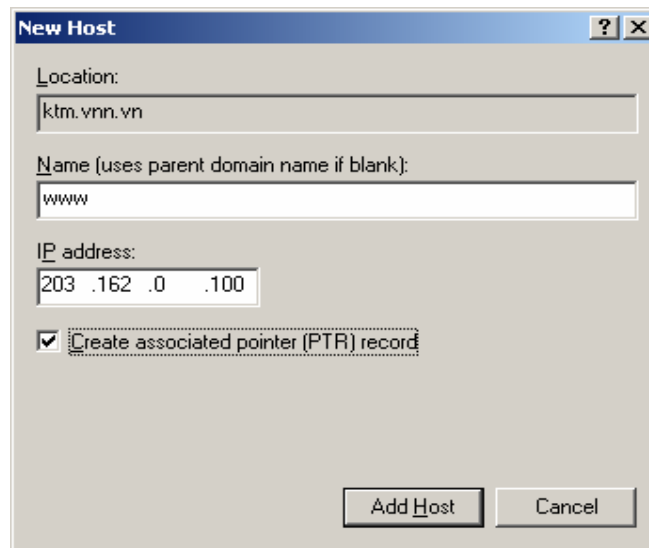


### Thêm một host mới

Tại cửa sổ quản lý DNS chọn zone đã tạo và bấm chuột phải chọn "new host"



Xuất hiện cửa sổ cho phép ta khai báo host mới



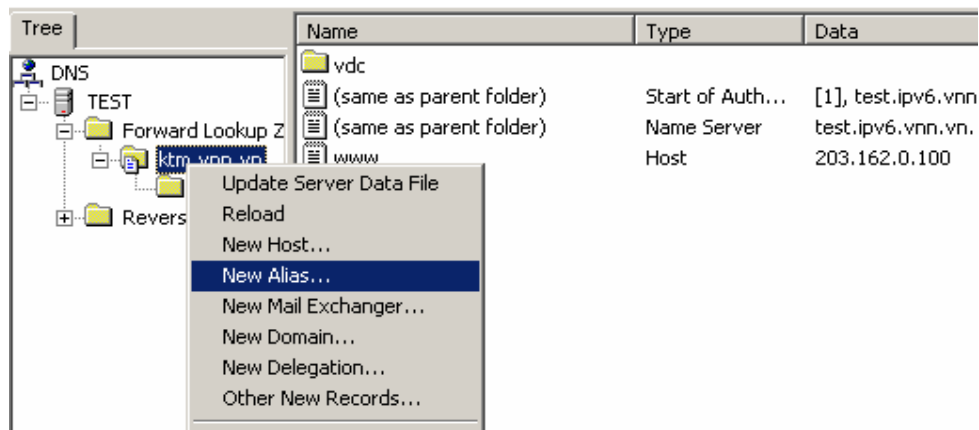
Bạn điền tên của host mà muốn tạo. Tên của host sẽ được tự động điền thêm phần domain để thành tên đầy đủ của host.

Ví dụ: như trên đây là vùng quản lý zone (*location*) là ktm.vnn.vn. Vậy khi bạn điền *Name* là www và *IP address* là 203.162.0.100 thì sẽ tương ứng với định nghĩa domain www.ktm.vnn.vn. trở đến địa chỉ IP 203.162.0.100

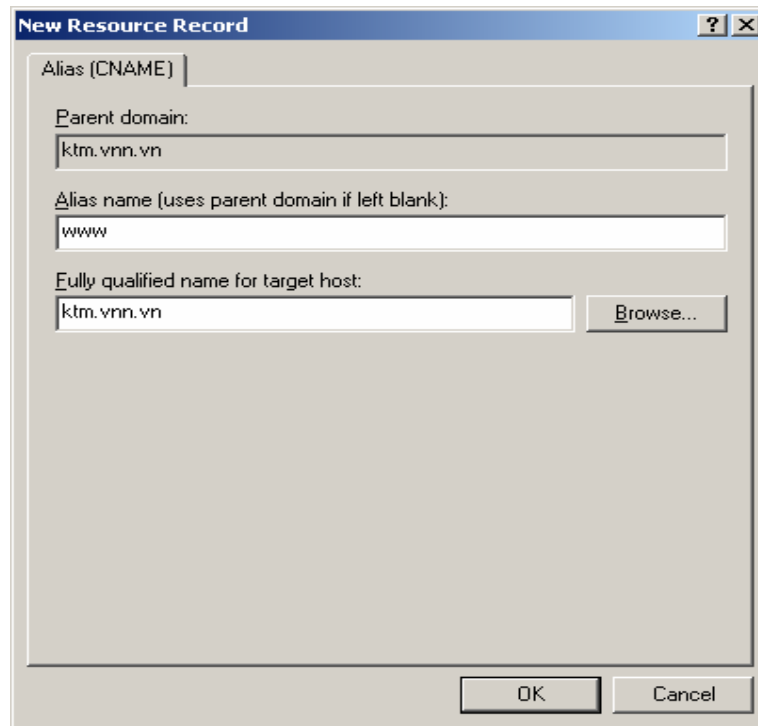
www.ktm.vnn.vn. IN A 203.162.0.100

### Tạo một bản ghi web (tạo bí danh)

Tại cửa sổ quản lý Domain và tên miền vừa tạo và bấm chuột phải và chọn "New Alias" để tạo một CNAME đến một host.



Bấm và "New Alias..." sẽ xuất hiện cửa sổ cho phép khai báo Alias



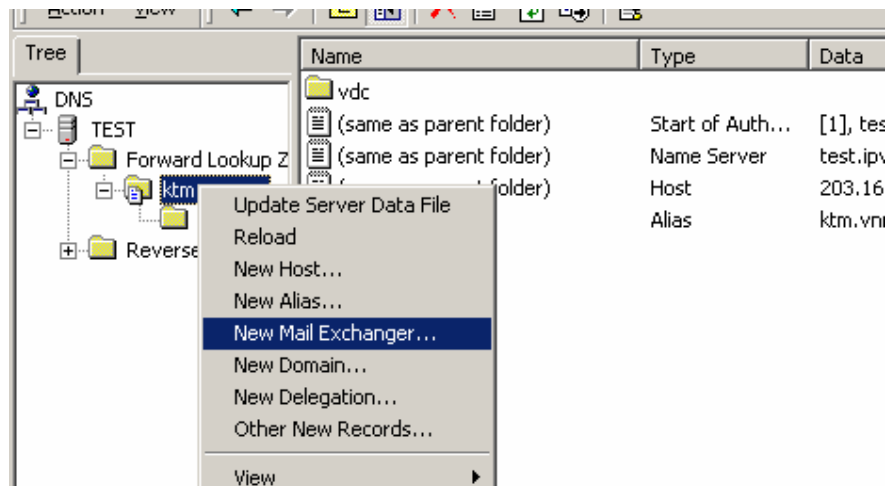
Tại phần "*Alias name*" điền tên tạo alias và tại phần "*Fully qualified name for target host*" điền tên đầy đủ của một host mà muốn tạo bí danh (thường được sử dụng cho webhosting)

Ví dụ : `www.ktm.vnn.vn. IN CNAME ktm.vnn.vn.`

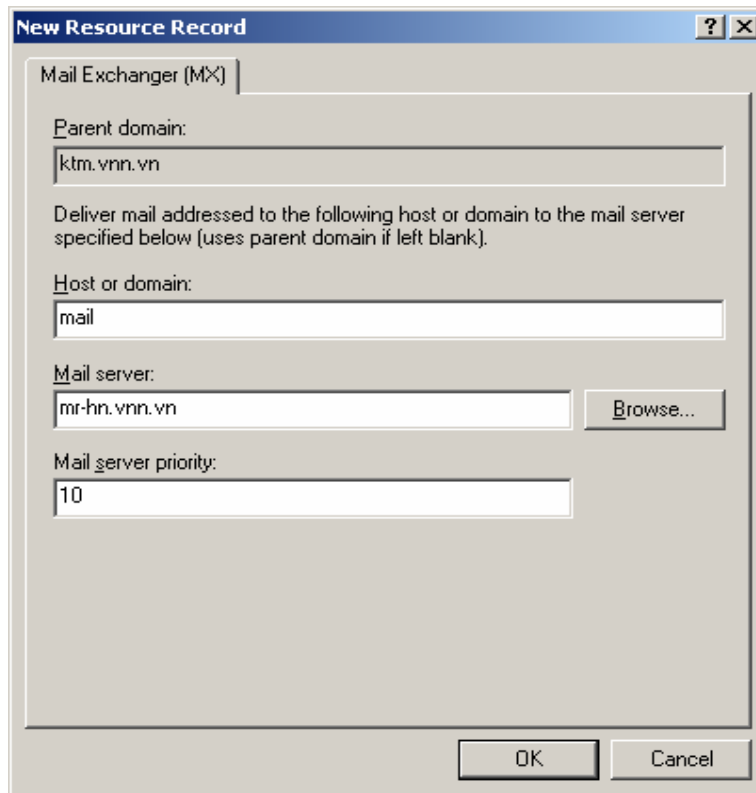
Ta sẽ có trang web `www.ktm.vnn.vn` đặt trên server web có tên là `ktm.vnn.vn`.

### Tạo một bản ghi thư điện tử (MX)

Tại cửa sổ quản lý DNS tại tên miền muốn tạo bản ghi MX bấm chuột phải



Sau khi bấm vào "*New Mail Exchanger..*" sẽ xuất hiện cửa sổ cho phép tạo các thông số cho bản ghi mx



Điền tại "*Host or domain*" điền tên hoặc để trống tên này kết hợp với phần zone "*Parent domain*" để tạo thành domain đầy đủ của bản ghi thư điện tử. Tại "*Mail server*" điền tên của server thư điện tử và tại "*Mail server priority*" điền mức độ ưu tiên của server thư điện tử (độ lớn càng nhỏ mức ưu tiên càng cao)

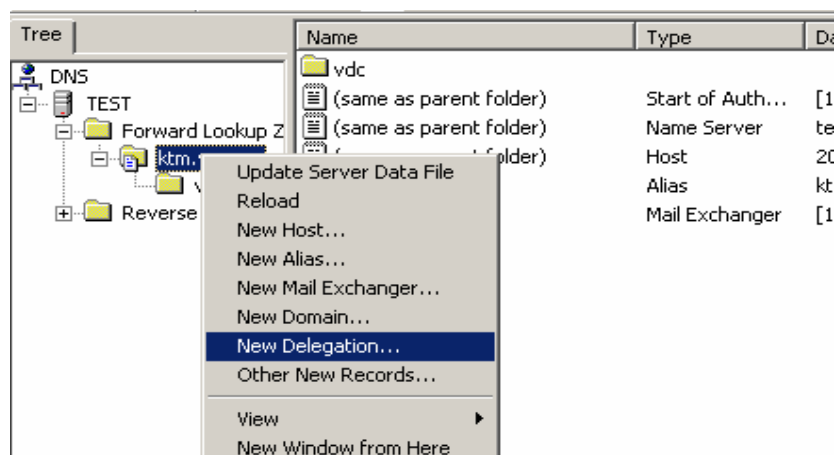
Ví dụ trên hình ta có:

mail.ktm.vnn.vn                      IN      MX 10                      mr-hn.vnn.vn.

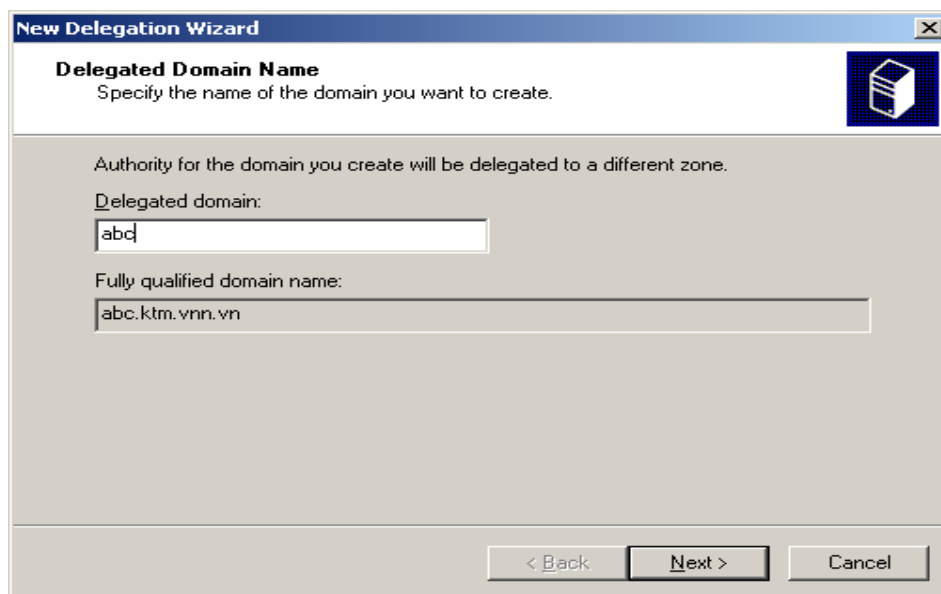
Ta có tên miền thư điện tử mail.ktm.vnn.vn. ( ta có thể tạo được các hộp thư abc@mail.ktm.vnn.vn ) được chứa tại server thư điện tử mr-hn.vnn.vn với mức ưu tiên là 10

### **Chuyển quyền quản lý tên miền (delegate)**

Tại cửa sổ quản lý DNS tại domain muốn chuyển quyền quản lý bấm chuột phải.

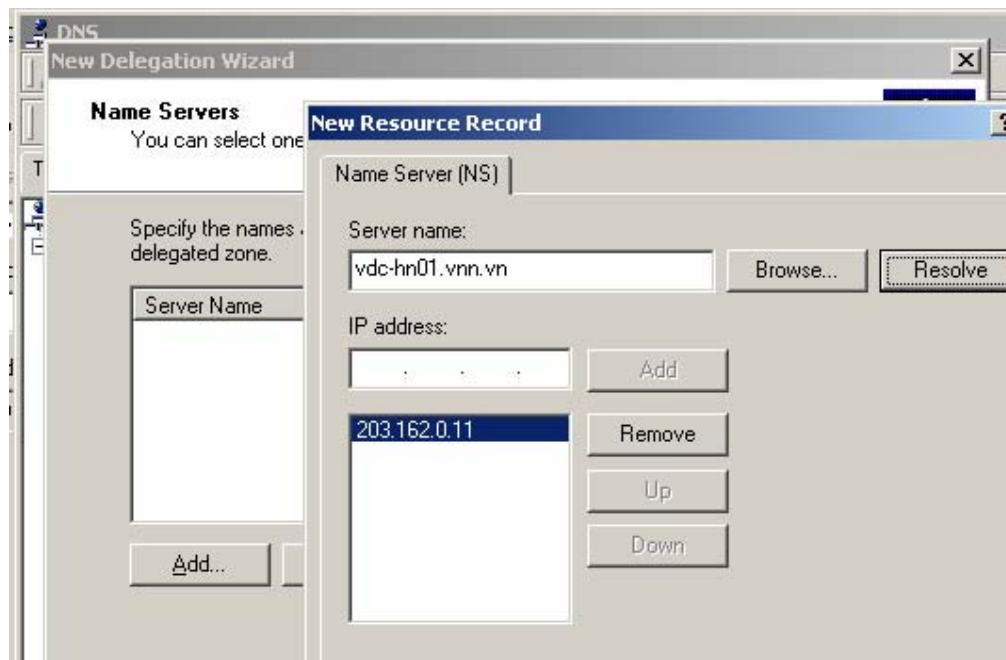


Bấm vào "New Delegation..." để hiện cửa sổ cho phép chuyển quyền quản lý tên miền



Điền phần domain mà bạn muốn chuyển quyền quản lý vào "Delegated domain"

Ví dụ ở đây điền là abc nghĩa là bạn muốn chuyển quyền quản lý domain abc.ktm.vnn.vn. Bấm "Next" để tiếp tục



Hiện cửa sổ điền vào "Server name" tên của DNS server sẽ được phép quản lý tên miền abc.ktm.vnn.vn. Bấm "Resolve" để xác định địa chỉ IP của DNS server. Sau đó bấm "Ok" để kết thúc.

Ví dụ abc.ktm.vnn.vn. IN NS vdc-hn01.vnn.vn.

Tương ứng tên miền abc.ktm.vnn.vn. sẽ được chuyển quyền về DNS server vdc-hn01.vnn.vn để quản lý.

## Bài 2: Cài đặt, cấu hình DNS cho Linux

Hiện tại trên Internet rất nhiều nhà cung cấp phần mềm miễn phí cho DNS. Nhưng phần mềm sử dụng DNS cho unix được sử dụng phổ biến hiện nay là gói phần mềm cho DNS là Bind

Bind được phát triển bởi một tổ chức phi lợi nhuận là Internet Software Consortium (www.isc.org) và nó cung cấp phần mềm bind miễn phí.

Hiện tại phần mềm bind có version là 9.2.2

Phần mềm Bind còn cung cấp tiện ích nslookup là công cụ rất tiện lợi cho việc kiểm tra tên miền

Khai báo DNS cho client/server

Với client sử dụng linux hoặc unix ta vào file /etc/resolv.conf

- ✓ Client chỉ lấy thông tin về các domain
- ✓ Client chỉ gửi query tới server và nhận trả lời

Cấu hình DNS server

- ✓ Cấu hình resolver như của (DNS client)
- ✓ Cấu hình Bind cho name server (named)

- ✓ Xây dựng cơ sở dữ liệu cho DNS (cho các zone file)

Cấu hình cho DNS client /etc/resolv.conf

| Các từ khóa               | Miêu tả                                                                  |
|---------------------------|--------------------------------------------------------------------------|
| nameserver <i>địa chỉ</i> | Địa chỉ IP của DNS server sẽ gửi truy vấn đến để lấy thông tin về domain |
| domain <i>name</i>        | xác định domain mặc định của client                                      |

---

*/etc/resolv.conf*

---

```
Domain name resolver configuration file
#
domain nuts.com
try yourself first
nameserver 172.16.12.2
try almond next
nameserver 172.16.12.1
finally try filbert
nameserver 172.16.1.2
```

---

Với DNS client chỉ cần cấu hình file resolv.conf

### Cài đặt DNS server.

Ta có thể lấy chương trình cài đặt bind cho DNS tại [www.isc.org](http://www.isc.org) lấy về server

```
cd /usr/src
```

```
mkdir bind-9.xx
```

```
cd bind-9.xx
```

Lấy chương trình cài đặt DNS về đây bind-9.xx-src.tar.gz

```
gunzip bind-9.xx-src.tar.gz
```

```
tar xf bind-9.xx-src.tar
```

```
rm bind-9.xx-src.tar
```

```
cd src
```

```
make clean
```

```
make depend
```

```
make install
```

Vậy là ta đã cài xong phần mềm named cho DNS và các zone file sẽ được chứa trong /var/named còn file cấu hình nằm trong /usr/local/etc vậy ta phải tạo và đặt file cấu hình và zone file vào các thư mục trên và chạy

```
#!/usr/local/sbin/named
```

Vậy là server đã sẵn sàng cho truy vấn DNS



## Cấu trúc file cơ sở dữ liệu (zone file)

Các file cơ sở dữ liệu zone được chỉ làm hai loại cho domain (có dạng db.domain hoặc domain.root) và các domain ngược ( db.address ) và nó nằm trong thư mục /var/named của DNS server.

Các dữ liệu nằm trong file cơ sở dữ liệu được gọi là DNS resource record. Các loại resource record trong file dữ liệu bao gồm:

SOA record

Chỉ rõ domain ở cột quản lý bởi name server ghi sau trường SOA. Trong trường hợp file db.domain

```
@ IN SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
1999082802 ; serial number
1800 ; refresh every 30 mins
3600 ; retry every hour
86400 ; expire after 24 hours
6400 ; minimum TTL 2 hours
)
IN NS vdc-hn01.vnn.vn.
IN NS hcm-server1.vnn.vn.
```

Khai báo zone ngược db.203.162.0

```
@ IN SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
1999082301 ; Serial
10800 ; Refresh after 3 hours
3600 ; Retry after 1 hour
604800 ; Expire after 1 week
86400) ; Minimum TTL of 1 day
; name servers
IN NS vdc-hn01.vnn.vn.
IN NS hcm-server1.vnn.vn.
6 IN PTR ldap.vnn.vn.
7 IN PTR hanoi-server1.vnn.vn.
8 IN PTR hanoi-server2.vnn.vn.
9 IN PTR mail.vnn.vn.
```

Trong mỗi zone chỉ khai một trường SOA. Như ví dụ trên trong trường hợp file db.com.vn, chữ @ biểu thị các tất cả các domain trong file quản lý bởi name server vdc-hn01.vnn.vn và địa chỉ mail của admin mạng là postmaster.vnn.vn. Ngoài ra trong phần SOA có 5 thông số cần quản tâm sau:

*Serial number* : Thông số này có tác dụng với tất cả các dữ liệu trong file. Khi secondary server yêu cầu primary server các thông tin về domain mà nó quản lý thì đầu tiên nó sẽ so sánh serial number của secondary và primary server.

Nếu serial number của secondary server nhỏ hơn của primary server thì dữ liệu của domain sẽ được cập nhập lại cho secondary server từ secondary server.

Mỗi khi ta thay đổi nội dung của file db.domain thì ta cần phải thay đổi serial number và thường ta đánh serial number theo nguyên tắc sau:

Serial number : yyymmddtt

trong đó : yyyy là năm

mm là tháng

dd là ngày

tt là số lần sửa đổi trong ngày

*Refresh*: là chu kỳ thời gian mà secondary server sẽ sánh và cập nhập lại dữ liệu của nó với primary server

*Retry*: nếu secondary server không kết nối được với primary server thì cứ sau một khoảng thời gian thì nó sẽ kết nối lại

*Expire* : là khoảng thời gian mà domain sẽ hết hiệu lực nếu secondary không kết nối được với primary server.

*TTL (time to live)* : khi một server bất kỳ yêu cầu thông tin về dữ liệu nào đó từ primary server, và dữ liệu đó sẽ được lưu giữ tại server đó và có hiệu lực trong khoảng thời gian của TTL. Hết khoảng thời gian đó nếu tiếp tục cần thì nó lại phải truy vấn lại primary server.

Các bản ghi thường dùng trong DNS server

*NS (name server)* : Bản ghi NS để xác định DNS server nào sẽ quản lý tên miền. Như ví dụ ở trên là DNS server vdc-hn01.vnn.vn. và hcm-server1.vnn.vn.

*A (address)* : Bản ghi dạng A cho tương ứng một domain name với một địa chỉ IP. Chỉ cho phép khai báo một bản ghi A cho một địa chỉ IP.

Ví dụ:

| Tên miền      | Internet | Loại bản ghi | Địa chỉ       |
|---------------|----------|--------------|---------------|
| mr.vnn.vn.    | IN       | A            | 203.162.4.148 |
| mr-hn.vnn.vn. | IN       | A            | 203.162.0.24  |
| mail.vnn.vn.  | IN       | A            | 203.162.0.9   |
| fmail.vnn.vn. | IN       | A            | 203.162.4.147 |
| hot.vnn.vn.   | IN       | A            | 203.162.0.23  |
| home.vnn.vn.  | IN       | A            | 203.162.0.12  |

|             |    |   |              |
|-------------|----|---|--------------|
| www.vnn.vn. | IN | A | 203.162.0.16 |
|-------------|----|---|--------------|

**CNAME (canonical name)** : là tên phụ cho một host có sẵn tên miền dạng A. Nó thường được sử dụng cho các server web, ftp

Ví dụ : các domain có dạng CNAME được chỉ tới các máy chủ web

| Tên miền                            | Internet | Loại bản ghi | Server       |
|-------------------------------------|----------|--------------|--------------|
| www.gpc.com.vn.                     | IN       | CNAME        | home.vnn.vn. |
| www.huonghai.com.vn.                | IN       | CNAME        | home.vnn.vn. |
| www.songmayip.com.vn.               | IN       | CNAME        | hot.vnn.vn.  |
| <a href="#">www.covato2.com.vn.</a> | IN       | CNAME        | hot.vnn.vn.  |

**MX (mail exchange)**: là tên phụ cho các dịch vụ mail trên các máy chủ đã có tên miền dạng A. Bản ghi này cho phép máy chủ có thể cung cấp dịch vụ mail cho các domain khác nhau. Có thể khai báo nhiều domain khác nhau cùng chỉ tới một server hoặc một domain trở tới nhiều server khác nhau ( sử dụng backup) trong trường hợp này giá trị ưu tiên phải đặt khác nhau. Với số ưu tiên càng nhỏ thì mức độ ưu tiên càng cao.

Ví dụ

| Tên miền           | Internet | Loại bản ghi | mức ưu tiên | Server              |
|--------------------|----------|--------------|-------------|---------------------|
| mr.vn.vnn.vn.      | IN       | MX           | 10          | mr.vnn.vn.          |
| clipsal.vn.vnn.vn. | IN       | MX           | 10          | mr-hn.vnn.vn.       |
| dbqnam.vnn.vn.     | IN       | MX           | 10          | mr-hn.vnn.vn.       |
| thangloi.vnn.vn.   | IN       | MX           | 50          | mail.netnam.vn.     |
|                    | IN       | MX           | 100         | fallback.netnam.vn. |

**PTR (Pointer)** : là bản ghi tương ứng địa chỉ IP với domain. Các file dạng db.address. Ví dụ db.203.162.0 cho tương ứng với các địa chỉ IP tương ứng với mạng 203.162.0.xxx

Chú ý:

Trước mỗi phần khai báo domain thường có dòng

\$ORIGIN domain.

Để khai báo giá trị mặc định của domain. Cho phép trong phần khai báo giá trị không phải khai báo lặp lại phần domain mặc định.

Ví dụ :

vdc.com.vn.                      IN        A        203.162.0.49

hoặc

```
$ORIGIN com.vn.
vdc IN A 203.162.0.49
```

Dấu ";" được sử dụng làm ký hiệu dòng chú thích, các phần sau dấu ";" đều không có tác dụng.

### Định nghĩa cấu hình (name.conf)

Khi các file cơ sở dữ liệu (zone file) thì cần phải cấu hình để DNS server đọc các zone file đó. Đối với hệ thống BIND cơ chế chỉ dẫn name server đọc các zone file được khai trong file named.conf nó được nằm trong thư mục /etc hoặc /usr/local/etc

Ví dụ : khai báo file db trong file named.conf:

```
; khai báo cho zone file domain.vn
zone "vn." in {
 type master;
 file "db.vn";
};
;khai báo cho zone file domain.gov.vn
zone "gov.vn." in {
 type master;
 file "db.gov.vn";
};
;khai báo cho zone ngược 203.162.0.xxx
zone "0.162.203.in-addr.arpa" in {
 type master;
 file "db.203.162.0";
};
;khai báo cho zone ngược 203.162.1.xxx
zone "1.162.203.in-addr.arpa" in {
 type master;
 file "db.203.162.1";
};
```

Chú ý: sau mỗi lần thay đổi dữ liệu để sửa đổi có tác dụng thì cần phải làm động tác để DNS server cập nhập thay đổi

```
%su
```

```
%password:
```

```
ps -ef | grep named
```

```
root 17413 1 5 Sep 07 ? 189:52 /usr/local/sbin/named
```

```
kill -HUP 17413
```

Còn để chạy DNS server

`#/usr/local/sbin/named`

Hướng dẫn sử dụng nslookup

nslookup - là công cụ trên internet cho phép truy vấn tên miền và địa chỉ IP một cách tương tác.

### **Cấu trúc câu lệnh**

`nslookup [ -option ... ] [ host-to-find | - [ server ] ]`

### **Miêu tả các lệnh của nslookup**

**server domain & lserver domain** Change the default server to domain. Lserver uses the initial server to look up information about domain while server uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.

**root** Thay đổi server mặc định sẽ làm root cho domain truy vấn.

**ls [option] domain [>> filename]**

Hiện danh sách thông tin của domain. Mặc định là hiện tên của host và địa chỉ IP. Ta có thể sử dụng các lựa chọn để hiện nhiều thông tin hơn:

**-t querytype** hiện danh sách tất cả bản ghi xác định bởi loại querytype

**-a** hiện danh sách các bí danh (alias) của domain host (tương tự như -t CNAME)

**-d** hiện danh sách các bản ghi của domain (tương tự như -t ANY)

**-h** hiện danh sách thông tin về CPU và thông tin về hệ điều hành của domain. (tương tự như -t HINFO)

**?** hiện danh sách các câu lệnh.

**exit** thoát khỏi chương trình.

**set keyword[=value]** câu lệnh dùng để thay đổi trạng thái thông tin mà có ảnh hưởng đến truy vấn. Các từ khoá:

**all** cho phép hiện tất cả các loại bản ghi

**[no]debug** bật chế độ tìm lỗi. Cho hiện rất nhiều loại thông tin cho phép xác định lỗi truy vấn đến domain. (mặc định=nodebug, viết tắt = [no]deb)

**[no]d2** Bật chế độ tìm lỗi mức cao hơn. Tất cả các gói tin truy vấn đều được xuất hiện. (mặc định=nod2)

**domain=name** Thay đổi domain mặc định vào tên. Khi truy vấn một tên nó sẽ tự động điền thêm domain vào sau.

**port=value** Chuyển cổng mặc định sử dụng cho TCP/UDP name server thành cổng được thiết lập bởi giá trị này (mặc định= 53, viết tắt = po)

**querytype=value**

**type=value** Chọn loại truy vấn thông tin. Có các loại sau:

**A** truy vấn host ( khai báo địa chỉ IP).

**CNAME** (canonical name) tạo tên bí danh ( thường dùng cho web)

**HINFO** truy vấn loại CPU và hệ điều hành của server.

**MINFO** thông tin về hộp thư hoặc mail list.

**MX** truy vấn về mail exchanger.

**NS** truy vấn về named zone.

**PTR** truy vấn chuyển từ địa chỉ IP sang domain.

**SOA** Thông tin về người quản lý về zone.

**TXT** Các thông tin khác.

**UINFO** Thông tin về người dùng.

**WKS** Hỗ trợ cho các dịch vụ khác.

Các loại khác (**ANY**, **AXFR**, **MB**, **MD**, **MF**, **NULL**) được miêu tả chi tiết trong tiêu chuẩn **RFC-1035** . (Mặc định = A, viết tắt = q, ty)

**[no]recurse** Yêu cầu name server truy vấn tới một server khác nếu nó không có thông tin về domain cần tìm. (mặc định = recurse, viết tắt = [no]rec)

**retry=number** Thiết lập số lần truy vấn. Khi truy vấn mà không nhận được trả lời trong khoảng thời gian nhất định (thiết lập bằng lệnh set timeout). Khi thời gian hết thì yêu cầu truy vấn sẽ được gửi lại. Và thiết lập ở đây để điều khiển số lần sẽ gửi lại trước khi từ bỏ truy vấn. (Mặc định = 4, viết tắt = ret)

**root=host** Đổi root server cho host

**timeout=number** Thiết lập thời gian timeout cho một quá trình truy vấn tính bằng giây. (mặc định = 5 giây, viết tắt = ti)

**[no]vc** sử dụng một virtual circuit để gửi yêu cầu truy vấn đến server. (mặc định là = novc, viết tắt = [no]v)

### **Phân tích lỗi**

Nếu truy vấn lookup không thành công thì một thông tin về lỗi sẽ được hiện ra. Và các lỗi có thể là :

#### ***Timed out***

Server không trả lời truy vấn sau một khoảng thời gian ( khoảng thời gian có thể thay đổi bằng câu lệnh *set timeout=value*) và and a certain number of retries (changed with *set retry=value*).

#### ***No response from server***

Không có name server đang chạy tại server mà client chỉ đến.

#### ***No records***

Server không có bản ghi tương ứng loại mà truy vấn cho host đã tồn tại. Loại truy vấn được thiết lập bằng câu lệnh "*set querytype*".

#### ***Non-existent domain***

Host hoặc domain name không tồn tại.

#### ***Connection refused***

### **Network is unreachable**

Kết nối tới name server hoặc finger server không thể được tại thời điểm này. Lệnh này thường xuất hiện với các yêu cầu của câu lệnh ls và finger.

### **Server failure**

Name server tìm thấy lỗi trong dữ liệu về domain và không thể đưa ra câu trả lời đúng.

### **Refused**

Name server từ chối yêu cầu trả lời.

### **Format error**

Name server thấy rằng các gói tin yêu cầu không đúng định dạng. Nó có thể là lỗi của chương trình nslookup.

Ví dụ :

```
Truy vấn DNS sử dụng bản ghi a cho domain
home.vnn.vn có địa chỉ IP là 203.162.0.12
Default Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
> set querytype=a
> home.vnn.vn
Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
Name: home.vnn.vn
Address: 203.162.0.12
>

Truy vấn bản ghi mx (mail) cho domain hn.vnn.vn
nó trỏ đến các host mu13.vnn.vn có địa chỉ 203.162.0.55 và
mu14.vnn.vn có địa chỉ 203.162.0.64
> set querytype=mx
> hn.vnn.vn
Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
hn.vnn.vn MX preference = 20, mail exchanger = mu13.vnn.vn
hn.vnn.vn MX preference = 10, mail exchanger = mu14.vnn.vn
vnn.vn nameserver = vdc-hn01.vnn.vn
vnn.vn nameserver = hcm-server1.vnn.vn
mu13.vnn.vn internet address = 203.162.0.55
mu14.vnn.vn internet address = 203.162.0.64
vdc-hn01.vnn.vn internet address = 203.162.0.11
hcm-server1.vnn.vn internet address = 203.162.4.1
>

Truy vấn loại ns > set querytype=ns
```

```
(name server) cho > vn
domain vn do các Server: vdc-hn01.vnn.vn
server nào quản lý Address: 203.162.0.11
sẽ cho ta một danh Aliases: 11.0.162.203.in-addr.arpa
sách các nameserver Non-authoritative answer:
quản lý các domain
có đuôi vn
vn nameserver = DNS-hcm01.vnnic.net.vn
vn nameserver = ns.ripe.net
vn nameserver = DNS1.vn
vn nameserver = ns1.gip.net
vn nameserver = ns2.gip.net
vn nameserver = ns3.rip.net
vn nameserver = DNS1.vnnic.net.vn
vn nameserver = cheops.anu.edu.au
DNS-hcm01.vnnic.net.vn internet address = 203.162.87.66
ns.ripe.net AAAA IPv6 address = 2001:610:240:0:53:0:0:193
ns.ripe.net internet address = 193.0.0.193
DNS1.vn internet address = 203.162.3.235
ns1.gip.net internet address = 204.59.144.222
ns2.gip.net internet address = 204.59.1.222
DNS1.vnnic.net.vn internet address = 203.162.57.105
cheops.anu.edu.au internet address = 150.203.224.24
>
```



## Chương 5

### Dịch vụ truy cập từ xa và dịch vụ Proxy

Chương 5 cung cấp các kiến thức cơ bản của hai nội dung dịch vụ phổ biến trên mạng máy tính: dịch vụ truy cập từ xa và dịch vụ proxy.

Việc truy cập từ xa là nhu cầu thiết yếu mở rộng phạm vi hoạt động mạng của các tổ chức, công ty. Nội dung truy cập từ xa giới thiệu trong chương này là truy cập qua mạng thoại PSTN. Đây là hình thức truy cập từ xa cho tốc độ truy cập thấp vừa phải nhưng lại có tính phổ biến rộng rãi và dễ thiết lập nhất.

Dịch vụ proxy trên mạng được phát triển cho các mục đích tăng cường tốc độ truy cập cho khách hàng trong mạng, tiết kiệm được tài nguyên mạng (địa chỉ IP) và đảm bảo được an toàn cho mạng lưới khi bắt buộc phải cung cấp truy cập ra mạng ngoài hay ra mạng Internet. Thiết lập dịch vụ proxy là công tác mọi quản trị hệ thống mạng cần biết vì các nhu cầu kết nối liên mạng và kết nối Internet càng ngày càng trở nên không thể thiếu cho bất kỳ tổ chức, công ty nào.

Chương 5 yêu cầu các học viên nên trang bị các kiến thức cơ bản về mạng điện thoại PSTN, kiến thức về các giao thức mạng WAN PPP, SLIP... các giao thức xác thực như RADIUS... Trong phần proxy, học viên cần làm quen với khái niệm chuyển đổi địa chỉ NAT, hoạt động của các giao thức TCP/IP.

### Mục 1: Dịch vụ truy cập từ xa (Remote Access)

#### 1. Các khái niệm và các giao thức

##### 1.1. Tổng quan về dịch vụ truy cập từ xa.

Dịch vụ truy cập từ xa (Remote Access Service) cho phép người dùng từ xa có thể truy cập từ một máy tính qua một môi trường mạng truyền dẫn (ví dụ mạng điện thoại công cộng) đến một mạng dùng riêng như thể máy tính đó được kết nối trực tiếp trong mạng đó. Người dùng từ xa kết nối tới mạng đó thông qua một máy chủ dịch vụ gọi là máy chủ truy cập (Access server). Khi đó người dùng từ xa có thể sử dụng tài nguyên trên mạng như là một máy tính kết nối trực tiếp trong mạng đó. Dịch vụ truy cập từ xa cũng cung cấp khả năng tạo lập một kết nối WAN thông qua các mạng phương tiện truyền dẫn giá thành thấp như mạng thoại công cộng. Dịch vụ truy cập từ xa cũng là cầu nối để một máy tính hay một mạng máy tính thông qua nó được nối đến Internet theo cách được coi là hợp lý với chi phí không cao, phù hợp với các doanh nghiệp, tổ chức qui mô vừa và nhỏ. Khi lựa chọn và thiết kế giải pháp truy cập từ xa, chúng ta cần thiết phải quan tâm đến các yêu cầu sau:

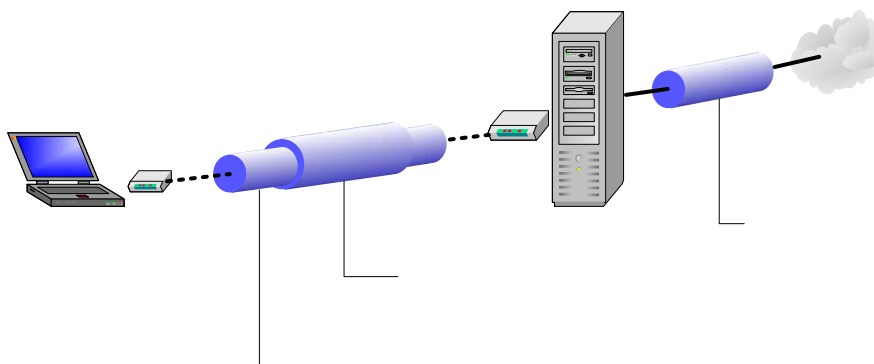
- Số lượng kết nối tối đa có thể để phục vụ người dùng từ xa.
- Các nguồn tài nguyên mà người dùng từ xa muốn muốn truy cập.

- Công nghệ, phương thức và thông lượng kết nối. Ví dụ, các kết nối có thể sử dụng modem thông qua mạng điện thoại công cộng PSTN, mạng số hoá tích hợp các dịch vụ ISDN...
- Các phương thức an toàn cho truy cập từ xa, phương thức xác thực người dùng, phương thức mã hoá dữ liệu
- Các giao thức mạng sử dụng để kết nối.

## 1.2.Kết nối truy cập từ xa và các giao thức sử dụng trong truy cập từ xa

### *Kết nối truy cập từ xa*

Tiến trình truy cập từ xa được mô tả như sau: người dùng từ xa khởi tạo một kết nối tới máy chủ truy cập. Kết nối này được tạo lập bằng việc sử dụng một giao thức truy cập từ xa (ví dụ giao thức PPP- Point to Point Protocol). Máy chủ truy cập xác thực người dùng và chấp nhận kết nối cho tới khi kết thúc bởi người dùng hoặc người quản trị hệ thống. Máy chủ truy cập đóng vai trò như một gateway bằng việc trao đổi dữ liệu giữa người dùng từ xa và mạng nội bộ. Bằng việc sử dụng kết nối này, người dùng từ xa gửi và nhận dữ liệu từ máy chủ truy cập. Dữ liệu được truyền trong các khuôn dạng được định nghĩa bởi các giao thức mạng (ví dụ giao thức TCP/IP) và sau đó được đóng gói bởi các giao thức truy cập từ xa. Tất cả các dịch vụ và các nguồn tài nguyên trong mạng người dùng từ xa đều có thể sử dụng thông qua kết nối truy cập từ xa này (hình 5.1)



Hình 5.1: Kết nối truy cập từ xa

### *Giao thức truy cập từ xa*

SLIP (Serial Line Interface Protocol), PPP và Microsoft RAS là các giao thức truy cập để tạo lập kết nối được sử dụng trong truy cập từ xa. SLIP là giao thức truy cập kết nối điểm-điểm và chỉ hỗ trợ sử dụng với giao thức IP, hiện nay hầu như không còn được sử dụng. Microsoft RAS là giao thức riêng của Microsoft hỗ trợ sử dụng cùng với các giao thức NetBIOS, NetBEUI và được sử dụng trong các phiên bản cũ của Microsoft.

PPP giao thức truy cập kết nối điểm-điểm với khá nhiều tính năng ưu việt, là một giao thức chuẩn được hầu hết các nhà cung cấp hỗ trợ. RFC 1661 định nghĩa về PPP. Chức năng cơ bản của PPP là đóng gói thông tin giao thức lớp mạng thông qua các liên kết điểm – điểm.

Cơ chế làm việc và vận hành của PPP như sau: Để thiết lập truyền thông, mỗi đầu cuối của liên kết PPP phải gửi các gói LCP (Link Control Protocol) để thiết lập và kiểm tra liên kết dữ liệu. Sau khi liên kết được thiết lập với các tính năng tùy chọn được sắp đặt và thỏa thuận giữa hai đầu liên kết, PPP gửi các gói NCP (Network Control Protocol) để lựa chọn và cấu hình một hoặc nhiều giao thức lớp mạng. Mỗi lần một giao thức lớp mạng lựa chọn đã được cấu hình, lưu lượng từ mỗi giao thức lớp mạng có thể gửi qua liên kết này. Liên kết tồn tại cho đến khi các gói LCP hoặc NCP đóng kết nối hoặc đến khi một sự kiện bên ngoài xảy ra (chẳng hạn như một sự kiện hẹn giờ hay một sự can thiệp của người quản trị). Nói cách khác PPP là một con đường mở đồng thời cho nhiều giao thức.

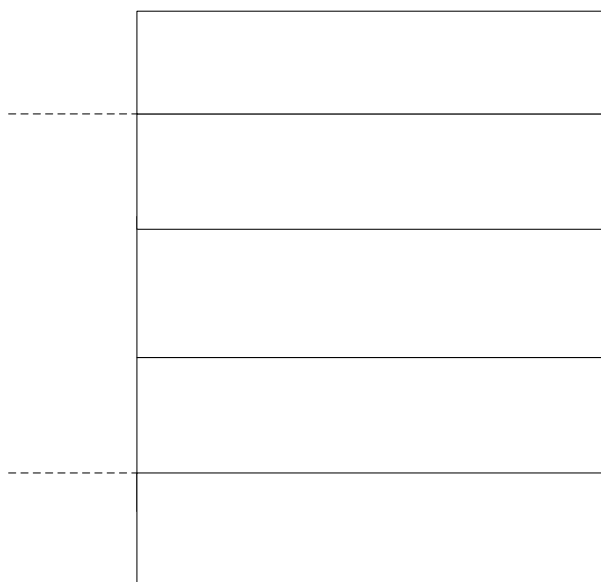
PPP khởi đầu được phát triển trong môi trường mạng IP, tuy nhiên nó thực hiện các chức năng độc lập với các giao thức lớp 3 và có thể được sử dụng cho các giao thức lớp mạng khác nhau. Như đã đề cập, PPP đóng gói các thủ tục lớp mạng đã được cấu hình để chuyển qua một liên kết PPP. PPP có nhiều các tính năng khiến nó rất mềm dẻo và linh hoạt, bao gồm:

- Ghép nối với các giao thức lớp mạng
- Lập cấu hình liên kết
- Kiểm tra chất lượng liên kết
- Nhận thực
- Nén các thông tin tiếp đầu
- Phát hiện lỗi
- Thỏa thuận các thông số liên kết

PPP hỗ trợ các tính năng này thông qua việc cung cấp LCP có khả năng mở rộng và NCP để thỏa thuận các thông số và các chức năng tùy chọn giữa các đầu cuối. Các giao thức, các tính năng tùy chọn, kiểu xác thực người dùng tất cả đều được truyền thông trong khi khởi tạo liên kết giữa hai điểm.

PPP có thể hoạt động trong bất kỳ giao diện DTE/DCE nào, PPP có thể hoạt động ở chế độ đồng bộ hoặc không đồng bộ. Ngoài những yêu cầu khác của các giao diện DTE/DCE, PPP không có hạn chế nào về tốc độ truyền dẫn.

Trong hầu hết các công nghệ mạng WAN, mô hình lớp được đưa ra để có những điểm liên hệ với mô hình OSI và để diễn tả vận hành của các công nghệ cụ thể. PPP không khác nhiều so với các công nghệ khác. PPP cũng có mô hình lớp để định nghĩa các cấu trúc và chức năng (hình 5.2)



Hình 5.2: Mô hình lớp PPP

Cũng như hầu hết các công nghệ, PPP có cấu trúc khung, cấu trúc này cho phép đóng gói bất cứ giao thức lớp 3 nào. Dưới đây là cấu trúc khung PPP (hình 5.3)



Hình 5.3: Cấu trúc khung PPP

Các trường của khung PPP như sau:

**Cờ:** độ dài 1 byte sử dụng để chỉ ra rằng đây là điểm bắt đầu hay kết thúc một khung, trường này là một dãy bit 01111110

**Địa chỉ:** độ dài 1 byte bao gồm dãy bit 11111111, là địa chỉ quảng bá chuẩn. PPP không gán từng địa chỉ riêng.

**Giao thức:** độ dài 2 byte, nhận dạng giao thức đóng gói. Giá trị cập nhật của trường này được chỉ ra trong RFC 1700

**Dữ liệu:** có độ dài thay đổi, có thể 0 hoặc nhiều byte là các dữ liệu cho kiểu giao thức cụ thể được chỉ ra trong trường giao thức. Phần cuối cùng của trường dữ liệu được nhận biết bằng cách đặt cờ và tiếp sau nó là 2 byte FCS. Giá trị ngầm định của trường này là 1500 byte. Tuy vậy giá trị lớn hơn có thể được sử dụng để tăng độ dài cho trường dữ liệu.

**FCS:** thường là 2 byte, có thể sử dụng 4 byte FCS để tăng khả năng phát hiện lỗi.

LCP có thể thỏa thuận để chấp nhận sự thay đổi cấu trúc khung PPP chuẩn giữa hai đầu cuối của liên kết. Các khung đã thay đổi luôn luôn dễ nhận biết hơn so với các khung chuẩn. LCP cung cấp phương pháp để thiết lập, cấu hình, duy trì và kết thúc một kết nối điểm-điểm. LCP thực hiện các chức năng này thông qua bốn giai đoạn. Đầu tiên, LCP thực hiện thiết lập và thỏa thuận cấu hình giữa liên kết điểm-điểm. Trước khi bắt kỳ đơn vị dữ liệu lớp mạng nào được chuyển, LCP đầu tiên phải mở kết nối và thỏa thuận các thông số thiết lập. Quá trình này được hoàn thành khi một khung nhận biết cấu hình đã được gửi và nhận. Tiếp theo, LCP xác định chất lượng liên kết. Liên kết được kiểm tra để xác định xem liệu chất lượng có đủ để khởi tạo các giao thức lớp mạng không. Việc truyền dẫn của giao thức lớp mạng bị đình lại cho đến khi giai đoạn này hoàn tất. LCP cho phép đây là một tùy chọn sau giai đoạn thiết lập và thỏa thuận cấu hình của liên kết. Sau đó LCP thực hiện thỏa thuận cấu hình giao thức lớp mạng. Các giao thức lớp mạng có thể được cấu hình riêng rẽ bởi NCP thích hợp và được khởi tạo hay dỡ bỏ vào bất kỳ thời điểm nào. Cuối cùng, LCP kết thúc liên kết khi xuất hiện yêu cầu từ người dùng hoặc theo các bộ định thời gian, do lỗi truyền dẫn hay do các yếu tố vật lý khác.

Ba kiểu khung LCP được sử dụng để hoàn thành các công việc đối với từng giai đoạn: khung thiết lập liên kết được sử dụng để thiết lập và cấu hình một liên kết, khung kết thúc liên kết được sử dụng để kết thúc một liên kết, khung duy trì liên kết được sử dụng để quản lý và gỡ rối liên kết.

#### *Các giao thức mạng sử dụng trong truy cập từ xa.*

Khi triển khai dịch vụ truy cập từ xa, các giao thức mạng thường được sử dụng là giao thức TCP/IP, IPX, NETBEUI.

TCP/IP là một bộ giao thức gồm có giao thức TCP và giao thức IP cùng làm việc với nhau để cung cấp phương tiện truyền thông trên mạng. TCP/IP là một bộ giao thức cơ bản, làm nền tảng cho truyền thông liên mạng là bộ giao thức mạng được sử dụng phổ biến nhất hiện nay. Với khả năng định tuyến và mở rộng, TCP/IP hỗ trợ một cách linh hoạt và phù hợp cho các tất cả các mạng.

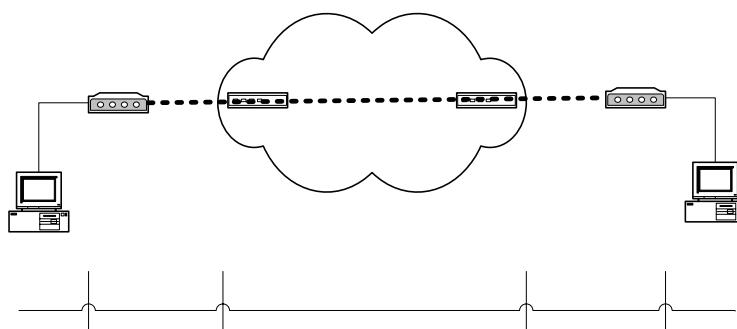
IPX (Internet Packet Exchange) là giao thức được sử dụng cho các mạng Novell NetWare. IPX là một giao thức có khả năng định tuyến và thường được sử dụng với các hệ thống mạng trước đây.

NetBEUI là giao thức dùng cho mạng cục bộ LAN của Microsoft. NetBEUI cho ta nhiều tiện ích và hầu như không phải làm gì nhiều với NetBEUI. Thông qua NetBEUI ta có thể truy cập tất cả các tài nguyên trên mạng. NETBEUI là một giao thức không có khả năng định tuyến và chỉ thích hợp với mô hình mạng nhỏ, đơn giản.

### 1.3. Modem và các phương thức kết nối vật lý.

#### 1. Modem.

Máy tính làm việc với dữ liệu dạng số, khi truyền thông trên môi trường truyền dẫn với các dạng tín hiệu khác (ví dụ như với mạng điện thoại công cộng làm việc với các tín hiệu tương tự) ta cần một thiết bị để chuyển đổi tín hiệu số thành tín hiệu thích nghi với môi trường truyền dẫn, thiết bị đó gọi là Modem (Modulator/demodulator). Như vậy Modem là một thiết bị chuyển đổi tín hiệu số sang dạng tín hiệu phù hợp với môi trường truyền dẫn và ngược lại. Hình dưới là một kết nối sử dụng modem qua mạng điện thoại điện hình (hình 5.4).



Hình 5.4: Kết nối sử dụng modem qua mạng điện thoại điện hình

Các modem sử dụng các phương pháp nén dữ liệu nhằm mục đích tăng tốc độ truyền dữ liệu. Hiệu suất nén dữ liệu phụ thuộc vào dữ liệu, có hai giao thức nén thường được sử dụng là V.42bis và MNP 5. hiệu suất nén của V.42bis và MNP 5 có thể thay đổi từ 0 đến 400 % hay cao hơn phụ thuộc vào dữ liệu tự nhiên

Chuẩn modem V.90 cho phép các modem nhận dữ liệu với tốc độ 56 Kbps qua mạng điện thoại công cộng (PSTN). V.90 xem mạng PSTN như là một mạng số và chúng sẽ mã hóa dòng dữ liệu xuống theo kỹ thuật số thay vì điều chế để gửi đi như các chuẩn điều chế trước đây. Trong khi đó theo hướng ngược lại từ khách hàng đến nhà cung cấp dịch vụ dòng dữ liệu lên vẫn được điều chế theo các nguyên tắc thông thường và tốc độ tối đa đạt được là 33.6 Kbps, giao thức hướng lên này dựa trên chuẩn V.34

Sự khác nhau giữa tín hiệu số ban đầu với tín hiệu số được phục hồi tại đầu nhận gọi là tạp âm lượng tử hóa (nhiều lượng tử), chính tạp âm này đã hạn chế tốc độ truyền dữ liệu. Giữa các modem đầu cuối có một cấu trúc hạ tầng cho việc kết nối đó là mạng thoại công cộng. Các chuẩn modem trước đây đều giả sử cả hai đầu của kết nối giống nhau là có một kết nối tương tự vào mạng điện thoại công cộng, công nghệ V.90 đã lợi dụng ưu điểm của tổ chức mạng mà một đầu kết nối giữa hệ thống truy cập từ xa và mạng thoại công cộng là dạng số hoàn toàn còn đầu kia vẫn được kết nối vào mạng PSTN theo dạng tương tự nhờ đó tận dụng được các ưu điểm của liên kết số tốc độ cao, vì chỉ có quá trình biến đổi A/D mới gây ra tạp âm với các kết nối số thì không có lượng tử hóa do đó nhiễu lượng tử rất ít trong cấu trúc mạng này.

Định luật shanon nói rằng đường dây điện thoại tương tự hạn chế tốc độ truyền dữ liệu ở khoảng 35 kbps mà không xem xét đến một thực tế là một đầu của truyền thông đã được số hóa nên giảm nhỏ lượng tạp âm gây ra sự chậm trễ trong việc truyền dữ liệu. Nhiều lượng tử đã giới hạn chuẩn truyền thông V.34 ở tốc độ 33.6 kbps, nhưng nhiều lượng tử chỉ có ảnh hưởng khi chuyển đổi tương tự - số mà không có ảnh hưởng khi chuyển đổi số-tương tự và đây chính là chìa khóa cho công nghệ V.90 đồng thời cũng giải thích được vì sao tốc độ download có thể đạt được 56 kbps còn khi upload tốc độ chỉ đạt 33.6 kbps. Dữ liệu chuyển đi từ modem số V.90 qua mạng PSTN là một dòng số với tốc độ 64 Kbps nhưng tại sao V.90 chỉ hỗ trợ tốc độ đến 56 Kbps, vì các lí do sau: Thứ nhất mặc dù nhiều lượng tử đã được bỏ qua nhưng nhiều mức thấp do bộ chuyển đổi số - tương tự là không tuyến tính, do ảnh hưởng của vòng loop nội hạt. Lý do thứ hai là các tổ chức quốc tế có qui định chặt chẽ về mức năng lượng tín hiệu nhằm hạn chế nhiễu xuyên âm giữa các dây dẫn đặt gần kề nhau, và qui định này tương ứng với mức năng lượng tối đa trên đường dây điện thoại tương ứng là 56 kbps

Để xây dựng một hệ thống truy cập từ xa qua mạng thoại công cộng đạt được tốc độ 56 kbps giữa hai đầu kết nối cần hội đủ ba điều kiện sau: thứ nhất, một đầu của kết nối (thường là đầu trung tâm mạng) phải là kết nối số tới mạng PSTN. Thứ hai, chuẩn modem V.90 hỗ trợ tại hai đầu cuối của nối kết. Thứ ba, chỉ có một chuyển đổi duy nhất số-tương tự trên mạng thoại giữa hai đầu của kết nối

Khi vận hành modem V.90 thăm dò đường thoại để quyết định xem nó sẽ làm việc theo tiêu chuẩn nào, nếu phát hiện ra bất kỳ một chuyển đổi số-tương tự nào thì nó đơn giản chỉ làm việc ở chuẩn V.34 và cũng cố gắng kết nối ở chuẩn này nếu modem đầu xa không hỗ trợ chuẩn V.90.

## *2. Các phương thức kết nối vật lý cơ bản:*

Một phương thức phổ biến và sẽ được dùng nhiều đó là kết nối qua mạng điện thoại công cộng (PSTN). Máy tính được nối qua một modem lắp đặt bên trong (Internal modem) hoặc qua cổng truyền số liệu nối tiếp COM port. Tốc độ truyền tối đa hiện nay có thể có được bằng phương thức này có thể lên đến 56 Kbps cho chiều lấy dữ liệu xuống và 33,6Kbps cho chiều truyền dữ liệu hướng lên với các chuẩn điều chế tín hiệu phổ biến V90, K56Flex, X2. Ta cũng có thể sử dụng modem có yêu cầu về hạ tầng cơ sở thấp hơn với chuẩn điều chế V.24, V.32Bis, V.32...

Phương thức thứ hai là sử dụng mạng truyền số liệu số đa dịch vụ ISDN. Phương thức này đòi hỏi chi phí cao hơn và ngày càng được phổ biến rộng rãi. Ta có được khá nhiều các lợi ích từ việc sử dụng mạng ISDN mà một trong số đó là tốc độ. Ta có thể sử dụng các lựa chọn ISDN 2B+D BRI (2x64Kbps dữ liệu + 16Kbps dùng cho điều khiển) hoặc 23B+D PRI (23x64Kbps + 64Kbps) thông qua thiết bị TA (Terminal Adapter) hay các card ISDN.

Một phương thức khác nhưng ít được sử dụng là qua mạng truyền số liệu X.25, tốc độ không cao nhưng an toàn và bảo mật cao hơn. Yêu cầu cho

người sử dụng trong trường hợp này là phải có sử dụng card truyền số liệu X.25 hoặc một thiết bị được gọi là PAD (Packet Assembled Disassembled). Ta cũng có thể sử dụng các kết nối trực tiếp qua cáp modem, phương thức này cho ta các kết nối tốc độ cao nhưng phải thông qua các modem truyền số liệu có giá thành cao.

## 2. An toàn trong truy cập từ xa

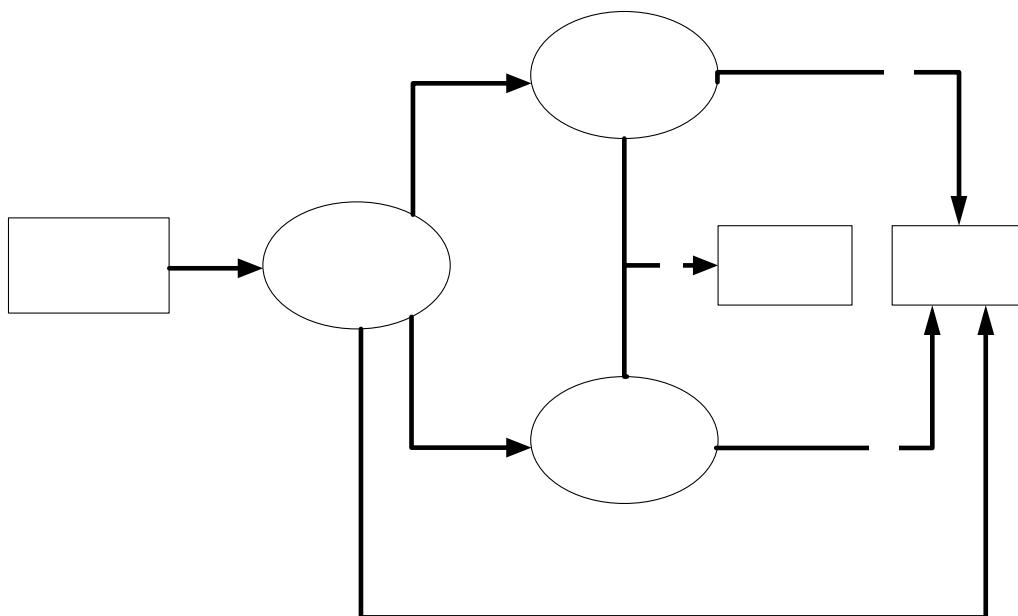
### 2.1. Các phương thức xác thực kết nối

#### 1. Quá trình nhận thực.

Tiến trình nhận thực với các giao thức xác thực được thực hiện khi người dùng từ xa có các yêu cầu xác thực tới máy chủ truy cập, một thỏa thuận giữa người dùng từ xa và máy chủ truy cập để xác định phương thức xác thực sẽ sử dụng. Nếu không có phương thức xác thực nào được sử dụng, tiến trình PPP sẽ khởi tạo kết nối giữa hai điểm ngay lập tức.

Phương thức xác thực có thể được sử dụng với các hình thức kiểm tra cơ sở dữ liệu địa phương (lưu trữ các thông tin về username và password ngay trên máy chủ truy cập) xem các thông tin về username và password được gửi đến có trùng với trong cơ sở dữ liệu hay không. Hoặc là gửi các yêu cầu xác thực tới một server khác để xác thực thường sử dụng là các RADIUS server (sẽ được trình bày ở phần sau)

Sau khi kiểm tra các thông tin gửi trả lại từ cơ sở dữ liệu địa phương hoặc từ RADIUS server. Nếu hợp lệ, tiến trình PPP sẽ khởi tạo một kết nối, nếu không yêu cầu kết nối của người dùng sẽ bị từ chối. (hình 5.5)

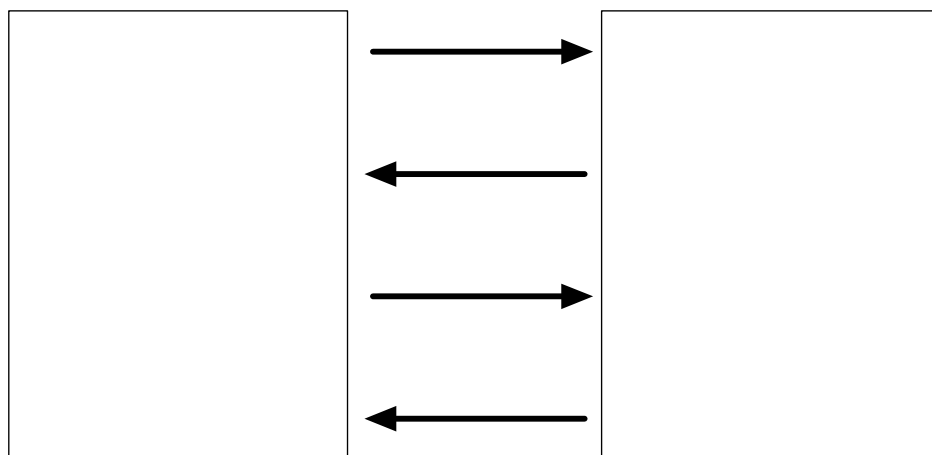


Hình 5.5: Xác thực kết nối



## 2. Giao thức xác thực PAP

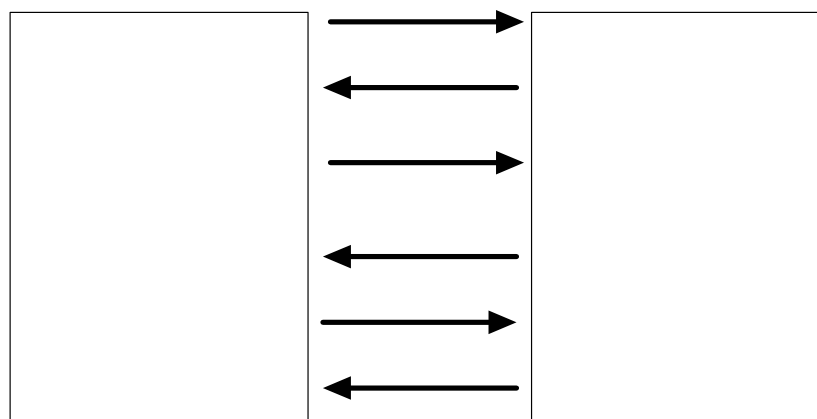
PAP là một phương thức xác thực kết nối không an toàn, nếu sử dụng một chương trình phân tích gói tin trên đường kết nối ta có thể nhìn thấy các thông tin về username và password dưới dạng đọc được. Điều này có nghĩa là các thông tin gửi đi từ người dùng từ xa tới máy chủ truy cập không được mã hóa mà được gửi đi dưới dạng đọc được đó chính là lý do PAP không an toàn. Hình dưới mô tả quá trình xác thực PAP, sau khi thỏa thuận giao thức xác thực PAP trên liên kết PPP giữa các đầu cuối, người dùng từ xa gửi thông tin (username:nntrong, password:ras123) tới máy chủ truy cập từ xa, sau khi kiểm tra các thông tin này trong cơ sở dữ liệu của mình, máy chủ truy cập từ xa sẽ quyết định xem liệu yêu cầu kết nối có được thực hiện hay không (hình 5.6)



Hình 5.6: Giao thức xác thực PAP

## 3. Giao thức xác thực CHAP

Sau khi thỏa thuận giao thức xác thực CHAP trên liên kết PPP giữa các đầu cuối, máy chủ truy cập gửi một “challenge” tới người dùng từ xa. Người dùng từ xa phúc đáp lại một giá trị được tính toán sử dụng tiến trình xử lý một chiều (hash). máy chủ truy cập kiểm tra và so sánh thông tin phúc đáp với giá trị hash mà tự nó tính được. Nếu các giá trị này bằng nhau việc xác thực là thành công, ngược lại kết nối sẽ bị hủy bỏ. Như vậy CHAP cung cấp cơ chế an toàn thông qua việc sử dụng giá trị challenge thay đổi, duy nhất và không thể đoán được. Các thông tin về username và password không được gửi đi dưới dạng đọc được trên mạng và do đó chống lại các truy cập trái phép bằng hình thức lấy trộm password trên đường kết nối (hình 5.7).



Remote user

Hình 5.7: Giao thức xác thực CHAP

#### 4. Giao thức xác thực mở rộng EAP

Ngoài các giao thức kiểm tra tính xác thực cơ bản PAP, CHAP, trong Microsoft Windows 2000 hỗ trợ thêm một số giao thức cho ta các khả năng nâng cao độ an toàn, bảo mật và đa truy nhập đó là giao thức xác thực mở rộng EAP (Extensible Authentication Protocol).

EAP cho phép có được một cơ cấu xác thực tùy ý để công nhận một kết nối gọi vào. Người sử dụng và máy chủ truy nhập từ xa sẽ trao đổi để tìm ra giao thức chính xác được sử dụng. EAP hỗ trợ các hình thức sau:

- Sử dụng các card vật lý dùng để cung cấp mật khẩu. Các card này dùng một số các phương thức xác thực khác nhau như sử dụng các đoạn mã thay đổi theo mỗi lượt sử dụng.
- Hỗ trợ MD5-CHAP, giao thức mã hoá tên người sử dụng, mật khẩu bằng thuật toán mã hoá MD5 (Message Digest 5).
- Hỗ trợ sử dụng cho các thẻ thông minh. Thẻ thông minh bao gồm thẻ và thiết bị đọc thẻ. Các thông tin xác thực về cá nhân người dùng được ghi lại trong các thẻ này.
- Các nhà phát triển phần mềm độc lập sử dụng giao diện chương trình ứng dụng EAP có thể phát triển các module chương trình cho các công nghệ áp dụng cho thẻ nhận dạng, thẻ thông minh, các phần cứng sinh học như nhận dạng võng mạc, các hệ thống sử dụng mật khẩu một lần.

Inputs name  
when

### 2.2. Các phương thức mã hóa dữ liệu

*Dịch vụ truy cập từ xa cung cấp cơ chế an toàn bằng việc mã hóa và giải mã dữ liệu truyền giữa người dùng truy cập từ xa và máy chủ truy cập.*

*Có hai phương thức mã hóa dữ liệu thường được sử dụng đó là mã hóa đối xứng và mã hóa phi đối xứng.*

*Phương thức mã hoá đối xứng*, thông tin ở dạng đọc được, được mã hoá sử dụng khóa bí mật (khóa mà chỉ có người mã hoá mới biết được) tạo thành thông tin đã được mã hoá. ở phía nhận, thông tin mã hoá được giải mã cùng với khóa bí mật thành dạng gốc ban đầu. Điểm chú ý của phương pháp mã hoá này là việc sử dụng khóa bí mật cho cả quá trình mã hoá và quá trình giải mã. Do đó, nhược điểm chính của phương thức này là cần có quá trình trao đổi khóa bí mật, dẫn đến tình trạng dễ bị lộ khóa bí mật.

*Phương pháp mã hoá phi đối xứng*, để khắc phục điểm hạn chế của phương pháp mã hoá đối xứng là quá trình trao đổi khóa bí mật, người ta đã sử dụng phương pháp mã hoá phi đối xứng sử dụng một cặp khóa tương ứng với nhau gọi là phương thức mã hoá phi đối xứng dùng khóa công khai. Phương thức mã hóa này sử dụng hai khóa là khóa công khai và khóa bí mật có các quan hệ toán học với nhau. Trong đó khóa bí mật được giữ bí mật và không có khả năng bị lộ do không cần phải trao đổi trên mạng. Khóa công khai không phải giữ bí mật và mọi người đều có thể nhận được khóa này. Do phương thức mã hóa này sử dụng 2 khóa khác nhau, nên người ta gọi nó là phương thức mã hóa phi đối xứng. Mặc dù khóa bí mật được giữ bí mật, nhưng không giống với "secret Key" được sử dụng trong phương thức mã hóa đối xứng sử dụng khóa bí mật do khóa bí mật không được trao đổi trên mạng. Khóa công khai và khóa bí mật tương ứng của nó có quan hệ toán học với nhau và được sinh ra sau khi thực hiện các hàm toán học; nhưng các hàm toán học này luôn thỏa mãn điều kiện là sao cho không thể tìm được khóa bí mật từ khóa công cộng và ngược lại. Do có mối quan hệ toán học với nhau, thông tin được mã hóa bằng khóa công khai chỉ có thể giải mã được bằng khóa bí mật tương ứng.

Giao thức thường được sử dụng để mã hóa dữ liệu hiện nay là giao thức IPsec. Hầu hết các máy chủ truy cập dựa trên phần cứng hay mềm hiện nay đều hỗ trợ IPsec. IPsec là một giao thức bao gồm các chuẩn mở bảo đảm các vấn đề bảo mật, an toàn và toàn vẹn dữ liệu cho các kết nối qua mạng sử dụng giao thức IP bằng các biện pháp mã hoá. IPsec bảo vệ chống lại các hành động phá hoại từ bên ngoài. Các client khởi tạo một mối liên quan bảo mật hoạt động tương tự như khóa công khai để mã hoá dữ liệu.

Ta có thể sử dụng các chính sách áp dụng cho IPsec để cấu hình nó. Các chính sách cung cấp nhiều mức độ và khả năng để bảo đảm an toàn cho từng loại dữ liệu. Các chính sách cho IPsec sẽ được thiết lập cho phù hợp với từng người dùng, từng nhóm người dùng, cho một ứng dụng, một nhóm miền hay toàn bộ hệ thống mạng.

### **3. Triển khai dịch vụ truy cập từ xa**

#### **3.1. Kết nối gọi vào và kết nối gọi ra**

Cấu hình máy chủ truy cập để tạo lập các kết nối gọi vào cho phép người dùng từ xa truy cập vào mạng. Các thông số cơ bản thường được cấu

hình khi tạo lập các kết nối gọi vào bao gồm xác định các phương thức xác thực người dùng, mã hóa hay không mã hóa dữ liệu, các phương thức mã hóa dữ liệu nếu yêu cầu, các giao thức mạng sẽ được sử dụng cho truy nhập từ xa, các thiết đặt về chính sách và các quyền truy nhập của người dùng từ xa, mức độ được phép truy nhập như thế nào, xác định phương thức cấp phát địa chỉ IP cho máy truy nhập từ xa, các yêu cầu cấu hình để tạo lập các kết nối VPN...

Kết nối gọi ra có thể được thiết lập để gọi ra tới một mạng dùng riêng hoặc tới một ISP. Trong windows 2000 hỗ trợ các hình thức kết nối sau:

*Nối tới mạng dùng riêng*, ta sẽ phải cung cấp số điện thoại nơi sẽ nối đến. Có thể là số điện thoại của ISP, của mạng dùng riêng hay của máy tính phía xa. Xác định quyền sử dụng kết nối này. .

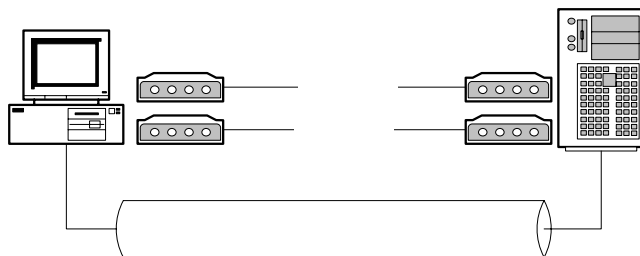
*Nối tới Internet*, hai lựa chọn có thể là sử dụng truy cập qua đường thoại và sử dụng truy cập qua mạng LAN. Sử dụng đường thoại, các vấn đề ta cần quan tâm là số điện thoại truy nhập, tên và mật khẩu được cung cấp bởi ISP. Sử dụng LAN, ta sẽ phải quan tâm đến proxy server và một số thiết đặt khác.

Tạo lập kết nối VPN, *VPN là một mạng sử dụng các kết nối dùng giao thức tạo đường hầm (PPTP, L2TP, IPSEC,...) để tạo được các kết nối an toàn, bảo đảm thông tin không bị xâm phạm khi truyền tải qua các mạng công cộng. Tương tự như khi tạo lập một kết nối gọi ra, Nếu cần thiết phải thông qua một ISP trung gian trước khi nối tới mạng dùng riêng, lựa chọn một kết nối gọi ra. Cung cấp địa chỉ máy chủ, địa chỉ mạng nơi mà ta đang muốn nối tới. Các thiết lập khác là thiết đặt các quyền sử dụng kết nối.*

*Tạo lập kết nối trực tiếp với máy tính khác*, lựa chọn này được sử dụng để kết nối trực tiếp hai máy tính với nhau thông qua một cáp được thiết kế cho nối trực tiếp hai máy tính. Một trong hai máy tính được lựa chọn là chủ và máy tính kia được lựa chọn là tớ. Lựa chọn thiết bị cổng nơi hai máy tính nối với nhau.

### 3.2. Kết nối sử dụng đa luồng (Multilink)

Multilink là sự kết hợp nhiều liên kết vật lý trong một liên kết logic duy nhất nhằm gia tăng băng thông cho kết nối. Multilink cho phép sử dụng hai hoặc nhiều hơn các cổng truyền thông như là một cổng duy nhất có tốc độ cao. Điều này có nghĩa là ta có thể sử dụng hai modem để kết nối Internet với tốc độ cao gấp đôi so với việc sử dụng một modem. Multilink gia tăng băng thông và giảm độ trễ giữa các hệ thống bằng cơ chế chia các gói dữ liệu và gửi đi trên các mạch song song. Multilink sử dụng giao thức MPPP cho việc quản lý các kết nối của mình. Để sử dụng, MPPP cần phải được hỗ trợ ở cả hai phía của kết nối (hình 5.8).



Hình 5.8: Kết nối sử dụng đa luồng

Hình vẽ mô tả kết nối sử dụng Multilink, khi người dùng từ xa sử dụng hai modem và hai đường thoại kết nối với máy chủ truy cập, mỗi kết nối là việc theo chuẩn V.90 có tốc độ 56 kbps sử dụng kỹ thuật Multilink cho phép đạt tốc độ 112 Kbps giữa máy truy cập từ xa và máy chủ truy cập.

### 3.3. Các chính sách thiết lập cho dịch vụ truy nhập từ xa

Chính sách truy nhập từ xa là tập hợp các điều kiện và các thiết đặt cho phép người quản trị mạng gán cho mỗi người dùng từ xa các quyền truy cập và mức độ sử dụng các nguồn tài nguyên trên mạng. Ta có thể dùng các chính sách để có được nhiều các lựa chọn phù hợp với từng mức độ người dùng, tăng tính mềm dẻo, tính năng động khi cấp quyền truy nhập cho người dùng.

Một chính sách truy nhập từ xa thông thường bao gồm ba thành phần nhằm cung cấp các truy nhập an toàn có kiểm soát đến máy chủ truy cập.

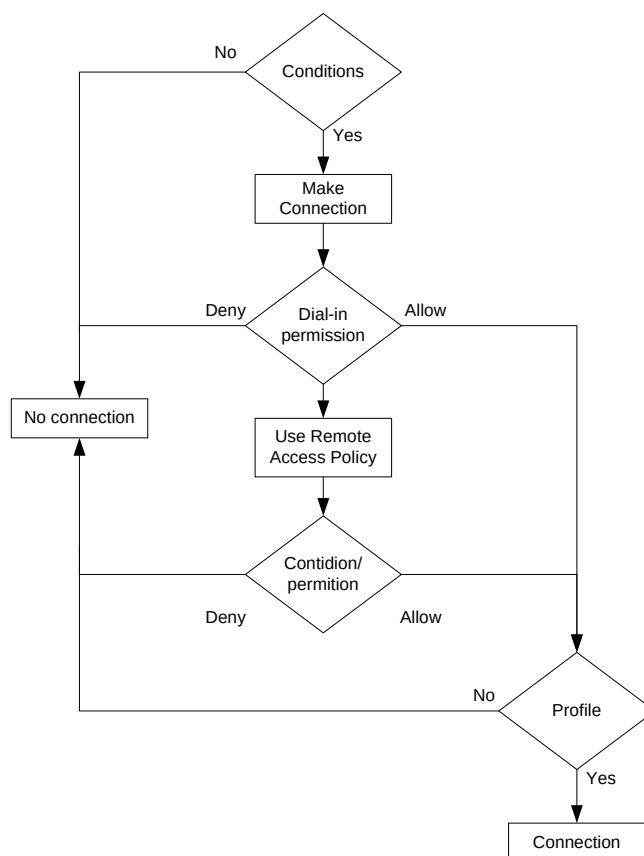
Các điều kiện (Conditions): là một danh sách các tham số như ngày tháng, nhóm người dùng, mã người gọi, địa chỉ IP phù hợp với máy trạm đang nối đến máy chủ truy cập. Bộ chính sách điều kiện đầu tiên này tương ứng với các thông số của yêu cầu kết nối gọi đến được xử lý đối với sự cho phép truy cập và cấu hình.

Sự cho phép (Permission): Các kết nối truy nhập từ xa được cho phép và gán trực tiếp tới mỗi người dùng bởi các thiết đặt trong các chính sách truy nhập từ xa. Ví dụ một chính sách có thể gán tất cả người dùng trong một nhóm nào đây quyền truy cập chỉ trong giờ làm việc hành chính từ 8:00 A.M đến 5:00 P.M, hay đồng thời gán cho một nhóm người dùng khác quyền truy cập liên tục 24/24.

Profile: Mỗi chính sách đều bao gồm một thiết đặt của profile áp dụng cho kết nối như là các thủ tục xác thực hay mã hóa. Các thiết đặt trong profile được thi hành ngay tới các kết nối. Ví dụ: nếu một profile thiết đặt cho một kết nối mà người dùng chỉ được phép sử dụng trong 30 phút mỗi lần thì người dùng sẽ bị ngắt kết nối tới máy chủ truy cập trong sau 30 phút.

Quá trình thực thi các chính sách truy cập từ xa được mô tả bằng hình dưới (hình 5.9)

Remote



Hình 5.9: Quá trình thực thi các chính sách truy cập từ xa

Các điều kiện được gửi tới để tạo một kết nối, nếu các điều kiện gửi tới này không thích hợp truy cập bị từ chối, nếu thích hợp các điều kiện này được sử dụng để xác định sự truy cập. Tiếp theo máy chủ truy cập kiểm tra các cho phép quay số vào người dùng sẽ bị từ chối nếu thiết đặt này là Deny và được phép truy cập nếu là Allow, nếu thiết đặt là sử dụng các chính sách truy cập để xác định quyền truy cập thì sự cho phép của các chính sách sẽ quyết định quyền truy cập của người dùng. Nếu các chính sách này từ chối truy cập người dùng sẽ bị ngắt kết nối, nếu là cho phép sẽ chuyển tới để kiểm tra các chính sách trong profile là bước cuối cùng để xác định quyền truy cập của người dùng.

### 3.4. Sử dụng dịch vụ gán địa chỉ động DHCP cho truy cập từ xa

Khi thiết lập một máy chủ truy cập để cho phép người dùng từ xa truy cập vào mạng, ta có thể lựa chọn phương thức mà các máy từ xa có thể nhận được địa chỉ IP.

Với phương thức cấu hình địa chỉ IP tĩnh ngay trên các máy trạm, người dùng phải cấu hình bằng tay địa chỉ IP trên mỗi máy truy cập. Sử dụng phương thức này phải đảm bảo rằng các thông tin cấu hình địa chỉ IP là hợp lệ và chưa được sử dụng trên mạng. Đồng thời các thông tin về default gateway, DNS...cũng phải được cấu hình bằng tay một cách chính xác. Vì lý do này

khuyến nghị không nên sử dụng phương pháp này cho việc gán IP cho các máy truy cập từ xa.

Máy chủ truy cập có thể gán động một địa chỉ IP cho các máy truy cập từ xa. Địa chỉ IP này thuộc trong khoảng địa chỉ mà ta đã cấu hình trên máy chủ truy cập. Sử dụng phương pháp này ta cần phải đảm bảo rằng khoảng địa chỉ IP này được dành riêng để cấp phát cho các máy truy cập từ xa.

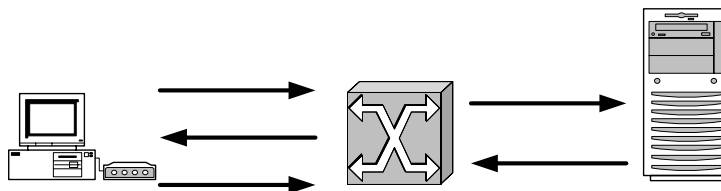
Phương thức sử dụng DHCP server, máy chủ truy cập nhận địa chỉ IP từ DHCP server và gán cho các máy truy cập từ xa. Phương thức này rất linh hoạt, không cần phải dành riêng một khoảng địa chỉ IP dự trữ cho máy truy cập từ xa và thường được sử dụng trong một mạng có tổ chức và đa dạng trong các hình thức kết nối. Địa chỉ IP được cấp phát cho các máy truy cập từ xa một cách tự động, các thông tin cấu hình khác (Gateway, DNS server...) cũng được cung cấp tập trung, chính xác tới từng máy truy cập đồng thời các máy truy cập cũng không cần thiết phải cấu hình lại khi có các thay đổi về cấu trúc mạng.

Hoạt động của DHCP được mô tả như sau: Mỗi khi DHCP client khởi động, nó yêu cầu một địa chỉ IP từ DHCP server. Khi DHCP server nhận yêu cầu, nó chọn một địa chỉ IP trong khoảng IP đã được định nghĩa trong cơ sở dữ liệu của nó. DHCP server cấp phát địa chỉ IP tới DHCP client. Nếu DHCP client chấp nhận địa chỉ IP này, DHCP server cho thuê địa chỉ IP này trong một khoảng thời gian cụ thể (tùy theo thiết đặt). Các thông tin về địa chỉ IP được gửi từ DHCP server tới DHCP client thường bao gồm các thành phần sau: địa chỉ IP, subnet mask, các giá trị lựa chọn khác (default gateway, địa chỉ DNS server).

### 3.5. Sử dụng RadiusServer để xác thực kết nối cho truy cập từ xa.

#### 1. Hoạt động của Radius server

RADIUS là một giao thức làm việc theo mô hình client/server. RADIUS cung cấp dịch vụ xác thực và tính cước cho mạng truy nhập gián tiếp. Radius client là một máy chủ truy cập tiếp nhận các yêu cầu xác thực từ người dùng từ xa và chuyển các yêu cầu này tới Radius server. Radius server nhận các yêu cầu kết nối của người dùng xác thực và sau đó trả về các thông tin cấu hình cần thiết cho Radius client để chuyển dịch vụ tới người sử dụng (hình 5.10).



Hình 5.10: Hoạt động của Radius server

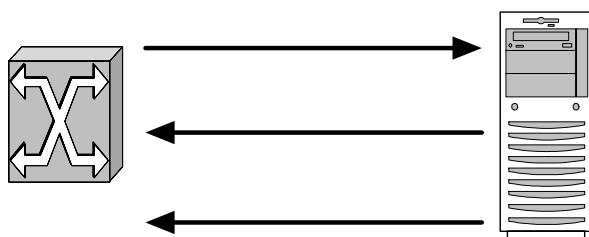
Quá trình hoạt động được mô tả như sau:

1. Người sử dụng từ xa khởi tạo quá trình xác thực PPP tới máy chủ truy cập
2. Máy chủ truy cập yêu cầu người dùng cung cấp thông tin về username và password bằng các giao thức PAP hoặc CHAP.
3. Người dùng từ xa phúc đáp và gửi thông tin username và password tới máy chủ truy cập.
4. Máy chủ truy cập (Radius client) gửi chuyển tiếp các thông tin username và password đã được mã hóa tới Radius server
5. Radius server trả lời với các thông tin chấp nhận hay từ chối. Radius client thực hiện theo các dịch vụ và các thông số dịch vụ đi cùng với các phúc đáp chấp nhận hay từ chối từ Radius server

## 2. Nhận thực và cấp quyền

Khi Radius server nhận yêu cầu truy cập từ Radius client, Radius server tìm kiếm trong cơ sở dữ liệu các thông tin về yêu cầu này. Nếu username không có trong cơ sở dữ liệu này thì hoặc một profile mặc định được chuyển hoặc một thông báo từ chối truy cập được chuyển tới Radius client.

Trong RADIUS nhận thực và cấp quyền đi đôi với nhau, nếu username có trong cơ sở dữ liệu và password được xác nhận là đúng thì Radius server gửi trả về thông báo truy cập được chấp nhận, thông báo này bao gồm một danh sách các cặp đặc tính- giá trị mô tả các thông số được sử dụng cho phiên làm việc. Các thông số điển hình bao gồm: kiểu dịch vụ, kiểu giao thức, địa chỉ gán cho người dùng (động hoặc tĩnh), danh sách truy cập được áp dụng hay một định tuyến tĩnh được cài đặt trong bảng định tuyến của máy chủ truy cập. Thông tin cấu hình trong Radius server sẽ xác định những gì sẽ được cài đặt trên máy chủ truy cập. Hình vẽ dưới đây mô tả quá trình nhận thực và cấp quyền của Radius server (hình 5.11)



Hình 5.11: Nhận thực và cấp quyền

## 3. Tính cước

Các vấn đề về xử lý cước của RADIUS hoạt động độc lập với nhận thực và cấp quyền. Chức năng tính cước cho phép ghi lại dữ liệu được gửi tại thời điểm bắt đầu và kết thúc của một phiên làm việc và đưa ra các con số về mặt sử dụng tài nguyên như (thời gian, số gói, số byte...) được sử dụng trong phiên làm việc đó.

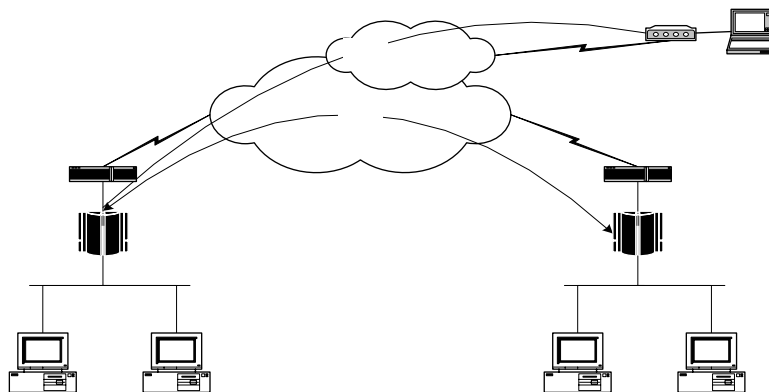


### 3.6. Mạng riêng ảo và kết nối dùng dịch vụ truy cập từ xa

VPN (Virtual Private Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (ví dụ mạng Internet), sử dụng mạng công cộng cho việc truyền thông riêng tư.

Giải pháp VPN cho phép người dùng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính bằng việc sử dụng hạ tầng mạng là một mạng công cộng như là Internet. Như vậy thay vì phải thực hiện một kết nối đường dài tới trụ sở chính người sử dụng chỉ cần tạo lập một kết nối nội hạt tới một ISP khi đó bằng công nghệ VPN một kết nối VPN sẽ được thiết lập giữa người dùng với mạng trung tâm. Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các địa điểm ở xa khác nhau thông qua các kết nối trực tiếp (leased line) từ các địa điểm đó tới một ISP. Như vậy kết nối VPN cho phép một tổ chức giảm chi phí gọi đường dài qua Dialup hay chi phí thuê đường leadline cho khoảng cách xa thay vì như vậy chỉ cần các kết nối nội hạt và điều này là tiết kiệm được chi phí. VPN gửi dữ liệu giữa các đầu cuối, dữ liệu được đóng gói, với các Header cung cấp thông tin định tuyến cho phép chuyển dữ liệu qua một liên kết hoặc một liên mạng công cộng tới đích. Dữ liệu chuyển đi được mã hoá để đảm bảo an toàn, các gói dữ liệu truyền thông trên mạng là không thể đọc mà không có khoá giải mã. Liên kết mà trong đó dữ liệu được đóng gói và mã hoá là một kết nối VPN.

*Các hình thức kết nối:* Có hai kiểu kết nối VPN, kết nối VPN truy cập từ xa và kết nối Site-to-site. Một kết nối VPN truy cập từ xa được thiết lập bởi một máy tính PC tới một mạng dùng riêng. VPN gateway cung cấp truy cập tới các tài nguyên của mạng dùng riêng. Các gói dữ liệu gửi qua kết nối VPN được khởi tạo từ các client. VPN client thực hiện việc xác thực tới VPN gateway. Kết nối site-to-site, được thiết lập bởi các VPN gateway và kết nối hai phần của một mạng dùng riêng. (hình 5.12).



Hình 5.12: Kết nối site-to-site

*Tunnel:* là một phần quan trọng trong việc xây dựng một mạng VPN. Các chuẩn truyền thông sử dụng để quản lý các tunnel và đóng gói dữ liệu của VPN bao gồm các giao thức làm việc ở lớp 2 như PPTP (Point-to-Point Tunneling Protocol) được phát triển bởi Microsoft hỗ trợ trong môi trường mạng

Windows, L2TP (Layer 2 Tunnelling Protocol) được phát triển bởi Cisco. IPsec là một giao thức làm việc ở lớp 3, IPsec được phát triển bởi IETF và ngày càng được sử dụng rộng rãi.

L2TP và PPTP có mục đích là cung cấp các đường hầm dữ liệu thông qua mạng truyền dữ liệu công cộng. L2TP khác với PPTP ở chỗ nó tạo lập đường hầm nhưng không mã hoá dữ liệu. L2TP cung cấp các đường hầm bảo mật khi cùng hoạt động với các công nghệ mã hoá khác như IPSec. IPSec không yêu cầu phải có L2TP nhưng các chức năng mã hoá của nó đưa đến cho L2TP khả năng cung cấp các kênh thông tin bảo mật, cung cấp các giải pháp VPN. L2TP và PPTP cùng sử dụng PPP để đóng gói, thêm bớt thông tin tiếp đầu và truyền tải dữ liệu qua mạng.

Các kết nối VPN có các đặc trưng sau: đóng gói (Encapsulation), xác thực (Authentication) và mã hoá dữ liệu (Data encryption)

*Đóng gói dữ liệu:* Công nghệ VPN sử dụng một phương thức đóng gói dữ liệu trong đó cho phép dữ liệu truyền được qua mạng công cộng qua các giao thức tạo đường hầm.

*Xác thực:* Khi một kết nối VPN được thiết lập, VPN gateway sẽ xác thực VPN client đang yêu cầu kết nối và nếu được được phép kết nối được thực hiện. Nếu sự xác thực kết nối là qua lại được sử dụng, thì VPN client sẽ thực hiện việc xác thực lại VPN gateway, để đảm bảo rằng đây chính là server mà mình cần gọi. Xác thực dữ liệu và tính toàn vẹn của dữ liệu: để xác nhận rằng dữ liệu đang được gửi từ một đầu của kết nối khác mà không bị thay đổi trong quá trình truyền, dữ liệu phải bao gồm một trường kiểm tra bằng mật mã dự trên một khoá mã hoá đã biết chỉ giữa người gửi và người nhận

*Mã hóa dữ liệu:* để đảm bảo dữ liệu truyền trên mạng, dữ liệu phải được mã hoá tại đầu gửi và giải mã tại đầu nhận. Việc mã hoá và giải mã dữ liệu phụ thuộc và người gửi và người nhận đang sử dụng phương thức mã hoá và giải mã nào.

### 3.7. Sử dụng Network and Dial-up Connection

Network and Dial-up Connection (NDC) là một công cụ được Microsoft phát triển để hỗ trợ việc tạo lập các kết nối trong đó bao gồm các kết nối cho truy cập từ xa. Với việc sử dụng NDC ta có thể truy cập tới các tài nguyên dù đang ở trong mạng hay ở một địa điểm ở xa. Các kết nối được khởi tạo, thiết lập cấu hình, lưu giữ và quản lý bởi NDC. Mỗi một kết nối bao gồm một bộ các đặc tính được sử dụng để thiết lập liên kết giữa một máy tính tới máy tính hoặc mạng khác. Các kết nối gọi ra được liên lạc với một máy chủ truy cập ở xa bằng các hình thức truy cập gián tiếp thương là qua các mạng truyền dẫn mạng thoại công cộng, mạng ISDN. NDC cũng hỗ trợ việc thiết lập các kết nối gọi vào có nghĩa là đóng vai trò như một máy chủ truy cập.

Bởi vì tất cả các dịch vụ và các phương thức truyền thông đều được thiết lập trong kết nối nên không cần phải sử dụng các công cụ khác để cấu hình cho kết nối. Ví dụ để thiết lập cho một kết nối dial-up bao gồm các đặc tính được

sử dụng trước, trong và sau khi kết nối. Các thông số này bao gồm: modem sẽ quay số, kiểu mã hóa password được sử dụng và các giao thức mạng sẽ sử dụng sau kết nối. Trạng thái kết nối bao gồm thời gian và tốc độ cũng được chính kết nối hiển thị mà không cần bất cứ một công cụ nào khác.

### 3.8. Một số vấn đề xử lý sự cố trong truy cập từ xa

Các vấn đề liên quan đến sự cố trong truy cập từ xa, thường bao gồm:

*Giám sát truy cập từ xa:* giám sát máy chủ truy cập là phương pháp tốt nhất thường sử dụng để tìm ra nguồn gốc của các vấn đề xảy ra sự cố. Mỗi một chương trình phần mềm hay thiết bị phần cứng máy chủ truy cập bao giờ cũng có các công cụ sử dụng để giám sát và ghi lại các sự kiện xảy ra (trong các file log) đối với mỗi phiên truy cập từ xa.

*Theo dõi các kết nối truy cập từ xa:* khả năng theo dõi các kết nối truy cập từ xa của một Máy chủ truy cập cho ta xử lý các vấn đề phức tạp về sự cố mạng. Các thông tin theo dõi một kết nối từ xa thường rất phức tạp và khá chi tiết do đó để phân tích và xử lý cần thiết người quản trị mạng phải có kinh nghiệm và trình độ về hệ thống mạng.

*Xử lý các sự cố về phần cứng:* bao gồm các thiết bị truyền thông tại người dùng và tại máy chủ truy cập. Đối với các thiết bị tại người dùng (thường là các modem, các mạng...), hãy xem tài liệu về sản phẩm đó hay hỏi nhà cung cấp thiết bị về sản phẩm của họ về các cách kiểm tra và xác định lỗi của sản phẩm này. Nếu kết nối sử dụng modem, hãy kiểm tra rằng modem đã được cài đặt đúng chưa. Trong Windows 2000 các bước kiểm tra như sau:

- o Trong Control Panel, kích Phone and Modem Options
- o Trong trang modem, kích tên modem, sau đó kích Properties
- o Kích Diagnostics, sau đó kích Query Modem.

Nếu modem đã được cài đặt đúng, bộ các thông số về modem sẽ được hiển thị, ngược lại hãy kiểm tra và cài đặt lại modem, trong trường hợp cuối cùng hãy hỏi nhà sản xuất thiết bị này. Để nhận thêm các thông tin về modem trong khi đang cố gắng tạo lập một kết nối, hãy xem thông tin trong log file để tìm ra nguyên nhân gặp sự cố. Để ghi các thông tin vào log file thực hiện theo các bước sau:

- o Trong Control Panel, kích Phone and Modem Options
- o Trong trang modem, kích tên modem, sau đó kích Properties
- o Kích Diagnostics, sau đó kích lựa chọn Record a log, sau đó kích

OK.

Đối với thiết bị truyền thông tại máy chủ truy cập: Kiểm tra các thiết bị phần cứng tương tự như trong trường hợp thiết bị tại người dùng, đồng thời kiểm tra log file về các sự kiện xảy ra với hệ thống để tìm ra nguyên nhân sự cố. Một cách khác để kiểm tra modem tại máy chủ truy cập là sử dụng một đường điện thoại và gọi tới modem đó sau đó nghe xem modem đó có trả lời và cố gắng tạo một kết nối hay không. Nếu không có tín hiệu tạo kết nối từ

modem đó thì có thể kết luận rằng đang có một vấn đề lỗi về modem tại máy chủ truy cập

*Xử lý các sự cố về đường truyền thông:* Thường là do cáp được đấu sai hay vì nguyên nhân từ nhà cung cấp dịch vụ điện thoại. Hãy kiểm tra đường điện thoại từ người dùng tới máy chủ truy cập bằng cách gọi điện thoại thông thường, thông qua chất lượng cuộc gọi ta cũng có thể phần nào dự đoán được chất lượng của đường truyền.

*Xử lý các thiết đặt về cấu hình:* Sau khi xác định rằng các vấn đề về phần cứng cũng như đường truyền thông đều tốt, bước tiếp theo ta kiểm tra các thiết đặt về cấu hình, bao gồm:

Các thiết đặt về mạng: lỗi cấu hình về mạng xảy ra khi đã tạo kết nối thành công nhưng vẫn không thể truy cập được các nguồn tài nguyên trên mạng, các lỗi thường xảy ra như việc phân giải tên chưa hoạt động, các lỗi về định tuyến...khi lỗi về cấu hình mạng xảy ra, trước tiên ta kiểm tra rằng các máy kết nối trực tiếp (không thông qua dịch vụ truy cập từ xa) có thể truy cập được vào các nguồn tài nguyên trên mạng. Sau đó kiểm tra các cấu hình về TCP/IP bằng việc sử dụng lệnh `ipconfig /all` trên máy client. Kiểm tra rằng các thông số như DNS, địa chỉ IP, các thông số về định tuyến đã được thiết đặt đúng chưa. Sử dụng lệnh `ping` để kiểm tra kết nối mạng đã làm việc.

Các thiết đặt Máy chủ truy cập: Các thiết đặt trên máy chủ truy cập với các thông số sai khi tạo lập kết nối có thể là nguyên nhân người dùng không thể truy cập vào các nguồn tài nguyên trên mạng. Để hỗ trợ cho việc xác định nguyên nhân gây lỗi, kiểm tra các sự kiện đã ghi log trên máy chủ truy cập và client, trong một số trường hợp cần thiết phải theo dõi (tracing) các kết nối trên máy chủ truy cập.

Các thiết đặt trên máy người dùng từ xa: kiểm tra các giao thức mạng làm việc trên client, các giao thức mạng làm việc trên client phải được hỗ trợ bởi máy chủ truy cập. Ví dụ, nếu người dùng từ xa thiết đặt trên client các giao thức NWLink, IPX/SPX và máy chủ truy cập chỉ hỗ trợ sử dụng TCP/IP, thì kết nối sẽ không thành công.

#### 4. Bài tập thực hành

*Yêu cầu về Phòng học lý thuyết:* Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

*Thiết bị thực hành:* Đã cài phần mềm Windows 2000 Advance Server. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

##### **Bài 1: Thiết lập dialup networking để tạo ra kết nối Internet. truy cập Internet và giới thiệu các dịch vụ cơ bản**

- ✓ Đăng nhập vào hệ thống với quyền Administrator.

- ✓ Kích Start, trở settings, sau đó kích Network and Dial-up Connections
- ✓ Trong Network and Dial-up Connections, kích đúp vào Make New Connection.
- ✓ Trong Network Connection Wizard, kích Next, có hai lựa chọn có thể sử dụng là Dial-up to private network hoặc Dial-up to the Internet.
- ✓ Nếu chọn Dial-up to private network, đưa vào số điện thoại truy cập của nhà cung cấp.
- ✓ Nếu chọn Dial-up to the Internet, lúc đó Internet Connection Wizard sẽ bắt đầu, làm theo các bước chỉ dẫn.
- ✓ Nếu muốn tất cả người dùng đều có thể sử dụng kết nối này thì lựa chọn, For all users, sau đó kích Next. Nếu muốn chỉ người dùng hiện tại sử dụng thì lựa chọn Only for myself, sau đó kích Next.
- ✓ Nếu đã lựa chọn Only for myself thì chuyển đến bước cuối cùng, Nếu lựa chọn For all users và muốn các máy tính khác trên mạng có thể chia sẻ kết nối này hãy lựa chọn Enable Internet Connection Sharing for this connection.
- ✓ Thiết đặt ngầm định là bất kỳ máy tính nào cũng có thể khởi tạo kết nối này một cách tự động, nếu muốn bỏ ngầm định này hãy xóa lựa chọn Enable on-demand dialing, sau đó kích next
- ✓ Đưa vào tên của kết nối và kích Finish.

## **Bài 2: Cài đặt và cấu hình dịch vụ truy cập từ xa cho phép người dùng từ xa truy cập vào mạng trên hệ điều hành Windows 2000 server.**

### **Bước 1:**

Cài đặt máy chủ dịch vụ truy cập từ xa

- ✓ Đăng nhập vào hệ thống với quyền Administrator
- ✓ Mở Routing and Remote Access từ menu Administrator Tools
- ✓ Kích chuột phải vào tên Server sau đó chọn Configure and Enable Routing and remote Access.
- ✓ Kích bản Routing and Remote Access Server Setup xuất hiện, kích next
- ✓ Trong trang common Configuration, chọn Remote access server, sau đó kích next
- ✓ Trong trang Remote Client Protocol, xác định các giao thức sẽ hỗ trợ cho truy cập từ xa, sau đó kích next
- ✓ Trong trang Network Selection, lựa chọn kết nối mạng sẽ gán cho các máy truy cập từ xa, sau đó kích next
- ✓ Trong trang IP Address Assignment, lựa chọn Automatically hoặc From specified range of addresses cho việc gán các địa chỉ IP tới các máy truy cập từ xa

- ✓ Trong trang Managing Multiple Remote Access Servers cho phép lựa chọn cấu hình RADIUS, kích next
- ✓ Kích Finish để kết thúc.

### **Bước 2:**

Thiết đặt tài khoản cho người dùng từ xa. Thiết lập một tài khoản có tên RemoteUser

- ✓ Đăng nhập với quyền Administrator
- ✓ Mở Active Directory Users and Computers từ menu Administrator Tools
- ✓ Kích chuột phải vào Users, chọn new và kích vào User
- ✓ Trong hộp thoại New Object-User, điền RemoteUser vào First name
- ✓ Trong hộp User logon name, gõ RemoteUser
- ✓ Thiết đặt Password cho tài khoản này, kích next sau đó kích Finish.
- ✓ Kích chuột phải vào RemoteUser sau đó kích Properties
- ✓ Trong trang Dial-In tab, kích Allow access, sau đó click OK

Thiết lập một Global group tên là RemoteGroup, sau đó thêm tài khoản người dùng vừa thiết lập vào nhóm này

- ✓ Kích chuột phải vào Users, chọn new sau đó kích Group
- ✓ Trong hộp thoại New Object-Group, mục Group name gõ vào RemoteGroup
- ✓ Trong mục Group scope kiểm tra Global đã được lựa chọn, trong mục Group type kiểm tra rằng Security đã được lựa chọn, sau đó kích OK
- ✓ Mở hộp thoại Properties của RemoteGroup
- ✓ Trong trang Member, kích Add
- ✓ Trong hộp thoại Select Users, Contacts, Computers, hoặc Group, Look in box, kiểm tra domain đã được hiển thị
- ✓ Trong danh sách các đối tượng, kích RemoteUser, kích Add sau đó kích OK
- ✓ Kích OK để đóng hộp thoại RemoteGroup Properties

### **Bước 3:**

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

### **Bước 4:**

Cấu hình cho phép tài khoản RemoteUser truy cập vào mạng được điều khiển truy cập bởi các chính sách truy cập từ xa (Remote access policy)

- ✓ Mở lại Active Directory Users and Computers từ menu Administrator Tools

- ✓ Mở hộp thoại Properties của tài khoản RemoteUser
- ✓ Trong trang Dial-in tab, kích Control access though Remote Policy sau đó kích OK, lưu ý rằng điều khiển vùng (Domain Controller) phải chạy ở chế độ Native.
- ✓ Thu nhỏ cửa sổ Active Directory Users and Computers

#### **Bước 5:**

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

#### **Bước 6:**

Sử dụng RRAS để thiết lập một chính sách mới đối với người dùng từ xa, tên chính sách này là Allow RemoteGroup Access cho phép người dùng trong nhóm RemoteGroup truy cập.

- ✓ Mở Routing and Remote Access từ menu Administrator Tools
- ✓ Mở rộng tên máy chủ đang cấu hình, kích chuột phải vào Remote Access Policy sau đó chọn New Remote Access Policy
- ✓ Trong trang Policy Name, gõ vào Allow RemoteGroup Access sau đó kích Next
- ✓ Trong trang Condition, kích Add trong hộp thoại Select Attribute kích Windows-Groups sau đó kích Add
- ✓ Trong hộp thoại Groups kích Add
- ✓ Trong hộp thoại Select Groups, trong danh sách Look in, kích vào tên domain
- ✓ Trong hộp thoại Select Groups, dưới Name kích RemoteGroups kích Add sau đó kích OK
- ✓ Trong hộp thoại Groups kích OK
- ✓ Trong trang Condition kích Next
- ✓ Trong trang Permissions kích Grant remote access permission sau đó kích Next
- ✓ Trong trang User Profile kích Finish
- ✓ Trong trang Routing and Remote Access kích Remote Access Policies sau đó kích chuột phải Allow RemoteGroup access sau đó kích Move Up

#### **Bước 7:**

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

#### **Bước 8:**

Cấu hình để default policy được thi hành trước:

- ✓ Mở trang Routing and Remote Access, kích chuột phải RemoteGroup sau đó kích Move Down.

- ✓ Đóng cửa sổ Routing and Remote Access

#### **Bước 9:**

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

#### **Bước 10:**

Cấu hình cho phép truy cập sử dụng Properties của RemoteUser

- ✓ Mở lại Active Directory Users and Computers từ menu Administrator Tools

- ✓ Mở Properties của RemoteUser

- ✓ Trong trang Dial-in, kích Allow access sau đó kích OK

- ✓ Đóng Active Directory Users and Computers.

#### **Bước 11:**

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại

### **Bài 3: Cấu hình VPN server và thiết lập VPN Client, kiểm tra kết nối từ VPN Client tới VPN server**

#### **Bước 1:**

Cấu hình cho kết nối VPN gọi vào

- ✓ Đăng nhập vào hệ thống với quyền Administrator

- ✓ Mở Routing and Remote Access từ menu Administrator Tools

- ✓ Kích chuột phải vào tên Server (Server là tên máy chủ đang cấu hình)

- ✓ Kích bản thiết lập Routing and Remote Access xuất hiện, kích next

- ✓ Trong trang Network Selection, mục Name kiểm tra tên đã lựa chọn sau đó Click next

- ✓ Trong trang IP Address Assignment, kích From a specified range of addresses

- ✓ Trong trang Address Range Assignment, kích New

- ✓ Điền địa chỉ IP vào ô Start IP address và điền vào số địa chỉ vào ô Number of Address

- ✓ Kích OK, sau đó kích next

- ✓ Trong trang Managing Multiple Remote Access Servers, lựa chọn No, I don't want to set up this server to use RADIUS now, kích next sau đó kích Finish



- ✓ Kích OK để đóng hộp thoại Routing and Remote Access.

Cấu hình cho phép tài khoản Administrator truy cập vào mạng

- ✓ Mở Active Directory Users and Computers từ menu Administrator Tools.

- ✓ Mở rộng tên domain kích Users, kích đúp chuột vào Administrator

- ✓ Trong mục Dial-in, chọn Allow acces sau đó kích OK.

- ✓ Đóng cửa sổ Active Directory Users and Computers

## **Bước 2:**

Cấu hình cho kết nối VPN gọi ra. Để kiểm tra dịch vụ truy cập từ xa đã làm việc phục vụ cho những người dùng từ xa, ta thiết lập một nối kết tới VPN server.

- ✓ Kích chuột phải vào My Network Places, sau đó kích Properties

- ✓ Trong cửa sổ Network Dialup Connections, kích đúp chuột vào Make new connection

- ✓ Trong trang Network Connection Type, kích Connect to a private network through the Internet, sau đó kích next

- ✓ Trong trang Destination Address page, gõ vào địa chỉ IP của máy cài đặt VPN server, sau đó kích next

- ✓ Trong trang Connection Availability, kích Only for my self, kích next sau đó kích Finish

- ✓ Khởi tạo kết nối tới VPN server

- ✓ Trong hộp thoại Connect Virtual Private Connection, kiểm tra tài khoản đăng nhập là Administrator và Password sau đó kích connect

- ✓ Kích OK để đóng thông báo Connnection Complete

- ✓ Đóng cửa sổ Network Dialup Connections.

Sử dụng tiện ích Ipconfig để xác nhận rằng bạn đã thiết lập được một kết nối VPN và nhận được địa IP cho kết nối này lưu ý rằng đại chỉ IP cho kết nối VPN này là dãy địa chỉ tĩnh mà VPN server cấp phát

Đóng kết nối

- ✓ Kích đúp vào biểu tượng Connection trong khay hệ thống

- ✓ Trong hộp thoại Vitual Private Connection Status, kích disconnect

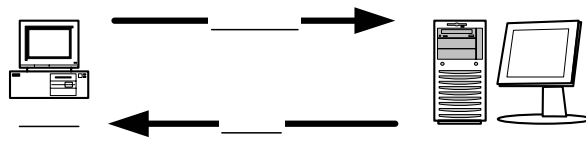
- ✓ Đóng tất cả các cửa sổ lại

## **Mục 2 : Dịch vụ Proxy - Giải pháp cho việc kết nối mạng dùng riêng ra Internet**

### **1. Các khái niệm**

#### **1.1. Mô hình client server và một số khả năng ứng dụng**

Mô hình chuẩn cho các ứng dụng trên mạng là mô hình client-server. Trong mô hình này máy tính đóng vai trò là một client là máy tính có nhu cầu cần phục vụ dịch vụ và máy tính đóng vai trò là một server là máy tính có thể đáp ứng được các yêu cầu về dịch vụ đó từ các client. Khái niệm client-server chỉ mang tính tương đối, điều này có nghĩa là một máy có thể lúc này đóng vai trò là client và lúc khác lại đóng vai trò là server. Nhìn chung, client là một máy tính cá nhân, còn các Server là các máy tính có cấu hình mạnh có chứa các cơ sở dữ liệu và các chương trình ứng dụng để phục vụ một dịch vụ nào đấy từ các yêu cầu của client (hình 5.13).



Hình 5.13: Mô hình client server

Cách thức hoạt động của mô hình client-server như sau: một tiến trình trên server khởi tạo luôn ở trạng thái chờ yêu cầu từ các tiến trình client, tiến trình tại client được khởi tạo có thể trên cùng hệ thống hoặc trên các hệ thống khác được kết nối thông qua mạng, tiến trình client thường được khởi tạo bởi các lệnh từ người dùng. Tiến trình client ra yêu cầu và gửi chúng qua mạng tới server để yêu cầu được phục vụ các dịch vụ. Tiến trình trên server thực hiện việc xác định yêu cầu hợp lệ từ client sau đó phục vụ và trả kết quả tới client và tiếp tục chờ đợi các yêu cầu khác. Một số kiểu dịch vụ mà server có thể cung cấp như: dịch vụ về thời gian (trả yêu cầu thông tin về thời gian tới client), dịch vụ in ấn (phục vụ yêu cầu in tại client), dịch vụ file (gửi, nhận và các thao tác về file cho client), thi hành các lệnh từ client trên server...

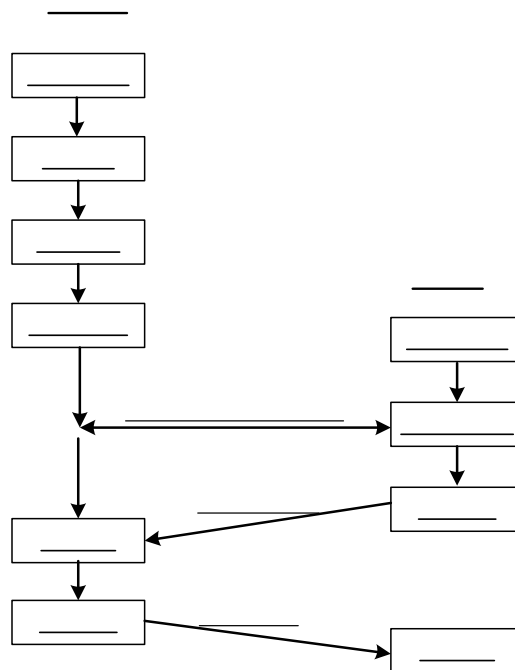
Dịch vụ web là một dịch vụ cơ bản trên mạng Internet hoạt động theo mô hình client-server. Trình duyệt Web (Internet Explorer, Netscape...) trên các máy client sử dụng giao thức TCP/IP để đưa ra các yêu cầu HTTP tới máy server. Trình duyệt có thể đưa ra các yêu cầu một trang web cụ thể hay yêu cầu thông tin trong các cơ sở dữ liệu. Máy server sử dụng phần mềm của nó phân tích các yêu cầu từ các gói tin nhận được kiểm tra tính hợp lệ của client và thực hiện phục vụ các yêu cầu đó cụ thể là gửi trả lại client một trang web cụ thể hay các thông tin trên cơ sở dữ liệu dưới dạng một trang web. Server là nơi lưu trữ nội dung thông tin các website, phần mềm trên server cho phép server xác định được trang cần yêu cầu và gửi tới client. Cơ sở dữ liệu và các ứng dụng tương tự khác trên máy chủ được khai thác và kết nối qua các chương trình như CGI (Common Gateway Interface), khi các máy server nhận được yêu cầu về tra cứu trong cơ sở dữ liệu, nó chuyển yêu cầu tới server có chứa cơ sở dữ liệu hoặc ứng dụng để xử lý qua CGI.

## 1.2. Socket

Một kết nối được định nghĩa như là một liên kết truyền thông giữa các tiến trình, như vậy để xác định một kết nối cần phải xác định các thành phần sau: {Protocol, local-addr, local-process, remote-addr, remote-process}

Trong đó local-addr và remote-addr là địa chỉ của các máy địa phương và máy từ xa. local-process, remote-process để xác định vị trí tiến trình trên mỗi hệ thống. Chúng ta định nghĩa một nửa kết nối là {Protocol, local-addr, local-process} và {Protocol, remote-addr, remote-process} hay còn gọi là một socket.

Chúng ta đã biết để xác định một máy ta dựa vào địa chỉ IP của nó, nhưng trên một máy có vô số các tiến trình ứng dụng đang chạy, để xác định vị trí các tiến trình ứng dụng này người ta định danh cho mỗi tiến trình một số hiệu cổng, giao thức TCP sử dụng 16 bit cho việc định danh các cổng tiến trình và qui ước số hiệu cổng từ 1-1023 được sử dụng cho các tiến trình chuẩn (như FTP qui ước sử dụng cổng 21, dịch vụ WEB qui ước cổng 80, dịch vụ gửi thư SMTP cổng 25...) số hiệu cổng từ 1024- 65535 dành cho các ứng dụng của người dùng. Như vậy một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. Một kết nối TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng.



Hình 5.14: Socket

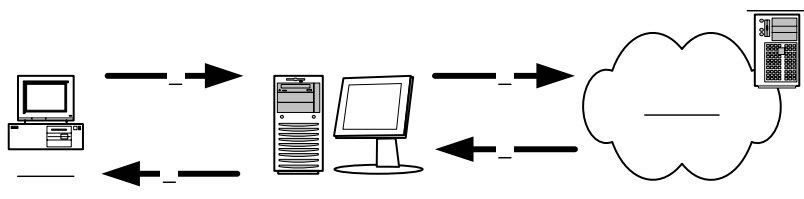
Quá trình thiết lập một socket với các lời gọi hệ thống được mô tả như sau: server thiết lập một socket với các thông số đặc tả các thủ tục truyền thông như (TCP, UDP, XNS...) và các kiểu truyền thông (SOCK\_STREAM,

SOCK\_DGRAM...), sau đó liên kết tới socket này các thông số về địa chỉ như IP và các cổng TCP/UDP sau đó server ở chế độ chờ và chấp nhận kết nối đến từ client.

### 1.3. Phương thức hoạt động và đặc điểm của dịch vụ Proxy

#### 1. Phương thức hoạt động

Dịch vụ proxy được triển khai nhằm mục đích phục vụ các kết nối từ các máy tính trong mạng dùng riêng ra Internet. Khi đăng ký sử dụng dịch vụ internet tới nhà cung cấp dịch vụ, khách hàng sẽ được cấp hữu hạn số lượng địa chỉ IP từ nhà cung cấp, số lượng IP nhận được không đủ để cấp cho các máy tính trạm. Mặt khác với nhu cầu kết nối mạng dùng riêng ra Internet mà không muốn thay đổi lại cấu trúc mạng hiện tại đồng thời muốn gia tăng khả năng thi hành của mạng qua một kết nối Internet duy nhất và muốn kiểm soát tất cả các thông tin vào ra, muốn cấp quyền và ghi lại các thông tin truy cập của người sử dụng... Dịch vụ proxy đáp ứng được tất cả các yêu cầu trên. Hoạt động trên cơ sở mô hình client-server. Quá trình hoạt động của dịch vụ proxy theo các bước như sau:

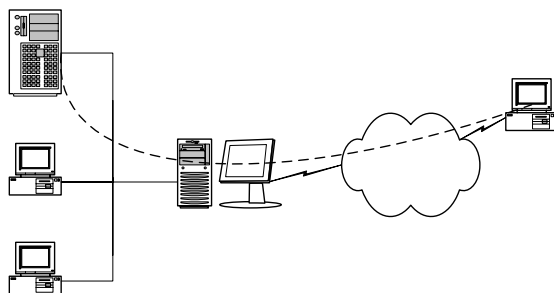


Hình 5.15: Hoạt động của dịch vụ Proxy

- 1 Client yêu cầu một đối tượng trên mạng Internet
- 1 Proxy server tiếp nhận yêu cầu, kiểm tra tính hợp lệ cũng như thực hiện việc xác thực client nếu thỏa mãn proxy server gửi yêu cầu đối tượng này tới server trên Internet.
- 1 Server trên Internet gửi đối tượng yêu cầu về cho proxy server.
- 1 Proxy server gửi trả đối tượng về cho client

Ta có thể thiết lập proxy server để phục vụ cho nhiều dịch vụ như dịch vụ truyền file, dịch vụ web, dịch vụ thư điện tử... Mỗi một dịch vụ cần có một proxy server cụ thể để phục vụ các yêu cầu đặc thù của dịch vụ đó từ các client.

Proxy server còn có thể được cấu hình để cho phép quảng bá các server thuộc mạng trong ra ngoài Internet với mức độ an toàn cao. Ví dụ ta có thể thiết lập một web server thuộc mạng trong và thiết lập các qui tắc quảng bá web trên proxy server để cho phép quảng bá web server này ra ngoài Internet. Tất cả các yêu cầu truy cập web đến được chấp nhận bởi proxy server và proxy server sẽ thực hiện việc chuyển tiếp yêu cầu tới web server thuộc mạng trong (hình 5.16)



Hình 5.16: Hoạt động của dịch vụ Proxy

Các client được tổ chức trong một cấu trúc mạng gọi là mạng trong (Inside network) hay còn gọi là mạng dùng riêng. IANA (Internet Assigned Numbers Authority) đã dành riêng 3 khoảng địa chỉ IP tương ứng với 3 lớp mạng tiêu chuẩn cho các mạng dùng riêng đó là:

- 10.0.0.0 - 10.255.255.255 (lớp A)
- 172.16.0.0 - 172.31.255.255 (lớp B)
- 192.168.0.0 - 192.168.255.255 (lớp C)

Các địa chỉ này sử dụng cho các client trong mạng dùng riêng mà không được gán cho bất cứ máy chủ nào trên mạng Internet. Trong việc thiết kế và cấu hình mạng dùng riêng khuyến nghị nên sử dụng các khoảng địa chỉ IP này.

Khái niệm mạng ngoài (Outside network) là để chỉ vùng mà các server thuộc vào. Các địa chỉ sử dụng trên mạng này là các địa chỉ IP được đăng ký hợp lệ của nhà cung cấp dịch vụ Internet.

Proxy server sử dụng hai giao tiếp, giao tiếp mạng trong và giao tiếp ngoài. Giao tiếp trong điển hình là các các mạng sử dụng cho việc kết nối giữa proxy server với mạng dùng riêng và có địa chỉ được gán là địa chỉ thuộc mạng dùng riêng. Tất cả các thông tin giữa client thuộc mạng dùng riêng và proxy server được thực hiện thông qua giao tiếp này. Giao tiếp ngoài thường bằng các hình thức truy cập gián tiếp qua mạng điện thoại công cộng và qua các mạng bằng kết nối trực tiếp tới mạng ngoài. Giao tiếp ngoài được gán địa chỉ IP thuộc mạng ngoài được cung cấp hợp lệ bởi nhà cung cấp dịch vụ Internet.

## 2. Đặc điểm

Proxy Server kết nối mạng dùng riêng với mạng Internet toàn cầu và cũng cho phép các máy tính trên mạng internet có thể truy cập các tài nguyên trong mạng dùng riêng.

Proxy Server tăng cường khả năng kết nối ra Internet của các máy tính trong mạng dùng riêng bằng cách tập hợp các yêu cầu truy cập Internet từ các máy tính trong mạng và sau khi nhận được kết quả từ Internet sẽ trả lời lại cho máy có yêu cầu ban đầu.

Ngoài ra proxy server còn có khả năng bảo mật và kiểm soát truy cập Internet của các máy tính trong mạng dùng riêng. Cho phép thiết đặt các chính sách truy cập tới từng người dùng.

Proxy server lưu trữ tạm thời các kết quả đã được lấy từ Internet về nhằm trả lời cho các yêu cầu truy cập Internet với cùng địa chỉ. Việc lưu trữ này cho phép các yêu cầu truy cập Internet với cùng địa chỉ sẽ không cần phải lấy lại kết quả từ Internet, làm giảm thời gian truy cập Internet, tăng cường hoạt động của mạng và giảm tải trên đường kết nối Internet. Các công việc lưu trữ này gọi là quá trình cache.

#### 1.4. Cache và các phương thức cache

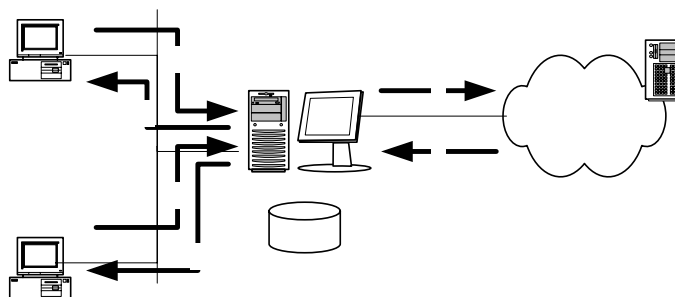
Nhằm tăng cường khả năng truy cập Internet từ các máy tính trạm trong mạng sử dụng dịch vụ proxy ta sử dụng các phương thức cache. Dịch vụ proxy sử dụng cache để lưu trữ bản sao của các đối tượng đã được truy cập trước đó. Tất cả các đối tượng đều có thể được lưu trữ (như hình ảnh và các tệp tin), tuy nhiên một số đối tượng như yêu cầu xác thực (Authenticate) và sử dụng SSL (Secure Socket Layer) không được cache. Như vậy với các đối tượng đã được cache, khi một yêu cầu từ một máy tính trạm tới proxy server, proxy server thay vì kết nối tới địa chỉ mà máy tính trạm yêu cầu sẽ tìm kiếm trong cache các đối tượng thỏa mãn và gửi trả kết quả về máy tính trạm. Như vậy cache cho phép cải thiện hiệu năng truy cập Internet của các máy trạm và làm giảm lưu lượng trên đường kết nối Internet. Vấn đề gặp phải khi sử dụng cache là khi các đối tượng được cache có sự thay đổi từ nguồn, các máy tính trạm yêu cầu một đối tượng tới proxy server, proxy server lấy đối tượng trong cache để phục vụ và như vậy thông tin chuyển tới các máy tính trạm là thông tin cũ so với nguồn, để giải quyết vấn đề này cần phải có các chính sách để cache các đối tượng đồng thời các đối tượng phải liên tục được cập nhật mới. Ví dụ: thông thường một địa chỉ WEB thì các đối tượng về hình ảnh ít có sự thay đổi còn nội dung text thường có sự thay đổi do đó ta có thể thiết đặt chỉ cache những đối tượng hình ảnh, những đối tượng có nội dung text thì không cache, điều này không ảnh hưởng tới hiệu suất truy cập vì các tệp tin về hình ảnh thường có kích thước rất lớn so với các đối tượng có nội dung text, việc cập nhật các đối tượng như thế nào phụ thuộc vào các phương thức cache mà ta sẽ trình bày dưới đây.

Proxy server thực thi cache cho các đối tượng được yêu cầu một cách có chu kỳ để tăng hiệu suất của mạng. Ta có thể thiết lập cache để đảm bảo rằng nó bao gồm những dữ liệu thường hay các client sử dụng nhất. Proxy server có thể sử dụng cho phép thông tin giữa mạng dùng riêng và Internet, việc thông tin có thể là client trong mạng truy cập Internet-trong trường hợp này proxy server thực hiện Forward caching, cũng có thể là client ngoài truy cập tới mạng trong (tới các server được quảng bá)-trong trường hợp này proxy server thực hiện reverse caching. Cả hai trường hợp đều có được từ khả năng của proxy server là lưu trữ thông tin (tạm thời) làm cho việc truyền thông tin được nhanh hơn, sau đây là các tính chất của cache proxy server:

- Phân cache: khi cài đặt một mảng các máy proxy server ta sẽ thiết lập được việc phân phối nội dung cache. Proxy server cho phép ghép nhiều hệ thống thành một cache logic duy nhất.
- Cache phân cấp: Khả năng phân phối cache còn có thể chuyên sâu hơn bằng cách cài đặt chế độ cache phân cấp liên kết một loạt các máy proxy server với nhau để client có thể truy cập tới gần chúng nhất.

- Cache định kỳ: sử dụng cache định kỳ nội dung download đối với các yêu cầu thường xuyên của các client
- Reverse cache: proxy server có thể cache các nội dung của các server quảng bá do đó tăng hiệu suất và khả năng truy cập, mọi đặc tính cache của proxy server đều có thể áp dụng cho nội dung trên các server quảng bá.

Proxy server có thể được triển khai như một Forward cache nhằm cung cấp tính năng cache cho các client mạng trong truy cập Internet. Proxy server duy trì bộ cache tập trung của các đối tượng Internet thường được yêu cầu có thể truy cập từ bất kỳ trình duyệt từ máy client. Các đối tượng phục vụ cho các yêu cầu từ các đĩa cache yêu cầu tác vụ xử lý nhỏ hơn đáng kể so với các đối tượng từ Internet, việc này tăng cường hiệu suất của trình duyệt trên client, giảm thời gian hồi đáp và giảm việc chiếm băng thông cho kết nối Internet. Hình vẽ sau mô tả proxy server xử lý các yêu cầu của người dùng ra sao (hình 6.17)



Hình 5.17: Hoạt động của dịch vụ Proxy

Hình trên mô tả quá trình các client trong mạng dùng riêng truy cập ra ngoài Internet nhưng tiến trình này cũng tương tự đối với các cache reverse (khi người dùng trên Internet truy cập vào các Server quảng bá) các bước bao gồm;

- 1 Client 1 yêu cầu một đối tượng trên mạng Internet
- 2 Proxy server kiểm tra xem đối tượng có trong cache hay không. Nếu đối tượng không có trong cache của proxy server thì proxy server gửi yêu cầu đối tượng tới server trên Internet.
- 3 Server trên Internet gửi đối tượng yêu cầu về cho proxy server .
- 4 proxy server giữ bản copy của đối tượng trong cache của nó và trả đối tượng về cho client1
- 5 Client 2 gửi một yêu cầu về đối tượng tương tự
- 6 Proxy server gửi cho client 2 đối tượng từ cache của nó chứ không phải từ Internet nữa.

Ta có thể triển khai dịch vụ proxy để quảng bá các server trong mạng dùng riêng ra ngoài Internet. Với các yêu cầu đến, proxy server có thể đóng vai trò như là một server bên ngoài, đáp ứng các yêu cầu của client từ các nội dung web trong cache của nó. Proxy server chuyển tiếp các yêu cầu cho server chỉ khi nào cache của nó không thể phục vụ yêu cầu đó (*Reverse cache*).

Lựa chọn các phương thức cache dựa trên các yếu tố: không gian ổ cứng sử dụng, đối tượng nào được cache và khi nào các đối tượng này sẽ được cập nhật. Về cơ bản ta có hai phương thức cache thụ động và chủ động.

Phương thức Cache thụ động (*passive cache*): Cache thụ động lưu trữ các đối tượng chỉ khi các máy tính trạm yêu cầu tới đối tượng. Khi một đối tượng được chuyển tới máy tính trạm, máy chủ Proxy xác định xem đối tượng này có thể cache hay không nếu có thể đối tượng sẽ được cache. Các đối tượng chỉ được cập nhật khi có nhu cầu. Đối tượng sẽ bị xóa khỏi cache dựa trên thời điểm gần nhất mà các máy tính trạm truy cập tới đối tượng. Phương thức này có lợi ích là sử dụng ít hơn bộ xử lý nhưng tốn nhiều không gian ổ đĩa hơn

Phương thức Cache chủ động (*active cache*): Cũng giống như phương thức cache thụ động, Cache chủ động lưu trữ các đối tượng khi các máy tính trạm ra yêu cầu tới một đối tượng máy chủ Proxy đáp ứng yêu cầu và lưu đối tượng này vào Cache. Phương thức này tự động cập nhật các đối tượng từ Internet dựa vào: số lượng yêu cầu đối với các đối tượng, đối tượng thường xuyên thay đổi như thế nào. Phương thức này sẽ tự động cập nhật các đối tượng khi mà máy chủ Proxy đang phục vụ ở mức độ thấp và do đó không ảnh hưởng đến hiệu suất phục vụ các máy tính trạm. Đối tượng trong cache sẽ bị xóa dựa trên các thông tin header HTTP, URL.

## 2. Triển khai dịch vụ proxy

### 2.1. Các mô hình kết nối mạng

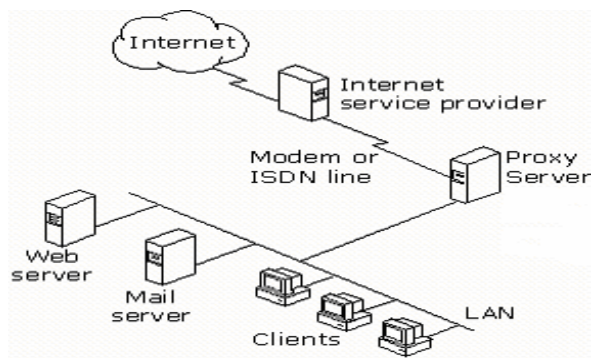
Đối tượng phục vụ của proxy server khá rộng, từ mạng văn phòng nhỏ, mạng văn phòng vừa tới mạng của các tập đoàn lớn. Với mỗi quy mô tổ chức sẽ có một cấu trúc mạng sử dụng proxy server cho phù hợp. Sau đây chúng ta sẽ xem xét một số mô hình cơ bản đối với mạng cỡ nhỏ, mạng cỡ trung bình và mạng tập đoàn lớn. Trong đó chúng ta sẽ đi sâu vào mô hình thứ nhất dành cho mạng văn phòng nhỏ bởi nó phù hợp quy mô tổ chức của các công ty vừa và nhỏ tại Việt nam.

Mô hình mạng văn phòng nhỏ:

- Bao gồm một mạng LAN độc lập.
- Sử dụng giao thức IP.
- Kết nối Internet bằng đường thoại (qua mạng điện thoại công cộng bằng các hình thức quay dial-up hay sử dụng công nghệ ADSL) hoặc đường trực tiếp (Leased Line).
- Ít hơn 250 máy tính trạm.

Mô hình kết nối mạng như hình vẽ (hình 5.18)





Hình 5.18: Mô hình kết nối mạng

Theo mô hình này, với mỗi phương thức kết nối Internet Proxy server sử dụng 02 giao tiếp như sau:

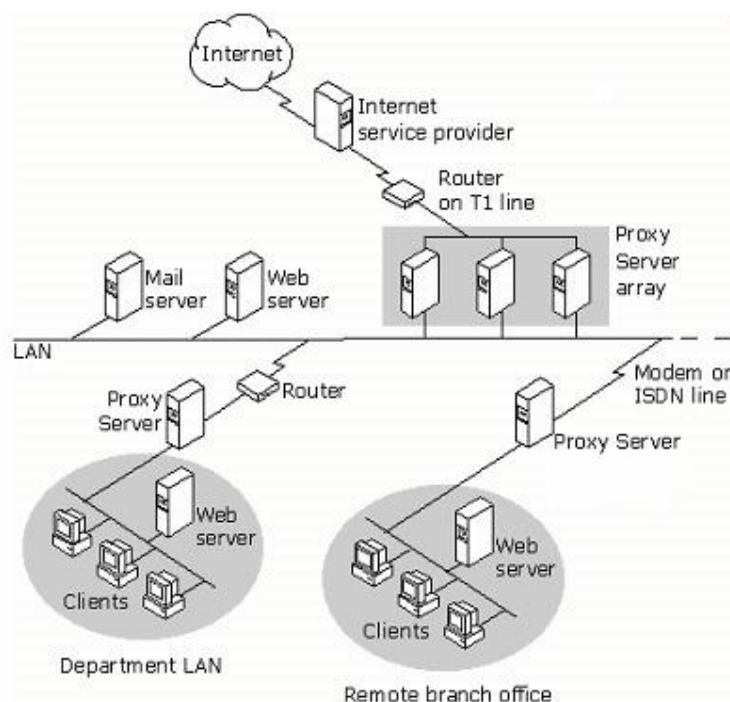
- Kết nối Internet bằng đường thoại qua mạng PSTN:
  - 01 giao tiếp với mạng nội bộ thông qua card mạng.
  - 01 giao tiếp với Internet thông qua Modem.
- Kết nối Internet bằng đường trực tiếp (Leased Line)
  - 01 giao tiếp với mạng nội bộ thông qua card mạng
  - 01 giao tiếp với Internet thông qua card mạng khác. Lúc này bảng địa chỉ nội bộ (LAT-Local Address Table) được xây dựng dựa trên danh sách địa chỉ IP mạng nội bộ.

Mô hình kết nối mạng cỡ trung bình

Đặc trưng của mạng văn phòng cỡ trung bình như sau:

- Văn phòng trung tâm với một vài mạng LAN
- Mỗi văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức IP.
- Kết nối bằng đường thoại từ văn phòng chi nhánh tới văn phòng trung tâm.
- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường thoại hoặc đường trực tiếp (Leased Line).
- Ít hơn 2000 máy tính trạm

Mô hình mạng như hình 5.19. Theo mô hình này, văn phòng chi nhánh sử dụng một máy chủ Proxy cung cấp khả năng lưu trữ thông tin nội bộ (local caching), quản trị kết nối và kiểm soát truy cập tới văn phòng trung tâm. Tại văn phòng trung tâm, một số máy chủ Proxy hoạt động theo kiến trúc mảng (array) cung cấp khả năng bảo mật chung cho toàn mạng, cung cấp tính năng lưu trữ thông tin phân tán (distributed caching) và cung cấp kết nối ra Internet.



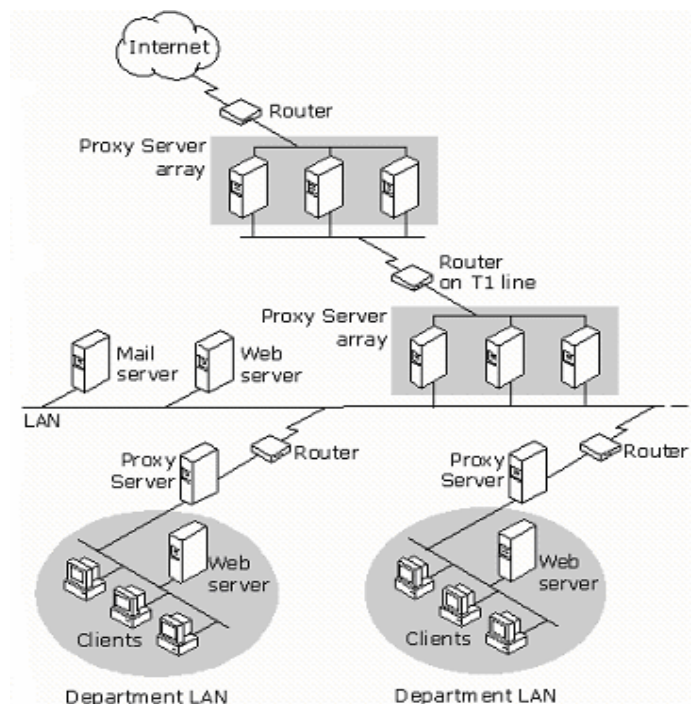
Hình 5.19: Mô hình kết nối mạng

Mô hình kết nối mạng tập đoàn lớn

Mạng của các tập đoàn lớn có đặc trưng như sau:

- Văn phòng trung tâm có nhiều mạng LAN và có mạng trực LAN.
- Có vài văn phòng chi nhánh, mỗi văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức mạng IP.
- Kết nối bằng đường thoại từ các văn phòng chi nhánh tới văn phòng trung tâm.
- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường trực tiếp (Leased Line).
- Có nhiều hơn 2000 máy tính trạm.

Mô hình mạng như hình 5.20. Theo mô hình này mạng tại các văn phòng chi nhánh cũng cấu hình tương tự như đối với mô hình các văn phòng cỡ trung bình. Các yêu cầu kết nối Internet không được đáp ứng bởi cache nội bộ tại máy chủ Proxy của văn phòng chi nhánh sẽ được chuyển tới một loạt máy chủ Proxy hoạt động theo kiến trúc mảng tại văn phòng trung tâm. Tại văn phòng trung tâm các máy chủ Proxy sử dụng 02 giao tiếp mạng (card mạng) trong đó 01 card mạng giao tiếp với mạng trực LAN và 01 card mạng giao tiếp với mạng LAN thành viên.



Hình 5.20: Mô hình kết nối mạng

## 2.2. Thiết lập chính sách truy cập và các qui tắc

### 1..Các qui tắc.

Ta có thể thiết lập proxy server để đáp ứng các yêu cầu bảo mật và vận hành bằng cách thiết lập các qui tắc để xác định xem liệu người dùng, máy tính hoặc ứng dụng có được quyền truy cập và truy cập như thế nào tới máy tính trong mạng hay trên Internet hay không. Thông thường một proxy server định nghĩa các loại qui tắc sau: Qui tắc về chính sách truy nhập, qui tắc về băng thông, qui tắc về chính sách quảng bá, các đặc tính lọc gói và qui tắc về định tuyến và chuỗi (chaining).

Khi một client trong mạng yêu cầu một đối tượng proxy server sẽ xử lý các qui tắc để xác định xem yêu cầu đó có được xác định chấp nhận hay không. Tương tự khi một client bên ngoài (Internet) yêu cầu một đối tượng từ một server trong mạng, proxy server cũng xử lý các bộ qui tắc xem yêu cầu có được cho phép không.

*Các qui tắc của chính sách truy nhập:* Ta có thể sử dụng proxy server để thiết lập chính sách bao gồm các qui tắc về giao thức, qui tắc về nội dung. Các qui tắc giao thức định nghĩa giao thức nào có thể sử dụng cho thông tin giữa mạng trong và Internet. Qui tắc giao thức sẽ được xử lý ở mức ứng dụng. Ví dụ một qui tắc giao thức có thể cho phép các Client sử dụng giao thức HTTP. Các qui tắc về nội dung qui định những nội dung nào trên các site nào mà client có thể truy nhập. Các qui tắc nội dung cũng được xử lý ở mức ứng dụng. Ví dụ một qui tắc về nội dung có thể cho phép các client truy nhập tới bất kỳ địa chỉ nào trên Internet.

*Qui tắc băng thông:* Qui tắc băng thông xác định kết nối nào nhận được quyền ưu tiên. Trong việc điều khiển băng thông thường thì proxy server không giới hạn độ rộng băng thông. Hơn nữa nó cho biết chất lượng dịch vụ (QoS) được cấp phát ưu tiên cho các kết nối mạng như thế nào. Thường thì bất kỳ kết nối nào không có qui tắc về băng thông kèm theo sẽ nhận được quyền ưu tiên ngầm định và bất kỳ kết nối nào có qui tắc băng thông đi kèm sẽ được sắp xếp với quyền ưu tiên hơn quyền ưu tiên ngầm định.

*Các qui tắc về chính sách quảng bá:* Ta có thể sử dụng proxy server để thiết lập chính sách quảng bá, bao gồm các qui tắc quảng bá server và qui tắc quảng bá web. Các qui tắc quảng bá server và web lọc tất cả các yêu cầu đến từ các yêu cầu của client ngoài mạng (internet) tới các server trong mạng. Các qui tắc quảng bá server và web sẽ đưa các yêu cầu đến cho các server thích hợp phía sau proxy server.

*Đặc tính lọc gói:* Đặc tính lọc gói của proxy server cho phép điều khiển luồng các gói IP đến và đi từ proxy server. Khi lọc gói hoạt động thì mọi gói trên giao diện bên ngoài đều bị rớt lại, trừ khi chúng được hoàn toàn cho phép hoặc là một cách cố định bằng các bộ lọc gói IP, hoặc là một cách động bằng các chính sách truy cập hay quảng bá. Thậm chí nếu bạn không để lọc gói hoạt động thì truyền thông giữa mạng Internet và mạng cục bộ được cho phép khi nào bạn thiết lập rõ ràng các qui tắc cho phép truy cập. Trong hầu hết các trường hợp, việc mở các cổng động thường được sử dụng hơn. Do đó, người ta thường khuyến nghị rằng bạn nên thiết lập các qui tắc truy cập cho phép client trong mạng truy nhập vào Internet hoặc các qui tắc quảng bá cho phép client bên ngoài truy nhập vào các server bên trong. Đó là do các bộ lọc gói IP mở một cách cố định những chính sách truy nhập và qui tắc quảng bá lại mở các cổng kiểu động. Giả sử bạn muốn cấp quyền cho mọi người dùng trong mạng truy cập tới các site HTTP. Bạn không nên thiết lập một bộ lọc gói IP để mở cổng 80. Nên thiết lập qui tắc về site, nội dung và giao thức cần thiết để cho phép việc truy nhập này. Trong một vài trường hợp ta sẽ phải sử dụng các lọc gói IP, ví dụ nên thiết lập các lọc gói IP nếu ta muốn quảng bá các Server ra bên ngoài.

*Qui tắc định tuyến và cấu hình chuỗi proxy (chaining):* thường là qui tắc được áp dụng sau cùng để định tuyến các yêu cầu của client tới một server đã được chỉ định để phục vụ các yêu cầu đó.

## 2. Xử lý các yêu cầu đi

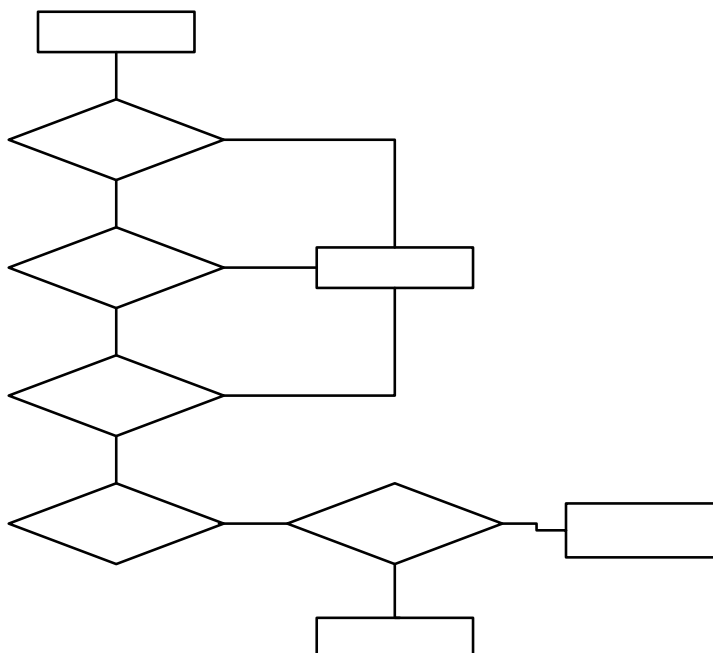
Một trong các chức năng chính của proxy server là khả năng kết nối mạng dùng riêng ra Internet trong khi bảo vệ mạng khỏi những nội dung có ác ý. Để thuận tiện cho việc kiểm soát kết nối này, ta dùng proxy server để tạo ra một chính sách truy cập cho phép các client truy cập tới các server trên Internet cụ thể, chính sách truy cập cùng với các qui tắc định tuyến quyết định các client truy cập Internet như thế nào.

Khi proxy server xử lý một yêu cầu đi, proxy server kiểm tra các qui tắc định tuyến các qui tắc về nội dung và các qui tắc giao thức để xem xét việc truy cập có được phép hay không. Yêu cầu chỉ được cho phép nếu cả quy tắc giao

thức, qui tắc nội dung và site cho phép và nếu không một qui tắc nào từ chối yêu cầu.

Một vài qui tắc có thể được thiết lập để áp dụng cho các client cụ thể. Trong trường hợp này, các client có thể được chỉ định hoặc là bằng địa chỉ IP hoặc bằng user name. Proxy server xử lý các yêu cầu theo cách khác nhau phụ thuộc vào kiểu yêu cầu của client và việc thiết lập proxy server. Với một yêu cầu, các qui tắc được xử lý theo thứ tự như sau: qui tắc giao thức, qui tắc nội dung, các lọc gói IP, qui tắc định tuyến hoặc cấu hình chuỗi proxy.

Hình dưới đưa ra quá trình xử lý đối với một yêu cầu đi (hình 5.21)



Hình 5.21: Quá trình xử lý đối với một yêu cầu đi

Trước tiên, proxy server kiểm tra các qui tắc giao thức, proxy server chấp nhận yêu cầu chỉ khi một qui tắc giao thức chấp nhận một cách cụ thể yêu cầu và không một qui tắc giao thức nào từ chối yêu cầu đó.

Sau đó, proxy server kiểm tra các qui tắc về nội dung. Proxy server chỉ chấp nhận yêu cầu nếu một qui tắc về nội dung chấp nhận yêu cầu và không có một qui tắc về nội dung nào từ chối nó.

Tiếp đến proxy server kiểm tra xem liệu có một bộ lọc gói IP nào được thiết lập để loại bỏ yêu cầu không để quyết định xem liệu yêu cầu có bị từ chối. Cuối cùng, proxy server kiểm tra qui tắc định tuyến để quyết định xem yêu cầu được phục vụ như thế nào.

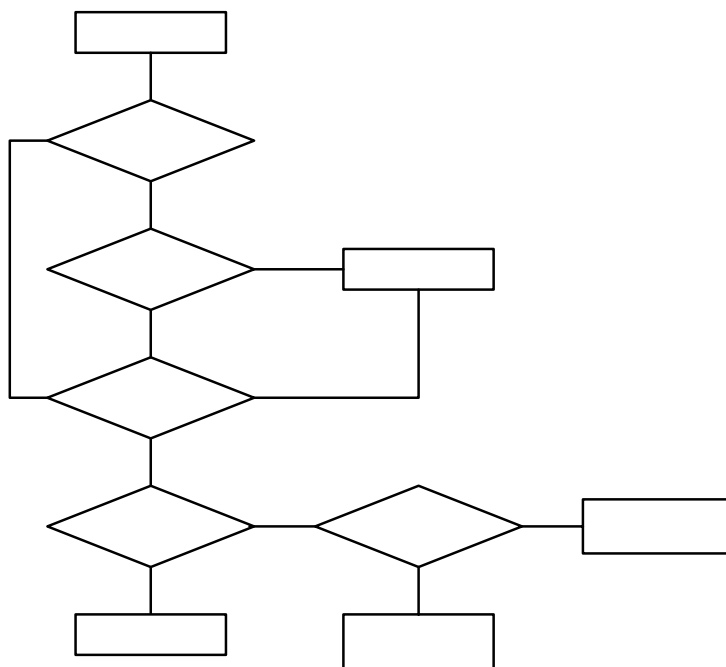
Giả sử cài đặt một proxy server trên một máy tính với hai giao tiếp kết nối, một kết nối với Internet và một kết nối vào mạng dùng riêng. Ta sẽ cho các chỉ dẫn để cho phép tất cả client truy cập vào tất cả các site. Trong trường hợp này, chính sách truy nhập chỉ là các qui tắc như sau: một qui tắc về giao thức

cho phép tất cả các client sử dụng mọi giao thức tại tất cả các thời điểm. Một qui tắc về nội dung cho phép tất cả mọi người truy cập tới mọi nội dung trên tất cả các site ở tất cả các thời điểm nào. Lưu ý rằng qui tắc này cho phép các client truy cập Internet nhưng không cho các client bên ngoài truy cập vào mạng của bạn.

### 3. Xử lý các yêu cầu đến

Proxy server có thể được thiết lập để các Server bên trong có thể truy cập an toàn đến từ các client ngoài. Ta có thể sử dụng proxy server để thiết lập một chính sách quảng bá an toàn cho các Server trong mạng. Chính sách quảng bá (bao gồm các bộ lọc gói IP, các qui tắc quảng bá Web, hoặc qui tắc quảng bá Server, cùng với các qui tắc định tuyến) sẽ quyết định các Server được quảng bá như thế nào.

Khi proxy server xử lý một yêu cầu xuất phát từ một client bên ngoài, nó sẽ kiểm tra các bộ lọc gói IP, các qui tắc quảng bá và các qui tắc định tuyến để quyết định xem liệu yêu cầu có được thực hiện hay không và Server trong nào sẽ thực hiện các yêu cầu đó.



Hình 5.22: Xử lý các yêu cầu đến

Giả sử rằng đã cài đặt proxy server với hai giao tiếp kết nối, một kết nối tới Internet và một kết nối vào mạng dùng riêng. Nếu lọc gói hoạt động và sau đó, bộ lọc gói từ chối yêu cầu thì yêu cầu sẽ bị từ chối. Nếu các qui tắc quảng bá web từ chối yêu cầu thì yêu cầu cũng bị loại bỏ. Nếu một qui tắc định tuyến được thiết lập yêu cầu được định tuyến tới một Server upstream hoặc một site chủ kế phiên thì Server được xác định đó sẽ xử lý yêu cầu. Nếu một qui tắc định tuyến chỉ ra rằng các yêu cầu được định tuyến tới một Server cụ thể thì web Server trong sẽ trả về đối tượng.

### 2.3. Proxy client và các phương thức nhận thực

Chính sách truy nhập và các qui tắc quảng bá của Proxy server có thể được thiết lập để cho phép hoặc từ chối một nhóm máy tính hay một nhóm các người dùng truy nhập tới một server nào đó. Nếu qui tắc được áp dụng riêng với các người dùng, Proxy server sẽ kiểm tra các đặc tính yêu cầu để quyết định người dùng được nhận thực như thế nào.

Ta có thể thiết lập các thông số cho các yêu cầu thông tin đi và đến để người dùng phải được proxy server nhận thực trước khi xử lý các qui tắc. Việc này đảm bảo rằng các yêu cầu chỉ được phép nếu người dùng đưa ra các yêu cầu đã được xác thực. Bạn cũng có thể thiết lập các phương pháp nhận thực được sử dụng và có thể thiết lập các phương pháp nhận thực cho các yêu cầu đi và yêu cầu đến khác nhau. Về cơ bản một Proxy server thường hỗ trợ các phương pháp nhận thực sau đây: phương thức nhận thực cơ bản., nhận thực Digest, nhận thực tích hợp Microsoft windows, chứng thực client và chứng thực server.

Đảm bảo rằng các chương trình proxy client phải hỗ trợ một trong các phương pháp nhận thực mà proxy server đã đưa ra. Trình duyệt IE 5 trở lên hỗ trợ hầu hết các phương pháp nhận thực, một vài trình duyệt khác có thể chỉ hỗ trợ phương pháp nhận thực cơ bản. Đảm bảo rằng các trình duyệt client có thể hỗ trợ ít nhất một trong số các phương pháp nhận thực mà Proxy server hỗ trợ.

#### *1. Phương pháp nhận thực cơ bản.*

Phương pháp nhận thực này gửi và nhận các thông tin về người dùng là các ký tự text dễ dàng đọc được. Thông thường thì các thông tin về user name và password sẽ được mã hoá thì trong phương pháp này không có sự mã hoá nào được sử dụng. Tiến trình nhận thực được mô tả như sau, proxy client nhắc người dùng đưa vào username và password sau đó thông tin này được client gửi cho proxy server. Cuối cùng username và password được kiểm tra như là một tài khoản trên proxy server.

#### *2. Phương pháp nhận thực Digest.*

Phương pháp này có tính chất tương tự như phương pháp nhận thực cơ bản nhưng khác ở việc chuyển các thông tin nhận thực. Các thông tin nhận thực qua một tiến trình xử lý một chiều thường được biết với cái tên là "hashing". Kết quả của tiến trình này gọi là hash hay message digest và không thể giải mã chúng. Thông tin gốc không thể phục hồi từ hash. Các thông tin được bổ sung vào password trước khi hash nên không ai có thể bắt được password và sử dụng chúng để giả danh người dùng thực. Các giá trị được thêm vào để giúp nhận dạng người dùng. Một tem thời gian cũng được thêm vào để ngăn cản người dùng sử dụng một password sau khi nó đã bị huỷ. Đây là một ưu điểm rõ ràng so với phương pháp nhận thực cơ bản bởi vì người dùng bất hợp pháp không thể chặn bắt được password.

#### *3. Phương pháp nhận thực tích hợp.*

Phương pháp này được sử dụng tích hợp trong các sản phẩm của Microsoft. Đây cũng là phương pháp chuẩn của việc nhận thực bởi vì username và password không được gửi qua mạng. Phương pháp này sử dụng hoặc giao

thức nhận thực V5 Kerberos hoặc giao thức nhận thực challenge/response của nó.

#### 4. Chứng thực client và chứng thực server

Ta có thể sử dụng các đặc tính của SSL để nhận thực. Chứng thực được sử dụng theo hai cách khi một client yêu cầu một đối tượng từ server: server nhận thực chính nó bằng cách gửi đi một chứng thực server cho client. Server yêu cầu client nhận thực chính nó (Trong trường hợp này client phải đưa ra một chứng thực client phù hợp tới server).

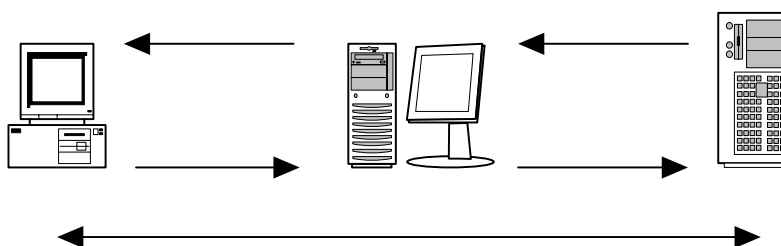
SSL nhận thực bằng cách kiểm tra nội dung của một chứng thực số được mã hoá do proxy client đệ trình lên trong quá trình đăng nhập (Các người dùng có thể có được các chứng thực số từ một tổ chức ngoài có độ tin tưởng cao). Các chứng thực về server bao gồm các thông tin nhận biết về server. Các chứng thực về client thường gồm các thông tin nhận biết về người dùng và tổ chức đưa ra chứng thực đó

*Chứng thực client:* Nếu chứng thực client được lựa chọn là phương thức xác thực thì proxy server yêu cầu client gửi chứng thực đến *trước* khi yêu cầu một đối tượng. Proxy server nhận yêu cầu và gửi một chứng thực cho client. Client nhận chứng thực này và kiểm tra xem có thực là thuộc về proxy server. Client gửi yêu cầu của nó cho proxy server, tuy nhiên proxy server yêu cầu một chứng thực từ client mà đã được đưa ra trước đó. Proxy server kiểm tra xem chứng thực có thực sự thuộc về client được phép truy cập không.

*Chứng thực server:* Khi một client yêu cầu một đối tượng SSL từ một server, client yêu cầu server phải nhận thực chính nó. Nếu proxy server kết thúc một kết nối SSL thì sau đó proxy server sẽ phải nhận thực chính nó cho client. Ta phải thiết lập và chỉ định các chứng thực về phía server để sử dụng khi nhận thực server cho client

#### 5. Nhận thực pass-through

Nhận thực pass-through chỉ đến khả năng của proxy server chuyển thông tin nhận thực của client cho server đích. Proxy server hỗ trợ nhận thực cho cả các yêu cầu đi và đến. Hình vẽ sau mô tả trường hợp nhận thực pass-through.



Hình 5.23: Nhận thực pass-through

Client gửi yêu cầu lấy một đối tượng trên một web server cho proxy server. Proxy server chuyển yêu cầu này cho web server, bắt đầu từ đây việc nhận thực qua các bước sau:



1 Webserver nhận được yêu cầu lấy đối tượng và đáp lại rằng client cần phải nhận thực. Web server cũng chỉ ra các kiểu nhận thực được hỗ trợ.

2 Proxy server chuyển yêu cầu nhận thực cho client

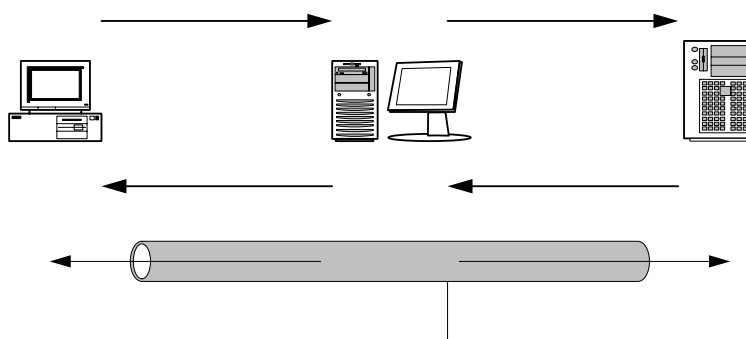
3 Client tiếp nhận yêu cầu và trả các thông tin nhận thực cho proxy server

4 Proxy server chuyển lại thông tin đó cho web server

5 Từ lúc này client liên lạc trực tiếp với web server

#### 6. SSL Tunneling.

Với đường hầm SSL, một client có thể thiết lập một đường hầm qua proxy server trực tiếp tới server yêu cầu với các đối tượng yêu cầu là HTTPS. Bất cứ khi nào client yêu cầu một đối tượng HTTPS qua proxy server nó sử dụng đường hầm SSL. Đường hầm SSL làm việc bởi sự ngầm định các yêu cầu đi tới các cổng 443 và 563.



Hình 5.24: SSL Tunneling.

Tiến trình tạo đường hầm SSL được mô tả như sau:

1 Khi client yêu cầu một đối tượng HTTPS từ một web server trên Internet, proxy server gửi một yêu cầu kết nối [https://URL\\_name](https://URL_name)

2 Yêu cầu tiếp theo được gửi tới cổng 8080 trên máy proxy server  
CONNECT *URL\_name*:443 HTTP/1.1

3 Proxy server kết nối tới Web server trên cổng 443

4 Khi một kết nối TCP được thiết lập, proxy server trả lại kết nối đã được thiết lập HTTP/1.0 200

5 Từ đây, client thông tin trực tiếp với Web server bên ngoài

#### 7. SSL bridging.

SSL bridging đề cập đến khả năng của proxy server trong việc mã hóa hoặc giải mã các yêu cầu của client và chuyển các yêu cầu này tới server đích. Ví dụ, trong trường hợp quảng bá (hoặc reverse proxy), proxy server có thể phục vụ một yêu cầu SSL của client bằng cách chấm dứt kết nối SSL với client và mở lại một kết nối mới với web server. SSL bridging được sử dụng khi proxy server kết thúc hoặc khởi tạo một kết nối SSL.

Khi một client yêu cầu một đối tượng HTTP. Proxy server mã hóa yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng đã mã hóa cho proxy server. Sau đó proxy server giải mã đối tượng và gửi lại cho client. Nói một cách khác các yêu cầu HTTP được chuyển tiếp như các yêu cầu SSL.

Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu, sau đó mã hóa lại một lần nữa và chuyển tiếp nó tới Web server. Web server trả về đối tượng mã hóa cho proxy server. Proxy server giải mã đối tượng và sau đó gửi nó cho client. Nói một cách khác các yêu cầu SSL được chuyển tiếp như là các yêu cầu SSL.

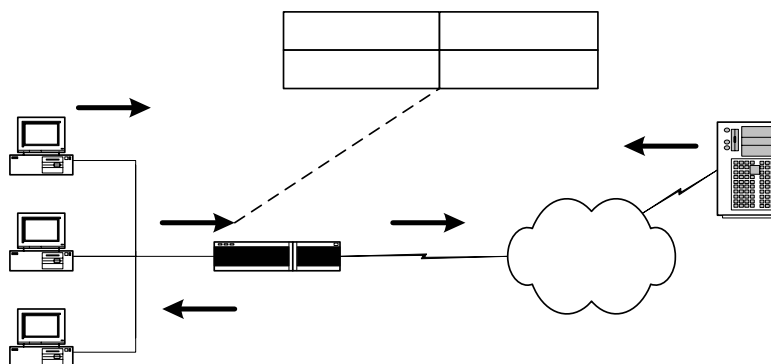
Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng HTTP cho proxy server. Proxy server mã hóa đối tượng và chuyển nó cho client. Nói cách khác các yêu cầu SSL được chuyển tiếp như các yêu cầu HTTP.

SSL bridging có thể được thiết lập cho các yêu cầu đi và đến. Tuy nhiên với các yêu cầu đi client phải hỗ trợ truyền thông bảo mật với proxy server.

## 2.4. NAT và proxy server

### Khái niệm NAT (Network Address Translation)

NAT là một giao thức cho ta khả năng bản đồ hóa một vùng địa chỉ IP sử dụng trong mạng dùng riêng ra mạng ngoài và ngược lại. NAT thường được thiết lập trên các bộ định tuyến là ranh giới giữa mạng dùng riêng và mạng ngoài (ví dụ như mạng công cộng Internet). NAT chuyển đổi các địa chỉ IP trên mạng dùng riêng thành các địa chỉ IP được đăng ký hợp lệ trước khi chuyển các gói từ mạng dùng riêng tới Internet hoặc tới mạng ngoài khác. Trong phần này chúng ta sẽ chỉ tìm hiểu sự vận hành của NAT khi NAT được thiết lập để cung cấp các chức năng chuyển đổi các địa chỉ mạng dùng riêng trong việc phục vụ cho việc kết nối truy cập ra mạng ngoài như thế nào. Để làm việc này, NAT dùng tiến trình các bước theo hình vẽ dưới đây.



Hình 5.25: NAT

1. Người dùng tại máy 10.1.1.25 muốn mở một kết nối ra ngoài tới server 203.162.0.12

2. Khi gói dữ liệu đầu tiên tới NAT router, NAT router thực hiện việc kiểm tra trong bảng NAT. Nếu sự chuyển đổi địa chỉ đã có trong bảng, NAT router thực hiện bước thứ 3. Nếu không có sự chuyển đổi nào được tìm thấy, NAT router xác định rằng địa chỉ 10.1.1.25 phải được chuyển đổi. NAT router xác định một địa chỉ mới và cấu hình một chuyển đổi đối với địa chỉ 10.1.1.25 tới địa chỉ hợp lệ ngoài mạng (Internet) từ dãy địa chỉ động đã được định nghĩa từ trước ví dụ 203.162.94.163.

3. NAT router thay thế địa chỉ 10.1.1.25 bằng địa chỉ 203.162.94.163 sau đó gói được chuyển tiếp tới đích.

4. Server 203.162.0.12 trên Internet nhận gói và phúc đáp trở lại NAT router với địa chỉ 203.162.94.163.

5. Khi NAT router nhận được gói phúc đáp từ Server với địa chỉ đích đến là 203.162.94.163, nó thực hiện việc tìm kiếm trong bảng NAT. Bảng NAT chỉ ra rằng địa chỉ mạng trong 10.1.1.25 (tương ứng được ánh xạ tới địa chỉ 203.162.94.163 ở mạng ngoài) sẽ nhận được gói tin này. NAT router thực hiện việc chuyển đổi địa chỉ đích trong gói tin là 10.1.1.25 và chuyển gói tin này tới đích (10.1.1.25). Máy 10.1.1.25 nhận gói và tiếp tục thực hiện với các gói tiếp theo với các bước tuần tự như trên.

Trong trường hợp muốn sử dụng một địa chỉ mạng ngoài cho nhiều địa chỉ mạng trong. NAT router sẽ duy trì các thông tin thủ tục mức cao hơn trong bảng NAT đối với các số hiệu cổng TCP và UDP để chuyển đổi địa chỉ mạng ngoài trở lại chính xác tới các địa chỉ mạng trong.

Như vậy NAT cho phép các client trong mạng dùng riêng với việc sử dụng các địa chỉ IP dùng riêng truy cập vào một mạng bên ngoài như mạng Internet. Cung cấp kết nối ra ngoài Internet trong các mạng không được cung cấp đủ các địa chỉ Internet có đăng ký. Thích hợp cho việc chuyển đổi địa chỉ trong hai mạng Intranet ghép nối nhau. Chuyển đổi các địa chỉ IP nội tại được ISP cũ phân bổ thành các địa chỉ được phân bổ bởi ISP mới mà không cần thiết lập thủ công các giao diện mạng cục bộ.

NAT có thể được sử dụng một cách cố định hoặc động. Chuyển đổi cố định xảy ra khi ta thiết lập thủ công một bảng địa chỉ cùng các địa chỉ IP. Một địa chỉ cụ thể ở bên trong mạng sử dụng một địa chỉ IP (được thiết lập thủ công bởi người quản trị mạng) để truy cập ra mạng ngoài. Các thiết lập động cho phép người quản trị thiết lập một hoặc nhiều các nhóm địa chỉ IP dùng chung đã đăng ký. Những địa chỉ trong nhóm này có thể được sử dụng bởi các client trên mạng dùng riêng để truy cập ra mạng ngoài. Việc này cho phép nhiều client trong mạng sử dụng cùng một địa chỉ IP.

NAT cũng có một số nhược điểm như làm tăng độ trễ của các gói tin trên mạng. NAT phải xử lý mọi gói để quyết định xem liệu các header được thay đổi như thế nào. Không phải bất kỳ ứng dụng nào cũng có thể chạy được với NAT. NAT hỗ trợ nhiều giao thức truyền thông và cũng rất nhiều giao thức không được hỗ trợ. Các giao thức được NAT hỗ trợ như: TCP, UDP, HTTP, TFTP, FTP... Các thông tin không được hỗ trợ như: IP multicast, BOOTP, DNS zone transfer, SNMP...

## Proxy và NAT

Như đã phân tích cả dịch vụ NAT và dịch vụ Proxy đều có thể là một giải pháp để kết nối các mạng dùng riêng ra Internet, tuy nhiên mỗi dịch vụ lại có các ưu điểm và nhược điểm riêng.

Dịch vụ proxy cho khả năng thi hành và tốc độ cao hơn nhờ tính năng cache, tuy nhiên sử dụng cache có thể đưa ra các đối tượng đã quá hạn cần phải có các chính sách cache hợp lý để đảm bảo tính thời sự của các đối tượng. Chính vì sử dụng cache nên giảm tải trên kết nối truy cập Internet. NAT không có tính năng cache.

Dịch vụ proxy phải được triển khai đối với từng ứng dụng, trong khi NAT là một tiến trình trong suốt hơn. Hầu hết các ứng dụng đều có thể làm việc được với NAT. NAT dễ cài đặt và vận hành, dường như không phải làm gì nhiều với NAT sau khi cài đặt.

Tại các client, đối với NAT không phải thiết đặt gì nhiều ngoài việc cấu hình tham số default gateway tới Server NAT. Trong khi sử dụng dịch vụ proxy, cần phải có các chương trình proxy client để làm việc với proxy server.

Dịch vụ proxy cho phép thiết đặt các chính sách tới người dùng, với NAT việc sử dụng các tính năng này có hạn chế rất nhiều, có thể nói sử dụng dịch vụ proxy là cách truy cập an toàn nhất để kết nối mạng dùng riêng ra ngoài Internet.

## 3. Các tính năng của phần mềm Microsoft ISA server 2000

### 3.1. Các phiên bản

ISA server bao gồm hai phiên bản được thiết kế để phù hợp với từng nhu cầu của người sử dụng đó là ISA server Standard và ISA server Enterprise.

- ISA server Standard cung cấp khả năng an toàn firewall và khả năng web cache cho một môi trường kinh doanh, các nhóm làm việc hay văn phòng nhỏ. ISA server Standard cung cấp việc bảo mật chặt chẽ, truy cập web nhanh, quản lý trực quan, giá cả hợp lý và khả năng thi hành cao.
- ISA server Enterprise được thiết kế để đáp ứng các nhu cầu về hiệu suất, quản trị và cân bằng trong các môi trường Internet tốc độ cao với sự quản lý server tập trung, chính sách truy cập đa mức và các khả năng chống lỗi cao. ISA server Enterprise cung cấp sự bảo mật, truy cập Internet nhanh cho các môi trường có sự đòi hỏi khắt khe.

### 3.2. Lợi ích

ISA server là một trong các phần mềm máy chủ thuộc dòng .NET Enterprise Server. Các sản phẩm thuộc dòng .NET Enterprise Server là các server ứng dụng toàn diện của Microsoft trong việc xây dựng, triển khai, quản lý, tích hợp, các giải pháp dựa trên web và các dịch vụ. ISA server mang lại một số các lợi ích cho các tổ chức cần kết nối Internet nhanh, bảo mật, dễ quản lý.

1. Truy cập Web nhanh với cache hiệu suất cao.

- Người dùng có thể truy cập web nhanh hơn bằng các đối tượng tại chỗ trong cache so với việc phải kết nối vào Internet lúc nào cũng tiềm tàng nguy cơ tắc nghẽn.

- Giảm giá thành bằng thông nhờ giảm lưu lượng từ Internet

- Phân tán nội dung của các Web server và các ứng dụng thương mại điện tử một cách hiệu quả, đáp ứng được nhu cầu khách hàng trên toàn cầu (khả năng phân phối nội dung web chỉ có trên phiên bản ISA server Enterprise)

2. Kết nối Internet an toàn nhờ Firewall nhiều lớp.

- Bảo vệ mạng trước các truy nhập bất hợp pháp bằng cách giám sát lưu lượng mạng tại nhiều lớp

- Bảo vệ các máy chủ web, email và các ứng dụng khác khỏi sự tấn công từ bên ngoài bằng việc sử dụng web và server quảng bá để xử lý một cách an toàn các yêu cầu đến

- Lọc lưu lượng mạng đi và đến để đảm bảo an toàn.

- Cung cấp truy cập an toàn cho người dùng hợp lệ từ Internet tới mạng nội tại nhờ sử dụng mạng riêng ảo (VPN)

3. Quản lý thống nhất với sự quản trị tích hợp.

- Điều khiển truy cập tập trung để đảm bảo tính an toàn và phát huy hiệu lực của các chính sách vận hành.

- Tăng hiệu suất nhờ việc giới hạn truy cập sử dụng Internet đối với một số các ứng dụng và đích đến.

- Cấp phát băng thông để phù hợp với các ưu tiên.

- Cung cấp các công cụ giám sát và các báo cáo để chỉ ra kết nối Internet được sử dụng như thế nào.

- Tự động hóa các nhiệm vụ bằng việc sử dụng các script

4. Khả năng mở rộng.

- Chú trọng tới an toàn và thi hành nhờ sử dụng ISA server Software Development Kit (SDK) với sự phát triển các thành phần bổ sung.

- Chức năng quản lý và an toàn mở rộng cho các nhà sản xuất thứ ba

- Tự động các tác vụ quản trị với các đối tượng Script COM (Component Object Model)

### 3.3. Các chế độ cài đặt

ISA server có thể được cài đặt ở ba chế độ khác nhau: Cache, Firewall và Integrated

1. Chế độ cache: Trong chế độ này ta có thể nâng cao hiệu suất truy cập và tiết kiệm băng thông bằng cách lưu trữ các đối tượng web thường được truy xuất từ người dùng. Ta cũng có thể định tuyến các yêu cầu của người dùng tới cache server khác đang lưu giữ các đối tượng đó.

2. Chế độ firewall: Trong chế độ này cho phép ta đảm bảo an toàn lưu lượng mạng nhờ sự thiết lập các qui tắc điều khiển thông tin giữa mạng trong và Internet. Ta cũng có thể quảng bá các server trong để chia sẻ dữ liệu trên mạng với các đối tác và khách hàng.

3. Chế độ tích hợp: Trong chế độ này ta có thể tích hợp các dịch vụ cache và firewall trên một server.

### 3.4. Các tính năng của mỗi chế độ cài đặt

Các tính năng khác nhau tùy thuộc vào chế độ mà ta cài đặt, bảng sau liệt kê các tính năng có trong chế độ firewall và cache, chế độ tích hợp có tất cả các tính năng đó

| Tính năng               | Mô tả                                                                                                                                  | Chế độ firewall | Chế độ cache       |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------|
| Chính sách truy cập     | Định nghĩa các giao thức và nội dung Internet mà người dùng có thể sử dụng và truy cập                                                 | Có              | Chỉ có HTTP và FTP |
| Cache                   | Lưu trữ định kỳ các đối tượng web vào RAM và đĩa cứng của ISA server                                                                   | Không           | Có                 |
| VPN                     | Mở rộng mạng riêng nhờ sử dụng các đường liên kết qua các mạng được chia sẻ hay mạng công cộng như Internet                            | Có              | Không              |
| Lọc gói                 | Điều khiển dòng gói IP đi và đến                                                                                                       | Có              | Không              |
| Lọc ứng dụng            | Thực thi các tác vụ của hệ thống hoặc của giao thức chỉ định, như là nhận thực để cung cấp một lớp bảo vệ bổ sung cho dịch vụ firewall | Có              | Không              |
| Quảng bá Web            | Quảng bá web trong mạng để người dùng trong mạng có thể truy cập                                                                       | Không           | Có                 |
| Quảng bá Server         | Cho phép các Server ứng dụng có thể phục vụ các client bên ngoài                                                                       | Có              | Không              |
| Giám sát thời gian thực | Cho phép giám sát tập trung các hoạt động của ISA server bao gồm các cảnh báo, giám sát các phiên làm việc và các dịch vụ              | Có              | Có                 |
| Cảnh báo                | Báo cho ta biết các sự kiện đặc biệt xuất hiện và thực thi các hoạt động phù hợp                                                       | Có              | Có                 |

|         |                                                                    |    |    |
|---------|--------------------------------------------------------------------|----|----|
| Báo cáo | Tổng hợp và phân tích hoạt động trên một hoặc nhiều máy ISA server | Có | Có |
|---------|--------------------------------------------------------------------|----|----|

#### 4. Bài tập thực hành.

*Yêu cầu về Phòng học lý thuyết:* Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB, FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

*Thiết bị thực hành:* Đã cài phần mềm Windows 2000 Advance Server, đĩa cài phần mềm ISA Server 2000. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

#### Bài 1: Các bước cài đặt cơ bản phần mềm ISA server 2000.

**Bước 1:** Các bước cài đặt cơ bản.

- ✓ Đăng nhập vào hệ thống với quyền Administrator
- ✓ Đưa đĩa cài đặt Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition vào ổ CD-ROM.
- ✓ Cửa sổ Microsoft ISA Server Setup mở ra. Nếu cửa sổ này không tự động xuất hiện, sử dụng Windows Explorer để chạy x:\ISAAutorun.exe (với x là tên ổ đĩa CD-ROM).
- ✓ Trong cửa sổ Microsoft ISA Server Setup, kích Install ISA Server.
- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Continue.
- ✓ Vào CD Key sau đó kích OK hai lần.
- ✓ Trong hộp thoại Microsoft ISA Server Setup kích I Agree.
- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Custom Installation.
- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Add-in services sau đó kích Change Option.
- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Add-in services kiểm tra lựa chọn Install H.323 Gatekeeper Service đã được chọn, chọn Message Screener sau đó kích OK.
- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Administration tools sau đó kích Change Option.
- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Administration tools, kiểm tra lựa chọn ISA Management đã được chọn, chọn H.323 Gatekeeper Administration Tools sau đó kích OK.

- ✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Continue. Hộp thoại Microsoft Internet Security and Acceleration Server Setup xuất hiện, lưu ý bạn rằng máy tính không thể tham gia vào array. Bạn sẽ cấu hình máy tính này là một stand-alone server.
- ✓ Kích Yes để cấu hình máy tính này là một stand-alone server.
- ✓ Trong hộp thoại Microsoft ISA Server Setup đọc mô tả các mode cài đặt đảm bảo rằng mode Integrated đã được lựa chọn sau đó kích Continue.
- ✓ Trong hộp thoại Microsoft Internet Security and Acceleration Server Setup đọc thông báo về IIS publishing sau đó kích OK để biết rằng ISA Server Setup đang dừng dịch vụ IIS publishing.
- ✓ Kích OK và đặt ngầm định các giá trị thiết đặt cho cache.

**Bước 2:** Cấu hình LAT để khai báo địa chỉ cho mạng riêng.

- ✓ Trong hộp thoại Microsoft Internet Security and Acceleration Server 2000 Setup kích Construct Table. Lưu ý rằng khi bạn thêm vào không đúng địa chỉ IP vào LAT, ISA server sẽ chuyển tiếp sai các gói tin do đó các máy client sẽ không thể truy cập Internet
- ✓ Trong hộp thoại Local Address Table, kích để xóa Add the following private ranges: 10.x.x.x, 192.168.x.x and 172.16.x.x-172.31.x.x
- ✓ Chọn adapter ip\_address (với tên các mạng và địa chỉ IP là địa chỉ mạng riêng), sau đó kích OK.
- ✓ Trong thông báo Setup Message, kích OK.
- ✓ Trong Internal IP Ranges, kích 10.255.255.255-10.255.255.255, sau đó kích Remove.
- ✓ Kiểm tra rằng Internal IP Ranges chỉ chứa IP addresses trong mạng trong của bạn sau đó kích OK.
- ✓ Kết thúc việc cài đặt ISA Server và khởi tạo cấu hình ISA Server.
- ✓ Trong hộp thoại Launch ISA Management Tool, kích để xóa
- ✓ Start ISA Server Getting Started Wizard check box, sau đó kích OK.
- ✓ Trong hộp thông báo Microsoft ISA Server (Enterprise Edition) Setup kích OK.
- ✓ Đóng cửa sổ Microsoft ISA Server Setup.
- ✓ Lấy đĩa Microsoft Internet Security and Acceleration Server Enterprise Edition từ ổ đĩa CD-ROM.

**Bước 3:** Cấu hình Default Web Site trong Internet Information Services sử dụng cổng 8008, sau đó khởi động Default Web Site.

- ✓ Mở Internet Services Manager từ Administrative Tools.
- ✓ Trong Internet Information Services, mở rộng server(server là tên máy tính của bạn), sau đó kích DefaultWeb Site (Stopped).



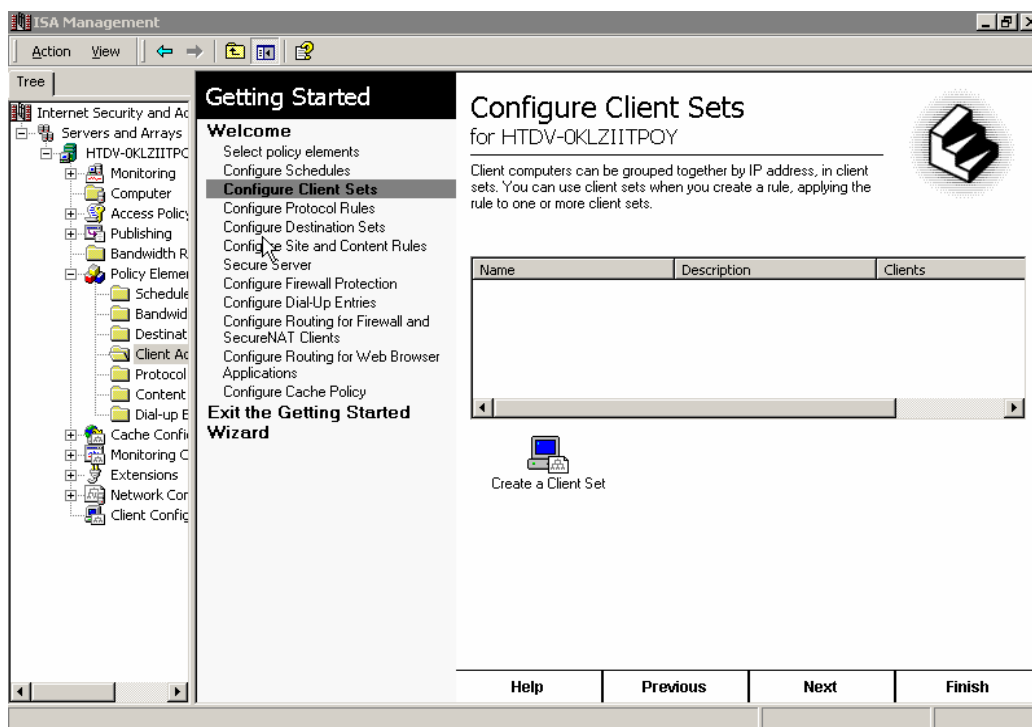
✓ Kích chuột phải Default Web Site (Stopped), sau đó kích Properties. Vì ISA Server sử dụng các cổng 80 and 8080, bạn phải cấu hình IIS để phục vụ các kết nối từ các client tới trên cổng khác. Bạn sẽ cấu hình IIS để phục vụ các yêu cầu này trên cổng TCP 8008.

✓ Trong hộp thoại Default Web Site (Stopped) Properties, trong hộp TCP Port, gõ 8008 sau đó kích OK.

✓ Kích chuột phải Default Web Site (Stopped), sau đó kích Start.

## **Bài 2: Cấu hình ISA Server 2000 cho phép một mạng nội bộ có thể truy cập, sử dụng các dịch vụ cơ bản trên Internet qua 01 modem kết nối qua mạng PSTN.**

**Bước 1:** Cấu hình và quản trị cấu hình cho ISA server sử dụng Getting Started Wizard, có các lựa chọn cấu hình sau:



- ✓ Select Policy elements, cấu hình ngầm định chọn tất cả các thành phần để có thể sử dụng khi tạo các qui tắc.
- ✓ Configure Schedules, cấu hình ngầm định có hai lịch là Weekends và Work Hours, ta có thể sửa các lịch này hoặc tạo các lịch mới.
- ✓ Configure Client sets, các máy tính Client có thể tạo thành nhóm với nhau bằng các địa chỉ IP sử dụng cho mục đích tạo các qui tắc ứng với từng nhóm client
- ✓ Configure Protocol Rule, đưa ra các qui tắc giao thức để các client sử dụng truy nhập Internet

- ✓ Configure Destination Sets, cho phép thiết lập các máy tính trên mạng Internet thành nhóm bởi tên hay địa chỉ IP, Destination Sets được sử dụng để tạo ra các qui tắc, áp dụng các qui tắc cho một hay nhiều Destination Sets
- ✓ Configure Site and Content Rules, cấu hình các qui tắc về nội dung.
- ✓ Secure Server cho phép bạn có thể đặt các mức độ bảo vệ thích hợp cho mạng.
- ✓ Configure Firewall Protection, Packet Filtering bảo đảm cho ISA server sẽ lọc không có packet nào qua trừ khi được phép
- ✓ Configure Dial-Up Entries, cho phép chọn giao diện để kết nối với Internet
- ✓ Configure Routing for firewall and secureNat client.
- ✓ Configure Routing for Web browser Applications cho phép tạo các qui tắc định tuyến, xác định rõ yêu cầu từ Web Proxy Client được gửi trực tiếp tới Internet hay tới Upstream server
- ✓ Configure Cache policy, cấu hình các chính sách về cache.

**Bước 2:** Cấu hình ISA server cho phép các client sử dụng được các dịch vụ của Internet qua mạng thoại công cộng

- ✓ Tạo một Dial-Up Entries, để kết nối với Internet
- ✓ Mở ISA Management, kích Servers and arrays, sau đó kích tên máy chủ ISA.
- ✓ Kích Access Policy, kích chuột phải vào Protocol Rule, sau đó chọn New --> Rule.
- ✓ Đặt tên của Protocol Rule, sau đó kích Next.
- ✓ Kiểm tra rằng **Allow đã được chọn**, kích Next, sau đó chọn **All IP traffic**, kích Next Chọn **Always**, kích Next sau đó chọn **Any Request**, kích Next, sau đó kích Finish.

**Bước 3:** Cấu hình Web Proxy Client: cấu hình Internet Explorer để sử dụng ISA server đối với các yêu cầu truy cập dịch vụ Web.

- ✓ Mở trình duyệt Internet Explorer.
- ✓ Trong Internet Connection Wizard, kích Cancel.
- ✓ Trong hộp thoại Internet Connection Wizard, chọn Do not show the Internet Connection wizard in the future, sau đó kích Yes.
- ✓ Trong Internet Explorer, trong ô Address , gõ http://vdc.com.vn sau đó chọn ENTER. Internet Explorer không thể kết nối tới trang web này.
- ✓ Trong menu Tools, kích Internet Options.
- ✓ Trong hộp thoại Internet Options, trong Connections kích LAN Settings.
- ✓ Trong hộp thoại Local Area Network (LAN) Settings , kích để bỏ lựa chọn Automatically detect settings. Chọn Use a proxy server, trong ô Address gõ vào địa chỉ IP của ISA Server .
- ✓ Trong hộp Port, gõ 8080

- ✓ Kiểm tra rằng lựa chọn Bypass proxy server for local addresses đã bỏ, sau đó kích OK hai lần.

### **Bài 3: Thiết đặt các chính sách cho các yêu cầu truy cập và sử dụng các dịch vụ trên mạng internet.**

#### **I. Thiết lập các thành phần chính sách**

##### **Bước 1: Thiết lập lịch trình**

- ✓ Đăng nhập vào hệ thống với quyền administrator
- ✓ Mở ISA Management từ thực đơn Microsoft ISA Server.
- ✓ Trong ISA Management, mở rộng Servers and Arrays, mở rộng server (server là tên của ISA Server ), mở rộng Policy Elements, sau đó kích Schedules.
- ✓ Kích Create a Schedule để thiết lập một lịch trình.
- ✓ Trong hộp thoại New schedule trong mục Name đưa vào một tên lịch trình ví dụ schedule1.
- ✓ Trong mục Description gõ vào Daily period of most network utilization
- ✓ Kéo để lựa chọn toàn bộ lịch trình sau đó kích Inactive.
- ✓ Kéo để lựa chọn vùng từ thời điểm hiện tại tới 2 h tiếp theo đối với tất cả các ngày trong tuần sau đó kích active ví dụ, nếu thời điểm hiện tại là 3:15 P.M., thì lựa chọn vùng từ 3:00 P.M. tới 5:00 P.M. cho tất cả các ngày trong tuần.
- ✓ Kích OK.

##### **Bước 2: Thiết lập destination set**

- ✓ Trong ISA Management, kích Destination Sets.
- ✓ Kích Create a Destination Set.
- ✓ Trong hộp thoại New Destination Set trong mục Name cho vào một tên cho thiết lập mới này ví dụ set1.
- ✓ Trong mục Description box, gõ vào một nội dung mô tả cho thiết lập mới này
- ✓ Kích Add.
- ✓ Trong hộp thoại Add/Edit Destination trong mục Destination gõ home.vnn.vn

##### **Bước 3: Thiết lập client address set**

- ✓ Trong ISA Management kích Client Address Sets.
- ✓ Kích Create a Client Set.
- ✓ Trong hộp thoại Client Set trong mục Name gõ vào một tên cho thiết lập mới, ví dụ Accounting Department.
- ✓ Trong mục Description gõ nội dung mô tả cho thiết lập mới này sau đó kích Add.

- ✓ Trong hộp thoại Add/Edit IP Addresses trong mục From gõ vào địa chỉ bắt đầu thuộc nhóm địa chỉ thuộc mạng dùng riêng .
- ✓ Trong mục To gõ vào địa chỉ kết thúc thuộc nhóm địa chỉ thuộc mạng dùng riêng kích OK hai lần.

**Bước 4:** Thiết lập protocol definition (sử dụng cổng UDP 39000 cho kết nối chính gọi ra và cổng TCP 39000 cho kết nối thứ hai)

- ✓ Trong ISA Management kích Protocol Definitions.
- ✓ Kích Create a Protocol Definition.
- ✓ Trong New Protocol Definition Wizard trong mục Protocol definition name gõ vào một tên cho thiết đặt mới sau đó kích Next.
- ✓ Trong trang Primary Connection Information trong mục Port number gõ vào 39000
- ✓ Trong danh sách Protocol type kích UDP.
- ✓ Trong danh sách Direction kích Send Receive sau đó kích Next.
- ✓ Trong trang Secondary Connections kích Yes sau đó kích New.
- ✓ Trong hộp thoại New/Edit Secondary Connection trong mục From và mục To gõ 39000
- ✓ Trong danh sách Protocol type kiểm tra rằng TCP đã được lựa chọn, trong mục Direction
- ✓ kích Outbound sau đó kích OK.
- ✓ Kích Next sau đó trong trang Completing the New Protocol Definition Wizard kích Finish.

## II. Thiết lập các qui tắc giao thức

**Bước 1:** Thiết lập một qui tắc giao thức cho phép HTTP, HTTP-S và FTP đối với mọi người dùng truy cập Internet tại mọi thời điểm bằng việc sử dụng các giao thức HTTP, HTTP-S và FTP .

- ✓ Mở trình duyệt Internet Explorer tại một máy trạm, trong ô Address gõ <http://home.vnn.vn> nhấn ENTER. Trình duyệt Internet Explorer không thể kết nối tới Web site vì ISA Server từ chối yêu cầu.
- ✓ Đóng Internet Explorer.
- ✓ Trong ISA Management mở rộng Access Policy sau đó kích Protocol Rules.
- ✓ Kích Create a Protocol Rule for Internet Access.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow HTTP, HTTP-S, and FTP sau đó kích Next.
- ✓ Trong trang Protocols kiểm tra rằng Selected protocols đã được chọn, kích để xóa Gopher check box sau đó kích Next.
- ✓ Trong trang Schedule kiểm tra rằng Always đã được lựa chọn sau đó kích Next.

- ✓ Trong trang Client Type kiểm tra rằng Any request đã được chọn, sau đó kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard kích Finish.
- ✓ Mở Internet Explorer tại một máy tính trạm, trong mục Address gõ `http://home.vnn.vn` sao đó ấn ENTER. Kiểm tra rằng trình duyệt kết nối thành công nội dung trang web được hiển thị
- ✓ Đóng Internet Explorer.

**Bước 2:** Thiết lập một qui tắc giao thức cho phép người dùng trong nhóm Domain Admins truy cập Internet sử dụng tất cả các giao thức.

- ✓ Trong ISA Management kích Create a Protocol Rule.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow All Access for Administrators sau đó kích Next.
- ✓ Trong trang Rule Action kiểm tra rằng Allow đã được chọn sau đó kích Next.
- ✓ Trong trang Protocols, trong danh sách Apply this rule to kiểm tra rằng All IP traffic đã được chọn sau đó kích Next.
- ✓ Trong trang Schedule, kiểm tra rằng Always đã được chọn sau đó kích Next.
- ✓ Trong trang Client Type, kích Specific users and groups, sau đó kích Next.
- ✓ Trong trang Users and Groups, kích Add.
- ✓ Trong hộp thoại Select Users or Groups, kích Domain Admins, kích Add, sau đó kích OK.
- ✓ Trong trang Users and Groups, kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard kích Finish.

**Bước 3:** Thiết lập một qui tắc giao thức từ chối người dùng trong nhóm Accounting Department đã định nghĩa trong client set truy cập Internet.

- ✓ Trong ISA Management, kích Create a Protocol Rule.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ vào Deny Access from Accounting Department , sau đó kích Next.
- ✓ Trong trang Rule Action, kích Deny, sau đó kích Next.
- ✓ Trong trang Protocols, trong danh sách Apply this rule to, kiểm tra rằng All IP traffic đã được lựa chọn, sau đó kích Next.
- ✓ Trong trang Schedule, kiểm tra rằng Always đã được lựa chọn, sau đó kích Next.
- ✓ Trong trang Client Type, kích Specific computers (client address sets), sau đó kích Next.
- ✓ Trong trang Client Sets, kích Add.

- ✓ Trong hộp thoại Add Client Sets, kích Accounting Department, kích Add, sau đó kích OK.
- ✓ Trong trang Client Sets, kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard, kích Finish.
- ✓ Kiểm tra để xác nhận việc truy cập không thành công từ nhóm nhóm Accounting Department

**Bước 4:** Xóa qui tắc giao thức từ chối người dùng trong nhóm Accounting Department

- ✓ Trong In ISA Management, kích Deny Access from Accounting Department
- ✓ Kích Delete a Protocol Rule.
- ✓ Trong hộp thoại Confirm Delete, kích Yes.

### **III. Thiết lập các qui tắc nội dung**

**Bước 1:** Thiết lập một qui tắc nội dung để từ chối truy cập tới nội dung đã được định nghĩa trong destination set và với lịch trình đã thiết lập ở mục 1

- ✓ Trong ISA Management, kích Site and Content Rules.
- ✓ Kích Create a Site and Content Rule.
- ✓ Trong New Site and Content Rule Wizard, trong mục Site and content rule name, gõ vào một tên ví dụ Deny Access Rule sau đó kích Next.
- ✓ Trong trang Rule Action, kiểm tra rằng Deny đã được chọn, sau đó kích Next.
- ✓ Trong trang Destination Sets, trong danh sách Apply this rule to, kích Specified destination set.
- ✓ Trong danh sách Name, lựa chọn set1 (đã thiết lập ở phần trên), sau đó kích Next.
- ✓ Trong trang Schedule, chọn schedule1 (đã thiết lập ở phần trên), sau đó kích Next.
- ✓ Trong trang Client Type, kiểm tra rằng Any request đã được chọn, sau đó kích Next.
- ✓ Trong trang Completing the New Site and Content Rule Wizard, kích Finish.

#### **Bước 2:**

Kiểm tra qui tắc vừa thiết lập

- ✓ Mở trình duyệt Internet Explorer.
- ✓ Trong ô Address, gõ http://home.vnn.vn sau đó ấn ENTER. kiểm tra rằng trang web này không được hiển thị, vì qui tắc nội dung đã thiết lập ở trên đã có hiệu lực
- ✓ Đóng trình duyệt Internet Explorer.

## Chương 6 - Bảo mật hệ thống và Firewall

Chương 6 tập trung vào các nội dung quan trọng về bảo mật hệ thống và mạng lưới. Nội dung của phần thứ nhất chương 6 cung cấp cho các học viên khái niệm về các hình thức tấn công mạng, các lỗ hổng, điểm yếu của mạng lưới. Các kỹ năng cơ bản trong phần một của chương 6 giúp người quản trị quản lý và xây dựng các chính sách bảo mật tương ứng cho các thành phần mạng, hệ thống hay dịch vụ ngay từ lúc bắt đầu hoạt động.

Phần 2 của chương 6 tập trung giới thiệu về thiết bị bảo mật mạnh và thông dụng trên mạng. Đó là thiết bị bức tường lửa (firewall). Học viên sẽ có được các kiến thức về cấu trúc firewall, các chức năng cơ bản và cách phân loại cũng như ưu nhược điểm của các loại firewall hoạt động theo các nguyên lý khác nhau. Những kỹ năng thiết lập cấu hình, luật, quản trị firewall với mô hình firewall checkpoint sẽ giúp cho các học viên hiểu cụ thể và các công việc quản trị và bảo mật hệ thống mạng

Chương 6 yêu cầu các học viên trang bị rất nhiều các kiến thức cơ bản như nắm vững các kiến thức quản trị hệ thống OS windows, linux, unix. Học viên cần hiểu sâu về giao thức TCP/IP, hoạt động của IP hay UDP, TCP. Học viên cần có hiểu biết về các port, socket của các giao thức dịch vụ như SMTP, POP3, WWW... Các kiến thức được trang bị trong các giáo trình quản trị hệ thống hoặc các tài liệu, sách giáo khoa về nội dung trên học viên nên tham khảo trước khi học chương 6 này.

### 1. Bảo mật hệ thống

#### 1.1. Các vấn đề chung về bảo mật hệ thống và mạng

Do đặc điểm của một hệ thống mạng là có nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên (mất mát, hoặc sử dụng không hợp lệ) trong môi trường mạng phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.

Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đôi tượng đồng thời đảm bảo mạng hoạt động ổn định, không bị tấn công bởi những kẻ phá hoại.

Có một thực tế là không một hệ thống mạng nào đảm bảo là an toàn tuyệt đối, một hệ thống dù được bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hoá bởi những kẻ có ý đồ xấu.

##### 1.1.1. Một số khái niệm và lịch sử bảo mật hệ thống

Trước khi tìm hiểu các vấn đề liên quan đến phương thức phá hoại và các biện pháp bảo vệ cũng như thiết lập các chính sách về bảo mật, ta sẽ tìm hiểu một số khái niệm liên quan đến bảo mật thông tin trên mạng Internet.

#### 1.1.1.1. Một số khái niệm

##### *a) Đối tượng tấn công mạng (Intruder):*

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.

Một số đối tượng tấn công mạng là:

- Hacker: Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.

- Masquerader: Là những kẻ giả mạo thông tin trên mạng. Có một số hình thức như giả mạo địa chỉ IP, tên miền, định danh người dùng ...

- Eavesdropping: Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị.

Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau như: ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

##### *b) Các lỗ hổng bảo mật:*

Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

##### *c) Chính sách bảo mật:*

Là tập hợp các qui tắc áp dụng cho mọi đối tượng có tham gia quản lý và sử dụng các tài nguyên và dịch vụ mạng.

Mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp các nhà quản trị thiết lập các biện pháp bảo đảm hữu hiệu trong quá trình trang bị, cấu hình, kiểm soát hoạt động của hệ thống và mạng

Một chính sách bảo mật được coi là hoàn hảo nếu nó xây dựng gồm các văn bản pháp qui, kèm theo các công cụ bảo mật hữu hiệu và nhanh chóng giúp người quản trị phát hiện, ngăn chặn các xâm nhập trái phép.



#### 1.1.1.2. Lịch sử bảo mật hệ thống

Có một số sự kiện đánh dấu các hoạt động phá hoại trên mạng, từ đó nảy sinh các yêu cầu về bảo mật hệ thống như sau:

- Năm 1988: Trên mạng Internet xuất hiện một chương trình tự nhân phiên bản của chính nó lên tất cả các máy trên mạng Internet. Các chương trình này gọi là "sâu". Tuy mức độ nguy hại của nó không lớn, nhưng nó đặt ra các vấn đề đối với nhà quản trị về quyền truy nhập hệ thống, cũng như các lỗi phần mềm.

- Năm 1990: Các hình thức truyền Virus qua địa chỉ Email xuất hiện phổ biến trên mạng Internet.

- Năm 1991: Phát hiện các chương trình trojans.

Cùng thời gian này sự phát triển của dịch vụ Web và các công nghệ liên quan như Java, Javascripts đã có rất nhiều các thông báo lỗi về bảo mật liên quan như: các lỗ hổng cho phép đọc nội dung các file dữ liệu của người dùng, một số lỗ hổng cho phép tấn công bằng hình thức DoS, spam mail làm ngưng trệ dịch vụ.

- Năm 1998: Virus Melissa lan truyền trên mạng Internet thông qua các chương trình gửi mail của Microsoft, gây những thiệt hại kinh tế không nhỏ.

- Năm 2000: Một loạt các Web Site lớn như yahoo.com và ebay.com bị tê liệt, ngừng cung cấp dịch vụ trong nhiều giờ do bị tấn công bởi hình thức DoS.

#### **1.1.2. Các lỗ hổng và phương thức tấn công mạng chủ yếu**

##### 1.1.2.1. Các lỗ hổng

Như phần trên đã trình bày, các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Windows 95, UNIX hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như word processing, các hệ databases...

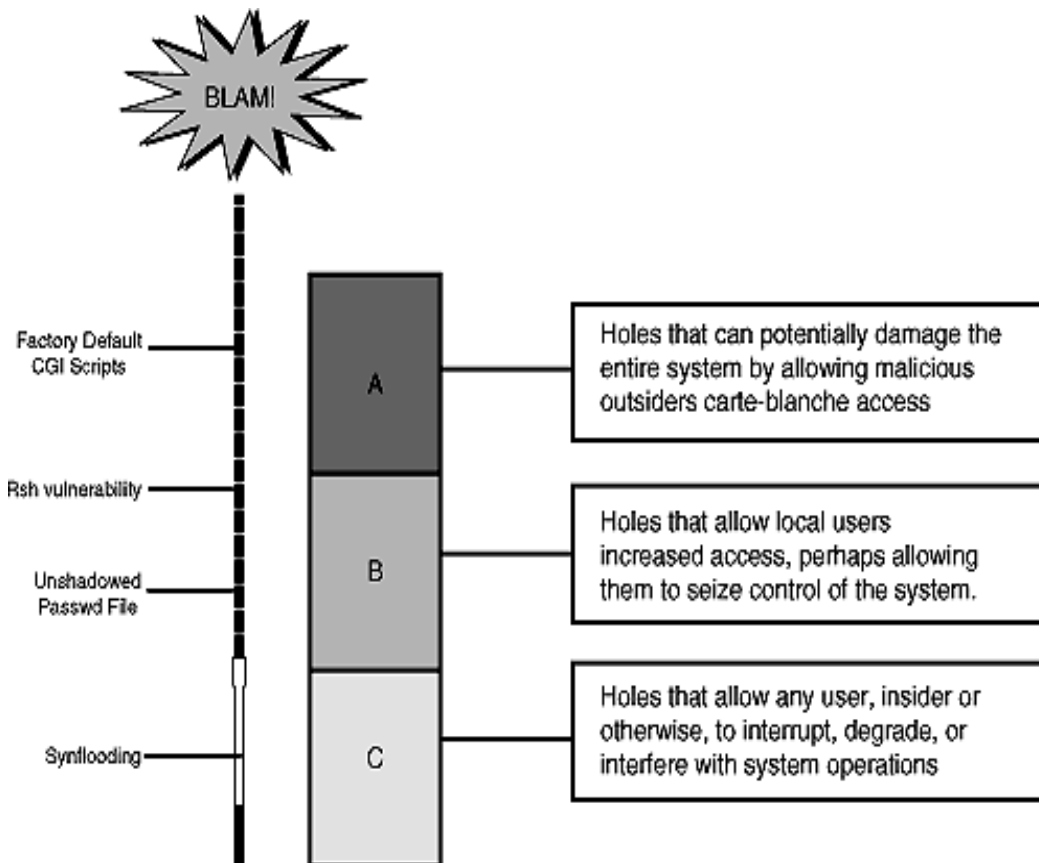
Có nhiều tổ chức khác nhau tiến hành phân loại các dạng lỗ hổng đặc biệt. Theo cách phân loại của Bộ quốc phòng Mỹ, các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

- Lỗ hổng loại C: các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services - Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống; không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.

- Lỗ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ nên có thể dẫn đến mất mát hoặc lộ thông tin yêu cầu bảo mật. Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống.

- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

Hình sau minh họa các mức độ nguy hiểm và loại lỗ hổng tương ứng:



Hình 6.1: Các loại lỗ hổng bảo mật và mức độ nguy hiểm

Sau đây ta sẽ phân tích một số lỗ hổng bảo mật thường xuất hiện trên mạng và hệ thống.

#### a) Các lỗ hổng loại C

Các lỗ hổng loại này cho phép thực hiện các cuộc tấn công DoS.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống. Một số lượng lớn các gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên quá tải, kết quả là server đáp ứng chậm hoặc không thể đáp ứng các yêu cầu từ client gửi tới.

Các dịch vụ có lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ. Hiện nay, chưa có một giải pháp toàn diện nào để khắc phục các lỗ

hồng loại này vì bản thân việc thiết kế giao thức ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của các lỗ hồng này.

Ví dụ điển hình của phương thức tấn công DoS là các cuộc tấn công vào một số Web Site lớn làm ngưng trệ hoạt động của web site này như: [www.ebay.com](http://www.ebay.com) và [www.yahoo.com](http://www.yahoo.com).

Tuy nhiên, mức độ nguy hiểm của các lỗ hồng loại này được xếp loại C, ít nguy hiểm vì chúng chỉ làm gián đoạn sự cung cấp dịch vụ của hệ thống trong một thời gian mà không làm nguy hại đến dữ liệu và những kẻ tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thống.

Một lỗ hồng loại C khác cũng thường thấy đó là các điểm yếu của dịch vụ cho phép thực hiện tấn công làm ngưng trệ hệ thống của người sử dụng cuối. Chủ yếu hình thức tấn công này là sử dụng dịch vụ Web. Giả sử trên một Web Server có những trang Web trong đó có chứa các đoạn mã Java hoặc JavaScripts, làm "treo" hệ thống của người sử dụng trình duyệt Web của Netscape bằng các bước sau:

- Viết các đoạn mã để nhận biết được Web Browsers sử dụng Netscape.
- Nếu sử dụng Netscape, sẽ tạo một vòng lặp vô thời hạn, sinh ra vô số các cửa sổ, trong mỗi cửa sổ đó nối đến các Web Server khác nhau.

Với một hình thức tấn công đơn giản này, có thể làm treo hệ thống trong khoảng thời gian 40 giây (đối với máy client có 64 MB RAM). Đây cũng là một hình thức tấn công kiểu DoS. Người sử dụng trong trường hợp này chỉ có thể khởi động lại hệ thống.

Một lỗ hồng loại C khác cũng thường gặp đối với các hệ thống mail là không xây dựng các cơ chế anti-relay (chống relay) cho phép thực hiện các hành động spam mail. Như chúng ta đã biết, cơ chế hoạt động của dịch vụ thư điện tử là lưu và chuyển tiếp. Một số hệ thống mail không có các xác thực khi người dùng gửi thư, dẫn đến tình trạng các đối tượng tấn công lợi dụng các máy chủ mail này để thực hiện spam mail. Spam mail là hành động nhằm làm tê liệt dịch vụ mail của hệ thống bằng cách gửi một số lượng lớn các message tới một địa chỉ không xác định, vì máy chủ mail luôn phải tốn năng lực đi tìm những địa chỉ không có thực dẫn đến tình trạng ngưng trệ dịch vụ. Các message có thể sinh ra từ các chương trình làm bom thư rất phổ biến trên mạng Internet.

*b) Các lỗ hồng loại B:*

Lỗ hồng loại này có mức độ nguy hiểm hơn lỗ hồng loại C, cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.

Ví dụ trên hình 12, lỗ hồng loại B có thể có đối với một hệ thống UNIX mà file `/etc/passwd` để ở dạng plaintext; không sử dụng cơ chế che mật khẩu trong UNIX (sử dụng file `/etc/shadow`)

Những lỗ hồng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng local được hiểu là người đã có quyền truy nhập vào hệ thống với một số quyền hạn nhất định.

Một loại các vấn đề về quyền sử dụng chương trình trên UNIX cũng thường gây nên các lỗ hổng loại B. Vì trên hệ thống UNIX một chương trình có thể được thực thi với 2 khả năng:

- Người chủ sở hữu chương trình đó kích hoạt chạy.
- Người mang quyền của người sở hữu file đó kích hoạt chạy.

Một dạng khác của lỗ hổng loại B xảy ra đối với các chương trình có mã nguồn viết bằng C. Những chương trình viết bằng C thường sử dụng một vùng đệm - một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng, qui định trường này dài 20 ký tự. Do đó họ sẽ khai báo:

```
char first_name [20];
```

Khai báo này sẽ cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm; nếu người sử dụng nhập vào 35 ký tự sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ. Đối với những kẻ tấn công, có thể lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt, để thực thi một số lệnh đặc biệt trên hệ thống. Thông thường, lỗ hổng này thường được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

#### *c) Các lỗ hổng loại A:*

Các lỗ hổng loại A có mức độ rất nguy hiểm, đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Một ví dụ thường thấy là trên nhiều hệ thống sử dụng Web Server là Apache, Đối với Web Server này thường cấu hình thư mục mặc định để chạy các script là cgi-bin; trong đó có một Scripts được viết sẵn để thử hoạt động của apache là test-cgi. Đối với các phiên bản cũ của Apache (trước version 1.1), có dòng sau trong file test-cgi:

```
echo QUERY_STRING = $QUERY_STRING
```

Biến môi trường QUERY\_STRING do không được đặt trong có dấu " (quote) nên khi phía client thực hiện một yêu cầu trong đó chuỗi ký tự gửi đến gồm một số ký tự đặc biệt; ví dụ ký tự "\*", web server sẽ trả về nội dung của toàn bộ thư mục hiện thời (là các thư mục chứa các script cgi). Người sử dụng có thể nhìn thấy toàn bộ nội dung các file trong thư mục hiện thời trên hệ thống server.

Một ví dụ khác cũng xảy ra tương tự đối với các Web server chạy trên hệ điều hành Novell: các web server này có một scripts là convert.bas, chạy scripts này cho phép đọc toàn bộ nội dung các files trên hệ thống.

Những lỗ hổng loại này hết sức nguy hiểm vì nó đã tồn tại sẵn có trên phần mềm sử dụng, người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng sẽ có thể bỏ qua những điểm yếu này.

Đối với những hệ thống cũ, thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này. Một loạt các chương trình phiên bản cũ thường sử dụng có những lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger...

#### 1.1.2.2. Một số phương thức tấn công mạng phổ biến

##### *a) Scanner*

Scanner là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc cục bộ hoặc trên một trạm ở xa. Với chức năng này, một kẻ phá hoại sử dụng chương trình Scanner có thể phát hiện ra những lỗ hổng về bảo mật trên một server ở xa.

Các chương trình scanner thường có một cơ chế chung là rà soát và phát hiện những port TCP/UDP được sử dụng trên một hệ thống cần tấn công từ đó phát hiện những dịch vụ sử dụng trên hệ thống đó. Sau đó các chương trình scanner ghi lại những đáp ứng trên hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tìm ra những điểm yếu trên hệ thống.

Những yếu tố để một chương trình Scanner có thể hoạt động như sau:

- Yêu cầu về thiết bị và hệ thống: Một chương trình Scanner có thể hoạt động được nếu môi trường đó có hỗ trợ TCP/IP (bất kể hệ thống là UNIX, máy tính tương thích với IBM, hoặc dòng máy Macintosh).
- Hệ thống đó phải kết nối vào mạng Internet.

Tuy nhiên không phải đơn giản để xây dựng một chương trình Scanner, những kẻ phá hoại cần có kiến thức sâu về TCP/IP, những kiến thức về lập trình C, PERL và một số ngôn ngữ lập trình shell. Ngoài ra người lập trình (hoặc người sử dụng) cần có kiến thức là lập trình socket, phương thức hoạt động của các ứng dụng client/server.

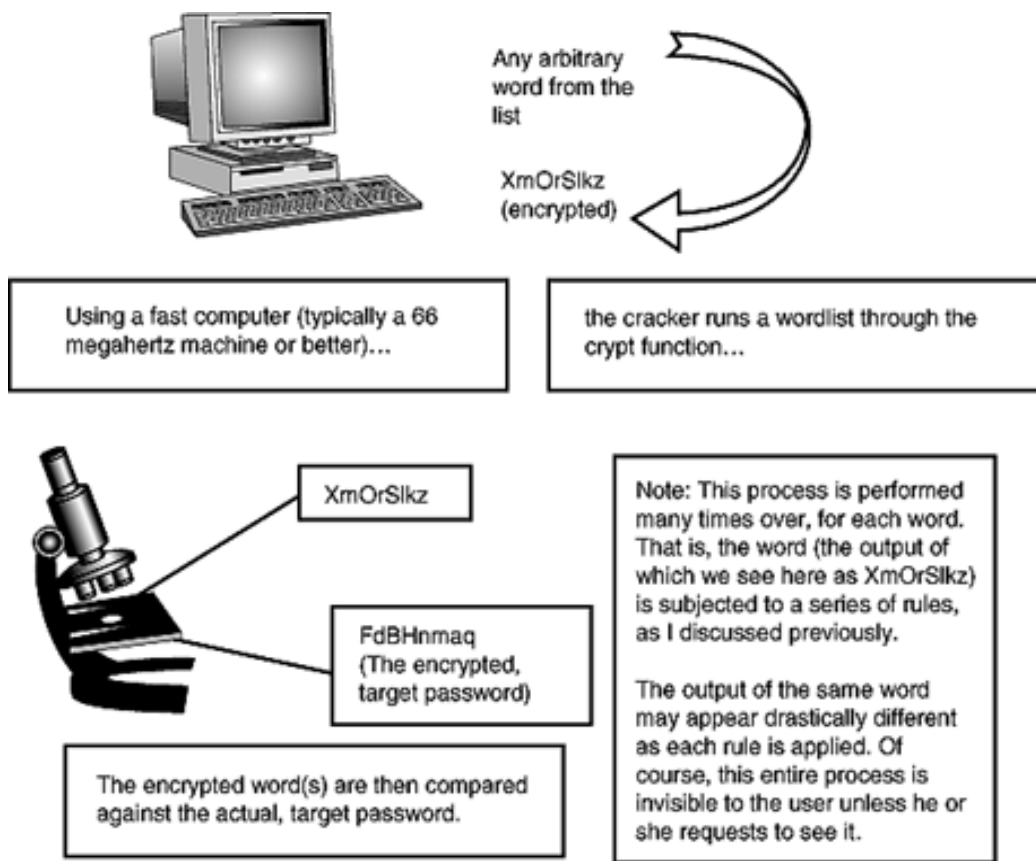
Các chương trình Scanner có vai trò quan trọng trong một hệ thống bảo mật, vì chúng có khả năng phát hiện ra những điểm yếu kém trên một hệ thống mạng. Đối với người quản trị mạng những thông tin này là hết sức hữu ích và cần thiết; đối với những kẻ phá hoại những thông tin này sẽ hết sức nguy hiểm.

##### *b) Password Cracker*

Password cracker là một chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.

Để hiểu cách thức hoạt động của các chương trình bẻ khoá, chúng ta cần hiểu cách thức mã hoá để tạo mật khẩu. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.

Quá trình hoạt động của các chương trình bẻ khoá được minh hoạ trong hình sau:



Hình 6.2: Hoạt động của các chương trình bẻ khoá

Theo sơ đồ trên, một danh sách các từ được tạo ra và được mã hoá đối với từng từ. Sau mỗi lần mã hoá, chương trình sẽ so sánh với mật khẩu đã mã hoá cần phá. Nếu không thấy trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là *brute-force*.

**Yếu tố về thiết bị phần cứng:** Trong hình trên máy tính thực hiện các chương trình phá khoá là một máy PC 66MHz hoặc cấu hình cao hơn. Trong thực tế yêu cầu các thiết bị phần cứng rất mạnh đối với những kẻ phá khoá chuyên nghiệp. Một phương thức khác có thể thay thế là thực hiện việc phá khoá trên một hệ thống phân tán; do vậy giảm bớt được các yêu cầu về thiết bị so với phương pháp làm tại một máy.

Nguyên tắc của một số chương trình phá khoá có thể khác nhau. Một vài chương trình tạo một danh sách các từ giới hạn, áp dụng một số thuật toán mã hoá, từ kết quả so sánh với password đã mã hoá cần bẻ khoá để tạo ra một danh sách khác theo một logic của chương trình, cách này tuy không chuẩn tắc nhưng khá nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng thường tuân theo một số qui tắc dễ thuận tiện khi sử dụng.

Đến giai đoạn cuối cùng, nếu thấy phù hợp với mật khẩu đã được mã hoá, kẻ phá khoá sẽ có được mật khẩu dạng text thông thường. Trong hình trên, mật khẩu dạng text thông thường được ghi vào một file.

Để đánh giá khả năng thành công của các chương trình bẻ khoá ta có công thức sau:

$$P = L \times R / S$$

Trong đó:

P: Xác suất thành công

L: Thời gian sống của một mật khẩu

R: Tốc độ thử

S: Không gian mật khẩu =  $A^M$  (M là chiều dài mật khẩu)

Ví dụ, trên hệ thống UNIX người ta đã chứng minh được rằng nếu mật khẩu dài quá 8 ký tự thì xác suất phá khoá gần như = 0. Cụ thể như sau:

Nếu sử dụng khoảng 92 ký tự có thể đặt mật khẩu, không gian mật khẩu có thể có là  $S = 92^8$

Với tốc độ thử là 1000 mật khẩu trong một giây có  $R = 1000/s$

Thời gian sống của một mật khẩu là 1 năm

Ta có xác suất thành công là :

$$P = 1 \times 365 \times 86400 \times 1000 / 92^8 = 1 / 1.000.000$$

Như vậy việc dò mật khẩu là không thể vì sẽ mất khoảng 100 năm mới tìm ra mật khẩu chính xác.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như:

- Các thông tin trong tập tin /etc/passwd
- Một số từ điển
- Từ lặp và các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục đối với cách thức phá hoại này là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

### c) Trojans

Dựa theo truyền thuyết cổ Hy Lạp "Ngựa thành Trojan", trojans là một chương trình chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Những chương trình này thực hiện những chức năng mà người sử dụng hệ thống thường không mong muốn hoặc không hợp pháp. Thông thường, trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã của nó bằng những mã bất hợp pháp.

Các chương trình virus là một loại điển hình của Trojans. Những chương trình virus che dấu các đoạn mã trong các chương trình sử dụng hợp

pháp. Khi những chương trình này được kích hoạt thì những đoạn mã ẩn dấu sẽ được thực thi để thực hiện một số chức năng mà người sử dụng không biết.

Một định nghĩa chuẩn tắc về các chương trình Trojans như sau: chương trình trojans là một chương trình thực hiện một công việc mà người sử dụng không biết trước, giống như ăn cắp mật khẩu hay copy file mà người sử dụng không nhận thức được.

Những tác giả của các chương trình trojan xây dựng một kết hoạch. Xét về khía cạnh bảo mật trên Internet, một chương trình trojan sẽ thực hiện một trong những công việc sau:

- Thực hiện một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

- Che dấu một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

Một vài chương trình trojan có thể thực hiện cả 2 chức năng này. Ngoài ra, một số chương trình trojans còn có thể phá hủy hệ thống bằng cách phá hoại các thông tin trên ổ cứng (ví dụ trường hợp của virus Melissa lây lan qua đường thư điện tử).

Hiện nay với nhiều kỹ thuật mới, các chương trình trojan kiểu này dễ dàng bị phát hiện và không có khả năng phát huy tác dụng. Tuy nhiên trong UNIX việc phát triển các chương trình trojan vẫn hết sức phổ biến.

Các chương trình trojan có thể lây lan qua nhiều phương thức, hoạt động trên nhiều môi trường hệ điều hành khác nhau (từ Unix tới Windows, DOS). Đặc biệt trojans thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet.

Việc đánh giá mức độ ảnh hưởng của các chương trình trojans hết sức khó khăn. Trong một vài trường hợp, nó chỉ đơn giản là ảnh hưởng đến các truy nhập của khách hàng như các chương trình trojans lấy được nội dung của file passwd và gửi mail tới kẻ phá hoại. Cách thức sửa đơn giản nhất là thay thế toàn bộ nội dung của các chương trình đã bị ảnh hưởng bởi các đoạn mã trojans và thay thế các password của người sử dụng hệ thống.

Tuy nhiên với những trường hợp nghiêm trọng hơn, là những kẻ tấn công tạo ra những lỗ hổng bảo mật thông qua các chương trình trojans. Ví dụ những kẻ tấn công lấy được quyền root trên hệ thống và lợi dụng nó để phá hủy toàn bộ hoặc một phần của hệ thống. Chúng dùng quyền root để thay đổi logfile, cài đặt các chương trình trojans khác mà người quản trị không thể phát hiện. Trong trường hợp này, mức độ ảnh hưởng là nghiêm trọng và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

#### d) Sniffer

Đối với bảo mật hệ thống sniffer được hiểu là các công cụ (có thể là phần cứng hoặc phần mềm) "bắt" các thông tin lưu chuyển trên mạng và từ các



thông tin "bắt" được đó để lấy được những thông tin có giá trị trao đổi trên mạng.

Hoạt động của sniffer cũng giống như các chương trình "bắt" các thông tin gõ từ bàn phím (key capture). Tuy nhiên các tiện ích key capture chỉ thực hiện trên một trạm làm việc cụ thể còn đối với sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.

Các chương trình sniffer (sniffer mềm) hoặc các thiết bị sniffer (sniffer cứng) đều thực hiện bắt các gói tin ở tầng IP trở xuống (gồm IP datagram và Ethernet Packet). Do đó, có thể thực hiện sniffer đối với các giao thức khác nhau ở tầng mạng như TCP, UDP, IPX, ...

Mặt khác, giao thức ở tầng IP được định nghĩa công khai, và cấu trúc các trường header rõ ràng, nên việc giải mã các gói tin này không khó khăn.

Mục đích của các chương trình sniffer đó là thiết lập chế độ promiscuous (mode dùng chung) trên các card mạng ethernet - nơi các gói tin trao đổi trong mạng - từ đó "bắt" được thông tin.

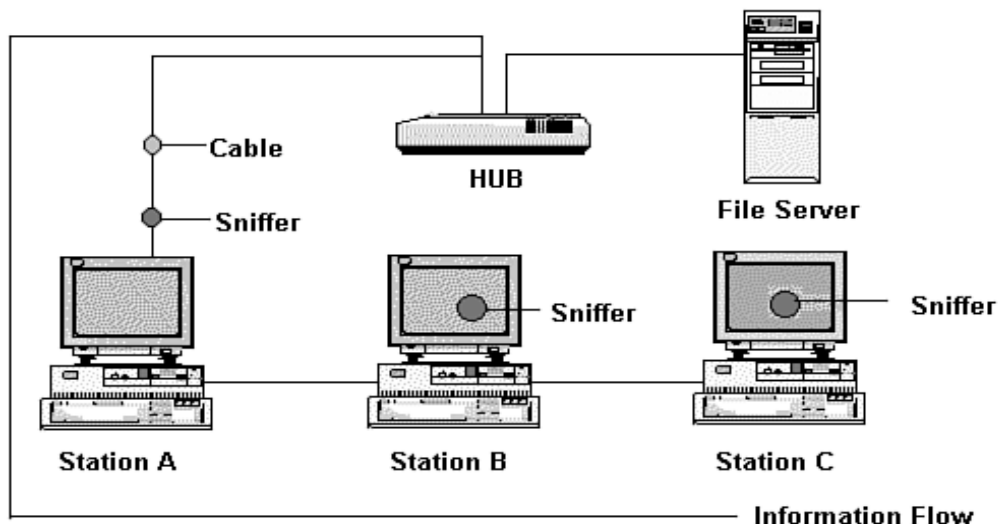
Các thiết bị sniffer có thể bắt được toàn bộ thông tin trao đổi trên mạng là dựa vào nguyên tắc broadcast (quảng bá) các gói tin trong mạng Ethernet.

Trên hệ thống mạng không dùng hub, dữ liệu không chuyển đến một hướng mà được lưu chuyển theo mọi hướng. Ví dụ khi một trạm làm việc cần được gửi một thông báo đến một trạm làm việc khác trên cùng một segment mạng, một yêu cầu từ trạm đích được gửi tới tất cả các trạm làm việc trên mạng để xác định trạm nào là trạm cần nhận thông tin (trạm đích). Cho tới khi trạm nguồn nhận được thông báo chấp nhận từ trạm đích thì luồng dữ liệu sẽ được gửi đi. Theo đúng nguyên tắc, những trạm khác trên segment mạng sẽ bỏ qua các thông tin trao đổi giữa hai trạm nguồn và trạm đích xác định. Tuy nhiên, các trạm khác cũng không bị bắt buộc phải bỏ qua những thông tin này, do đó chúng vẫn có thể "nghe" được bằng cách thiết lập chế độ promiscuous mode trên các card mạng của trạm đó. Sniffer sẽ thực hiện công việc này.

Một hệ thống sniffer có thể kết hợp cả các thiết bị phần cứng và phần mềm, trong đó hệ thống phần mềm với các chế độ debug thực hiện phân tích các gói tin "bắt" được trên mạng.

Hệ thống sniffer phải được đặt trong cùng một segment mạng (network block) cần nghe lén.

Hình sau minh họa vị trí đặt sniffer:



Hình 6.3: Các vị trí đặt sniffer trên 1 segment mạng

Phương thức tấn công mạng dựa vào các hệ thống sniffer là rất nguy hiểm vì nó được thực hiện ở các tầng rất thấp trong hệ thống mạng. Với việc thiết lập hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng. Các thông tin đó có thể là:

- Các tài khoản và mật khẩu truy nhập
- Các thông tin nội bộ hoặc có giá trị cao...

Tuy nhiên việc thiết lập một hệ thống sniffer không phải đơn giản vì cần phải xâm nhập được vào hệ thống mạng đó và cài đặt các phần mềm sniffer. Đồng thời các chương trình sniffer cũng yêu cầu người sử dụng phải hiểu sâu về kiến trúc, các giao thức mạng.

Mặc khác, số lượng các thông tin trao đổi trên mạng rất lớn nên các dữ liệu do các chương trình sniffer sinh ra khá lớn. Thông thường, các chương trình sniffer có thể cấu hình để chỉ thu nhập từ 200 - 300 bytes trong một gói tin, vì thường những thông tin quan trọng như tên người dùng, mật khẩu nằm ở phần đầu gói tin.

Trong một số trường hợp quản trị mạng, để phân tích các thông tin lưu chuyển trên mạng, người quản trị cũng cần chủ động thiết lập các chương trình sniffer, với vai trò này sniffer có tác dụng tốt.

Việc phát hiện hệ thống bị sniffer không phải đơn giản, vì sniffer hoạt động ở tầng rất thấp, và không ảnh hưởng tới các ứng dụng cũng như các dịch vụ hệ thống đó cung cấp. Một số biện pháp sau chỉ có tác dụng kiểm tra hệ thống như:

- Kiểm tra các tiến trình đang thực hiện trên hệ thống (bằng lệnh ps trên Unix hoặc trình quản lý tài nguyên trong Windows NT). Qua đó kiểm tra các tiến trình lạ trên hệ thống; tài nguyên sử dụng, thời gian khởi tạo tiến trình... để phát hiện các chương trình sniffer.

- Sử dụng một vài tiện ích để phát hiện card mạng có chuyển sang chế độ promiscuous hay không. Những tiện ích này giúp phát hiện hệ thống của bạn có đang chạy sniffer hay không.

Tuy nhiên việc xây dựng các biện pháp hạn chế sniffer cũng không quá khó khăn nếu ta tuân thủ các nguyên tắc về bảo mật như:

- Không cho người lạ truy nhập vào các thiết bị trên hệ thống
- Quản lý cấu hình hệ thống chặt chẽ
- Thiết lập các kết nối có tính bảo mật cao thông qua các cơ chế mã hoá.

### **1.1.3. Một số điểm yếu của hệ thống**

#### 1.1.3.1. Deamon fingerd

Một lỗ hổng của deamon fingerd là cơ hội để phương thức tấn công worm "sâu" trên Internet phát triển: đó là lỗi tràn vùng đệm trong các tiến trình fingerd (lỗi khi lập trình). Vùng đệm để lưu chuỗi ký tự nhập được giới hạn là 512 bytes. Tuy nhiên chương trình fingerd không thực hiện kiểm tra dữ liệu đầu vào khi lớn hơn 512 bytes. Kết quả là xảy ra hiện tượng tràn dữ liệu ở vùng đệm khi dữ liệu lớn hơn 512 bytes. Phần dữ liệu dư thừa chứa những đoạn mã để kích một script khác hoạt động; scripts này tiếp tục thực hiện finger tới một host khác. Kết quả là hình thành một mắt xích các "sâu" trên mạng Internet.

#### 1.1.3.2. File hosts.equiv

Nếu một người sử dụng được xác định trong file host.equiv cũng với địa chỉ máy của người đó, thì người sử dụng đó được phép truy nhập từ xa vào hệ thống đã khai báo. Tuy nhiên có một lỗ hổng khi thực hiện chức năng này đó là nó cho phép người truy nhập từ xa có được quyền của bất cứ người nào khác trên hệ thống. Ví dụ, nếu trên máy A có một file /etc/host.equiv có dòng định danh B julie, thì julie trên B có thể truy nhập vào hệ thống A và có bất được quyền của bất cứ người nào khác trên A. Đây là do lỗi của thủ tục ruserok() trong thư viện libc khi lập trình.

#### 1.1.3.3. Thư mục /var/mail

Nếu thư mục /var/mail được set là với quyền được viết (writeable) đối với tất cả mọi người trên hệ thống, thì bất cứ ai có thể tạo file trong thư mục này. Sau đó tạo một file với tên của một người đã có trên hệ thống rồi link tới một file trên hệ thống, thì các thư tới người sử dụng có tên trùng với tên file link sẽ được gán thêm vào trong file mà nó link tới.

Ví dụ, một người sử dụng tạo link từ /var/mail/root tới /etc/passwd, sau đó gửi mail bằng tên một người mới tới root thì tên người sử dụng mới này sẽ được gán thêm vào trong file /etc/passwd; Do vậy thư mục /var/mail không bao giờ được set với quyền writeable.

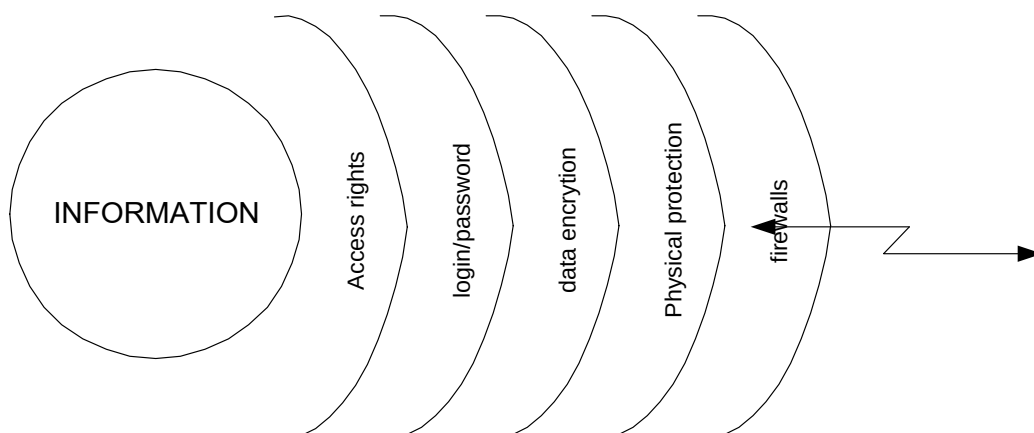
#### 1.1.3.4. Chức năng proxy của FTPd

Chức năng proxy server của FTPd cho phép một người sử dụng có thể truyền file từ một ftpd này tới một ftpd server khác. Sử dụng chức năng này sẽ có thể bỏ qua được các xác thực dựa trên địa chỉ IP.

Nguyên nhân là do người sử dụng có thể yêu cầu một file trên ftp server gửi một file tới bất kỳ địa chỉ IP nào. Nên người sử dụng có thể yêu cầu ftp server đó gửi một file gồm các lệnh là PORT và PASV tới các server đang nghe trên các port TCP trên bất kỳ một host nào; kết quả là một trong các host đó có ftp server chạy và tin cậy người sử dụng đó nên bỏ qua được xác thực địa chỉ IP.

#### 1.1.4. Các mức bảo vệ an toàn mạng

Vì không có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các server của mạng. Hình sau mô tả các lớp rào chắn thông dụng hiện nay để bảo vệ thông tin tại các trạm của mạng:



Hình 6.4: Các mức độ bảo vệ mạng

Như minh họa trong hình trên, các lớp bảo vệ thông tin trên mạng gồm:

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiện nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp.

- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải có đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động

của mạng và xác định quyền truy nhập của những người sử dụng khác tùy theo thời gian và không gian.

- Lớp thứ ba là sử dụng các phương pháp mã hoá (encryption). Dữ liệu được biến đổi từ dạng clear text sang dạng mã hoá theo một thuật toán nào đó.

- Lớp thứ tư là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khoá trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...

- Lớp thứ năm: Cài đặt các hệ thống bức tường lửa (firewall), nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó.

## 1.2. Các biện pháp bảo vệ mạng máy tính

### 1.2.1. Kiểm soát hệ thống qua logfile

Một trong những biện pháp dò tìm các dấu vết hoạt động trên một hệ thống là dựa vào các công cụ ghi logfile. Các công cụ này thực hiện ghi lại nhật ký các phiên làm việc trên hệ thống. Nội dung chi tiết thông tin ghi lại phụ thuộc vào cấu hình người quản trị hệ thống. Ngoài việc rà soát theo dõi hoạt động, đối với nhiều hệ thống các thông tin trong logfile giúp người quản trị đánh giá được chất lượng, hiệu năng của mạng lưới.

#### 1.2.1.1. Hệ thống logfile trong Unix

Trong Unix, các công cụ ghi log tạo ra logfile là các file dưới dạng text thông thường cho phép người sử dụng dùng những công cụ soạn thảo file text bất kỳ để có thể đọc được nội dung. Tuy nhiên, một số trường hợp logfile được ghi dưới dạng binary và chỉ có thể sử dụng một số tiện ích đặc biệt mới có thể đọc được thông tin.

##### a) Logfile lastlog:

Tiện ích này ghi lại những lần truy nhập gần đây đối với hệ thống. Các thông tin ghi lại gồm tên người truy nhập, thời điểm, địa chỉ truy nhập ... Các chương trình login sẽ đọc nội dung file lastlog, kiểm tra theo UID truy nhập vào hệ thống và sẽ thông báo lần truy nhập vào hệ thống gần đây nhất. Ví dụ như sau:

```
Last login: Fri Sep 15 2000 14:11:38
Sun Microsystems Inc. SunOS 5.7 Generic October 1998
No mail.
Sun Microsystems Inc. SunOS 5.7 Generic October 1998
/export/home/ptthanh
```

*b) Logfile UTMP*

Logfile này ghi lại thông tin về những người đang login vào hệ thống, thường nằm ở thư mục `/etc/utmp`. Để xem thông tin trong logfile có thể sử dụng các tiện ích như `who`, `w`, `finger`, `rwho`, `users`. Ví dụ nội dung của logfile dùng lệnh `who` như sau:

```
/export/home/vhai% who
root console Aug 10 08:45 (:0)
ptthanh pts/4 Sep 15 15:27 (203.162.0.87)
ptthanh pts/6 Sep 15 15:28 (203.162.0.87)
root pts/12 Sep 7 16:35 (:0.0)
root pts/13 Sep 7 11:35 (:0.0)
root pts/14 Sep 7 11:39 (:0.0)
```

*c) Logfile WTMP*

Logfile này ghi lại các thông tin về các hoạt động login và logout vào hệ thống. Nó có chức năng tương tự với logfile UTMP. Ngoài ra còn ghi lại các thông tin về các lần shutdown, reboot hệ thống, các phiên truy nhập hoặc ftp và thường nằm ở thư mục `/var/adm/wtmp`. Logfile này thường được xem bằng lệnh `"last"`. Ví dụ nội dung như sau:

```
/export/home/vhai% last | more
ptthanh pts/10 203.162.0.85 Mon Sep 18 08:44 still logged in
ptthanh pts/10 Sat Sep 16 16:52 - 16:52 (00:00)
vtoan pts/10 203.162.0.87 Fri Sep 15 15:30 - 16:52 (1+01:22)
vtoan pts/6 203.162.0.87 Fri Sep 15 15:28 still logged in
vtoan pts/4 Fri Sep 15 15:12 - 15:12 (00:00)
```

*d) Tiện ích Syslog*

Đây là một công cụ ghi logfile rất hữu ích, được sử dụng rất thông dụng trên các hệ thống UNIX. Tiện ích syslog giúp người quản trị hệ thống dễ dàng trong việc thực hiện ghi logfile đối với các dịch vụ khác nhau. Thông thường tiện ích syslog thường được chạy dưới dạng một daemon và được kích hoạt khi hệ thống khởi động. Daemon syslogd lấy thông tin từ một số nguồn sau:

- `/dev/log`: Nhận các messages từ các tiến trình hoạt động trên hệ thống
- `/dev/klog`: nhận messages từ kernel
- port 514: nhận các messages từ các máy khác qua port 514 UDP.

Khi syslogd nhận các messages từ các nguồn thông tin này nó sẽ thực hiện kiểm tra file cấu hình của dịch vụ là `syslog.conf` để tạo log file tương ứng. Có thể cấu hình file `syslog.conf` để tạo một message với nhiều dịch vụ khác nhau.

Ví dụ nội dung một file syslog.conf như sau:

```
This file is processed by m4 so be careful to quote (') names
that match m4 reserved words. Also, within ifdef's, arguments
containing commas must be quoted.
#
*.err;kern.notice;auth.notice /dev/console
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages
*.alert;kern.err;daemon.err operator
*.alert root
*.emerg *
if a non-loghost machine chooses to have authentication messages
```

Trong nội dung file syslog.conf chỉ ra, đối với các message có dạng \*.emerg (message có tính khẩn cấp) sẽ được thông báo tới tất cả người sử dụng trên hệ thống; Đối với các messages có dạng \*.err, hoặc kern.debug và những hoạt động truy cập không hợp pháp sẽ được ghi log trong file /var/adm/messages.

Mặc định, các messages được ghi vào logfile /var/adm/messages.

#### e) Tiện ích sulog

Bất cứ khi nào người sử dụng dùng lệnh "su" để chuyển sang hoạt động hệ thống dưới quyền một user khác đều được ghi log thông qua tiện ích sulog. Những thông tin logfile này được ghi vào logfile /var/adm/sulog. Tiện ích này cho phép phát hiện các trường hợp dùng quyền root để có được quyền của một user nào khác trên hệ thống.

Ví dụ nội dung của logfile sulog như sau:

```
more /var/adm/sulog
SU 01/04 13:34 + pts/1 ptthanh-root
SU 01/04 13:53 + pts/6 ptthanh-root
SU 01/04 14:19 + pts/6 ptthanh-root
SU 01/04 14:39 + pts/1 ptthanh-root
```

#### f) Tiện ích cron

Tiện ích cron sẽ ghi lại logfile của các hoạt động thực hiện bởi lệnh crontabs. Thông thường, logfile của các hoạt động cron lưu trong file /var/log/cron/log. Ngoài ra, có thể cấu hình syslog để ghi lại các logfile của hoạt động cron.

Ví dụ nội dung của logfile cron như sau:

```
more /var/log/cron/log
! *** cron started *** pid = 2367 Fri Aug 4 16:32:38 2000
> CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
> ptthanh 2386 c Fri Aug 4 16:34:01 2000
< ptthanh 2386 c Fri Aug 4 16:34:02 2000
> CMD: /export/home/mrtg/getcount.pl
> ptthanh 2400 c Fri Aug 4 16:35:00 2000
< ptthanh 2400 c Fri Aug 4 16:35:10 2000
> CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
```

*g) Logfile của sendmail*

Hoạt động ghi log của sendmail có thể được ghi qua tiện ích syslog. Ngoài ra chương trình sendmail còn có lựa chọn "-L + level security" với mức độ bảo mật từ "debug" tới "crit" cho phép ghi lại logfile. Vì sendmail là một chương trình có nhiều bug, với nhiều lỗ hổng bảo mật nên người quản trị hệ thống thường xuyên ghi lại logfile đối với dịch vụ này.

*h) Logfile của dịch vụ FTP*

Hầu hết các daemon FTP hiện nay đều cho phép cấu hình để ghi lại logfile sử dụng dịch vụ FTP trên hệ thống đó. Hoạt động ghi logfile của dịch vụ FTP thường được sử dụng với lựa chọn "-l", cấu hình cụ thể trong file /etc/inetd.conf như sau:

```
more /etc/inetd.conf
ftp stream tcp nowait root /etc/ftpd/in.ftpd in.ftpd -l
```

Sau đó cấu hình syslog.conf tương ứng với dịch vụ FTP; cụ thể như sau:

```
Logfile FTP
daemon.info ftplogfile
```

Với lựa chọn này sẽ ghi lại nhiều thông tin quan trọng trong một phiên ftp như: thời điểm truy nhập, địa chỉ IP, dữ liệu get/put ... vào site FTP đó. Ví dụ nội dung logfile của một phiên ftp như sau:

```
Sun Jul 16 21:55:06 2000 12 nms 8304640 /export/home/ptthanh/PHSS_17926.depot b _ o r
ptthanh ftp 0 * c
Sun Jul 16 21:56:45 2000 96 nms 64624640 /export/home/ptthanh/PHSS_19345.depot b _ o
r ptthanh ftp 0 * c
Sun Jul 16 21:57:41 2000 4 nms 3379200 /export/home/ptthanh/PHSS_19423.depot b _ o r
ptthanh ftp 0 * c
Sun Jul 16 22:00:38 2000 174 nms 130396160 /export/home/ptthanh/PHSS_19987.depot b _
o r ptthanh ftp 0 * c
```



*i) Logfile của dịch vụ Web:*

Tùy thuộc vào Web server sử dụng sẽ có các phương thức và cấu hình ghi logfile của dịch vụ Web khác nhau. Hầu hết các web server thông dụng hiện nay đều hỗ trợ cơ chế ghi log. Ví dụ nội dung logfile của dịch vụ Web sử dụng Web server Netscape như sau:

```
202.167.123.170 - - [03/Aug/2000:10:59:43 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
203.162.46.67 - - [03/Sep/2000:22:50:52 +0700] "GET http://www.geocities.com/ HTTP/1.1" 401 223
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
203.162.0.85 - ptthanh [15/Sep/2000:07:43:22 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 404 207
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
```

1.2.1.2. Một số công cụ hữu ích hỗ trợ phân tích logfile:

Đối với người quản trị, việc phân tích logfile của các dịch vụ là hết sức quan trọng. Một số công cụ trên mạng giúp người quản trị thực hiện công việc này dễ dàng hơn, đó là:

- Tiện ích chklastlog và chkwtmpt giúp phân tích các logfile lastlog và WTMP theo yêu cầu người quản trị.

- Tiện ích netlog giúp phân tích các gói tin, gồm 3 thành phần:

- + TCPlogger: log lại tất cả các kết nối TCP trên một subnet

- + UDPlogger: log lại tất cả các kết nối UDP trên một subnet

- + Extract: Xử lý các logfile ghi lại bởi TCPlogger và UDBlogger.

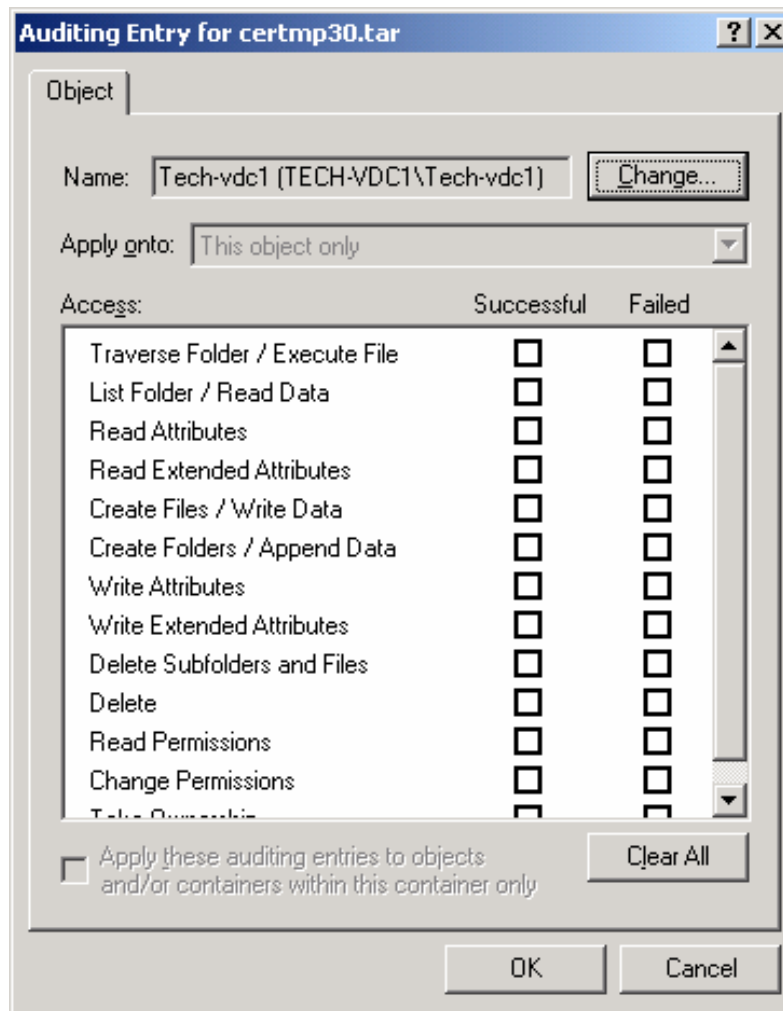
- Tiện ích TCP wrapper: Tiện ích này cho phép người quản trị hệ thống dễ dàng giám sát và lọc các gói tin TCP của các dịch vụ như systat, finger, telnet, rlogin, rsh, talk ...

1.2.1.3. Các công cụ ghi log thường sử dụng trong Windows NT và 2000

Trong hệ thống Windows NT 4.0 và Windows 2000 hiện nay đều hỗ trợ đầy đủ các cơ chế ghi log với các mức độ khác nhau. Người quản trị hệ thống tùy thuộc vào mức độ an toàn của dịch vụ và các thông tin sử dụng có thể lựa chọn các mức độ ghi log khác nhau. Ngoài ra, trên hệ thống Windows NT còn hỗ trợ các cơ chế ghi logfile trực tiếp vào các database để tạo báo cáo giúp người quản trị phân tích và kiểm tra hệ thống nhanh chóng và thuận tiện. Sử dụng tiện ích event view để xem các thông tin logfile trên hệ thống với các mức độ như Application log; Security log; System log. Các hình dưới đây sẽ minh họa một số hoạt động ghi logfile trên hệ thống Windows:

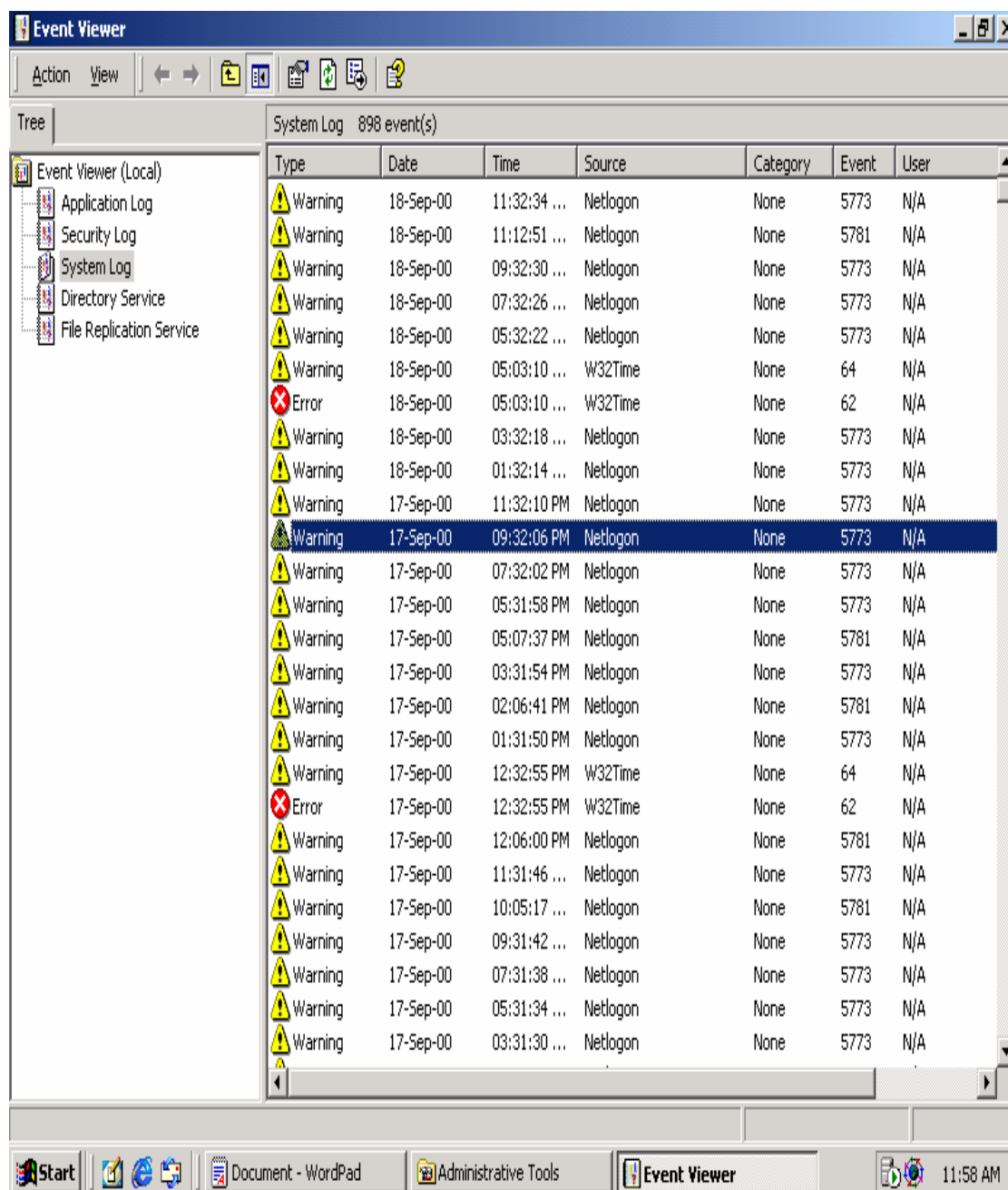
Ví dụ: Để ghi lại hoạt động đọc, viết, truy nhập.... đối với một file/thư mục là thành công hay không thành công người quản trị có thể cấu hình như sau:

Chọn File Manager - User Manager - Security - Auditing. Ví dụ hình sau minh họa các hoạt động có thể được ghi log trong Windows 2000:



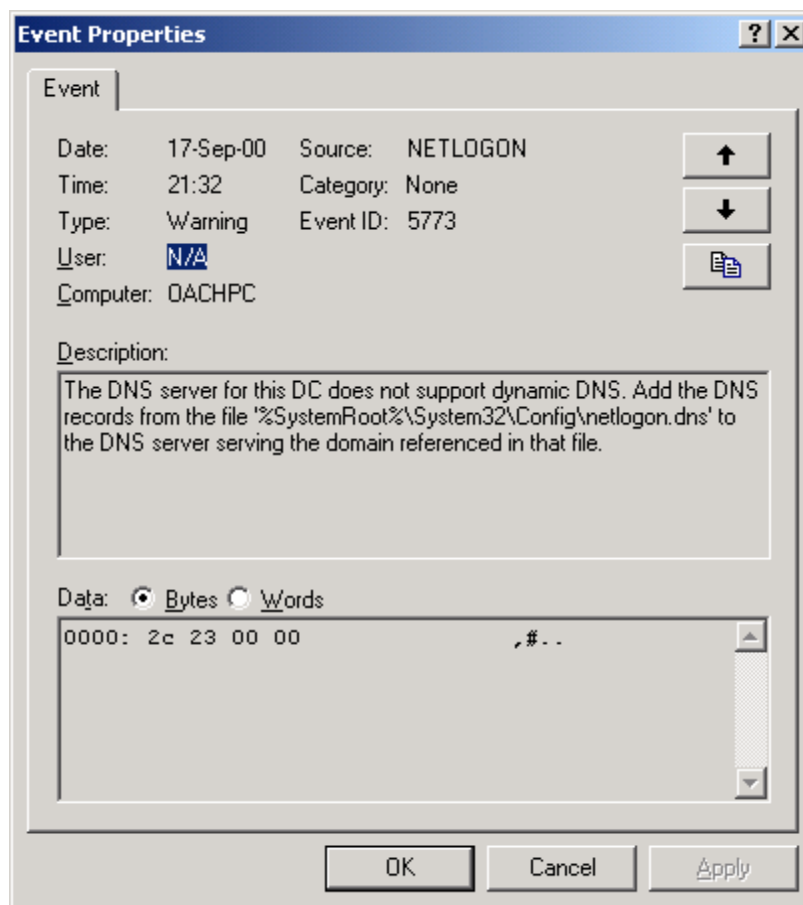
Hình 6.5: Ghi log trong Windows 2000

- Sử dụng tiện ích Event View cho phép xem những thông tin logfile như sau:



Hình 6.6: Công cụ Event View của Windows 2000

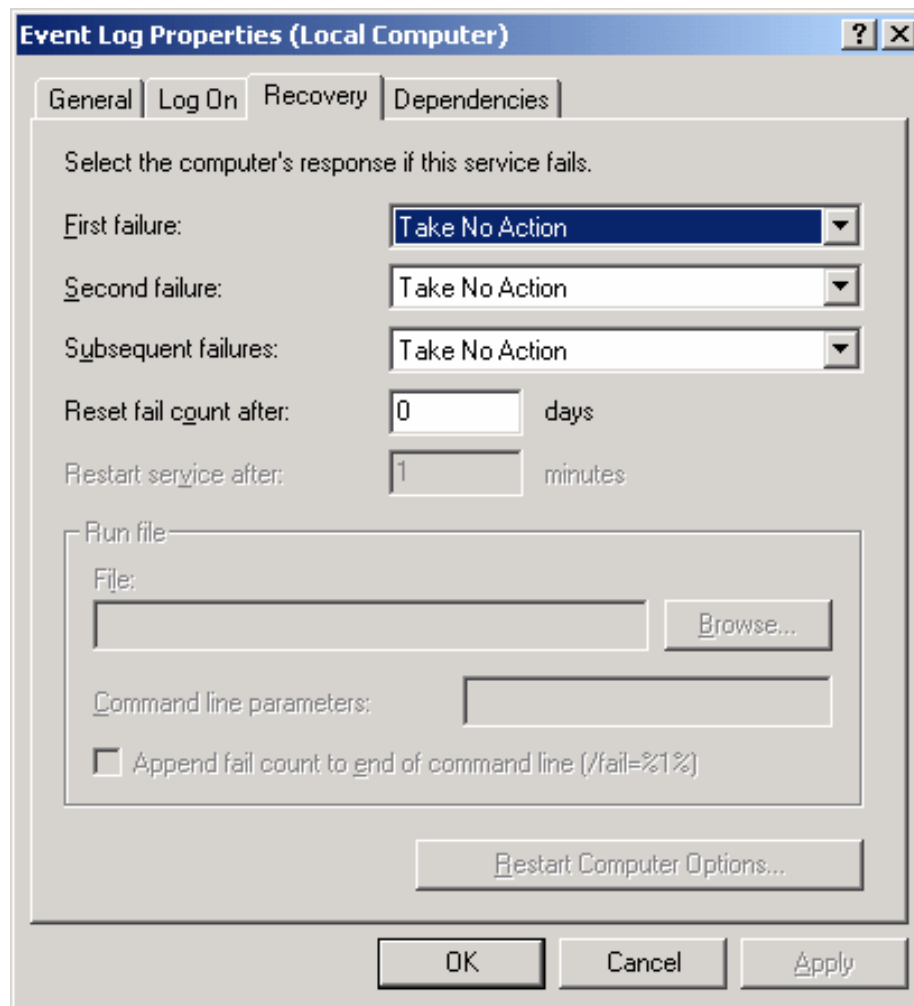
Xem chi tiết nội dung một message:



Hình 6.7: Chi tiết 1 thông báo lỗi trong Windows 2000

Thông báo này cho biết nguyên nhân, thời điểm xảy ra lỗi cũng như nhiều thông tin quan trọng khác.

Có thể cấu hình Event Service để thực hiện một action khi có một thông báo lỗi xảy ra như sau:



Hình 6.8: Cấu hình dịch vụ ghi log trong Windows 2000

Ngoài ra, cũng giống như trên UNIX, trong Windows NT cũng có các công cụ theo dõi logfile của một số dịch vụ thông dụng như FTP, Web. Tùy thuộc vào loại server sử dụng có các phương pháp cấu hình khác nhau.

### 1.2.2. Thiết lập chính sách bảo mật hệ thống

Trong các bước xây dựng một chính sách bảo mật đối với một hệ thống, nhiệm vụ đầu tiên của người quản trị là xác định được đúng mục tiêu cần bảo mật. Việc xác định những mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp các nhà quản trị thiết lập các biện pháp đảm bảo hữu hiệu trong quá trình trang bị, cấu hình và kiểm soát hoạt động của hệ thống. Những mục tiêu bảo mật bao gồm:

#### 1.2.2.1. Xác định đối tượng cần bảo vệ

Đây là mục tiêu đầu tiên và quan trọng nhất trong khi thiết lập một chính sách bảo mật. Người quản trị hệ thống cần xác định rõ những đối tượng nào là

quan trọng nhất trong hệ thống cần bảo vệ và xác định rõ mức độ ưu tiên đối với những đối tượng đó. Ví dụ các đối tượng cần bảo vệ trên một hệ thống có thể là: các máy chủ dịch vụ, các router, các điểm truy nhập hệ thống, các chương trình ứng dụng, hệ quản trị CSDL, các dịch vụ cung cấp ...

Trong bước này cần xác định rõ phạm vi và ranh giới giữa các thành phần trong hệ thống để khi xảy ra sự cố trên hệ thống có thể cô lập các thành phần này với nhau, dễ dàng dò tìm nguyên nhân và cách khắc phục. Có thể chia các thành phần trên một hệ thống theo các cách sau:

- Phân tách các dịch vụ tùy theo mức độ truy cập và độ tin cậy.
- Phân tách hệ thống theo các thành phần vật lý như các máy chủ (server), router, các máy trạm (workstation)...
- Phân tách theo phạm vi cung cấp của các dịch vụ như: các dịch vụ bên trong mạng (NIS, NFS ...) và các dịch vụ bên ngoài như Web, FTP, Mail ...

#### 1.2.2.2. Xác định nguy cơ đối với hệ thống

Các nguy cơ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộc tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn. Thông thường, một số nguy cơ này nằm ở các thành phần sau trên hệ thống:

##### *a) Các điểm truy nhập:*

Các điểm truy nhập của hệ thống bất kỳ (Access Points) thường đóng vai trò quan trọng đối với mỗi hệ thống vì đây là điểm đầu tiên mà người sử dụng cũng như những kẻ tấn công mạng quan tâm tới. Thông thường các điểm truy nhập thường phục vụ hầu hết người dùng trên mạng, không phụ thuộc vào quyền hạn cũng như dịch vụ mà người sử dụng dùng. Do đó, các điểm truy nhập thường là thành phần có tính bảo mật lỏng lẻo. Mặt khác, đối với nhiều hệ thống còn cho phép người sử dụng dùng các dịch vụ như Telnet, rlogin để truy nhập vào hệ thống, đây là những dịch vụ có nhiều lỗ hổng bảo mật.

##### *b) Không kiểm soát được cấu hình hệ thống*

Không kiểm soát hoặc mất cấu hình hệ thống chiếm một tỷ lệ lớn trong số các lỗ hổng bảo mật. Ngày nay, có một số lượng lớn các phần mềm sử dụng, yêu cầu cấu hình phức tạp và đa dạng hơn, điều này cũng dẫn đến những khó khăn để người quản trị nắm bắt được cấu hình hệ thống. Để khắc phục hiện tượng này, nhiều hãng sản xuất phần mềm đã đưa ra những cấu hình khởi tạo mặc định, trong khi đó những cấu hình này không được xem xét kỹ lưỡng trong một môi trường bảo mật. Do đó, nhiệm vụ của người quản trị là phải nắm được hoạt động của các phần mềm sử dụng, ý nghĩa của các file cấu hình quan trọng, áp dụng các biện pháp bảo vệ cấu hình như sử dụng phương thức mã hóa hashing code (MD5).

##### *c) Những bug phần mềm sử dụng*

Những bug phần mềm tạo nên những lỗ hổng của dịch vụ là cơ hội cho các hình thức tấn công khác nhau xâm nhập vào mạng. Do đó, người quản trị

phải thường xuyên cập nhật tin tức trên các nhóm tin về bảo mật và từ nhà cung cấp phần mềm để phát hiện những lỗi của phần mềm sử dụng. Khi phát hiện có bug cần thay thế hoặc ngừng sử dụng phần mềm đó chờ nâng cấp lên phiên bản tiếp theo.

*d) Những nguy cơ trong nội bộ mạng*

Một hệ thống không những chịu tấn công từ ngoài mạng, mà có thể bị tấn công ngay từ bên trong. Có thể là vô tình hoặc cố ý, các hình thức phá hoại bên trong mạng vẫn thường xảy ra trên một số hệ thống lớn. Chủ yếu với hình thức tấn công ở bên trong mạng là kẻ tấn công có thể tiếp cận về mặt vật lý đối với các thiết bị trên hệ thống, đạt được quyền truy nhập bất hợp pháp tại ngay hệ thống đó. Ví dụ nhiều trạm làm việc có thể chiếm được quyền sử dụng nếu kẻ tấn công ngồi ngay tại các trạm làm việc đó.

1.2.2.3. Xác định phương án thực thi chính sách bảo mật

Sau khi thiết lập được một chính sách bảo mật, một hoạt động tiếp theo là lựa chọn các phương án thực thi một chính sách bảo mật. Một chính sách bảo mật là hoàn hảo khi nó có tính thực thi cao. Để đánh giá tính thực thi này, có một số tiêu chí để lựa chọn đó là:

- Tính đúng đắn
- Tính thân thiện
- Tính hiệu quả

1.2.2.4. Thiết lập các qui tắc/thủ tục

*a) Các thủ tục đối với hoạt động truy nhập bất hợp pháp*

Sử dụng một vài công cụ có thể phát hiện ra các hành động truy nhập bất hợp pháp vào một hệ thống. Các công cụ này có thể đi kèm theo hệ điều hành, hoặc từ các hãng sản xuất phần mềm thứ ba. Đây là biện pháp phổ biến nhất để theo dõi các hoạt động hệ thống.

- Các công cụ logging: hầu hết các hệ điều hành đều hỗ trợ một số lượng lớn các công cụ ghi log với nhiều thông tin bổ ích. Để phát hiện những hoạt động truy nhập bất hợp pháp, một số qui tắc khi phân tích logfile như sau:

+ So sánh các hoạt động trong logfile với các log trong quá khứ. Đối với các hoạt động thông thường, các thông tin trong logfile thường có chu kỳ giống nhau như thời điểm người sử dụng login hoặc log out, thời gian sử dụng các dịch vụ trên hệ thống...

+ Nhiều hệ thống sử dụng các thông tin trong logfile để tạo hóa đơn cho khách hàng. Có thể dựa vào các thông tin trong hóa đơn thanh toán để xem xét các truy nhập bất hợp pháp nếu thấy trong hóa đơn đó có những điểm bất thường như thời điểm truy nhập, số điện thoại lạ ...

+ Dựa vào các tiện ích như syslog để xem xét, đặc biệt là các thông báo lỗi login không hợp lệ (bad login) trong nhiều lần.

+ Dựa vào các tiện ích kèm theo hệ điều hành để theo dõi các tiến trình đang hoạt động trên hệ thống; để phát hiện những tiến trình lạ, hoặc những chương trình khởi tạo không hợp lệ ...

- Sử dụng các công cụ giám sát khác: Ví dụ sử dụng các tiện ích về mạng để theo dõi các lưu lượng, tài nguyên trên mạng để phát hiện những điểm nghi ngờ.

*b) Các thủ tục bảo vệ hệ thống*

- Thủ tục quản lý tài khoản người sử dụng
- Thủ tục quản lý mật khẩu
- Thủ tục quản lý cấu hình hệ thống
- Thủ tục sao lưu và khôi phục dữ liệu
- Thủ tục báo cáo sự cố

1.2.2.5. Kiểm tra, đánh giá và hoàn thiện chính sách bảo mật

Một hệ thống luôn có những biến động về cấu hình, các dịch vụ sử dụng, và ngay cả nền tảng hệ điều hành sử dụng, các thiết bị phần cứng .... do vậy người thiết lập các chính sách bảo mật mà cụ thể là các nhà quản trị hệ thống luôn luôn phải rà soát, kiểm tra lại chính sách bảo mật đảm bảo luôn phù hợp với thực tế. Mặt khác kiểm tra và đánh giá chính sách bảo mật còn giúp cho các nhà quản lý có kế hoạch xây dựng mạng lưới hiệu quả hơn.

*a) Kiểm tra, đánh giá*

Công việc này được thực hiện thường xuyên và liên tục. Kết quả của một chính sách bảo mật thể hiện rõ nét nhất trong chất lượng dịch vụ mà hệ thống đó cung cấp. Dựa vào đó có thể kiểm tra, đánh giá được chính sách bảo mật đó là hợp lý hay chưa. Ví dụ, một nhà cung cấp dịch vụ Internet có thể kiểm tra được chính sách bảo mật của mình dựa vào khả năng phản ứng của hệ thống khi bị tấn công từ bên ngoài như các hành động spam mail, DoS, truy nhập hệ thống trái phép ...

Hoạt động đánh giá một chính sách bảo mật có thể dựa vào một số tiêu chí sau:

- Tính thực thi.
- Khả năng phát hiện và ngăn ngừa các hoạt động phá hoại.
- Các công cụ hữu hiệu để hạn chế các hoạt động phá hoại hệ thống.

*b) Hoàn thiện chính sách bảo mật:*

Từ các hoạt động kiểm tra, đánh giá nêu trên, các nhà quản trị hệ thống có thể rút ra được những kinh nghiệm để có thể cải thiện chính sách bảo mật hữu hiệu hơn. Cải thiện chính sách có thể là những hành động nhằm đơn giản công việc người sử dụng, giảm nhẹ độ phức tạp trên hệ thống ...

Những hoạt động cải thiện chính sách bảo mật có thể diễn ra trong suốt thời gian tồn tại của hệ thống đó. Nó gắn liền với các công việc quản trị và duy



trì hệ thống. Đây cũng chính là một yêu cầu trong khi xây dựng một chính sách bảo mật, cần phải luôn luôn mềm dẻo, có những thay đổi phù hợp tùy theo điều kiện thực tế.

## 2. Tổng quan về hệ thống firewall

## 2.1. Giới thiệu về Firewall

### 2.1.1. Khái niệm Firewall

Firewall là thiết bị nhằm ngăn chặn sự truy nhập không hợp lệ từ mạng ngoài vào mạng trong. Hệ thống firewall thường bao gồm cả phần cứng và phần mềm. Firewall thường được dùng theo phương thức ngăn chặn hay tạo các luật đối với các địa chỉ khác nhau.

### 2.1.2. Các chức năng cơ bản của Firewall

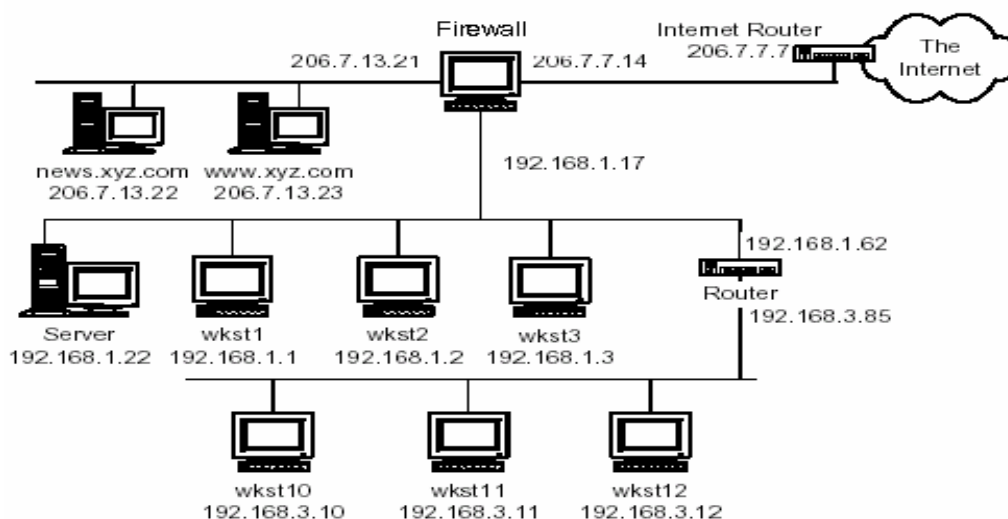
Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ (Trusted Network) và Internet thông qua các chính sách truy nhập đã được thiết lập.

- Cho phép hoặc cấm các dịch vụ truy nhập từ trong ra ngoài và từ ngoài vào trong.
- Kiểm soát địa chỉ truy nhập, và dịch vụ sử dụng.
- Kiểm soát khả năng truy cập người sử dụng giữa 2 mạng.
- Kiểm soát nội dung thông tin truyền tải giữa 2 mạng.
- Ngăn ngừa khả năng tấn công từ các mạng ngoài.

Xây dựng firewalls là một biện pháp khá hữu hiệu, nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ do đó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng. Thông thường, một hệ thống firewall là một cổng (gateway) giữa mạng nội bộ giao tiếp với mạng bên ngoài và ngược lại

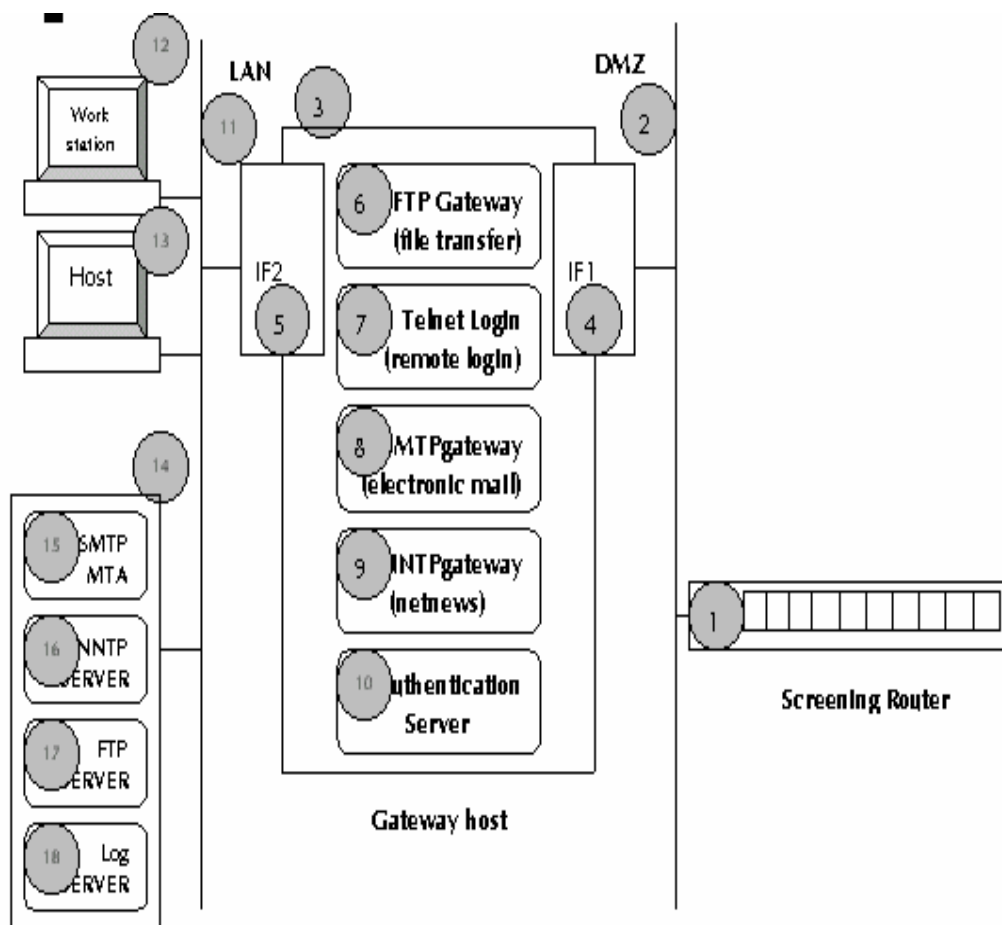
### 2.1.3. Mô hình mạng sử dụng Firewall

Kiến trúc của hệ thống có firewall như sau:



Hình 6.9: Kiến trúc hệ thống có firewall

Nhìn chung, mỗi hệ thống firewall đều có các thành phần như sau:



Hình 6.10: Các thành phần của hệ thống firewall

Firewall có thể bao gồm phần cứng hoặc phần mềm nhưng thường là cả hai. Về mặt phần cứng thì firewall có chức năng gần giống một router, nó cho phép hiển thị các địa chỉ IP đang kết nối qua nó. Điều này cho phép bạn xác định được các địa chỉ nào được phép và các địa chỉ IP nào không được phép kết nối.

Tất cả các firewall đều có chung một thuộc tính là cho phép phân biệt đối xử hay khả năng từ chối truy nhập dựa trên các địa chỉ nguồn.

Theo hình trên các thành phần của một hệ thống firewall bao gồm:

- Screening router: Là chặng kiểm soát đầu tiên cho LAN.
- DMZ: Khu "phi quân sự", là vùng có nguy cơ bị tấn công từ Internet.
- Gateway: là cổng ra vào giữa mạng LAN và DMZ, kiểm soát mọi liên lạc, thực thi các cơ chế bảo mật.
- IF1: Interface 1: Là card giao tiếp với vùng DMZ.
- IF2: Interface 2: Là card giao tiếp với vùng mạng LAN.

- FTP gateway: Kiểm soát truy cập FTP giữa LAN và vùng DMZ. Các truy cập ftp từ mạng LAN ra Internet là tự do. Các truy cập FTP vào LAN đòi hỏi xác thực thông qua Authentication Server.

- Telnet Gateway: Kiểm soát truy cập telnet giữa mạng LAN và Internet. Giống như FTP, người dùng có thể telnet ra ngoài tự do, các telnet từ ngoài vào yêu cầu phải xác thực qua Authentication Server

- Authentication Server: được sử dụng bởi các cổng giao tiếp, nhận diện các yêu cầu kết nối, dùng các kỹ thuật xác thực mạnh như one-time password/token (mật khẩu sử dụng một lần). Các máy chủ dịch vụ trong mạng LAN được bảo vệ an toàn, không có kết nối trực tiếp với Internet, tất cả các thông tin trao đổi đều được kiểm soát qua gateway.

#### **2.1.4. Phân loại Firewall**

Có khá nhiều loại firewall, mỗi loại có những ưu và nhược điểm riêng. Tuy nhiên để thuận tiện cho việc nghiên cứu người ta chia hệ thống làm 2 loại chính:

- Packet filtering: là hệ thống firewall cho phép chuyển thông tin giữa hệ thống trong và ngoài mạng có kiểm soát.

- Application-proxy firewall: là hệ thống firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.

##### **2.1.4.1. Packet Filtering**

Kiểu firewall chung nhất là kiểu dựa trên mức mạng của mô hình OSI. Firewall mức mạng thường hoạt động theo nguyên tắc router hay còn được gọi là router, có nghĩa là tạo ra các luật cho phép quyền truy nhập mạng dựa trên mức mạng. Mô hình này hoạt động theo nguyên tắc lọc gói tin (packet filtering).

Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát. Sau khi địa chỉ IP nguồn được xác định thì nó được kiểm tra với các luật đã được đặt ra trên router. Ví dụ người quản trị firewall quyết định rằng không cho phép bất kỳ một gói tin nào xuất phát từ mạng microsoft.com được kết nối với mạng trong thì các gói tin xuất phát từ mạng này sẽ không bao giờ đến được mạng trong.

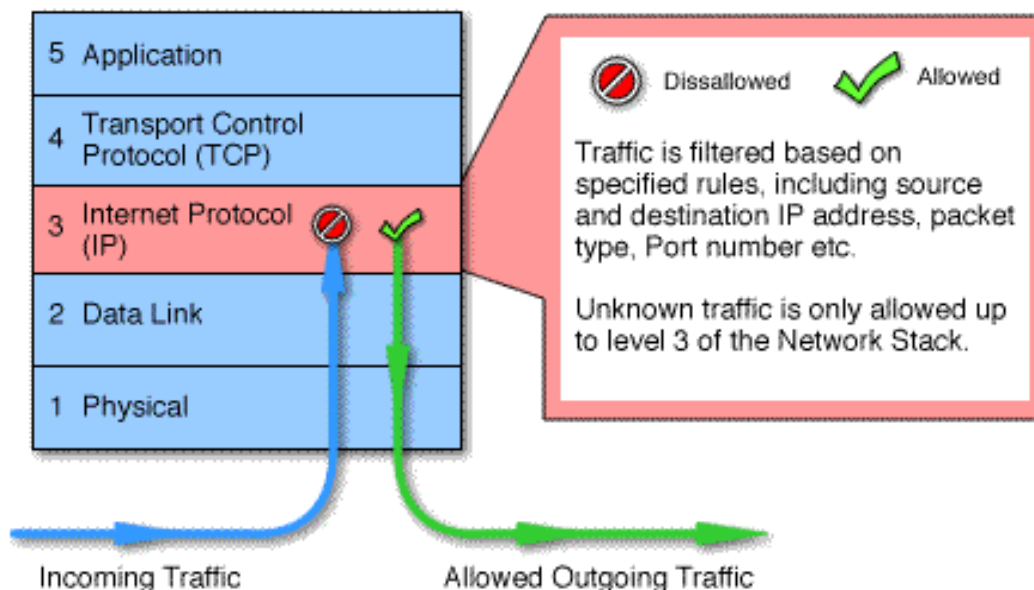
Các firewall hoạt động ở lớp mạng (tương tự như một router) thường cho phép tốc độ xử lý nhanh bởi nó chỉ kiểm tra địa chỉ IP nguồn mà không có một lệnh thực sự nào trên router, nó không cần một khoảng thời gian nào để xác định xem là địa chỉ sai hay bị cấm. Nhưng điều này bị trả giá bởi tính tin cậy của nó. Kiểu firewall này sử dụng địa chỉ IP nguồn làm chỉ thị, điều này tạo ra một lỗ hổng là nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì như vậy nó sẽ có được một số mức truy nhập vào mạng trong của bạn.

Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục yếu điểm này. Ví dụ như đối với các công nghệ packet filtering phức tạp thì không chỉ có trường địa chỉ IP được kiểm tra bởi router mà còn có các trường khác nữa được kiểm tra với các luật được tạo ra trên

firewall, các thông tin khác này có thể là thời gian truy nhập, giao thức sử dụng, port ...

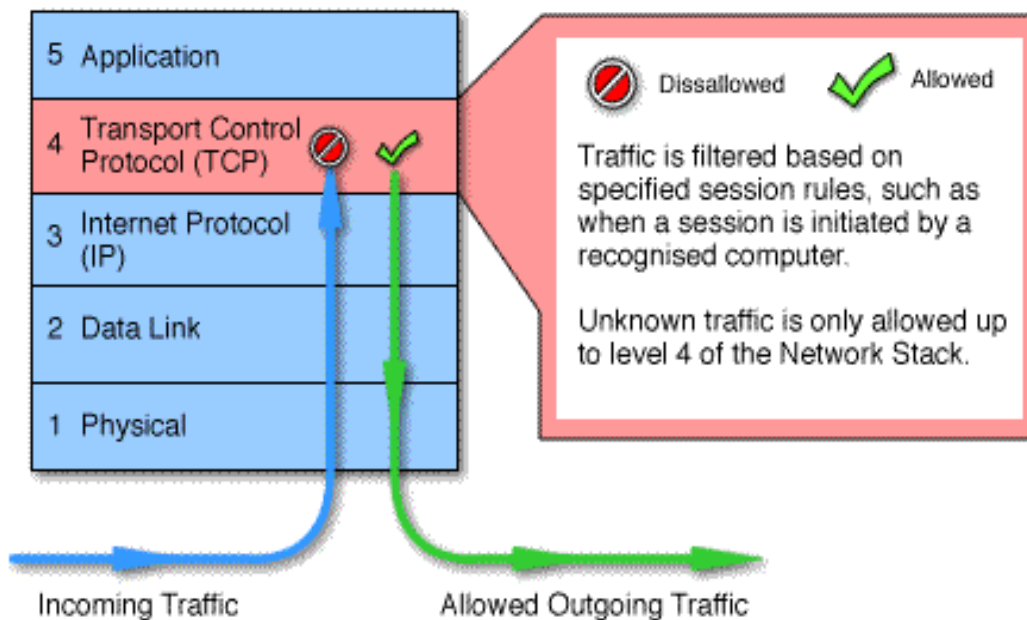
Firewall kiểu Packet Filtering có thể được phân thành 2 loại:

a) *Packet filtering firewall*: hoạt động tại lớp mạng của mô hình OSI hay lớp IP trong mô hình giao thức TCP/IP.



Hình 6.11: Packet filtering firewall

b) *Circuit level gateway*: hoạt động tại lớp phiên (session) của mô hình OSI hay lớp TCP trong mô hình giao thức TCP/IP.



Hình 6.12: Circuit level gateway

#### 2.1.4.2. Application-proxy firewall

Kiểu firewall này hoạt động dựa trên phần mềm. Khi một kết nối từ một người dùng nào đó đến mạng sử dụng firewall kiểu này thì kết nối đó sẽ bị chặn lại, sau đó firewall sẽ kiểm tra các trường có liên quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các luật đã đặt ra trên firewall thì firewall sẽ tạo một cái cầu kết nối giữa hai node với nhau.

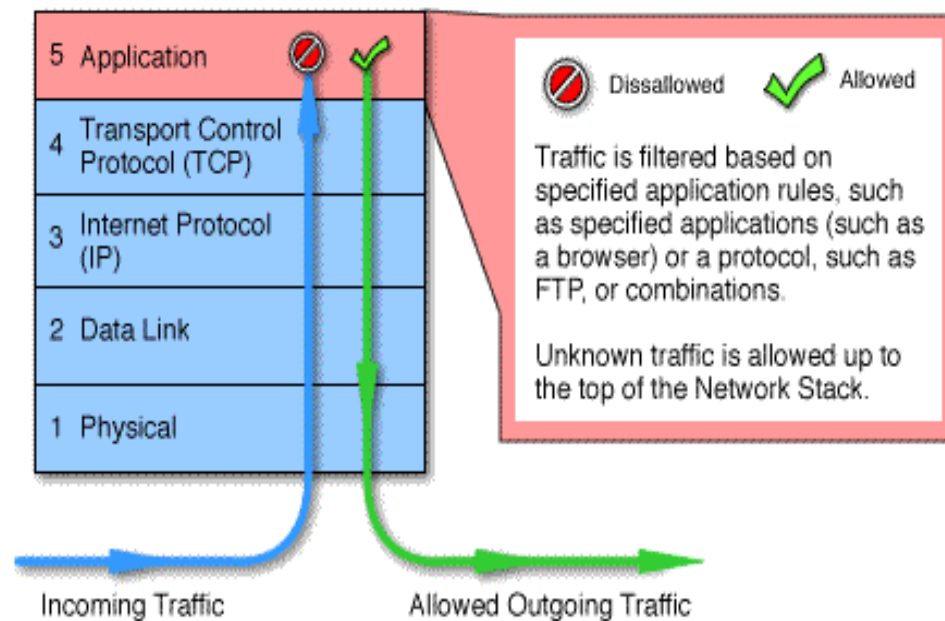
Ưu điểm của kiểu firewall loại này là không có chức năng chuyển tiếp các gói tin IP, hơn nữa ta có thể điều khiển một cách chi tiết hơn các kết nối thông qua firewall. Đồng thời nó còn đưa ra nhiều công cụ cho phép ghi lại các quá trình kết nối. Tất nhiên điều này phải trả giá bởi tốc độ xử lý, bởi vì tất cả các kết nối cũng như các gói tin chuyển qua firewall đều được kiểm tra kỹ lưỡng với các luật trên firewall và rồi nếu được chấp nhận sẽ được chuyển tiếp tới node đích.

Sự chuyển tiếp các gói tin IP xảy ra khi một máy chủ nhận được một yêu cầu từ mạng ngoài rồi chuyển chúng vào mạng trong. Điều này tạo ra một lỗ hổng cho các kẻ phá hoại (hacker) xâm nhập từ mạng ngoài vào mạng trong.

Nhược điểm của kiểu firewall hoạt động dựa trên ứng dụng là phải tạo cho mỗi dịch vụ trên mạng một trình ứng dụng ủy quyền (proxy) trên firewall ví dụ như phải tạo một trình ftp proxy dịch vụ ftp, tạo trình http proxy cho dịch vụ http... Như vậy ta có thể thấy rằng trong kiểu giao thức client-server như dịch vụ telnet làm ví dụ thì cần phải thực hiện hai bước để cho hai máy ngoài mạng và trong mạng có thể kết nối được với nhau. Khi sử dụng firewall kiểu này các máy client (máy yêu cầu dịch vụ) có thể bị thay đổi. Ví dụ như đối với dịch vụ telnet thì các máy client có thể thực hiện theo hai phương thức: một là bạn telnet vào firewall trước sau đó mới thực hiện việc telnet vào máy ở mạng khác; cách thứ hai là bạn có thể telnet thẳng tới đích tùy theo các luật trên firewall có cho phép hay không mà việc telnet của bạn sẽ được thực hiện. Lúc này firewall là hoàn toàn trong suốt, nó đóng vai trò như một cầu nối tới đích của bạn.

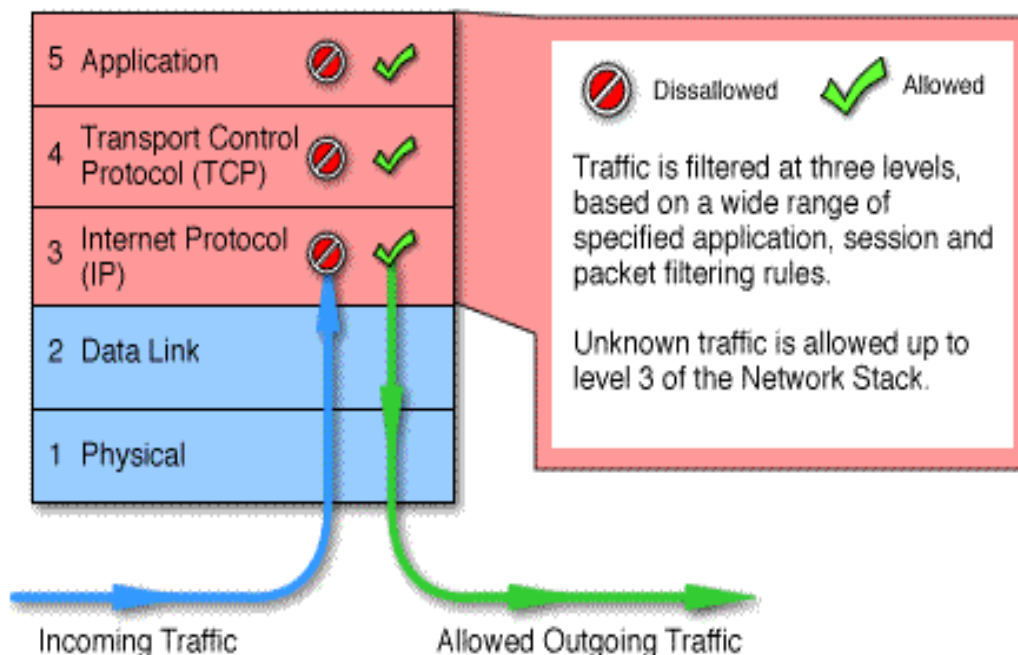
Firewall kiểu Application-proxy có thể được phân thành 2 loại:

a) *Application level gateway*: tính năng tương tự như loại circuit-level gateway nhưng lại hoạt động ở lớp ứng dụng trong mô hình giao thức TCP/IP.



Hình 6.13: Application level gateway

b) *Stateful multilayer inspection firewall*: đây là loại kết hợp được các tính năng của các loại firewall trên: lọc các gói tại lớp mạng và kiểm tra nội dung các gói tại lớp ứng dụng. Firewall loại này cho phép các kết nối trực tiếp giữa các client và các host nên giảm được các lỗi xảy ra do tính chất "không trong suốt" của firewall kiểu Application gateway. Stateful multilayer inspection firewall cung cấp các tính năng bảo mật cao và lại trong suốt đối với các end users.



Hình 6.14: Stateful multilayer inspection firewall

## 2.2. Một số phần mềm Firewall thông dụng

### 2.2.1. Packet filtering

Kiểu lọc gói tin này có thể được thực hiện mà không cần tạo một firewall hoàn chỉnh, có rất nhiều các công cụ trợ giúp cho việc lọc gói tin trên Internet (kể cả phải mua hay được miễn phí). Sau đây ta có thể liệt kê một số tiện ích như vậy

#### 2.2.1.1. TCP\_Wrappers

TCP\_Wrappers là một chương trình được viết bởi Wietse Venema. Chương trình hoạt động bằng cách thay thế các chương trình thường trú của hệ thống và ghi lại tất cả các yêu cầu kết nối, thời gian yêu cầu, và địa chỉ nguồn. Chương trình này cũng có khả năng ngăn chặn các địa chỉ IP hay các mạng không được phép kết nối.

#### 2.2.1.2. NetGate

NetGate được đưa ra bởi Smallwork là một hệ thống dựa trên các luật về lọc gói tin. Nó được viết ra để sử dụng trên các hệ thống Sun Sparc OS 4.1.x. Tương tự như các kiểu packet filtering khác, NetGate kiểm tra tất cả các gói tin nó nhận được và so sánh với các luật đã được tạo ra.

#### 2.2.1.3. Internet Packet Filter

Phần mềm này hoàn toàn miễn phí, được viết bởi Darren Reed. Đây là một chương trình khá tiện lợi, nó có khả năng ngăn chặn được việc tấn công bằng địa chỉ IP giả. Một số ưu điểm của chương trình là nó không chỉ có khả

năng huỷ bỏ các gói tin TCP không đúng hoặc chưa hoàn thiện mà còn không gửi lại bản tin ICMP lỗi. Chương trình này cho phép bạn có thể kiểm tra thử các luật bạn ra trước khi sử dụng chúng.

## 2.2.2. Application-proxy firewall

### 2.2.2.1. TIS FWTK

TIS FWTK (Trusted information Systems Firewall Tool Kit) là một phần mềm đầu tiên đầy đủ tính năng của firewall và đặc trưng cho kiểu firewall hoạt động theo phương thức ứng dụng. Những phiên bản đầu tiên của phần mềm này là miễn phí và bao gồm nhiều thành phần riêng rẽ. Mỗi thành phần phục vụ cho một kiểu dịch vụ trên mạng. Các thành phần chủ yếu bao gồm: Telnet, FTP, rlogin, sendmail và http.

Phần mềm này là một hệ thống toàn diện, tuy nhiên nó không có khả năng bảo vệ mạng ngay sau khi cài đặt vì việc cài đặt và cấu hình không phải là dễ dàng. Khi cấu hình phần mềm này bạn phải thực sự hiểu mình đang làm gì bởi có thể với các luật bạn tạo ra thì mạng của bạn không thể được kết nối với bất kỳ mạng nào khác thậm chí ngay cả những mạng quen thuộc. Điểm đặc trưng nhất của phần mềm này là nó có sẵn nhiều tiện ích giúp bạn điều khiển được truy nhập đối với toàn mạng, một phần mạng hay thậm chí chỉ riêng một địa chỉ.

### 2.2.2.2. Raptor

Raptor là phần mềm firewall cung cấp đầy đủ các tính năng của một firewall chuyên nghiệp với hai giao diện quản lý, một trên hệ điều hành Unix (RCU) và một trên hệ điều hành Windows (RMC). Raptor có thể được cấu hình để bảo vệ mạng theo bốn phương thức: Standard Proxies, Generic Service Passer, Virtual Private Network tunnels và Raptor Mobile. Tuy việc cấu hình cho Raptor khá phức tạp với việc tạo các route, định nghĩa các entity, user và group, thiết lập các authorization rule ... nhưng bù lại ta có thể sử dụng được rất nhiều tính năng ưu việt do Raptor cung cấp để tùy biến các mức bảo vệ đối với mạng của mình.

## 2.3. Thực hành cài đặt và cấu hình firewall Check Point v4.0 for Windows

### 2.3.1. Yêu cầu phần cứng:

- Cấu hình tối thiểu đối với máy cài GUI Client

|                      |                                        |
|----------------------|----------------------------------------|
| Hệ điều hành         | Windows 95, Windows NT, X/Motif        |
| Dung lượng đĩa trống | 20 Mbytes                              |
| Bộ nhớ               | 16 Mbytes                              |
| Card mạng            | Các loại card được hệ điều hành hỗ trợ |
| Thiết bị khác        | CD-ROM                                 |



- Cấu hình tối thiểu đối với máy cài Management Server

|                      |                                        |
|----------------------|----------------------------------------|
| Hệ điều hành         | Windows NT (Intel x86 và Pentium)      |
| Dung lượng đĩa trống | 20 Mbytes                              |
| Bộ nhớ               | tối thiểu 16MB, nên dùng 24MB          |
| Card mạng            | Các loại card được hệ điều hành hỗ trợ |
| Thiết bị khác        | CD-ROM                                 |

- Cấu hình tối thiểu đối với máy cài Modul Firewall

|                      |                                                                             |
|----------------------|-----------------------------------------------------------------------------|
| Hệ điều hành         | Windows NT (Intel x86 và Pentium)                                           |
| Dung lượng đĩa trống | 20 Mbytes                                                                   |
| Bộ nhớ               | 16 Mbytes                                                                   |
| Card mạng            | Tối thiểu phải có 3 card mạng thuộc các loại card được hệ điều hành hỗ trợ. |
| Thiết bị khác        | CD-ROM                                                                      |

### 2.3.2. Các bước chuẩn bị trước khi cài đặt

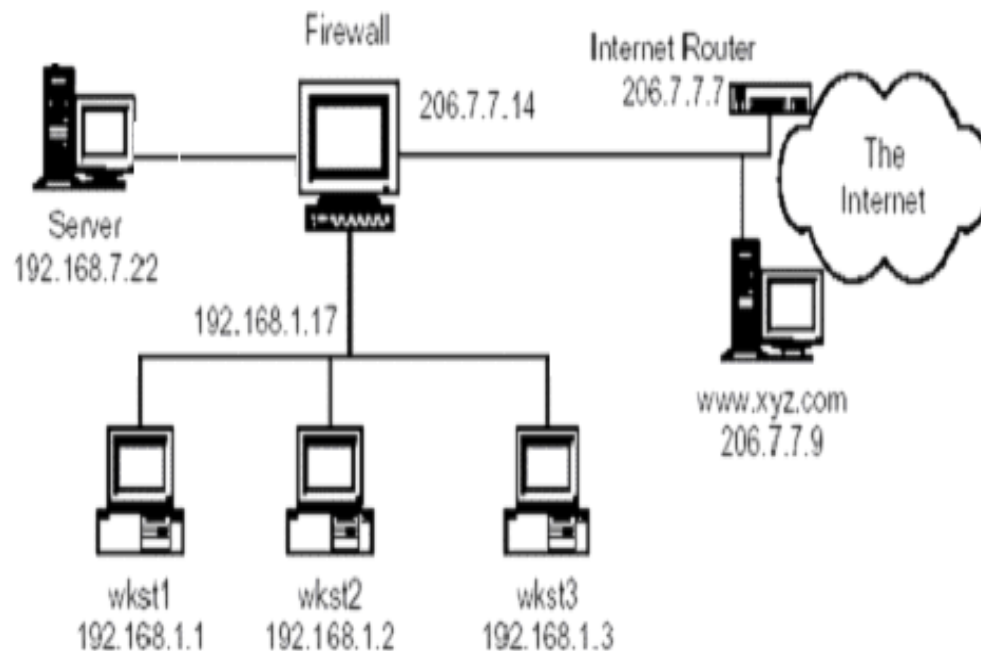
- Thắt chặt an ninh cho máy chủ cài firewall và các module của firewall như GUI Client và Management Server (tắt các dịch vụ không cần thiết, update các patch sửa lỗi của hệ điều hành ...).

- Kiểm tra các kết nối mạng trên các giao diện mạng, đảm bảo từ máy chủ cài Module Firewall có thể ping được các IP trên các giao diện mạng (sử dụng lệnh `ifconfig` , `ping` ...).

- Kiểm tra bảng Routing (sử dụng lệnh `netstat -rn` ...).

- Kiểm tra dịch vụ DNS (sử dụng lệnh `nslookup`).

- Lập sơ đồ mạng thử nghiệm, đối với máy chủ có 3 giao diện mạng có thể lập sơ đồ như sau:



Hình 6.15: Sơ đồ mạng thử nghiệm đối với máy chủ có 3 giao diện mạng

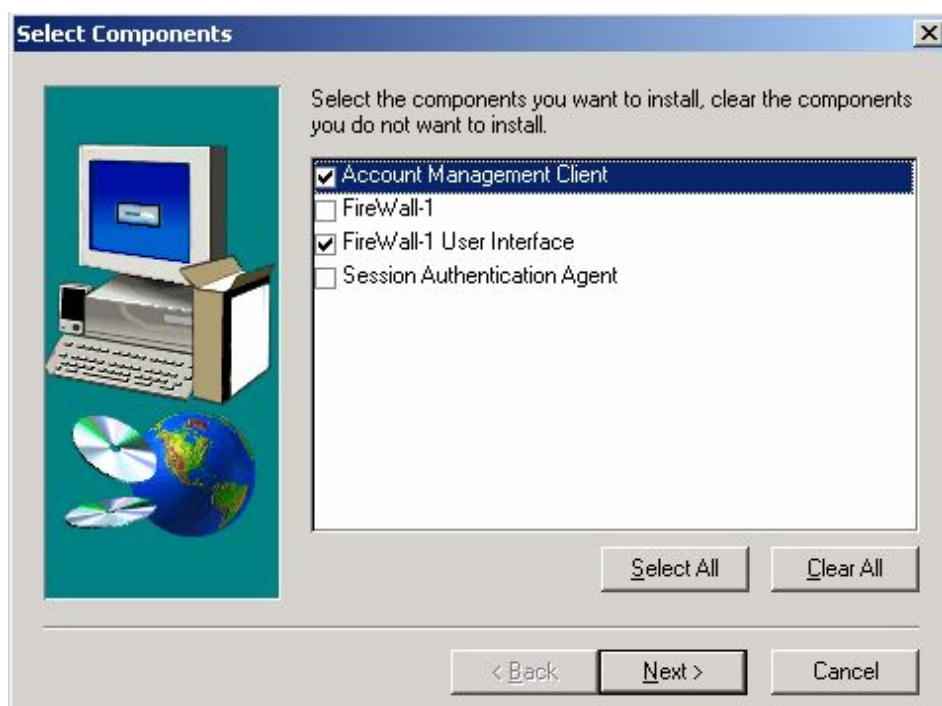
### 2.3.3. Tiến hành cài đặt

Login dưới quyền Administrator và cài đặt hệ thống Firewall Checkpoint trên các máy theo trình tự sau:

- Cài đặt GUI Client và Management Server.
- Cài đặt Module Firewall.

#### 2.3.3.1. Cài đặt GUI Client và Management Server

Đưa đĩa CD Checkpoint và chạy lệnh setup trong thư mục Windows, chọn Account Management Client và FireWall-1 User Interface trong cửa sổ Select Components:



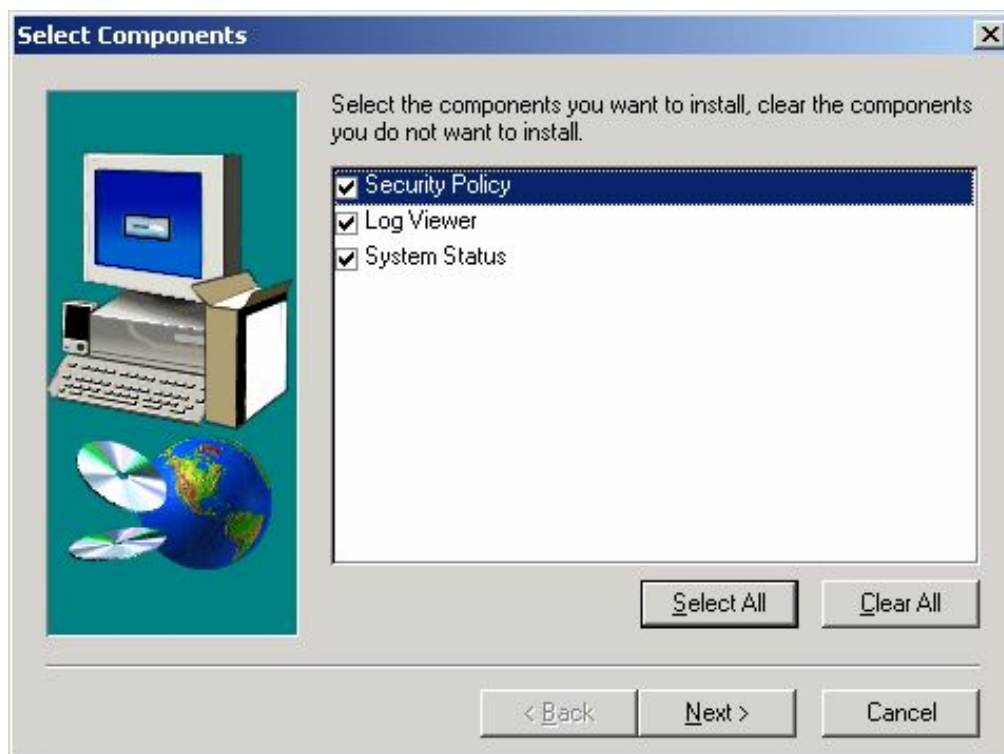
Chọn Next, màn hình sẽ hiện ra như sau:



Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



Chọn Next rồi chọn các thành phần trong cửa sổ Select Components:

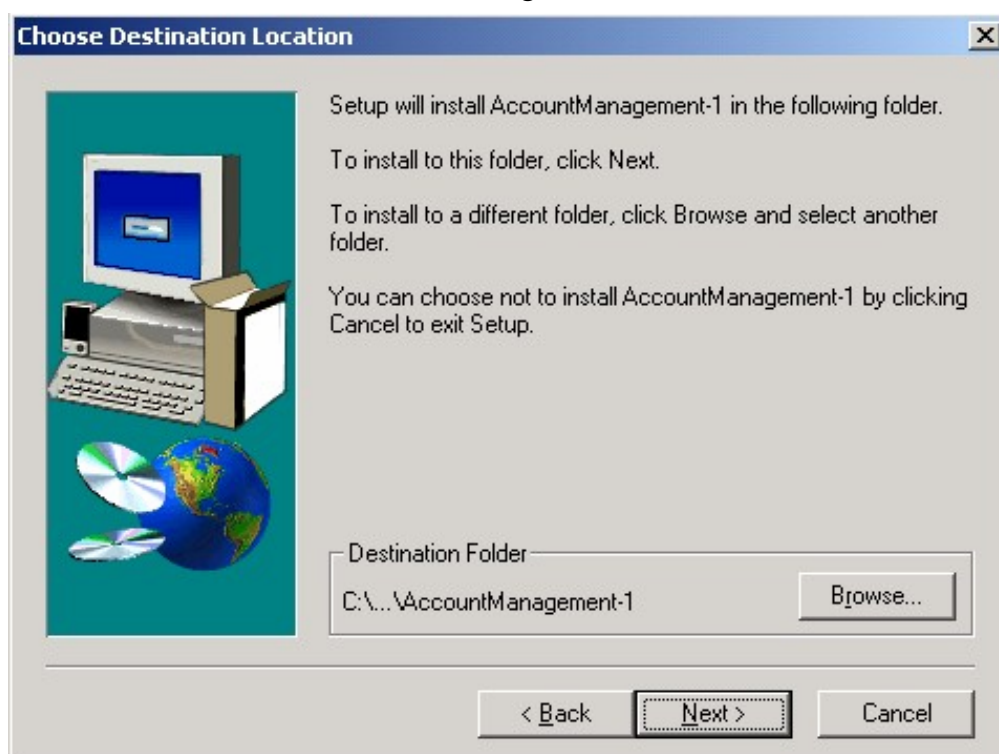


Chọn Next để bắt đầu quá trình cài đặt.

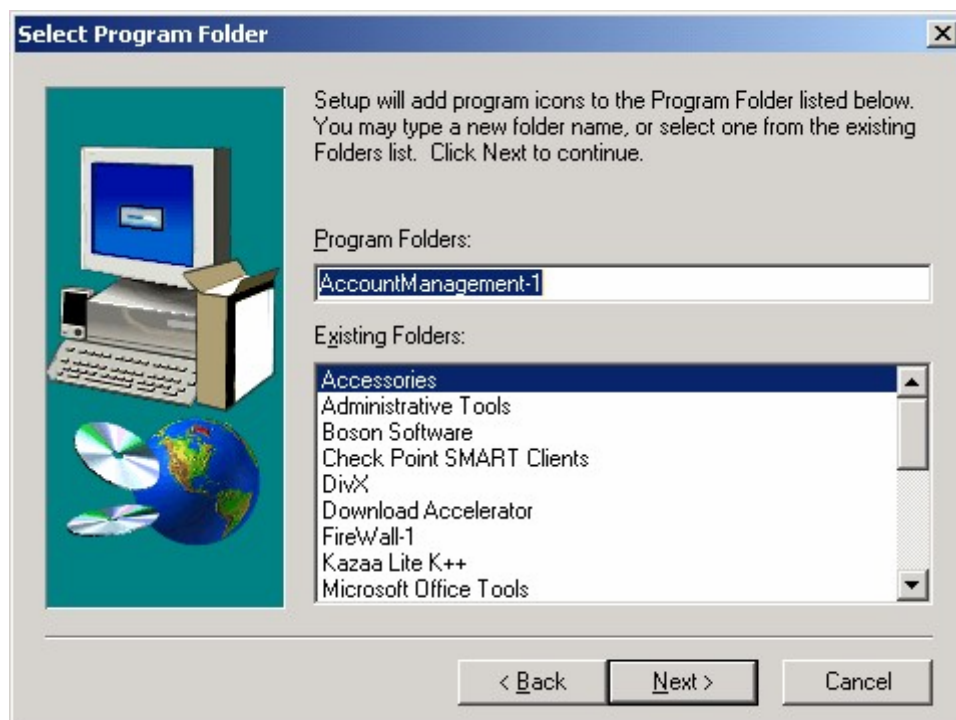
Sau khi cài xong GUI Client, màn hình sẽ tự động hiện ra phần cài đặt Account Management Client With Encryption Installation:



Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



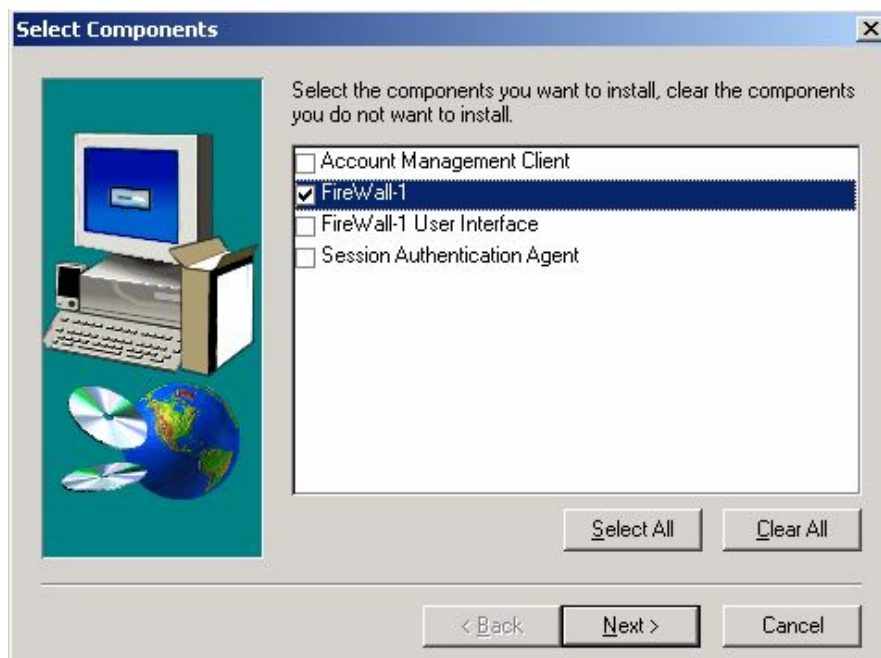
Chọn Next rồi chọn Folder trong cửa sổ Select Program Folder:



Chọn Next để bắt đầu quá trình cài đặt

#### 2.3.3.2. Cài đặt Module Firewall:

Chọn FireWall-1 trong cửa sổ Select Components ban đầu:



Chọn Next, màn hình sẽ hiện ra như sau:





Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



Chọn Next rồi chọn FireWall-1 FireWall Module trong cửa sổ Selecting Product Type:



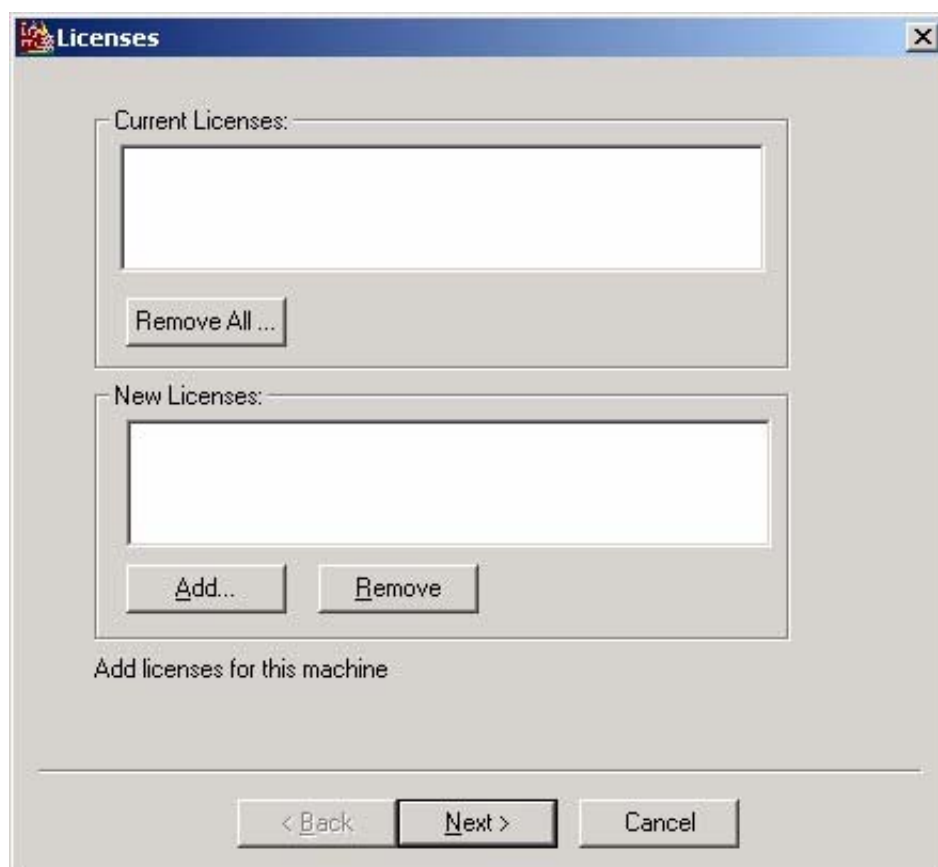
Chọn Next rồi tùy theo phiên bản Checkpoint đăng ký để chọn số license phù hợp:



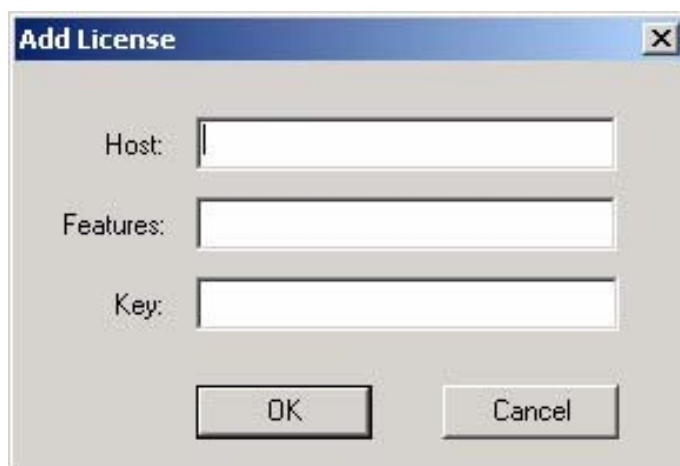
Chọn Next để bắt đầu quá trình cài đặt.

Sau khi cài xong, màn hình cài đặt license sẽ hiện lên như sau:

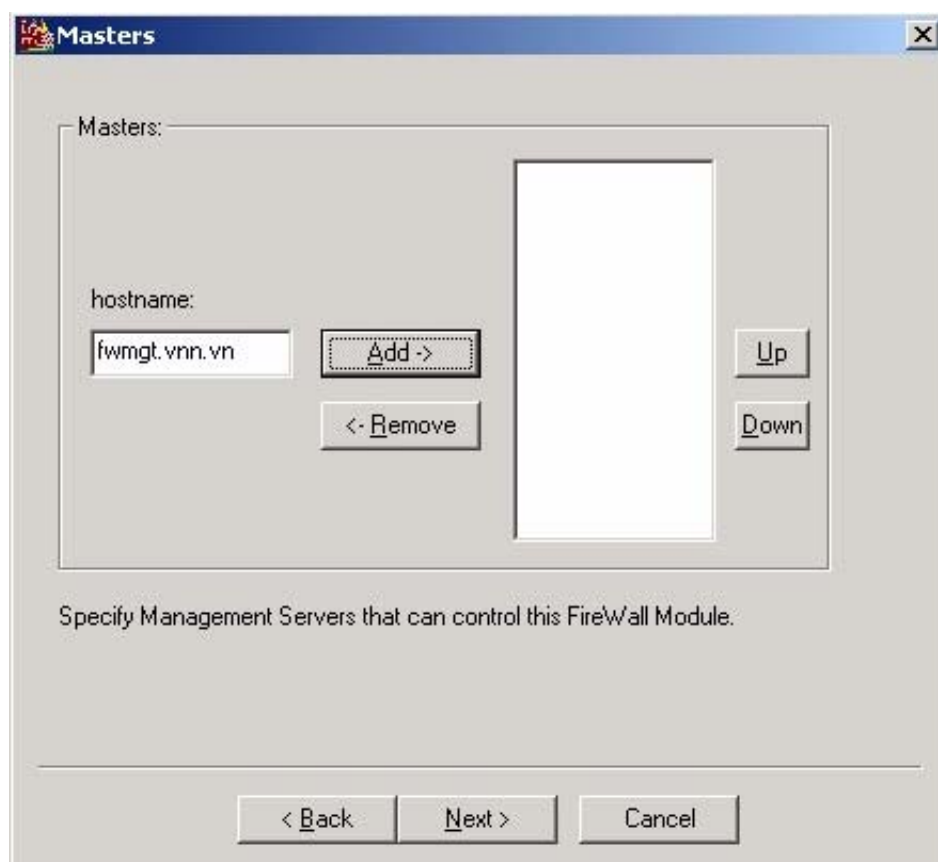




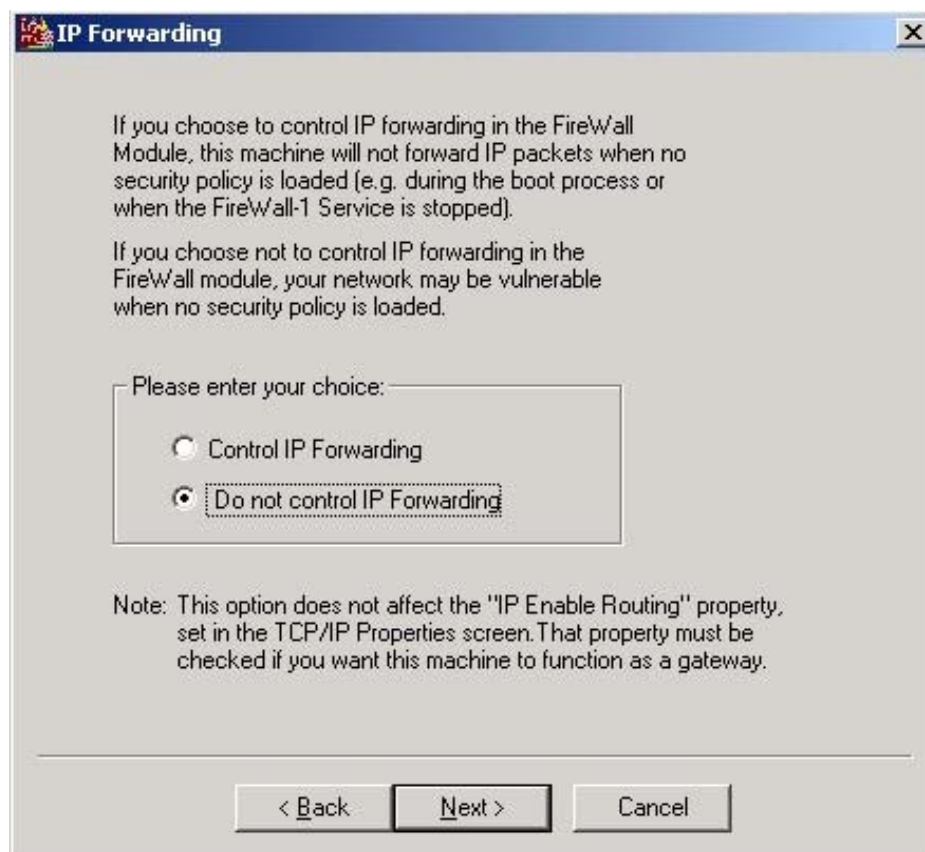
Chọn Add rồi nhập license vào cửa sổ sau :



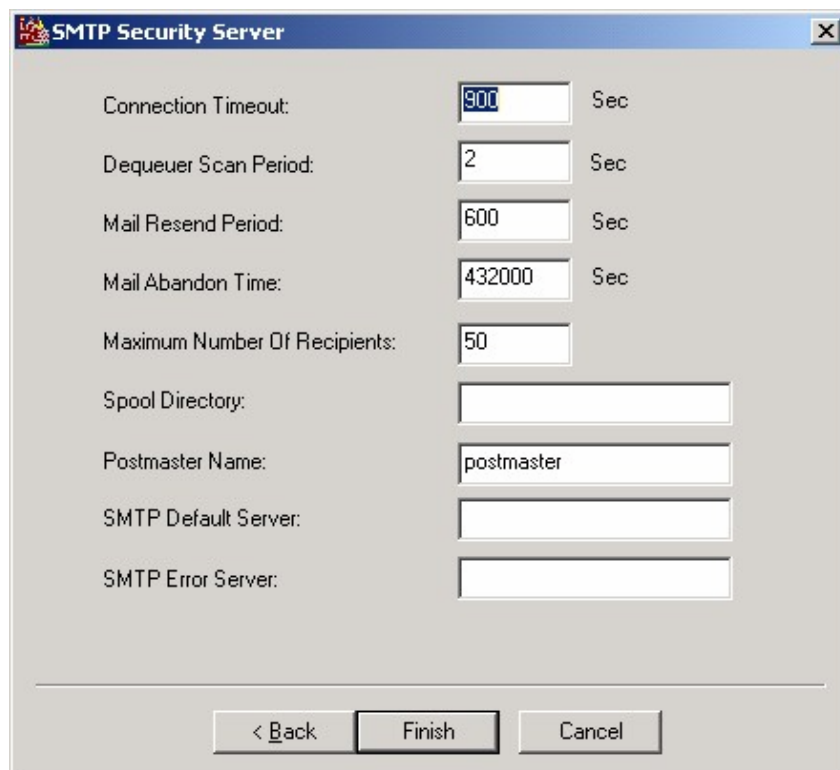
Chọn hostname của Management Server:



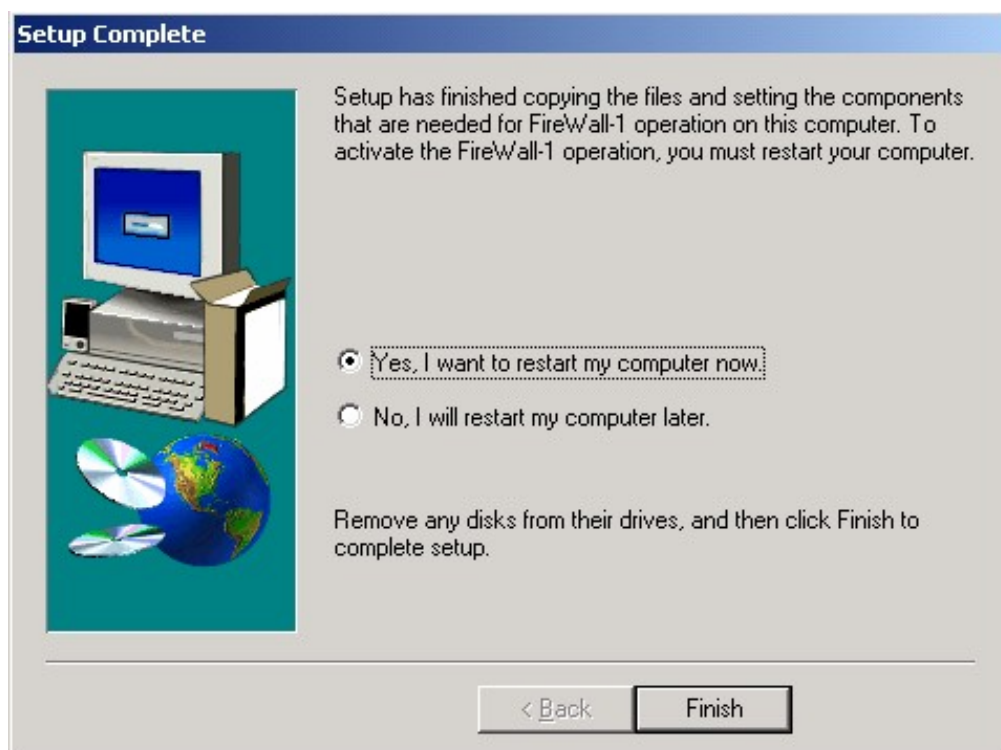
Chọn chế độ IP Forwarding:



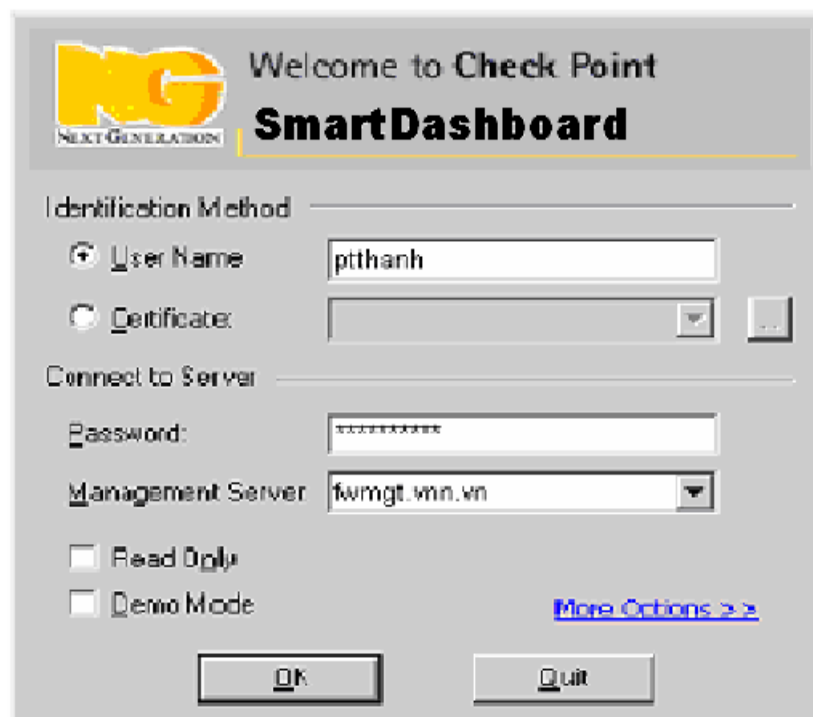
Đặt các tham số cho SMTP Security Server:



Chọn Finish để kết thúc quá trình cài đặt rồi Restart lại máy.



Sau khi restart lại máy, login vào màn hình console của CheckPoint với user và password đã tạo để thiết lập cấu hình cho firewall:



### 2.3.4. Thiết lập cấu hình

Sau khi login vào màn hình điều khiển của CheckPoint, ta bắt đầu tiến hành quá trình thiết lập cấu hình cho firewall theo các bước sau:

- Định nghĩa cho các giao tiếp (Interface) thuộc mạng trong (Inside network) và mạng ngoài (Outside network) của máy chủ cài CheckPoint.
- Tạo các Network thuộc mạng trong: Theo mô hình thử nghiệm ở đây là mạng 192.168.7.0 và 192.168.1.0.
- Nhóm các Inside network thành một group để tiện quản lý.
- Thiết lập các luật để cho phép hoặc cấm các truy nhập từ trong ra ngoài và từ ngoài vào trong. Các luật này gồm các thành phần cơ bản sau:
  - + Số thứ tự: biểu thị mức độ ưu tiên của luật. Luật nào có số thứ tự càng nhỏ thì mức độ ưu tiên càng lớn.
  - + Nguồn (SOURCE)
  - + Đích (DESTINATION)
  - + Giao tiếp (IF VIA)
  - + Dịch vụ (SERVICE): các dịch vụ được cho phép/cấm
  - + Hành động (ACTION): cho phép/cấm
  - + Ngoài ra còn có các tham số khác như TRACK, INSTALL ON, TIME ...

Sau đây là một ví dụ về thiết lập luật cho firewall CheckPoint:

| No. | Source                                                                                       | Destination                                                                                    | Service                                                                                  | Action                                                                                     | Track | Install On                                                                                     |
|-----|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-------|------------------------------------------------------------------------------------------------|
| 1   |  Any      |  mailserver |  smtp |  accept |       |  Gateways |
| 2   |  Any      |  London     |  Any  |  drop   |       |  Gateways |
| 3   |  localnet |  DMZ        |  ftp  |  accept |       |  Gateways |
| 4   |  localnet |  DMZ        |  http |  accept |       |  Gateways |
| 5   |  localnet |  DMZ        |  ftp  |  accept |       |  Gateways |
| 6   |  localnet |  DMZ        |  http |  accept |       |  Gateways |
| 7   |  Any      |  Any        |  Any  |  reject |       |  Gateways |

## TÀI LIỆU THAM KHẢO

1. **Interconnecting Cisco Network Devices** - Steve McQuerry, 03/2000
2. **Building Scalable Cisco Internetworks** - Catherine Paquet, 01/2003
3. **Routing TCP/IP Volume I** - Jeff Doyle, 09/1998
4. **Cisco Internetworking Basic** - Cisco Press, 07/2001
5. **Cisco WEB site** <http://www.cisco.com> - Technologies
6. **Microsoft Windows 2000 advanced server** - Microsoft Press, 1985-1999
7. **DNS and BIND, 3trd Edition** - Paul Albitz and Cricket Liu, 09/1998
8. **Internet System Consortium WEB site** <http://www.isc.org>
9. **Remote Access Study Guide** - Robert Padjen, Todd Lammle, Wade Edwards, 9/2002
10. **Building Cisco Remote Access Networks** - Catherine Paquet, 08/1999.
11. **Complete Book of Remote Access:Connectivity and Security** , Victor Kasacavage (Editor), Weikai Yan, 12/2002
12. **Designing & Implementing Microsoft Proxy Server-** David Wolfe, Sams Net Publishing.
13. **ISA Server 2000 Administration Study Guide-** William Heldman (Sybex-MCSE).
14. **Configuring ISA server for an Enterprise-**Microsoft Training and Certification, 02/2001
15. **Designing & Implementting Microsoft Windows2000 Network Infrastructure**, Microsoft Training and Certification, 05/2000
16. **Firewalls and Internet Security: Repelling the Wily Hacker**, Steven M. Bellovin, 01/2003
17. **Inside Network Perimeter Security**, Karen Fredericks and Lenny Zeltser and Scott Winters, 01/2002
18. **CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide**, Greg Bastien and Christian Degu, 01/2003
19. **Building Internet Firewalls**, Elizabeth D. Zwicky & Simon Cooper, 01/2000
20. **Firewalls: A Complete Guide**, Marcus Goncalves, 01/1999
21. **Configuring ISA server for an Enterprise-**Microsoft Training and Certification, 02/2001