ỦY BAN NHÂN DÂN TỈNH ĐỒNG THÁP

TRƯỜNG CAO ĐẲNG CỘNG ĐỒNG ĐỒNG THÁP

GIÁO TRÌNH

MÔN HỌC: TRIỂN KHAI HỆ THỐNG MẠNG

NGÀNH, NGHỀ: TRUYỀN THÔNG VÀ MẠNG MÁY TÍNH

TRÌNH ĐỘ: TRUNG CẤP

(Ban hành kèm theo Quyết định số /QĐ-CĐCĐ ngày tháng năm 20…
của Hiệu trưởng trường Cao đẳng Cộng đồng Đồng Tháp)

Đồng Tháp, năm 2017

TUYÊN BỐ BẢN QUYỀN

LỜI NÓI ĐẦU

Những năm qua ngành công nghệ thông tin không ngừng phát triển sôi động và mạnh mẽ, đem lại nhiều lợi ích to lớn, rút ngắn khoảng cách giữa mọi người. Chiếc máy vi tính đa năng, tiện lợi và hiệu quả mà chúng ta đang dùng, giờ đây đã trở nên chật hẹp và bất tiện so với các máy vi tính nối mạng với nhau.

Từ khi xuất hiện mạng máy tính, tính hiệu quả tiện lợi của mạng đã làm thay đổi phương thức khai thác máy tính cổ điển. Mạng và công nghệ về mạng mặc dù ra đời cách đây không lâu nhưng nó đã được triển khai ứng dụng trên rất nhiều lĩnh vực của cuộc sống.

Trong xu thế đó, Khoa CNTT trường CĐN KTCN cũng đã xây dựng và ngày càng củng cố mạng riêng của mình phục vụ trực tiếp cho nhu cầu khai thác thông tin, liên lạc phục vụ cho công tác học tập và làm viêc. Chính vì vậy những kiến thức về viễn thông tin học nói chung và về mạng nói riêng sẽ trở thành kiến thức phổ thông không thể thiếu được cho những người khai thác máy tính. Trong ngành nghề, việc lắp đặt và khai thác mạng máy tính trong vòng mấy năm trở lại đây ngày càng gia tăng. Đồng thời cùng với việc khai thác các thông tin trên mạng, yêu cầu về việc quản trị mạng nhằm khai thác mạng hiệu quả và an toàn đang ngày càng trở nên cần thiết và cấp bách.

Trong khuôn khổ một giáo trình, tôi không thể đề cập được toàn bộ các vấn đề kể trên. Tuy nhóm tác giả đã có nhiều cố gắng khi biên soạn, nhưng giáo trình không tránh khỏi những khiếm khuyết. Rất mong nhận được sự góp ý của bạn đọc.

MỤC LỤC

GIÁO TRÌNH MÔ ĐUN: TRIỂN KHAI HỆ THỐNG MẠNG

Mã mô đun: MĐ 27

Thời gian thực hiện mô đun: 90 giờ (Lý thuyết: 18 giờ; thực hành, thí nghiệm, thảo luận, bài tập: 58 giờ; kiểm tra: 4 giờ)

I.VỊ TRÍ, TÍNH CHẤT CỦA MÔ ĐUN:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong môn, mô đun: Mạng máy tính, Quản trị mạng 1.
- Tính chất: Là mô đun chuyên nghành bắt buộc.

II. MỤC TIÊU MÔ ĐUN:

- Có khả năng tinh chỉnh và giám sát mạng Windows Server;
- Triển khai được dịch vụ Routing and Remote Access (RRAS);
- Có khả năng phát hiện và khôi phục Server bị hỏng;
- Có khả năng cài đặt và quản lý máy tính từ xa thông qua RAS;
- Xây dựng được một mạng riêng ảo VPN;
- Trình bày được các tính năng và những nét đặc trưng của ISA Server;
- Cài đặt và cấu hình được ISA Server trên windows Server;
- Thực hiện được các Rule theo yêu cầu;
- Cài đặt và cấu hình được các chính sách mặc định của Firewall, thực hiện chính xác thao tác sao lưu cấu hình mặc định của Firewall;
- Trình bày được các cơ chế sao lưu, phục hồi toàn bộ máy ISA Server ;
- Thực hiện được thao tác xuất, nhập các chính sách của Firewall ra thành file;
- Hiểu được các loại ISA Server Client đồng thời cài đặt và cấu hình đúng qui trình cho từng loại ISA Server Clien và những tính năng riêng trên mỗi loại.
- Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.

III. NỘI DUNG MÔ ĐUN:

1. Nội dung tổng quát và phân phối thời gian :

Số TT	Tên các bài trong mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
1	Dịch vụ Windows terminal services	10	3	7	
	1. Tại sao phải dùng Terminal services 2. Mô hình xử lý của Terminal Services 3. Yêu cầu đối với Server của máy khách 4. Cài đặt, gỡ bỏ các phần mềm hổ trợ cho Terminal service 5. Tạo các máy khách Terminal service 6. Điều chỉnh các thiết định của tài khoản kết nối 7. Cấp phép sử dụng Terminal services 8. Quản lý các phiên làm việc của				

Số TT	Tên các bài trong mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
	Terminal services				
2	Tinh chỉnh và giám sát mạng Windows server 1. Tổng quan về cụng cụ tinh chỉnh 2. Quan sát các đường biểu diễn hiệu năng bằng System Monitor 3. Giải quyết trục trặc bằng Event Viewer 4. Sử dụng Task Manager	10	3	7	
3	Khôi phục server khi bị hỏng 1. Các biện pháp phòng ngừa 2. Các phương pháp sao lưu dự phòng 3. Tìm và quản trị Pan phần cứng bằng công cụ System Information 4. Giải quyết các trục trặc trong quá trình khởi động	5	2	2	1
4	Cài đặt và quản lý remote access services (RAS) trong Windows server 1. Những ứng dụng thường gặp của RAS 2. Dự trù và những lưu ý về thông lượng đường truyền 3. Các yêu cầu về phần cứng để thực hiện RAS 4. Tiếp nhận các cuộc gọi từ người dùng ở xa 5. Kết nối một mạng VPN	10	3	6	
5	Group Policy Object 1. Giới thiệu Group policy 2. Tạo và tổ chức các đối tượng trong Group policy 3. Thiết lập các chính sách trên Domain Controller 4. Sử dụng GPO để triển khai Ms office	10	4	5	1
6	Giới thiệu về ISA Server 1. Định nghĩa Firewall 2. Phân loại Firewall 3. Chức năng của Firewall 4. Các kiến trúc Firewall cơ bản 5. Giới thiệu về ISA server 6. Các mô hình Firewall cơ bản và phức tạp 7. Sơ Đồ hoạt động của ISA	4	4		

Số TT	Tên các bài trong mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
7	Cài Đặt và cấu hình sử dụng các Rule trong ISA 1. Cài đặt ISA 2. Tạo rule cho Admin đi ra ngoài Internet sử dụng tất cả các giao thức 3. Cấu hình cho các clien ra Internet chỉ sử dụng giao thức HTTP , HTTPS 4. Cấu hình DNS phân giải tên	13	3	10	
8	Dịch vụ Virtual Private Network 1. Giới thiệu về VPN 2. Mô hình VPN Client to Site dùng giao thức PPTP 3. Mô hình VPN Client to Site dùng giao thức L2TP/IPSec 4. Mô hình VPN Client to Site dùng chương trình No-IP 6. Mô hình VPN Site to Site	8	3	4	1
9	Publishing 1. Cài Đặt hệ thống Mail Mdaemon và gửi mail qua lại 2. Publishing Mail 3. Cấu hình Lọc mail 4. Publishing Web 5. Publishing FTP 6. Publishing Terminal Services	13	3	9	1
10	Monitor ISA Server 1. Trình bày các tab trong Monitor 2. Phát hiện các đợt tấn công gửi mail cho admin 3. Network Templates 4. Backup và Restore	7	2	5	
	Cộng	90	30	56	4

Bài mở đầu: GIỚI THIỆU TỔNG QUAN

Mã bài: MĐ 27.00

Mục tiêu:

- Kể tên được các dịch vụ mạng.
- Vẽ và giải thích được sơ đồ giao thức TCP/IP
- Hiểu được về IP V4

1.Giới thiệu

Mục tiêu:

- *Kể tên được các dịch vụ mạng.*
- *Vẽ và giải thích được sơ đồ giao thức TCP/IP*

1.1.Tổng quan về các dịch vụ mạng

Các dịch vụ mạng phổ biến nhất là:

- Dịch vụ tập tin.
- Dịch vụ in ấn.
- Dịch vụ thông điệp.
- Dịch vụ thư mục.
- Dịch vụ ứng dụng.
- Dịch vụ cơ sở dữ liệu.
- Dịch vụ Web.

1.1.1. Dịch vụ tập tin (Files Services)

Dịch vụ tập tin cho phép các máy tính chia sẻ các tập tin, thao tác trên các tập tin chia sẻ này như: lưu
trữ, tìm kiếm, di chuyển...

Truyền tập tin: không có mạng, các khả năng truyền tải tập tin giữa các máy tính bị hạn chế. Ví dụ như chúng ta muốn sao chép một tập tin từ máy tính cục bộ ở Việt Nam sang một máy tính server đặt tại Pháp thì chúng ta dùng dịch vụ FTP để sao chép. Dịch vụ này rất phổ biến và đơn giản.

Lưu trữ tập tin: phần lớn các dữ liệu quan trọng trên mạng đều được lưu trữ tập trung theo nhiều cách khác nhau:

Lưu trữ trực tuyến (online storage): dữ liệu được lưu trữ trên đĩa cứng nên truy xuất dễ dàng, nhanh chóng, bất kể thời gian. Nhưng phương pháp này có một khuyết điểm là chúng không thể tháo rời để trao đổi hoặc lưu trữ tách rời, đồng thời chi phí lưu trữ một MB dữ liệu tương đối cao.

Lưu trữ ngoại tuyến (offline storage): thường áp dụng cho dữ liệu ít khi cần truy xuất (lưu trữ, backup). Các thiết bị phổ biến dùng cho phương pháp này là băng từ, đĩa quang.

Lưu trữ cận tuyến (near- line storage): phương pháp này giúp ta khắc phục được tình trạng truy xuất chậm của phương pháp lưu trữ ngoại tuyến nhưng chi phí lại không cao đó là chúng ta dùng thiết bị Jukebox để tđộng quản lý các băng từ và đĩa quang.

Di trú dữ liệu (data migration) là công nghệ tự động dời các dữ liệu ít dùng từ kho lưu trữ trực tuyến sang kho lưu trữ cận tuyến hay ngoại tuyến. Nói cách khác đây là quá trình chuyển các tập tin từ dạng lưu trữ này sang dạng lưu trữ khác.

Đồng bộ hóa việc cập nhật tập tin: dịch vụ này theo dõi các thay đổi khác nhau lên cùng một tập tin để đảm bảo rằng tất cả mọi người dùng đều có bản sao mới nhất của tập tin và tập tin không bị hỏng.

Sao lưu dự phòng (backup) là quá trình sao chép và lưu trữ một bản sao dữ liệu từ thiết bị lưu trữ chính. Khi thiết bị lưu trữ chính có sự cố thì chúng ta dùng bản sao này để phục hồi dữ liệu.

1.1.2. Dịch vụ in ấn (Print Services)

Dịch vụ in ấn là một ứng dụng mạng điều khiển và quản lý việc truy cập các máy in, máy fax mạng.

Các lợi ích của dịch vụ in ấn:

Giảm chi phí cho nhiều người có thể chia nhau dùng chung các thiết bị đắt tiền như máy in màu, máy vẽ, máy in khổ giấy lớn.

Tăng độ linh hoạt vì các máy tính có thể đặt bất kỳ nơi nào, chứ không chỉ đặt cạnh PC của người dùng.

Dùng cơ chế hàng đợi in để ấn định mức độ ưu tiên nội dung nào được in trước, nội dung nào được in sau.

1.1.3. Dịch vụ thông điệp (Message Services)

Là dịch vụ cho phép gởi/nhận các thư điện tử (e-mail). Công nghệ thư điện tử này rẻ tiền, nhanh chóng, phong phú cho phép đính kèm nhiều loại file khác nhau như: phim ảnh, âm thanh... Ngoài ra dịch vụ này còn cung cấp các ứng dụng khác như: thư thoại (voice mail), các ứng dụng nhóm làm việc (workgroup application).

1.1.4. Dịch vụ thư mục (Directory Services)

Dịch vụ này cho phép tích hợp mọi thông tin về các đối tượng trên mạng thành một cấu trúc thư mục dùng chung nhờ đó mà quá trình quản lý và chia sẻ tài nguyên trở nên hiệu quả hơn.

1.1.5. Dịch vụ ứng dụng (Application Services)

Dịch vụ này cung cấp kết quả cho các chương trình ở client bằng cách thực hiện các chương trình trên server. Dịch vụ này cho phép các ứng dụng huy động năng lực của các máy tính chuyên dụng khác trên mạng.

1.1.6. Dịch vụ cơ sở dữ liệu (Database Services)

Dịch vụ cơ sở dữ liệu thực hiện các chức năng sau:

- Bảo mật cơ sở dữ liệu.
- Tối ưu hóa tiến trình thực hiện các tác vụ cơ sở dữ liệu.
- Phục vụ số lượng người dùng lớn, truy cập nhanh vào các cơ sở dữ liệu.
- Phân phối dữ liệu qua nhiều hệ phục vụ CSDL.

1.1.7. Dịch vụ Web

Dịch vụ này cho phép tất cả mọi người trên mạng có thể trao đổi các siêu văn bản với nhau. Các siêu bản này có thể chứa hình ảnh, âm thanh giúp các người dùng có thể trao đổi nhanh thông tin và sống động hơn.

1.2.Kiến trúc bộ giao trúc TCP/IP

Bộ giao thức TCP/IP được phân làm 4 tầng:

Network access Layer: tương ứng với tầng Physical và Datalink của OSI.

Internet Layer: tương ứng với tầng Network của OSI.

Transport Layer: tương ứng với tầng Transport của OSI.

Application Layer: tương ứng với 3 tầng cao nhất(Session, Presentation, Application) trong OSI.

Có nhiều loại giao thức có trong bộ giao thức truyền thống TCP/IP, nhưng có hai giao thức quan trọng nhất được lấy để đặt tên cho bộ giao thức này là TCP(Transmission Control Protocol) và IP(Internet Protocol). Cụ thể sẽ là: Các giao thức hoạt đông ở tầng Application:

FTP (File transfer Protocol): Giao thức truyền tệp, cho phép người dùng lấy hoặc gửi một tệp tin đến một máy khác.

Telnet: Chương trình mô phỏng thiết bị đầu cuối cho phép người dùng login vào máy chủ từ một máy khác trên mạng.

SMTP (Simple Mail Transfer Protocol): Một giao thức để truyền thư
DNS (Domain Name Service): Dịch vụ tên miền cho phép nhận ra một máy tính từ tên miền của nó thay vì phải đánh vào địa chỉ IP khó nhớ. Nhiều bạn thường nhầm DNS là Domain Name Server – Sai.

SNMP (Simple Network Management Protocol): Giao thức cung cấp các công cụ quản trị mạng.

Các giao thức hoạt đông ở tầng Transport:

UDP (User Datagram Protocol): Giao thức truyền không tin cậy nhưng ưu điểm của nó là nhanh và tiết kiệm.

TCP (Transmission Control Protocol): Cung cấp một phương thức truyền tin cậy

Các giao thức hoạt đông ở tầng Internet:

IP (Internet Protocol): Giao thức Internet, cung cấp các thông tin để làm sao các gói tin có thể đến được đích.

ARP (Address Resolution Protocol): Giao thức chuyển địa chỉ IP thành địa mạng chỉ vật lý

ICMP (Internet Control Message Protocol): Một giao thức thông báo lỗi xảy ra trên đường truyền.

Các công nghệ thường gặp ở tầng vật lý: Ethernet, Token Ring, Token Bus, Fiber.

Cũng giống như mô hình tham chiếu OSI, dữ liệu từ tầng Application đi xuống các tầng dưới, nơi mà mỗi tầng có nhưng định nghĩa riêng về dữ liệu mà nó sử dụng, chúng thêm vào các header của riêng mình trước khi chuyển tiếp xuống tầng tiếp theo, quá trình nhận diễn ra ngược lại.

2.IP V4

Mục tiêu:

- *Trình bày được địa chỉ IP và các lớp.*
- *Hiểu được về kỹ thuật VLSM và CIDR.*

2.1. Địa chỉ IP và các lớp

Sơ đồ địa chỉ hoá để định danh các trạm (host) trong liên mạng được gọi là 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. Mục đích của địa chỉ IP là để định danh duy nhất cho một host bất kỳ trên liên mạng.

Có hai cách cấp phát địa chỉ IP, nó phụ thuộc vào cách ta kết nối mạng.

Nếu mạng của ta kết nối vào mạng Internet, địa mạng chỉ được xác nhận bởi NIC (Network Information Center). Nếu mạng của ta không kết nối Internet, người quản trị mạng sẽ cấp phát địa chỉ IP cho mạng này. Còn các host ID được cấp phát bởi người quản trị 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>

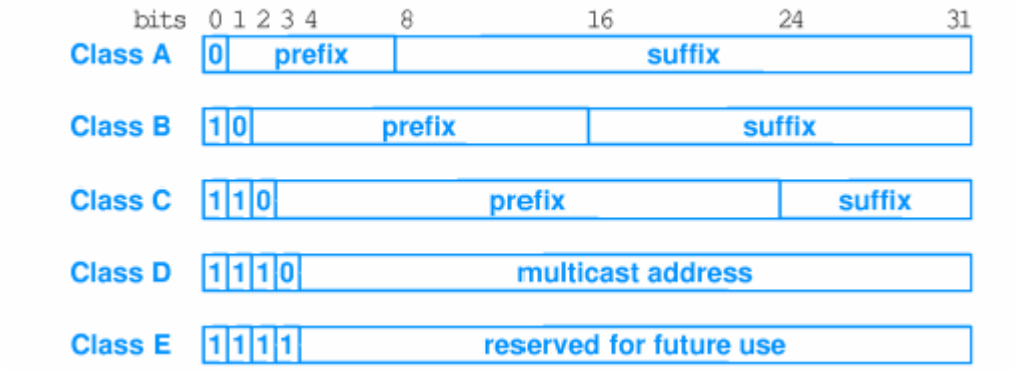
- Phần định danh địa chỉ mạng Network Number.
- Phần định danh địa chỉ các trạm làm việc trên mạng đó Host Number.

Ví dụ 128.4.70.9 là một địa chỉ IP

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 với cấu trúc được xác định trên hình 2.2.

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).

- Lớp A cho phép định danh tới 126 mạng (sử dụng byte đầu tiên), với tối đa 16 triệu host (3 byte còn lại, 24 bits) cho mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn. Tại sao lại có 126 mạng trong khi dùng 8 bits? Lí do đầu tiên, 127.x (01111111) dùng cho địa chỉ loopback, thứ 2 là bit đầu tiên của byte đầu tiên bao giờ cũng là 0, 1111111(127). Dạng địa chỉ lớp A (network number. host.host.host). Nếu dùng ký pháp thập phân cho phép 1 đến



Hình 0.1. Cách đánh địa chỉ TCP/IP

- Lớp B cho phép định danh tới 16384 mạng (10111111.11111111.host.host), với tối đa 65535 host trên mỗi mạng. Dạng của lớp B (network number. Network number.host.host). Nếu dùng ký pháp thập phân cho phép 128 đến 191 cho vùng đầu, 1 đến 255 cho các vùng còn lại.

- Lớp C cho phép định danh tới 2.097.150 mạng và tối đa 254 host cho mỗi mạng. Lớp này được dùng cho các mạng có ít trạm. Lớp C sử dụng 3 bytes đầu định danh địa chỉ mạng (110xxxxx). Dạng của lớp C (network number. Network number.Network number.host). Nếu dùng dạng ký pháp thập phân cho phép 129 đến 233 cho vùng đầu và từ 1 đến 255 cho các vùng còn lại.

- Lớp D dùng để gửi IP datagram tới một nhóm các host trên một mạng. Tất cả các số lớn hơn 233 trong trường đầu là thuộc lớp D

- Lớp E dự phòng để dùng trong tương lai

Như vậy địa chỉ mạng cho lớp: A: từ 1 đến 126 cho vùng đầu tiên, 127 dùng cho địa chỉ loopback, B từ 128.1.0.0 đến 191.255.0.0, C từ 192.1.0.0 đến 233.255.255.0

Ví dụ:

192.1.1.1 địa chỉ lớp C có địa chỉ mạng 192.1.1.0, địa chỉ host là 1

200.6.5.4 địa chỉ lớp C có địa chỉ mạng 200.6.5, địa chỉ mạng là 4

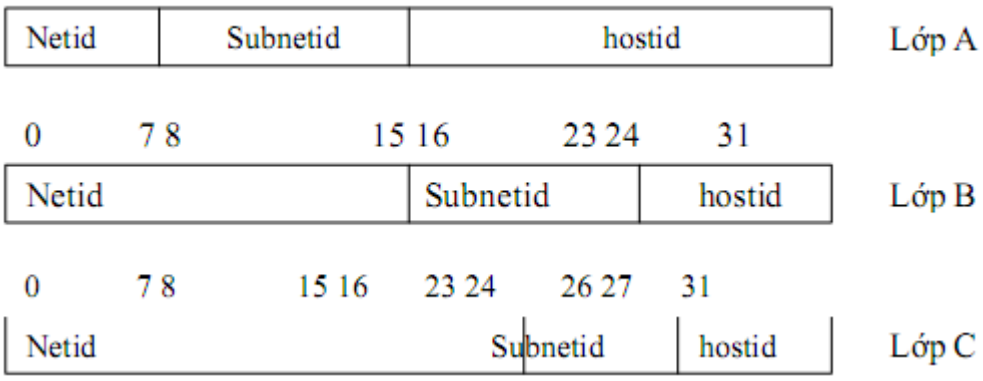
150.150.5.6 địa chỉ lớp B có địa chỉ mạng 150.150.0.0, địa chỉ host là 5.6

9.6.7.8 địa chỉ lớp A có địa chỉ mạng 9.0.0.0, địa chỉ host là 6.7.8

128.1.0.1 địa chỉ lớp B có địa chỉ mạng 128.1.0.0, địa chỉ host là 0.1

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:



Hình 0.2 Bổ sung vùng subnetid

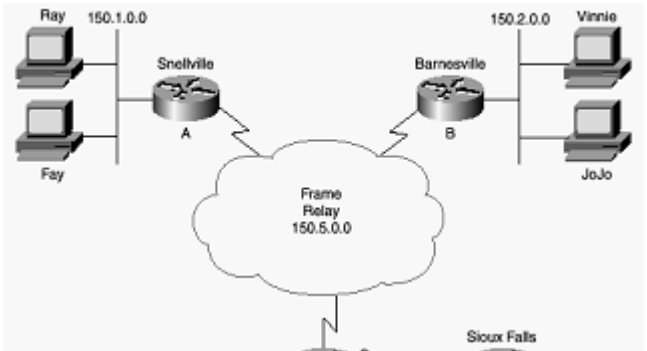
Ví dụ:

17.1.1.1 địa chỉ lớp A có địa chỉ mạng 17, địa chỉ subnet 1, địa chỉ host 1.1

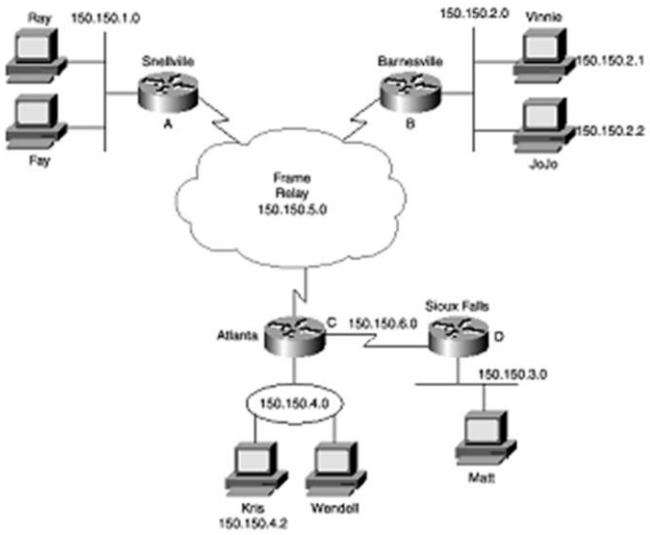
129.1.1.1 địa chỉ lớp B có địa chỉ mạng 129.1, địa chỉ subnet 1, địa chỉ host 1.

2.2. Chia mạng con (subnetting).

Giả sử ta phải tiến hành đặt địa chỉ IP cho hệ thống có cấu trúc như sau:



Theo hình trên, ta bắt buộc phải dùng đến tất cả là sáu đường mạng riêng biệt để đặt cho hệ thống mạng của mình, mặc dù trong mỗi mạng chỉ dùng đến vài địa chỉ trong tổng số 65534 địa chỉ hợp lệ, đó là một sự phí phạm to lớn. Thay vì vậy, khi sử dụng kỹ thuật chia mạng con, ta chỉ cần sử dụng một đường mạng 150.150.0.0 và chia đường mạng này thành sáu mạng con theo hình bên dưới:

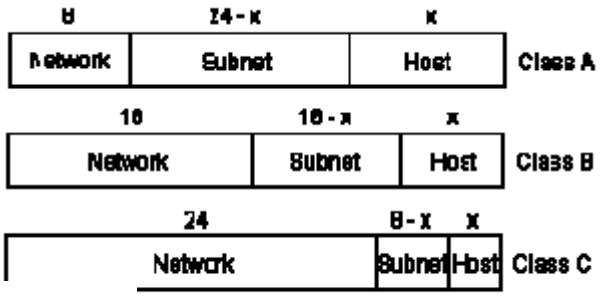


– Hệ thống mạng có 6 đường mạng (sau khi chia Subnet)

Rõ ràng khi tiến hành cấp phát địa chỉ cho các hệ thống mạng lớn, người ta phải sử dụng kỹ thuật chia mạng con trong tình hình địa chỉ IP ngày càng khan hiếm. Ví dụ trong hình trên hoàn toàn chưa phải là chiến lược chia mạng con tối ưu. Thật sự người ta còn có thể chia mạng con nhỏ hơn nữa, đến một mức độ không bỏ phí một địa chỉ IP nào khác.

Xét về khía cạnh kỹ thuật, chia mạng con chính là việc mượn một số bit trong phần host_id ban đầu để đặt cho các mạng con. Lúc này, cấu trúc của địa

chỉ IP gồm có ba phần: network_id, subnet_id và host_id. Số bit dùng cho phần subnet_id bao nhiêu là tuỳ thuộc vào chiến lược chia mạng con của người quản trị, có thể là một con số tròn byte (8 bit) hoặc một số bit lẻ vẫn được. Tuy nhiên subnet_id không thể chiếm trọn số bit có trong host_id ban đầu, cụ thể là (số bit làm subnet_id) ≤ (số bit làm host_id)-2.



Hình 0.5

Hình 3.6 – Số lượng **Subnet** tối đa được phép

Số lượng host trong mỗi mạng con được xác định bằng số bit trong phần host_id; 2x – 2 là số địa chỉ hợp lệ có thể đặt cho các host trong mạng con. Tương tự, số bit trong phần subnet_id xác định số lượng mạng con. Giả sử số bit là y ¬ 2y – 2 là số lượng mạng con có được (trường hợp đặc biệt thì có thể sử dụng được 2y mạng con).

Một số khái niệm mới:

- Địa chỉ mạng con (địa chỉ đường mạng): bao gồm cả phần network_id và subnet_id, phần host_id chỉ chứa các bit 0. Theo hình bên trên thì ta có các địa chỉ mạng con sau: 150.150.1.0, 150.150.2.0, …

- Địa chỉ broadcast trong một mạng con: Giữ nguyên các bit dùng làm địa chỉ mạng con, đồng thời bật tất cả các bit trong phần host_id lên 1. Ví dụ địa chỉ broadcast của mạng con 150.150.1.0 là 150.150.1.255.

- Mặt nạ mạng con (subnet mask): giúp máy tính xác định được địa chỉ mạng con của một địa chỉ host. Để xây dựng mặt nạ mạng con cho một hệ thống địa chỉ, ta bật các bit trong phần network_id và subnet_id lên 1, tắt các bit trong phần host_id thành 0. Ví dụ mặt nạ mạng con dùng cho hệ thống mạng trong hình trên là 255.255.255.0.

Vấn đề đặt ra là khi xác định được một địa chỉ IP (ví dụ 172.29.8.230) ta không thể biết được host này nằm trong mạng nào (không thể biết mạng này có chia mạng con hay không, và nếu có chia thì dùng bao nhiêu bit để chia). Chính vì vậy khi ghi nhận địa chỉ IP của một host, ta cũng phải cho biết subnet mask là bao nhiêu (subnet mask có thể là giá trị thập phân, cũng có thể là số bit dùng làm subnet mask).

+ Ví dụ địa chỉ IP ghi theo giá trị thập phân của subnet mask là 172.29.8.230/255.255.255.0

+ Hoặc địa chỉ IP ghi theo số bit dùng làm subnet mask là 172.29.8.230/24.

2.3.Kỹ thuật VLSM và CIDR

Mục tiêu:

- *Trình bày được kỹ thuật VLSM và CIDR.*

2.3.1. Kỹ thuật VLSM

*** Khái niệm**

VLSM (Variable Length Subnet Mask) là một kỹ thuật cho phép người quản trị dùng nhiều giá trị subnet mask khác nhau trong cùng một địa chỉ mạng. Ip được chia thành các lớp A, B, C để tiện sử dụng. Tuy nhiên theo thời gian thì số địa chỉ Ip này ngày càng cạn kiệt. Chính vì vậy người ta mới đưa ra giải pháp chia subnet để việc sử dụng Ip hiệu quả hơn. Chúng ta có thể tham khảo theo mô hình bên dưới

Mô hình chia subnet cho mạng lớp A.

Với mô hình mạng trên thì mạng 172.16.0.0/16 được chia thành các sub-net nhỏ hơn, với các sub-net mask /24, /27, /30.

Ví dụ ta có yêu cầu thiết kế cho một hệ thống mạng như sau:

- LAN NewStar cần 300 địa chỉ IP
- LAN Cisco cần 200 địa chỉ IP
- LAN Server cần 4 địa chỉ IP
- Liên kết Serial cần 2 địa chỉ IP
- Địa chỉ lớp B được cấp cho là 172.16.0.0/16

Ta làm như sau:

Bước 1: Lập bảng như sau:

Bước 2:

Chọn LAN có số lượng host lớn nhất: Ở đây chọn Lan NewStar với 9 bit làm host => 7 bit làm network. Với 7 bit là network ta co 2^128 sub-net như sau.

Ở đây ta chọn subnet 1 (172.16.0.0/23) làm địa chỉ mạng cho LAN NEWSTAR

Bước 3: Tiếp tục tính tiếp cho LAN Cisco (200 host).

Ta thấy, địa chỉ được cấp đầu tiên 172.16.0.0/16. Ta đã chia địa chỉ này thành 27=128 subnet, mỗi subnet có 23 bit là host. Ở trên, ta đã dùng 1 subnet cho segment 300 host, như vậy số lượng subnet chưa dùng là 127 (mỗi subnet có 23 net-bit và 11 host-bit).

Ta sẽ chọn 1 trong 127 subnet này để tính cho segment 200 host. Ví dụ, ta sử dụng subnet subnet 2: 172.16.2.0/23

Tương tự như trên, bây giờ ta chỉ quan tâm đến subnet 172.16.2.0/23 để giải quyết cho segment 200 host (8 bit là host).

Bước 4: Tiếp tục tính tiếp cho LAN Server (4 host). Sử dụng 172.16.3.0/24

Bước 5: Tiếp tục tính tiếp cho Liên kết Serial (2 host). Sử dụng 172.16.3.8/24

Như vậy: Ta đã thiết lập được địa chỉ cho hệ thống mạng sư dụng VLSM

2.3.2. Kỹ thuật CIDR

Classess Interdomain Routing (CIDR) là một giải pháp khác cho tình trạng thiếu địa chỉ IP public (bên cạnh IPv6). CIDR được giới thiệu từ năm 1993 và triển khai một năm sau đó. Cơ chế đánh địa chỉ này được xem là cấp phát hiệu quả hơn so với cách đánh địa chỉ theo lớp A, B, C, D, E truyền thống,

với một cơ chế ít lãng phí và linh hoạt hơn, làm tăng hiệu quả và tính mở rộng cho IPv4.

CIDR cung cấp cơ chế supernetting, một cải tiến cho việc thu thập định tuyến (route). Khi mạng Internet ngày càng phình to, các router đòi hỏi phải có các bảng lưu trữ khổng lồ để chứa tất cả các thông tin định tuyến. Suppernetting rút ngắn và kết hợp nhiều thông tin định tuyến vào một entry duy nhất, bằng cách này sẽ giúp làm giảm kích thước các bảng lưu trữ của router và tăng tốc quá trình tìm kiếm.

Ví dụ cho địa chỉ mạng CIDR:

192.168.54.0/23

Nework address là 192.168.54.0, prefix là /23, do đó 9 bit còn lại có thể được dùng để đánh địa chỉ host. (Lưu ý phần prefix không giống với các Class chuẩn).

IANA cấp phát những block các địa chỉ Ipv4 cho các nhà cung cấp dịch vụ, những nhà cung cấp này sau đó dùng CIDR để cấp phát lại địa chỉ cho khách hàng theo những chính sách riêng của họ. Ví dụ, nếu bạn yêu cầu nhiều hơn 254 địa chỉ host, bạn có thể được gán cho một địa chỉ /23 thay vì phung phí toàn bộ cả địa chỉ lớp B, hỗ trợ đến 65,534 host.

Các mạng CIDR còn được biết như là mạng "slash x" – x đại diện cho số bit trong phần network của địa chỉ IP. Chẳng hạn lớp C là mạng slash 24 – InterNIC là tổ chức quản lý 24 bit đầu tiên (trong 32 bit của địa chỉ Ipv4), và 8 bit còn lại có thể được dùng để cấp phát.

CIDR có thể tổng hợp nhiều mạng phân lớp chuẩn thành một mạng lớn hơn. Bằng cách đó, số lượng entry trong bảng định tuyến của router giảm xuống và tăng số lượng host được cấp phát trong network. Ta đạt được điều này mà không cần phải dùng đến network ID của lớp lớn hơn như theo cách phân lớp thông thường.

Khi dùng CIDR, một tổ chức sẽ không yêu cầu địa chỉ từ một trung tâm có thẩm quyền, mà sẽ yêu cầu từ ISP. ISP sẽ đánh giá yêu cầu của tổ chức và cấp phát vùng địa chỉ từ block địa chỉ CIDR của nó. Những CIDR block này thường được các RIR (Regional Internet Registry – ở châu Á là APNIC, xem thêm ở đây) gán cho các chính phủ, nhà cung cấp dịch vụ, doanh nghiệp, và các tổ chức.

Ví dụ, một ISP có block địa chỉ 192.168.0.0/16. Công ty A mua một block địa chỉ nhỏ hơn là 192.168.0.0/23 từ ISP. Như vậy nó có thể dùng 9 bit cho địa chỉ host, trừ đi địa chỉ network và địa chỉ broadcast thì A có thể đánh địa chỉ cho 2^9-2 = 510 máy.

Với hệ thống không phân lớp này, ISP chịu trách nhiệm quản lý không gian địa chỉ. Các router trên Internet lưu giữ một supernet route (còn gọi là summary route) đến mạng của nhà cung cấp. ISP sẽ lưu giữ các route chi tiết hơn đến các mạng khách hàng của chính ISP đó. Phương pháp này giúp giảm kích thước bảng định tuyến trên Internet rất hiệu quả.

Bài 1: Xây dựng LAN Router

Mã bài: MĐ32.01

Mục tiêu:

- Nhận biết được các thành phần của LAN Router
- Trình bày được các ứng dụng của Dynamic và Static Routes
- Xây dựng được LAN Rounter
- Xử lý các sự cố thông dụng về Routing.
- Tự tin trong thao tác triển khai Routing.
- Tinh thần tương trợ lẫn nhau trong học tập.

1.Giới thiệu về định tuyến.

Mục tiêu:

- Trình bày được khái niệm định tuyến.

- Kể tên được các loại định tuyến.

1.1. Khái niệm cơ bản

Định tuyến là gì ?

Là chức năng của router giúp xác định quá trình tìm đường đi cho các gói tin từ nguồn tới đích thông qua hệ thống mạng.

Để định tuyến thì router cần phải biết các thông tin sau:

* Địa chỉ đích
* Các nguồn mà nó có thể học
* Các tuyến (routes)
* Tuyến tốt nhất (best route)
* Bảo trì và kiểm tra thông tin định tuyến

1.2.Các loại giao thức định tuyến.

Có hai loại định tuyến là : định tuyến tĩnh và định tuyến động

1.2.1.Định tuyến tĩnh – static routing

Định tuyến tĩnh là một quá trình định tuyến sử dụng các tuyến do người quản trị cấu hình thủ công trên router.

Lệnh: ip route

* Dùng để cấu hình static route, ta cấu hình bằng tay cho bảng định tuyến.

* Dùng ở mode global configuration

* Cú pháp

* ip route <destination-network> <subnet-mask> <address | interface>

Trong đó:

destination-network: là địa chỉ mạng cần đi tới

subnet-mask: subnet mask của destination-network

address: địa chỉ IP của cổng trên router mà packet sẽ đi ra

interface: cổng của router mà packet sẽ đi ra

Ví dụ: Cấu hình trên router Cisco A để học mạng 172.16.1.0/24

Mô hình mạng cấu hình static route

RouterA(config)#ip route 172.16.1.0 255.255.255.0 S0

Hoặc:

RouterA(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2

* Cú pháp khác:

* ip route <destination-network> <subnet-mask> <nexthop-address>

Trong đó:

Cú pháp này thường được sử dụng hơn cú pháp đã trình bày phần trước.

Ví dụ: Tương tự như mô hình trên, ta cấu hình theo cú pháp này trên router Cisco A như sau

Router(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1

Static route không có hoạt động gửi thông tin cập nhật như các giao thức định tuyến động.

1.2.2.Định tuyến động.

Là những tuyến do router học được từ các router khác nhờ giao thức định tuyến động. Một số giao thức định tuyến động như RIP, EIGRP, OSPF, IS-IS, BGP…

2.Giới thiệu về bộ định tuyến.

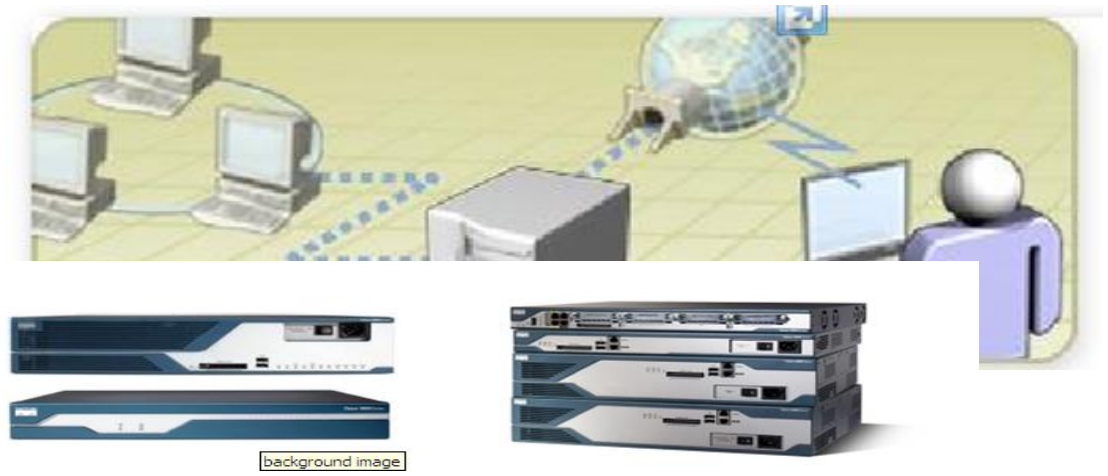
Mục tiêu:

- Trình bày được khái niệm bộ định tuyến, các thành phần của định tuyến.

2.1. Khái niệm

Router là một thiết bị cho phép gửi các gói dữ liệu dọc theo mạng. Một R outer được kết nối tới ít nhất là hai thông thường hai mạng đó là LAN, WAN hoặc là một LAN và mạng ISP của nó.

Router gồm có hai loại: Router Cứng và Router Mềm



Hình 1.2: Bộ định tuyến

2.2.2. Routing Protocol

Giao thức định tuyến (Routing Protocol) là ngôn ngữ mà một router trao đổi với router khác để chia sẻ thông tin định tuyến về khả năng đến được cũng như trạng thái của mạng.