BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT HƯNG YÊN

GIÁO TRÌNH MẠNG DOANH NGHIỆP

TRÌNH ĐỘ ĐÀO TẠO: **ĐẠI HỌC**

NGÀNH ĐÀO TẠO: **CÔNG NGHỆ THÔNG TIN**
(INFORMATION TECHNOLOGY)

Hưng Yên, tháng 12 năm 2008

http://www.ebook.edu.vn

LỜI NÓI ĐẦU

Cùng với sự phát triển nhanh chóng của nền kinh tế. Vấn đề ứng dụng hệ thống Mạng thông tin vào điều hành và sản xuất trong doanh nghiệp ngày càng được đẩy mạnh. Nhà quản lý mong muốn Quản trị viên mạng thông tin phải nắm được hầu hết các công nghệ mạng để nhanh chóng triển khai, ứng dụng những công nghệ mạng tiên tiến vào phục vụ điều hành sản xuất cũng như lập kế hoạch xây dựng và bảo vệ hệ thống thông tin nội bộ của doanh nghiệp tránh khỏi mọi nguy cơ tấn công.

Với cuốn giáo trình này, tôi cố gắng tập trung đi sâu vào các công nghệ mới nhất hiện đang được áp dụng trong doanh nghiệp tại thời điểm hiện tại.

Giáo trình này gồm 16 bài trong đó có 09 bài giảng, 06 bài thực hành và 01 bài thảo luận. Mục tiêu cuốn sách đi vào các vấn đề chính sau:

- Thiết kế lược đồ địa chỉ IP cho doanh nghiệp
- Cơ bản về công nghệ mạng không dây
- Vấn đề định tuyến và chuyển mạch trong mạng doanh nghiệp
- Triển khai các dịch vụ máy chủ (Mail Server, Web Server, DNS, DHCP…)
- Cơ bản về bảo mật

Mong muốn thì nhiều nhưng trong thời gian 3 tín chỉ của môn học này chúng ta chưa thể bao quát toàn bộ các công nghệ mạng áp dụng cho doanh nghiệp mà chỉ có thể đi vào những công nghệ chính. Hi vọng từ đó sinh viên tự nghiên cứu, học hỏi để có thể làm chủ được các công nghệ và áp dụng tốt kiến thức đã học vào công việc mai sau.

Mọi ý kiến đóng góp của sinh viên và các bạn đồng nghiệp xin gửi về theo địa chỉ sau

http://www.ebook.edu.vn

Địa chỉ liên hệ:

Vũ Khánh Quý - Bộ môn Mạng máy tính và Truyền thông - Khoa Công nghệ Thông tin, Đại học Sư phạm Kỹ thuật Hưng Yên

Tel: (03213) 713153

Email: quyvk@utehy.edu.vn

URL: http://www.utehy.edu.vn

http://www.ebook.edu.vn

Tên Module: Thiết kế mạng doanh nghiệp
Mã Module:
Giáo viên: Vũ Khánh Quý
Ngành học: Công nghệ Thông tin **Số giờ học:** 140(30/30)
Loại hình đào tạo: Chính qui **Thời gian thực hiện: Học kỳ III**
Năm học: 2008/2009 **Loại Module: LT+TH**
Phiên bản: 20090105

---

1. Mục tiêu:

Sau khi hoàn thành module này, người học có khả năng:
Sau khi hoàn thành module này, người học có khả năng:

- Đánh giá được các hoạt động của các thiết bị phần cứng và phần mềm trong một mô hình mạng LAN, WAN sẵn có
- Tư vấn trong việc lựa chọn các thiết bị phần cứng phần mềm để thiết kế mạng LAN, WAN phù hợp với nhu cầu của doanh nghiệp nhỏ
- Đánh giá được các yêu cầu về quản lý mạng, an ninh mạng và các ràng buộc khác trong quá trình thiết kế mạng
- Thiết kế được mạng LAN trong tòa nhà phục vụ cho công tác giảng dạy và nghiên cứu
- Thiết kế được mạng WAN cho Trường học phục vụ công tác đào tạo và quản lý của Nhà trường.

Module này giúp người học phát triển các năng lực: Phân tích (2); Tư vấn (2); Thực hiện (3); Thiết kế (3) và Bảo trì (2).

2. Điều kiện tiên quyết:

Người học đã học Mạng máy tính.

3. Mô tả module:

Module này nhằm cung cấp cho người học các kiến thức để Thiết kế được các hệ thống mạng LAN/WAN; Kiểm tra, đánh giá hiệu năng hoạt động của hệ thống; Xử lý được các sự cố xảy ra; Có kỹ năng cơ bản về bảo mật trong hệ thống mạng doanh nghiệp nhỏ.

http://www.ebook.edu.vn

4. Nội dung module:

Bài 1: Tổng quan về mạng doanh nghiệp

1.1.Giới thiệu môn học, phương pháp học

1.2.Cách sử dụng các phần mềm thiết kế giả lập VMWare, Boson

1.3.Giới thiệu hệ thống mạng thực tế của một số doanh nghiệp

Bài 2: Địa chỉ mạng

2.1.Địa chỉ IP và Subnetmask

2.2.Các loại địa chỉ IP

2.2.1.Địa chỉ IP Private, Public

2.2.3.Địa chỉ IP Unicast, Multicast, Broadcast

2.3.Nguyên lý dịch chuyển địa chỉ IP (NAT)

2.4 Nguyên lý cấp phát DHCP

Bài 3: Công nghệ Wireless

3.1. Tổng quan về Wireless

3.2. Các chuẩn Wireless

3.3. Cấu hình mạng Wireless

3.3.1. Các thành phần thiết lập mạng mạng WLAN

3.3.2. WLAN và SSID

3.3.3. Cấu hình một mạng WLAN đơn giản

Bài 4: Cơ bản về cấu hình định tuyến

4.1. Các giao thức định tuyến

4.2. Giao thức định tuyến nội vùng RIP

4.3. Giao thức định tuyến động OSPF

Bài 5:Thực hành về định tuyến

Cấu hình định tuyến cho các mạng

Bài 6:Cấu hình NAT trên Router

6.1. Khái niệm về NAT

6.2. Nat tĩnh – Static NAT

6.3. Nat động – Dynamic NAT

http://www.ebook.edu.vn

6.4. Nat Overload – PAT

Bài 7:Thực hành Cấu hình NAT trên Router

Bài 8:Cấu hình chuyển mạch (Switching)

8.1. Cơ bản về cấu hình Switch

8.2. Cấu hình VLAN

Bài 9:Thực hành Cấu hình chuyển mạch và VLAN

Bài 10: Thảo luận

Một số chủ đề thảo luận

- Các kỹ năng cần có của một kỹ sư trong vai trò HelpDesk
- Quy trình thiết kế và nâng cấp hệ thống mạng đã có
- Tìm hiểu các giao thức mã hoá trong mạng WLAN
- Mạng Wimax
- Tìm hiểu VoIP
- Công nghệ VPN

Bài 11: Cấu hình các Web Server, DNS Server

11.1. Dịch vụ phân giải tên miến – DNS Server

11.1.1. Nguyên lý phân giải tên miền

11.1.2. Xây dựng máy chủ phân giải tên miền cho mạng doanh nghiệp

11.2. Dịch vụ Web Server

11.2.1. Giao thức HTTP và HTTPS

11.2.2. Triển khai Website doanh nghiệp trên Server

Bài 12: Thực hành cấu hình các dịch vụ mạng cơ bản

12.1. Cấu hình Active Directory (AD)

12.2 Cấu hình IIS

12.3 Cấu hình DNS

12.4 Cấu hình DHCP

Bài 13. Xây dựng một Mail Server

13.1. Giao thức SMTP, POP3, IMAP

13.2. Triển khai Mail Server cho doanh nghiệp

Bài 14. Thực hành Xây dựng một Mail Server

Triển khai Mail Server cho doanh nghiệp

Bài 15: Thực hành Proxy và Firewall

http://www.ebook.edu.vn

15.1. Nguyên lý hoạt động của Proxy

15.2. Nguyên lý hoạt động của Firewall

15.3. Triển khai xây dựng hệ thống tường lửa cho doanh nghiệp

Bài 16. Cơ bản về bảo mật

16.1 Các nguy cơ tiềm tàng trên mạng

16.2. Các phương thức tấn công

16.2.1 Viruses, Worms, Trojan Horses.

16.2.2 Denial of Service (DoS) và Brute Force Attack

16.3. Các chính sách bảo mật

5. Tài liệu tham khảo:

Sách giáo trình, Slide do giáo viên biên soạn.

Sách tham khảo:

[1]. Cisco System, "CCNA Discovery1 4.0", Cisco System, 2007

[2]. Cisco System, "CCNA Discovery2 4.0", Cisco System, 2007

[3]. J.C. Mackin and Ian McLean, “Windows Server 2003 Network Infrastructure”, Microsoft Press, 2005

6. Học liệu:

Giáo trình lưu hành nội bộ, sách tham khảo, hệ thống bài tập mẫu, bài tập tự làm, máy tính, tài nguyên trên Internet, Projector.

7. Đánh giá:

Hình thức đánh giá:

- Kiểm tra giữa kỳ (Triển khai trên môi trường giả lập): 20%
- Đánh giá quá trình (kết quả các buổi thực hành): 10%
- Kiểm tra cuối kỳ: 70%

Tiêu chí đánh giá:

- Kỹ năng thiết kế, xây dựng bài toán
- Kỹ năng cài đặt bài toán

Người đánh giá: Giáo viên giảng dạy và người học.

8. Kế hoạch học tập

Bố trí giảng dạy module Mạng doanh nghiệp (3 tín chỉ) như sau:

27 tiết lý thuyết (thực hiện trong 9 buổi, mỗi buổi 3 tiết), 36 tiết sinh viên làm tiểu luận (giáo viên tự bố trí lịch gặp, hướng dẫn sinh viên), 18 tiết thực hành (thực hiện trong 6 buổi, mỗi buổi 3 tiết) và 90 giờ chuẩn bị cá nhân (đề cương 130 trang)

http://www.ebook.edu.vn

http://www.ebook.edu.vn

8. Kế hoạch học tập:

Bài	Mục tiêu	Hoạt động giáo viên	SG GV	Hoạt động sinh viên	SG SV	Điều kiện thực hiện
1	- Xác định được vị trí, vai trò và nội dung của Module trong chương trình đào tạo - Xây dựng được kế hoạch và phương pháp học tập phù hợp. - Lựa chọn được nguồn học liệu phục vụ cho môn học - Trình bày được những lợi ích đem lại cho doanh nghiệp khi có hệ thống mạng. - Trình bày được các bước để trở thành một nhà quản trị mạng trong doanh nghiệp	- Nêu mục tiêu, nội dung và kế hoạch học tập của Module - Giới thiệu nguồn học liệu phục vụ cho học Mudule, phương pháp học tập và các tiêu chí đánh giá - Tổ chức thảo luận các lợi ích đem lại cho doanh nghiệp khi có hệ thống mạng - Quá trình để trở thành một nhà nhà quản trị mạng trong doanh nghiệp - Kết luận và tổng kết các nội dung thảo luận - Trả lời các câu hỏi của sinh viên - Phát phiếu yêu cầu các nội dung cần nghiên cứu trong bài 2	3h	- Lĩnh hội và đặt các câu hỏi thắc mắc - Lựa chọn được phương pháp học tập và nguồn học liệu phục vụ cho Module - Thảo luận các nội dung trong phiếu yêu cầu - Ghi chú những vấn đề cơ bản - Nêu các câu hỏi thắc mắc	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.
2	- Trình bày cấu trúc địa chỉ IP v4 - Mối quan hệ giữa Subnetmask và địa chỉ IP.	- Tổ chức thảo luận về kiến trúc Ipv4 và mối liên quan giữa địa chỉ IP và Subnetmask - Đưa ra bài tập yêu cầu sinh viên	3h	- Trình bày được cấu trúc IP v4 - Hiểu rõ mối quan hệ giữa địa chỉ IP và Subnetmask	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.

http://www.ebook.edu.vn

	- Thự hiện phân chia dải địa chỉ IP thành các Subnet có subnetmask bằng nhau và không bằng nhau - Thiết kế được lược đồ IP phù hợp cho một doanh nghiệp.	thực hiện phân chia địa chỉ IP thành các Subnet có Subnetmask bằng nhau và không bằng nhau. - Tư vấn và giải đáp các vấn đề khó khăn khi sinh viên gặp vướng mắc		cũng như cách tính toán và phân chia một dải IP thành các Subnet theo đáp ứng yêu cầu của người sử dụng - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra		
3	- Phân tích được các ưu nhược điểm của mạng không dây và mạng có dây - Trình bày được các mô hình ứng dụng mạng không dây - Trình bày được các chuẩn mạng 802.11a,b,g và đặc điểm của mỗi chuẩn. - Trình bày được chức năng của các thiết bị cơ bản trong mạng WLAN - Trình bày được khái niệm kênh truyền và SSID trong mạng WLAN	- Tổ chức thảo luận về mạng WLAn, các ưu nhược điểm và các mô hình ứng dụng - Giải đáp cho sinh viên các vấn đề khó khăn và định hướng cho sinh viên thảo luận theo đúng chủ đề - Trả lời các câu hỏi thắc mắc của sinh viên - Cấu hình thử nghiệm mạng WLAN	3h	- Thảo luận theo các nội dung giáo viên đưa ra - Nêu các câu hỏi, thắc mắc trong quá trình thảo luận - Quan sát các gợi ý và phân tích của giáo viên và để từ đó đưa ra những nhận định và ý kiến của mình về vấn đề thảo luận. - Cấu hình thử nghiệm mạng WLAN với chức năng cơ bản	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu, AccessPoint, Card mạng không dây.

http://www.ebook.edu.vn

	- Cấu hình mạng WLAN đơn giản					
4	- Trình bày được các giao thức định tuyến - So sánh định tuyến tĩnh và động, Distance Vector và Link State - Đặc điểm của định tuyến Rip v1 - Cấu hình định tuyến hệ thống sử dụng Rip v1	- Tổ chức thảo luận về định tuyến và Router - Tổ chức thảo luận về định tuyến tĩnh và định tuyến động, Distance Vector và Linkstate - Hướng dẫn sinh viên cấu hình định tuyến hệ thống mạng nội bộ - Trả lời các câu hỏi thắc mắc của sinh viên	3h	- Thảo luận về các chủ đề do giáo viên hướng dẫn - Quan sát và thực hiện cấu hình LAB định tuyến với giao thức Rip V1 - Quan sát cách gợi ý và phân tích của giáo viên để từ đó đưa ra những nhận định và ý kiến của mình về vấn đề thảo luận.	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.
5	- Thiết kế được lược đồ địa chỉ IP cho doanh nghiệp - Thực hiện cấu hình định tuyến cho các mạng bằng định tuyến tĩnh và định tuyến động với Rip v1, Rip v2 - Đánh giá được ưu nhược điểm giữa định tuyến tĩnh và định tuyến động	- Đưa trước tài liêu thảo luận cho sinh viên - Thảo luận thiết kế lược đồ địa chỉ IP - Cho sinh viên phát biểu ý kiến về các vấn đề thảo luận theo nhóm đã phân công trước - Trả lời các câu hỏi thắc mắc của sinh viên - Nhận xét, đánh giá và tổng kết vấn	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra - Thiết kế lược đồ địa chỉ IP cho doanh nghiệp và cấu	6h	Phòng học thực hành có trang bị máy tính, máy chiếu.

http://www.ebook.edu.vn

		đề thảo luận		hình định tuyến giữa các mạng		
6	- Trình bày được các khái niệm về NAT tĩnh, NAT động - So sánh ưu nhược điểm của các loại NAT - Trình bày nguyên lý hoạt động của PAT - Cấu hình PAT trên Router cho phép các IP trong LAN ra IP Public	- Tổ chức thảo luận cho sinh viên hiểu rõ khái niệm về NAT, so sánh ưu nhược điểm mỗi loại - Tổ chức thảo luận về PAT và sự cần thiết có PAT - Hướng dẫn sinh viên thực hiện bài lab cấu hình PAT - Cung cấp các tài liệu liên quan đến kiến thức NAT - Trả lời các câu hỏi thắc mắc của sinh viên trong quá trình thực hành - Nhận xét, đánh giá và tổng kết vấn đề thảo luận	3h	- Chủ động tham gia thảo luận về chủ đề do giáo viên hướng dẫn - Trình bày các nội dung mà mình đã tìm hiểu - Thực hiện tìm hiểu và cấu hình bài lab do giáo viên đưa ra	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.

http://www.ebook.edu.vn

7	- So sánh ưu nhược điểm mỗi loại NAT - Cấu hình PAT trên Router để NAT các IP trong LAN ra IP Public - Phân tích được nguyên lý hoạt động chuyển đổi địa chỉ IP	- Thảo luận thiết kế lược đồ địa chỉ IP - Cho sinh viên phát biểu ý kiến về các vấn đề thảo luận theo nhóm đã phân công trước - Chuẩn bị bài thực hành - Trả lời các câu hỏi thắc mắc của sinh viên trong quá trình thực hành - Kiểm tra tiến độ thực hiện bài tập thực hành của sinh viên - Giao công việc cho tuần tiếp theo	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra - Thực hành NAT các IP trong LAN ra IP Public	6h	Phòng học thực hành có trang bị máy tính, máy chiếu.
8	- Trình bày nguyên lý hoạt động cơ bản của Switch - Trình bày khái niệm VLAN và những ứng dụng của VLAN trong thực tiễn - Cấu hình VLAN trên Switch - Sử dụng Router định tuyến giữa các VLAN	- Tổ chức thảo luận cho sinh viên tìm hiểu nguyên lý hoạt động của Switch hỗ trợ VLAN, khái niệm VLAN và nguyên lý hoạt động của gói tin trong VLAN - Cung cấp các tài liệu liên quan đến kiến thức VLAN, định tuyến giữa các VLAN với Router - Trả lời các câu hỏi thắc mắc của sinh viên trong quá trình thực hành - Nhận xét, đánh giá và tổng kết vấn đề thảo luận	3h	- Chủ động tham gia thảo luận về chủ đề do giáo viên hướng dẫn - Trình bày các nội dung mà mình đã tìm hiểu - Quan sát cách gợi ý và phân tích của giáo viên để từ đó đưa ra những nhận định và ý kiến của mình về vấn đề thảo luận. - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.

http://www.ebook.edu.vn

9	- Trình bày nguyên lý hoạt động của VLAN và các ứng dụng VLAN trong thực tiễn - Cấu hình VLAN trên Switch hỗ trợ VLAN - Cấu hình định tuyến giữa các VLAN sử dụng Router -Ứng dụng mô hình mạng có VLAN vào thiết kế hệ thống mạng trong doanh nghiệp	- Thảo luận nguyên lý hoạt động của VLAN - Cho sinh viên phát biểu ý kiến về các vấn đề thảo luận theo nhóm đã phân công trước - Chuẩn bị bài thực hành - Trả lời các câu hỏi thắc mắc của sinh viên trong quá trình thực hành - Kiểm tra tiến độ thực hiện bài tập thực hành của sinh viên - Giao công việc cho tuần tiếp theo	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra - Thực hành bài lab chia VLAN và định tuyến giữa các VLAN sử dụng Router	6h	Phòng học thực hành có trang bị máy tính, máy chiếu, Switch hỗ trợ VLAN và Router.
10	- Phân nhóm và giao chủ đề thảo luận cho từng nhóm	- Phân nhóm sinh viên - Chuẩn bị các chủ đề thảo luận - Hướng dẫn sinh viên các bước thực hiện và nguồn tài liệu cần tìm hiểu - Nhận xét, đánh giá và tổng kết vấn đề giao chủ đề		- Nhận nhóm và báo cáo chủ đề mong muốn tìm hiểu với giáo viên nếu có - Tham gia các hoạt động do giáo viên tổ chức và đưa ra các câu hỏi thắc mắc cần giải đáp - Tìm hiểu các nguồn tài liệu do giáo viên cung cấp		Phòng học lý thuyết có trang bị máy tính, máy chiếu

http://www.ebook.edu.vn

11	- Trình bày nguyên lý phân giải tên miền của máy chủ DNS và nhiệm vụ của việc phân giải tên miền - So sánh hai giao thức http và https - Trình bày cách cấu hình máy chủ DNS và Web Server	- Thảo luận vê nhiệm vụ của viện phân giải tên miền và nguyên lý phân giải tên miền - Thảo luận các giao thức truy cập web http và https - Hướng dẫn thực hiện lab cấu hình web server và DNS server - Trả lời các câu hỏi, thắc mắc của sinh viên - Kết luận, tổng kết các nội dung thảo luận	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra - Quan sát cách gợi ý và phân tích của giáo viên để từ đó đưa ra những nhận định và ý kiến của mình về vấn đề thảo luận	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.
12	- Phân tích được nguyên lý làm việc của máy chủ DNS và web Server - Thực hiện Public một website đơn giản cho phép truy cập website với tên miền Nam - Bảo mật dữ liệu truy cập với https - Cấu hình cấp phát IP động cho các Client	- Phát tài liêu thảo luận cho sinh viên - Thảo luận về nguyên lý làm việc của DNS Server và web Server - Thảo luận về sự cần thiết xây dựng một site nội bộ cho doanh nghiệp - Giao bài thực hành - Kiểm tra tiến độ thực hiện bài tập thực hành của sinh viên - Đánh giá và gợi ý các cách làm cho sinh viên - Giao công việc cho tuần tiếp theo	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Thực hiện bài lab xây dựng một site nội bộ cho doanh nghiệp cho phép các nhân viên truy cập vào thông qua tên miền với Ip cho các Client được cấp phát động	6h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.

http://www.ebook.edu.vn

13	- Trình bày các giao thức gửi nhận mail POP3, SMTP, IMAP - Gửi và nhận thư sử dụng SMTP qua Telnet - Cấu hình Mail server phục vụ cho doanh nghiệp	- Thảo luận về nhu cầu và sự cần thiết triển khai hệ thống mail trong doanh nghiệp - Thảo luận về các giao thức gửi nhận mail POP3, SMTP, IMAP - Hướng dẫn sinh viên thực hiện Lab cấu hình triển khai hệ thống Mail với Mdaemon Server - Đánh giá và gợi ý các cách làm cho sinh viên - Nhận xét, đánh giá và tổng kết vấn đề thảo luận	3h	- Tham gia vào thảo luận, đưa ra câu hỏi - Tham gia trả lời những câu hỏi tình huống mà giáo viên đưa ra - Tham gia thực hiện bài lab do giáo viên đưa ra - Quan sát cách gợi ý và phân tích của giáo viên để từ đó đưa ra những nhận định và ý kiến của mình về vấn đề thảo luận	4h	Phòng học lý thuyết có trang bị máy tính, máy chiếu.
14	- Phân tích được nguyên lý làm việc của máy chủ Mail Server - Gửi và nhận thư sử dụng giao thức SMTP thông qua telnet - Cấu hình máy chủ Mail Server	- Tổ chức thảo luận về nguyên lý làm việc của máy chủ Mail Server - Các lệnh thực hiện nhận và gửi mail sử dụng SMTP qua telnet - Giao bài thực hành - Kiểm tra tiến độ thực hiện bài tập thực hành của sinh viên - Đánh giá và gợi ý các cách làm cho sinh viên - Giao công việc cho tuần tiếp theo	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Thực hiện bài Lab triển khai Mail Server cho doanh nghiệp	6h	Phòng học thực hành có trang bị máy tính, máy chiếu.

http://www.ebook.edu.vn

15	- So sánh ưu nhược điểm và nguyên lý hoạt động của mỗi loại Firewall - Xây dựng mô hình hệ thống mạng doanh nghiệp và thiết lập hệ thống tường lửa bảo vệ hệ thống mạng doanh nghiệp	- Tổ chức thảo luận các loại firewall và ưu nhược điểm mỗi loại - Giao bài thực hành - Kiểm tra tiến độ thực hiện bài tập thực hành của sinh viên - Đánh giá và gợi ý các cách làm cho sinh viên	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Thực hiện bài Lab triển khai tường lửa bảo vệ hệ thống mạng của doanh nghiệp	6h	Phòng thực hành Tài liệu tham khảo
16	- Trình bày các nguy cơ trên mạng - Phân biệt được các đặc điểm của Virus, Trojan, Worm - Nhận dạng các kiểu tấn công DoS - Giải mã Pass với Brute Force Attack - Các chính sách bảo mật	- Tổ chức thảo luận các nguy cơ trên mạng - Tổ chức thảo luận các laọi Virus, Worm, Trojan - Tổ chức thảo luận các kiểu tấn công DoS - Đánh giá và gợi ý các cách làm cho sinh viên - Nhận xét, đánh giá và tổng kết vấn đề thảo luận	3h	- Sinh viên đọc trước tài liệu về vấn đề thảo luận - Tham gia vào thảo luận, đưa ra câu hỏi - Thực hiện bài Lab triển khai tường lửa bảo vệ hệ thống mạng của doanh nghiệp	4h	Phòng lý thuyết có trang bị máy chiếu Tài liệu tham khảo

Thông qua khoa/ bộ môn

Giáo viên

http://www.ebook.edu.vn

http://www.ebook.edu.vn

http://www.ebook.edu.vn

http://www.ebook.edu.vn

Bài 1: Tổng quan về mạng doanh nghiệp

1.1 Giới thiệu môn học, phương pháp học

Với xu thế ứng dụng hệ thống thông tin vào tất cả các hoạt động sản xuất của các doanh nghiệp, vấn đề triển khai một hệ thống mạng khi xây dựng một doanh nghiệp là điều tất yếu. Do vậy nhu cầu nhân lực ở trình độ chuyên gia trong lĩnh vực mạng doanh nghiệp trên thị trường lao động hiện nay đang rất nhiều.

Mạng doanh nghiệp là môn học được giảng dạy sau Module Mạng cơ bản và trước Module Bảo mật mạng và Module Mạng thế hệ mới. Mục đích của môn học giúp sinh viên đạt được các kỹ năng về quản trị mạng LAN, tư vấn, thiết kế và xây dựng được một hệ thống mạng cho doanh nghiệp có quy mô nhỏ với các yêu cầu cụ thể như sau:

- Đánh giá được các hoạt động của các thiết bị phần cứng và phần mềm trong một mô hình mạng LAN, WAN sẵn có
- Tư vấn trong việc lựa chọn các thiết bị phần cứng phần mềm để thiết kế mạng LAN, WAN phù hợp với nhu cầu của doanh nghiệp nhỏ
- Đánh giá được các yêu cầu về quản lý mạng, an ninh mạng và các ràng buộc khác trong quá trình thiết kế mạng
- Thiết kế được mạng LAN trong tòa nhà phục vụ cho công tác giảng dạy và nghiên cứu
- Thiết kế được mạng WAN cho Trường học phục vụ công tác đào tạo và quản lý của Nhà trường.

Đây là môn học mang tính ứng dụng thực tiễn rất cao do vậy đòi hỏi sinh viên chuẩn bị kỹ các tài liệu và phương tiện học tập cần thiết. Gồm có

- Các phần mềm giả lập thiết kế mạng :
    - VMWare Simulator, Boson Netsim Simulator
    - ISA Server
    - Mail Exchange Server, Mail Mdeamon Server
- Sách giáo trình, Slide do giáo viên biên soạn.

http://www.ebook.edu.vn

- Sách tham khảo:

[1]. Cisco System, "CCNA Discovery1 4.0", Cisco System, 2007

[2]. Cisco System, "CCNA Discovery2 4.0", Cisco System, 2007

[3]. J.C. Mackin and Ian McLean, "Windows Server 2003 Network Infrastructure", Microsoft Press, 2005

Trong quá trình học tập sinh viên cần chủ động đọc trước tài liệu tại nhà, các tài liệu do giáo viên giao cho về nhà tự học, tham gia trao đổi kiến thức trên forum của nhà trường và các forum khác như :

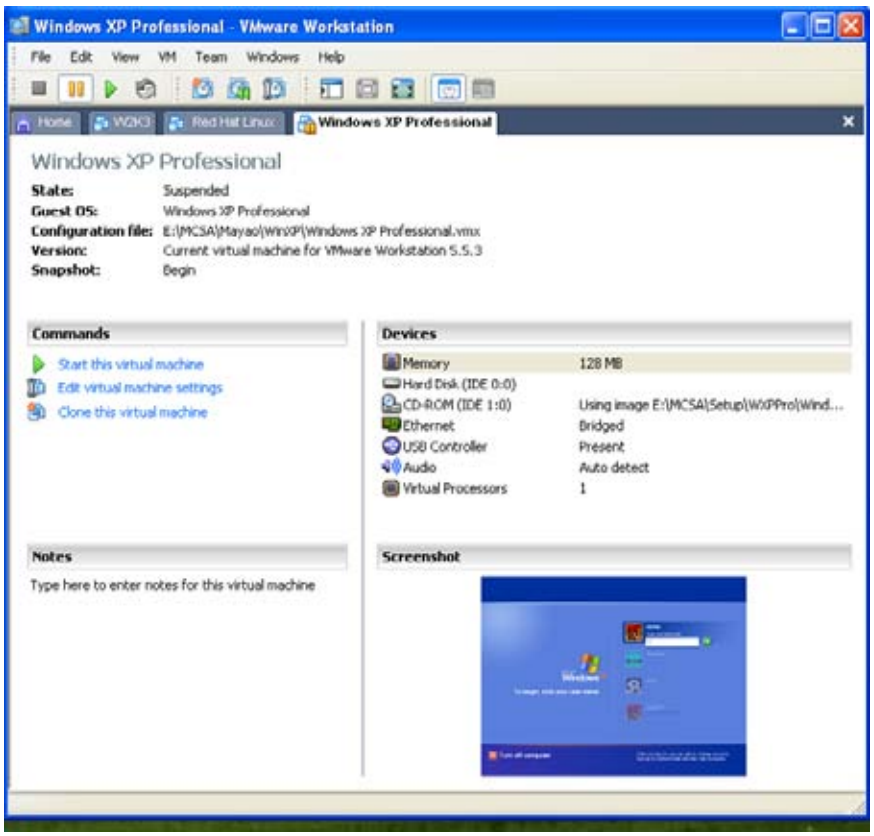
- http://quantrimang.com
- http://nhatnghe.com.vn
- http://vnpro.org.

1.2.Cách sử dụng các phần mềm thiết kế giả lập VMWare, Boson

1.2.1 Phần mềm VMWare

VMWare là phần mềm giả lập cho phép cài đặt nhiều hệ điều hành trên một máy tính có cấu hình mạnh. VMWare cho phép chúng ta cài nhiều hệ điều hành khác nhau như Window XP, Window Server 2003, Window Vista, Window Server 2008, Linux... trên cùng một máy tính và tại một thời điểm có thể cùng khởi động nhiều máy tính ảo trên một máy tính thật. Đây là một tiện ích vô cùng thú vị và cần thiết cho các sinh viên khi học về mạng máy tính và cần cấu hình một lúc nhiều hệ thống khác nhau tạo thành một hệ thống mạng ảo.

http://www.ebook.edu.vn



Trên đây là hình khi máy ảo VMWare đang cùng lúc được cài đặt và chạy cả 03 hệ điều hành gồm Window Server 2003, Window XP và Red Hat Linux để thực tập.

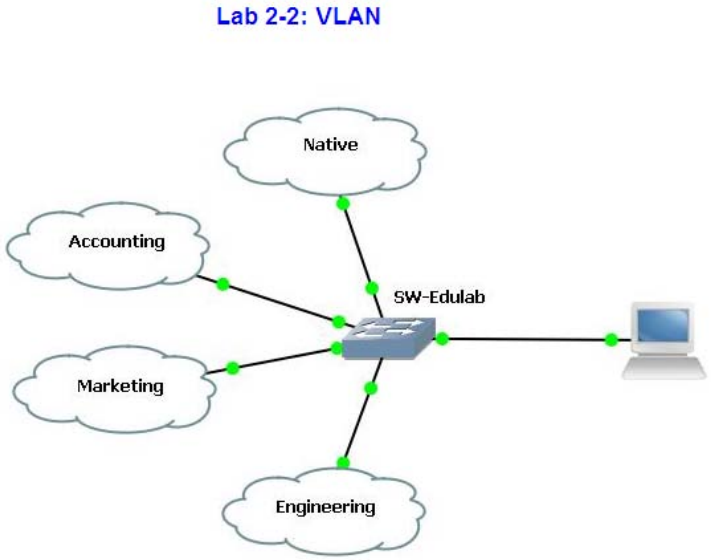
1.2.2 Phần mềm Boson Netsim

Boson Netsim là phần mềm cho phép giả lập các hoạt động của các thiết bị mạng Cisco. Với thị phần chiếm trên 70% toàn thế giới về thiết bị mạng, các thiết bị mạng của cisco luôn là lựa chọn số một cho tất cả các nhà thiết kế và triển khai hệ thống do độ ổn định và tính tin cậy cũng như sự bảo đảm của Cisco trong vấn đề an toàn thông tin. Boson Netsim sau khi cài đặt gồm 02 tiện ích con :

- Boson Netsim Design
- Boson netsim Simulator

http://www.ebook.edu.vn

Boson Netsim Design là tiện ích cho phép chúng ta thiết kế các mô hình mạng ảo khi không có điều kiện tiếp xúc với thiết bị thật. Dù vậy Boson Design có thể cho phép giả lập đến 90% các mô hình thật.

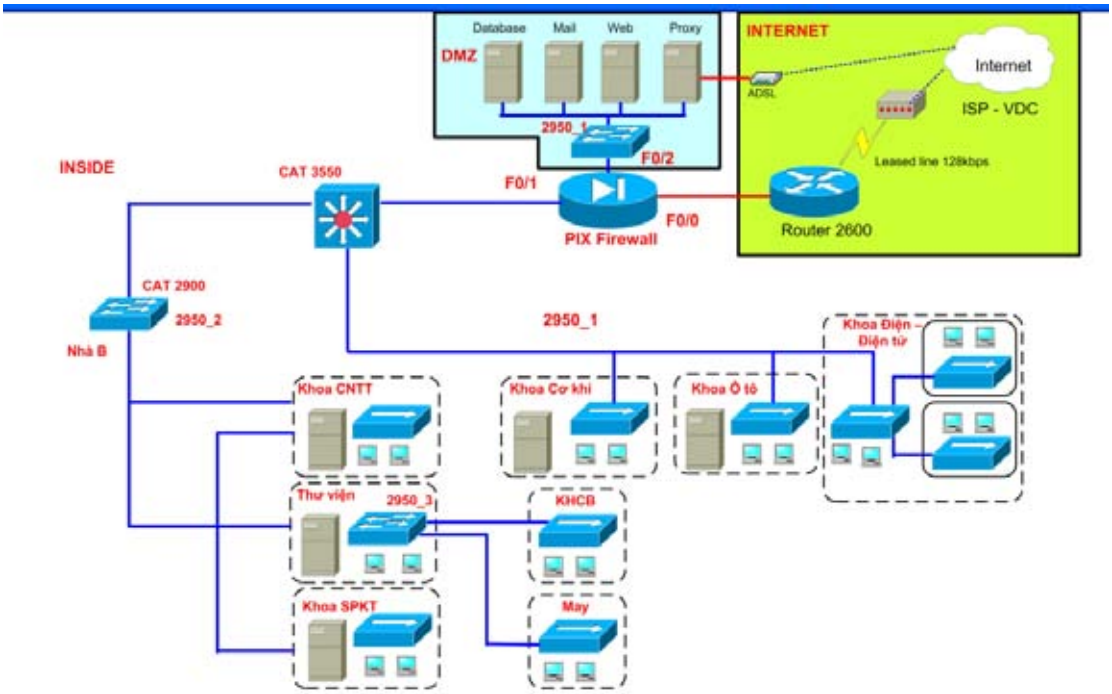


Boson Netsim được thực hiện sau khi bạn đã thiết kế hệ thống giả lập. Nhiệm vụ của nó là tạo ra môi trường giả lập để thực hiện các câu lệnh cấu hình hệ thống đã được thiết kế bởi Boson Design trên môi trường CLI (Conmand Line Interface).

1.3. Giới thiệu hệ thống mạng thực tế của một số doanh nghiệp

Giới thiệu tổng quan sơ đồ hệ thống mạng một số doanh nghiệp. Trong hình là sơ đồ hệ thống mạng Trường ĐH SPKT Hưng Yên.

http://www.ebook.edu.vn



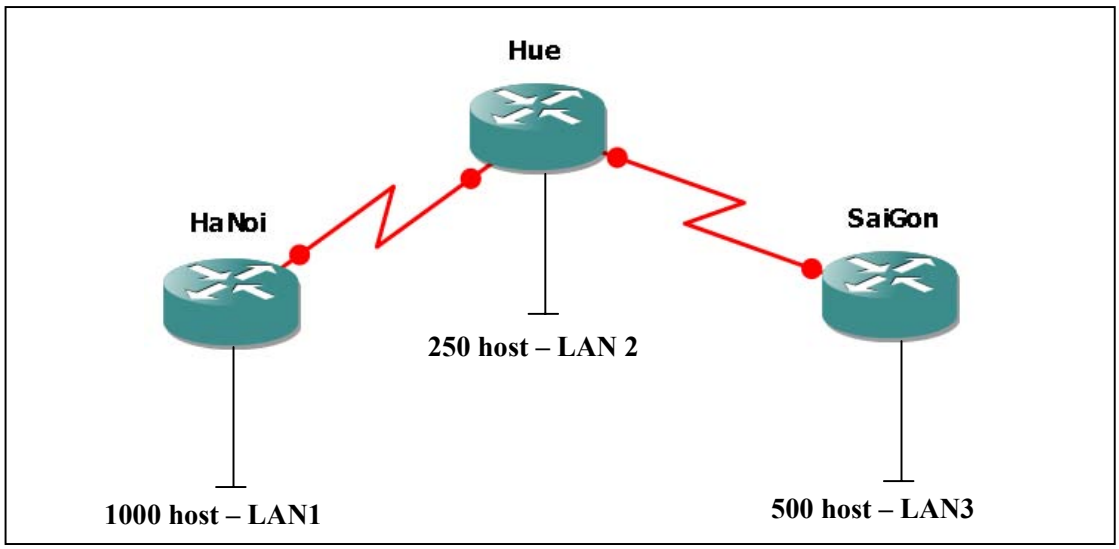
http://www.ebook.edu.vn

Bài 2: Địa chỉ mạng

2.1.Địa chỉ IP và Subnetmask

Kiến thức về địa chỉ IP và các kiến thức liên quan đến Mô hình TCP/IP, Subneting đã được trang bị tại Module Mạng cơ bản, đây là một khối kiến thức nền tảng rất quan trọng, sinh viên cần xem lại tài liệu đã học. Để ôn tập lại khối kiến thức này sinh viên cần hoàn tất bài tập sau:.

Hệ thống mạng của công ty ABC như hình vẽ, công ty được cấp phát dải đỉa chỉ 192.168.0.0/16. Thực hiện chia dải địa chỉ trên thành các Subnet thoả mãn điều kiện số host trong mỗi Subnet như trên hình với điều kiện tối ưu hoá không gian địa chỉ IP.



2.2. Các loại địa chỉ IP

2.2.1. Địa chỉ IP Private, IP Public

IP private là những IP không được định tuyến trên Internet, bao gồm các dải địa chỉ sau:

10.0.0.0 --> 10.255.255.255

172.16.0.0 --> 172.16.31.255

192.168.0.0 --> 192.168.255.255

http://www.ebook.edu.vn

Các dải địa chỉ IP còn lại của lớp A, B, C là những địa chỉ IP Public (thuộc quyền sở hữu của ISP và nhà cung cấp địa chỉ Internet)

2.2.2.Địa chỉ IP Unicast, Multicast, Broadcast

Địa chỉ Broadcast là địa chỉ quảng bá cho một Subnet theo chiều từ PC đến tất cả các PC trong cùng Subnet : PC-> all PC

Địa chỉ Unicast là địa chỉ cho phép gửi từ một địa chỉ đến một địa chỉ khác :

PC->PC

Địa chỉ Multicast là địa chỉ cho phép gửi từ một host đến một nhóm host khác: PC-> Group PC, các địa chỉ này thuộc lớp D.

2.3.Nguyên lý dịch chuyển địa chỉ IP (NAT)

2.3.1 Các thuật ngữ trong NAT

Khi một máy thực hiện NAT sẽ có cả 2 chiều out và in theo quy định của Interface

- Cisco sử dụngthuật ngữ 2 chiều này của NAT gọi là inside và outside, các nhóm địa chỉ trong NAT bao gồm:

+ **Inside local**: nhóm địa chỉ bên trong

+ **Inside global:** địa chỉ toàn cục bên trong (địa chỉ này đại diện cho các host của bạn kết nối ra ngoài Internet, chính là địa chỉ mà ISP cấp cho bạn)

+ **Outside local address :** là địa chỉ riêng của host bên ngoài mạng nội bộ

+ **Outside global address:** là địa chỉ public của host bên ngoài (vd www.yahoo.com) khi host bên trong thực hiện NAT để chuyển đổi IP, quá trình NAT như sau:

inside local ip address ----- inside global ip address ----- outside global ip address

vd: 192.168.1.2 ----- 58.187.41.17:2412 ------- 209.191.93.52

http://www.ebook.edu.vn

Chẳng hạn, khi vào trang web www.yahoo.com, đầu tiên sẽ có một request tới web server yahoo, đây chính là thực hiện NAT outside, khi bạn nhận được reply từ Yahoo server, quá trình ngược lại, lúc này chính là thực hiện NAT inside

NAT inside ngược lại với NAT outside, khi gói dữ liệu đến được thiết bị thực hiện NAT, nó xem trong bảng NAT (NAT table) và thấy rằng 58.187.41.17:2412 tương ứng với 192.168.1.2, lúc đó NAT sẽ thực hiện đổi lại địa chỉ IP của gói tin và gói dữ liệu đó sẽ đến được đúng địa chỉ của máy trong LAN của bạn.

Hoàn toàn tương tự như vậy với inbound và outbound (chỉ khác nó là thuật ngữ của Microsoft), nếu có dùng chỉ số port trong quá trình chuyển đổi thì đó là PAT, còn chỉ dùng địa chỉ IP thì lúc đó chuyển đổi là NAT

Câu lệnh **net use** thường dùng để map share trong mạng lan (tuy vậy bạn có thể map một máy khác qua Internet, nếu máy đó phép share như vậy - chẳng hạn đã NAT hết port và cho phép hết các service), kết nối trong Lan, hay kết nối qua Internet đều có thể thực hiện giống nhau, qua Internet thì chỉ bị hạn chế bởi tốc độ và chất lượng, thường là chậm hơn nhiều so với mạng LAN, tuy vậy ít ai dùng lệnh net use để map một share từ ngoài Internet, thường dùng các công cụ khác, như là FTP, HTTP... và các công cụ chia sẻ qua Internet.

2.3.2. Các kiểu NAT

Có 2 kiểu NAT cơ bản là NAT và PAT :

Giống nhau

Dùng để chuyển đổi địa chỉ IP private thành địa chỉ IP public, giúp cho máy trong mạng Lan của bạn có thể kết nối với Internet, và giúp tiết kiệm không gian của địa chỉ IP public, một cty có thể chỉ cần 1 hay vài địa chỉ IP public mà vẫn cho phép toàn bộ mạng của họ kết nối ra thế giới bên ngoài.Khác nhau :

http://www.ebook.edu.vn

NAT : Network Address Translation : chuyển đổi địa chỉ IP thành địa chỉ bên ngoài (có 2 dạng chuyển đổi là 1-1 : static, và chuyển đổi overload, khi bạn được cấp nhiều IP từ ISP)

Ví dụ: chuyển đổi 1-1 là : 192.168.0.1 <---> 186.15.4.2, còn chuyển đổi overload thì một địa chỉ bên trong sẽ được chuyển đổi thành một địa chỉ bên ngoài (nếu như địa chỉ bên ngoài chưa sử dụng)

PAT (Port Address Translation), thường là các router ADSL mặc định dùng kiểu chuyển đổi này, vì ban chỉ có 1 IP public, nếu toàn bộ LAN của bạn đều muốn kết nối ra ngoài - với một địa chỉ IP public (58.187.168.41)=> lúc đó địa chỉ bên trong sẽ được chuyển đổi thành địa chỉ đó kết hợp với chỉ số port, nếu port đó chưa sử dụng

Ví dụ: Bạn có một LAN nhỏ với dải IP : 192.168.1.x , khi đó các máy trong lan sẽ được chuyển đổi chẳng hạn với vài máy:

192.168.1.3 <-->58.187.168.41:2413

192.168.1.4 <-->58.187.168.41:2414

192.168.1.5 <-->58.187.168.41:2415

192.168.1.6 <-->58.187.168.41:2416

....

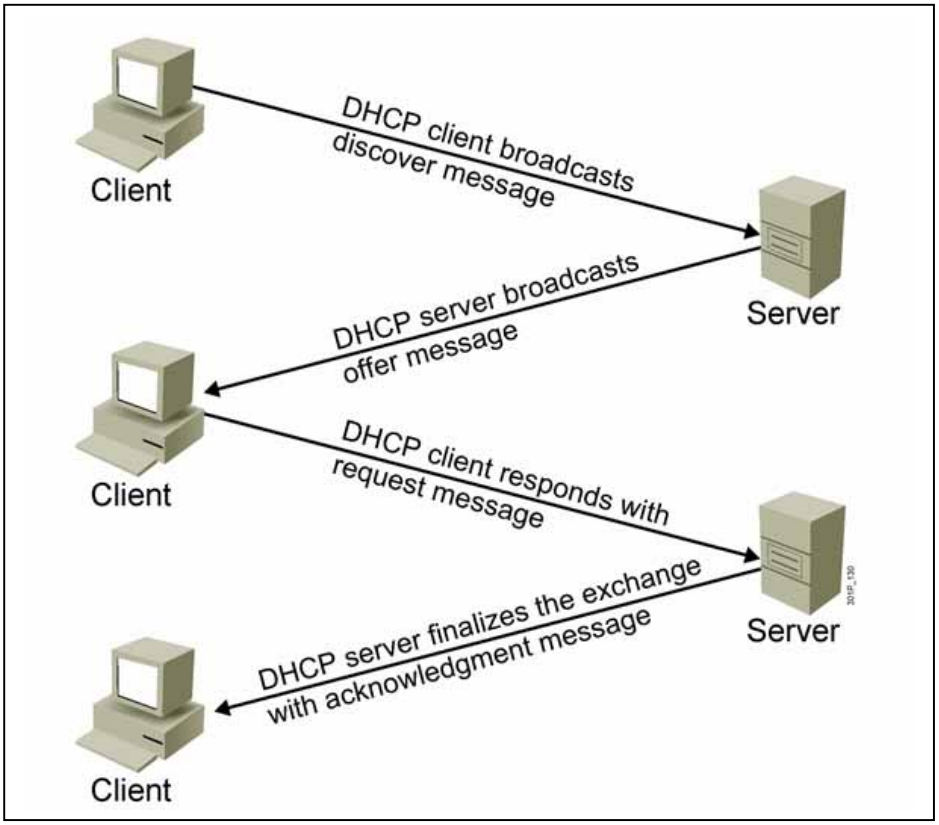
Các chỉ số port thường dùng từ 1024 đến 65535 (not well-known port), vì well-known port là chủ yếu dùng cho server, số port này đáp ứng được hầu hết các mạng LAN.

2.4. Nguyên lý thu nhận một địa chỉ IP từ DHCP Server.

Có hai cách để một host có thể thu nhận được một địa chỉ IP, người sử dụng có thể cấu hình TCP/IP bằng tay bằng cách tự nhập vào các thông số, cách thứ 2 thường được sử dụng trong các công ty vì các nhân viên văng phòng thường

http://www.ebook.edu.vn

không thể nhớ được các con số do người quản trị hệ thống mạng trong công ty cung cấp. Để host có thể thu nhận tự động một IP từ Server, bạn phải cài đặt dịch vụ DHCP trên máy chủ. Client và Server sẽ đàm phán với nhau để cấp một IP cho Client theo sơ đồ sau:



http://www.ebook.edu.vn

Bài 3: Công nghệ Wireless

3.1. Tổng quan về Wireless

Wireless hay mạng 802.11 là hệ thống mạng không dây sử dụng sóng vô tuyến, giống như điện thoại di động, truyền hình và radio. Hệ thống này hiện nay đang được triển khai rộng rãi tại nhiều điểm công cộng hay tại nhà riêng. Hệ thống cho phép truy cập Internet tại những khu vực có sóng của hệ thống này, hoàn toàn không cần đến cáp nối. Ngoài các điểm kết nối công cộng (hotspots), WiFi có thể được thiết lập ngay tại nhà riêng.

Tên gọi 802.11 bắt nguồn từ viện IEEE (Institute of Electrical and Electronics Engineers). Viện này tạo ra nhiều chuẩn cho nhiều giao thức kỹ thuật khác nhau, và nó sử dụng một hệ thống số nhằm phân loại chúng; 3 chuẩn thông dụng của Wireless hiện nay là 802.11a/b/g.

3.2. Các chuẩn Wireless

Wireless truyền và phát tín hiệu ở tần số 2.4 GHz hoặc 5GHz. Tần số này cao hơn so với các tần số sử dụng cho điện thoại di động, các thiết bị cầm tay và truyền hình. Tần số cao hơn cho phép tín hiệu mang theo nhiều dữ liệu hơn.

Wireless sử dụng chuẩn 802.11:

Chuẩn 802.11b là phiên bản đầu tiên trên thị trường. Đây là chuẩn chậm nhất và rẻ tiền nhất, và nó trở thành ít phổ biến hơn so với các chuẩn khác. 802.11b phát tín hiệu ở tần số 2.4 GHz, nó có thể xử lý đến 11 megabit/giây.

Chuẩn 802.11g cũng phát ở tần số 2.4 GHz, nhưng nhanh hơn so với chuẩn 802.11b, tốc độ xử lý đạt 54 megabit/giây. Chuẩn 802.11g nhanh hơn vì nó sử dụng mã OFDM (orthogonal frequency-division multiplexing), một công nghệ mã hóa hiệu quả hơn.

Chuẩn 802.11a phát ở tần số 5 GHz và có thể đạt đến 54 megabit/ giây. Nó cũng sử dụng mã OFDM. Những chuẩn mới hơn sau này như 802.11n còn nhanh hơn chuẩn 802.11a, nhưng 802.11n vẫn chưa phải là chuẩn cuối cùng.

http://www.ebook.edu.vn

3.3. Cấu hình mạng Wireless

3.3.1. Các thành phần thiết lập mạng WLAN

Card mạng không dây (NIC_Wireless)

Các máy tính nằm trong vùng phủ sóng WiFi cần có các bộ thu không dây, adapter, để có thể kết nối vào mạng. Các bộ này có thể được tích hợp vào các máy tính xách tay hay để bàn hiện đại. Hoặc được thiết kế ở dạng để cắm vào khe PC card hoặc cổng USB, hay khe PCI. Khi đã được cài đặt adapter không dây và phần mềm điều khiển (driver), máy tính có thể tự động nhận diện và hiển thị các mạng không dây đang tồn tại trong khu vực.

Access Point (AP)

AP là thiết bị phổ biến nhất trong WLAN chỉ đứng sau PC card không dây. Như tên của nó đã chỉ ra, AP cung cấp cho client một điểm truy cập vào mạng. AP là một thiết bị half-duplex có mức độ thông minh tương đương với một Switch Ethernet phức tạp. Hình dưới đây mô tả AP và nơi sử dụng chúng trong mạng WLAN.

http://www.ebook.edu.vn

AP có thể giao tiếp với các client không dây, với mạng có dây và với các AP khác. Có 3 mode hoạt động chính mà bạn có thể cấu hình trong một AP

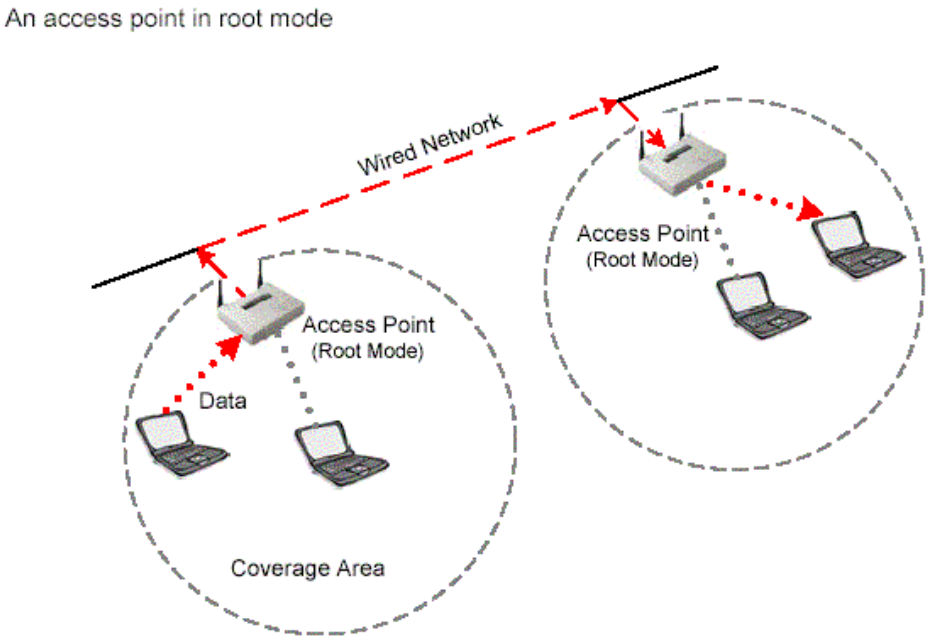
- Root mode
- Repeater mode
- Bridge mode

Root mode

Root mode được sử dụng khi AP được kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP sẽ hỗ trợ các mode khác ngoài root mode, tuy nhiên root mode là cấu hình mặc định. Khi một AP được kết nối với phân đoạn có dây thông qua cổng ethernet của nó, nó sẽ được cấu hình để hoạt động trong root mode. Khi ở trong root mode, các AP được kết nối với cùng một hệ thống phân phối có dây có thể nói chuyện được với nhau thông qua phân đoạn có dây. AP giao tiếp với nhau để thực hiện các chức năng của roaming như reassociation. Các client không dây có thể giao tiếp với các client không dây khác nằm trong những cell (ô tế bào, hay vùng phủ sóng của AP) khác nhau thông qua AP tương ứng mà chúng kết nối vào, sau đó các

http://www.ebook.edu.vn

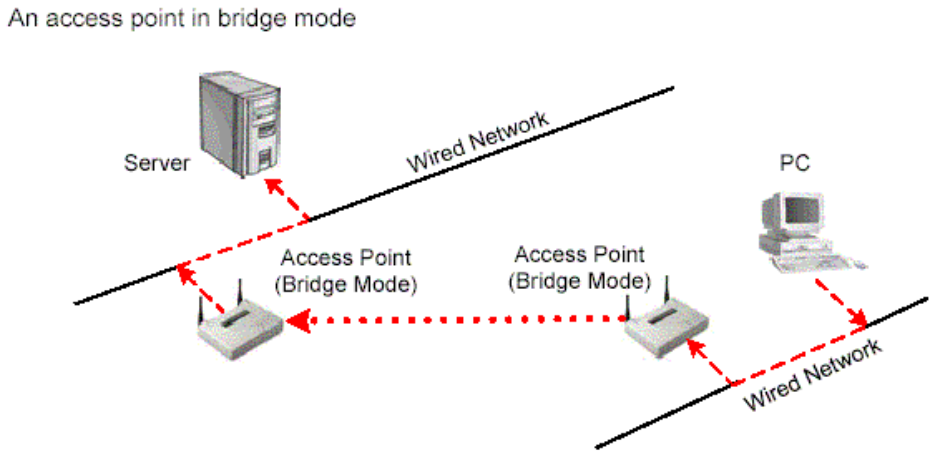
AP này sẽ giao tiếp với nhau thông qua phân đoạn có dây như ví dụ trong hình dưới.



Bridge mode

Trong Bride mode, AP hoạt động hoàn toàn giống với một Bridge không dây (sẽ được thảo luận ở phần sau). Thật vậy, AP sẽ trở thành một Bridge không dây khi được cấu hình theo cách này. Chỉ một số ít các AP trên thị trường có hỗ trợ chức năng Bridge, điều này sẽ làm cho thiết bị có giá cao hơn đáng kể. Chúng ta sẽ giải thích một cách ngắn gọn Bridge không dây hoạt động như thế nào, nhưng bạn có thể thấy từ hình dưới rằng Client không kết nối với Bridge, nhưng thay vào đó, Bridge được sử dụng để kết nối 2 hoặc nhiều đoạn mạng có dây lại với nhau bằng kết nối không dây.

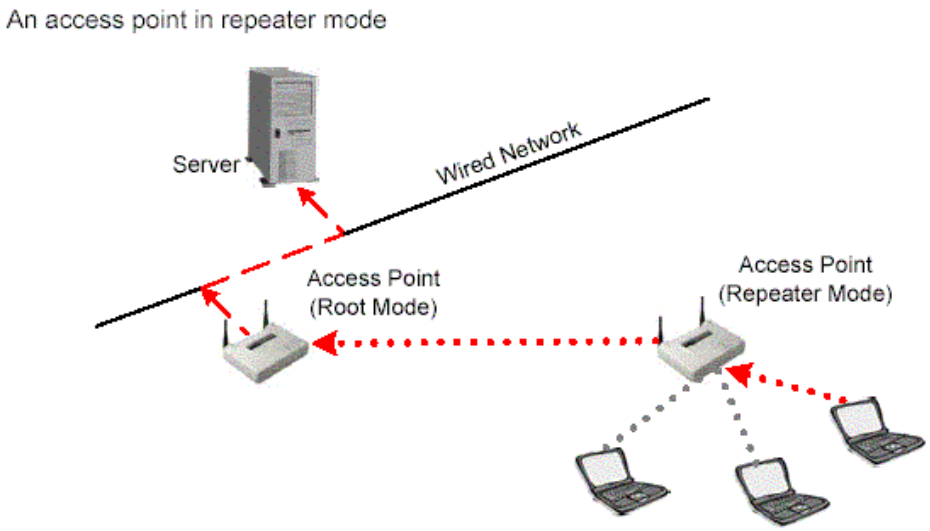
http://www.ebook.edu.vn



Repeater Mode

Trong Repeater mode, AP có khả năng cung cấp một đường kết nối không dây upstream vào mạng có dây thay vì một kết nối có dây bình thường. Như bạn thấy trong hình dưới, một AP hoạt động như là một root AP và AP còn lại hoạt động như là một Repeater không dây. AP trong repeater mode kết nối với các client như là một AP và kết nối với upstream AP như là một client. Việc sử dụng AP trong Repeater mode là hoàn toàn không nên trừ khi cực kỳ cần thiết bởi vì các cell xung quanh mỗi AP trong trường hợp này phải chồng lên nhau ít nhất là 50%. Cấu hình này sẽ giảm trầm trọng phạm vi mà một client có thể kết nối đến repeater AP. Thêm vào đó, Repeater AP giao tiếp cả với client và với upstream AP thông qua kết nối không dây, điều này sẽ làm giảm throughput trên đoạn mạng không dây. Người sử dụng được kết nối với một Repeater AP sẽ cảm nhận được throughput thấp và độ trễ cao. Thông thường thì bạn nên disable cổng Ethernet khi hoạt động trong repeater mode.

http://www.ebook.edu.vn



Các tùy chọn phổ biến (Common Options)

AP có sẵn nhiều tùy chọn phần cứng và phần mềm khác nhau. Các tùy chọn phổ biến bao gồm:

+ Anten cố định hay có thể tháo lắp.

+ Khả năng lọc cao cấp

+ Antenna có thể tháo được (Removeable hay Modular)

+ Thay đổi công suất phát

+ Các kiểu khác nhau của kết nối có dây

Fixed or Detachable Antenna

Tùy thuộc vào nhu cầu doanh nghiệp của bạn hay nhu cầu của khách hàng, bạn sẽ cần phải chọn giữa AP có anten cố định hay AP có anten có thể tháo lắp. Một AP với anten có thể tháo lắp cho bạn khả năng sử dụng các loại anten khác nhau để kết nối với AP sử dụng cable có chiều dài khác nhau tùy nhu cầu của bạn.

Ví dụ: Nếu bạn cần treo một AP ở trong nhà nhưng lại cho phép người sử dụng truy cập vào mạng ở bên ngoài thì bạn sẽ cần kết nối với cable và anten ngoài trời trực tiếp với AP và chỉ treo anten bên ngoài.

http://www.ebook.edu.vn

AP có thể có hoặc không có anten diversity (tính năng đa dạng anten). WLAN anten diversity là việc sử dụng nhiều anten với nhiều input trên một receiver duy nhất để lấy mẫu tín hiệu đến thông qua mỗi anten. Việc lấy mấu tín hiệu từ 2 anten cho phép xác định được tín hiệu input của anten nào là tốt hơn. Hai anten có thể có mức độ nhận tín hiệu khác nhau bởi vì một hiện tượng được gọi là multipath.

Advanced Filtering Capability

Các chức năng lọc MAC hay protocol có thể được bao gồm trong AP. Lọc thường được sử dụng để ngăn chặn kẻ xâm nhập vào mạng WLAN của bạn. Như là một phương thức bảo mật cơ bản, một AP có thể được cấu hình để lọc những thiết bị không nằm trong danh sách lọc MAC của AP.

Việc lọc protocol cho phép admin quyết định và điều khiển giao thức nào nên được sử dụng trong mạng WLAN.

Ví dụ: Nếu Admin chỉ muốn cho phép truy cập http trong mạng WLAN để người dùng có thể lướt web và truy cập mail dạng web (yahoo), thì việc cấu hình lọc giao thức http sẽ ngăn chận tất cả các loại giao thức khác.

Removable (Modular) Radio Card

Một số nhà sản xuất cho phép bạn thêm vào và tháo ra các radio card từ khe PCMCIA trên AP. Một số AP có thể có 2 Anten dành cho các mục đích đặc biệt. Việc có 2 Anten trong một AP cho phép một radio card có thể hoạt động như là một AP trong khi một radio card khác hoạt động như là một Bridge. Một cách khác là sử dụng mỗi radio card như là một AP độc lập. Việc có mỗi card hoạt động như là một AP độc lập cho phép gấp đôi số lượng người sử dụng trong cùng một không gian vật lý mà không cần phải mua thêm một AP khác. Khi AP được cấu hình theo cách này, mỗi radio card sẽ được cấu hình trên một kênh không chồng lên nhau, lý tưởng là kênh 1 và kênh 11.

Variable Output Power

http://www.ebook.edu.vn

Việc thay đổi công suất phát cho phép admin điều khiển công suất (miliwatt) mà AP sử dụng để truyền dữ liệu. Việc điều khiển công suất phát ra có thể là cần thiết trong một số trường hợp khi các node ở xa không thể xác định được AP. Nó cũng cho phép bạn điều khiển vùng phủ sóng của một AP. Khi công suất phát ra trên một AP tăng lên, client có thể di chuyển xa AP hơn mà không mất kết nối với AP. Tính năng này cũng hữu ích trong việc bảo mật bằng cách cho phép thay đổi kích thước của cell RF làm cho các kẻ xâm nhập không thể kết nối với mạng từ bên ngoài tòa nhà của công ty.

Ngoài AP có công suất phát thay đổi thì ta cũng có thể sử dụng AP có công suất phát cố định. Với AP có công suất phát cố định thì bạn có thể sử dụng các bộ khuếch đại, bộ suy hao, cable dài, hay anten có độ lợi cao. Điều quan trọng trong việc điều khiển công suất phát ra trên cả AP và Anten là phải tuân theo qui định của FCC

Varied Types of Connectivity

Các tùy chọn kết nối cho một AP có thể bao gồm 10BaseTx, 100BaseTx, 10/100BaseTx, 100BaseFx, Token Ring, … Bởi vì AP thường là thiết bị mà client kết nối vào và giao tiếp với backbone mạng có dây, vì thế admin phải hiểu làm thế nào để kết nối AP vào mạng có dây. Thiết kế và kết nối AP chính xác sẽ giúp ngăn chặn việc nghẽn cổ chai ở AP hoặc xa hơn có thể là trục trặc thiết bị.

Hãy xét việc sử dụng một AP chuẩn trong mạng WLAN. Nếu trong trường hợp này AP đã được xác định là sẽ đặt ở vị trí cách 150m từ wiring closet gần nhất, thì việc sử dụng cable CAT5 ethernet sẽ không thể hoạt động được. Đây là một vấn đề bởi vì ethernet qua cable CAT5 chỉ hoạt động được trong phạm vi 100m. Trong trường hợp này việc mua một AP có kết nối 100BaseFx và chạy cable quang từ wiring closet đến AP đã làm trước đó rồi thì vấn đề sẽ dễ dàng hơn.

Configuration and Management

Các phương pháp được sử dụng để cấu hình và quản lý AP sẽ khác nhau tùy nhà sản xuất. Hầu hết họ đều cung cấp ít nhất là console, telnet, USB, hay web server. Một số AP còn có phần mềm cấu hình và quản lý riêng. Nhà sản xuất cấu hình AP với một IP address trong cấu hình khởi tạo. Nếu admin cần thiết lập lại

http://www.ebook.edu.vn

thiết lập mặc định, thường thì sẽ có một nút phục vụ chức năng này nằm bên ngoài AP.

Các chức năng trên AP là khác nhau. Tuy nhiên, có một điều là không đổi: AP có càng nhiều tính năng thì giá của nó càng cao. Ví dụ, một số AP SOHO sẽ có WEP, MAC filter và thậm chí là Web server. Nếu các tính năng như xem bảng association, hỗ trợ 802.1x/EAP, VPN, Routing, Inter AP Protocol, RADIUS thì giá của nó sẽ gấp nhiều lần so với AP thông thường.

Thậm chí các tính năng chuẩn trên các AP tương thích Wi-Fi đôi khi cũng khác nhau tùy nhà sản xuất. Ví dụ 2 dòng SOHO AP khác nhau có thể hỗ trợ MAC filter nhưng chỉ một trong số chúng cho phép bạn permit hay deny cụ thể một trạm nào đó. Một số AP hỗ trợ kết nối có dây full-duplex 10/100Mbps, trong khi một số khác chỉ có kết nối 10BaseT half-duplex.

Việc hiểu tính năng nào là cần thiết cho AP trong môi trường SOHO, mid-range, hay enterprise-level là một điều quan trọng nếu bạn muốn trở thành một nhà quản trị mạng không dây. Dưới đây là danh sách các tính năng cần có cho một AP trong môi trường SOHO và Enterprise. Danh sách này không có nghĩa là đầy đủ bởi vì một số nhà sản xuất đã có nhiều tính năng mới. Danh sách này chỉ cung cấp một điểm bắt đầu để chọn AP cho SOHO.

Small Office, Home Office (SOHO)

+ Mac filter

+ WEP (64 hay 128 bit)

+ Giao diện cấu hình USB hay console

+ Giao diện cấu hình Web đơn giản

+ Các phần mềm cấu hình đơn giản

Enterprise

+ Phần mềm cấu hình cao cấp

+ Giao diện cấu hình web cao cấp

http://www.ebook.edu.vn

+ Telnet

+ SNMP

+ 802.1x/EAP

+ RADIUS client

+ VPN client và server

+ Routing (dynamic hoặc static)

+ Chức năng Repeater

+ Chức năng Bridge

Việc sử dụng sách hướng dẫn của nhà sản xuất sẽ cung cấp nhiều thông tin chi tiết cho mỗi dòng sản phẩm. Nếu bạn là một nhà quản trị mạng WLAN thì bạn nên biết môi trường hoạt động của bạn để tìm kiếm những sản phẩm thỏa mãn nhu cầu sử dụng cũng như bảo mật, sau đó hãy so sánh các tinh năng của 3 hay 4 nhà sản xuất khác nhau để chọn được thiết bị tối ưu. Quá trình này có thể tốn nhiều thời gian, nhưng thời gian sử dụng để học về các sản phẩm khác nhau trên thị trường là rất hữu ích. Các nguồn tài nguyên tốt nhất để tìm hiểu về dòng sản phẩm nào đó trên thị trường chính là website của nhà sản xuất. Khi chọn một AP, hãy nhớ chọn nhà sản xuất có hỗ trợ ngoài các tính năng và giá cả.

3.3.2. WLAN và SSID

Mạng không dây nội bộ theo chuẩn IEEE 802.11 bảo mật dùng thông số cấu hình SSID (Service Set ID). Kỹ thuật này hoạt động theo 2 chế độ

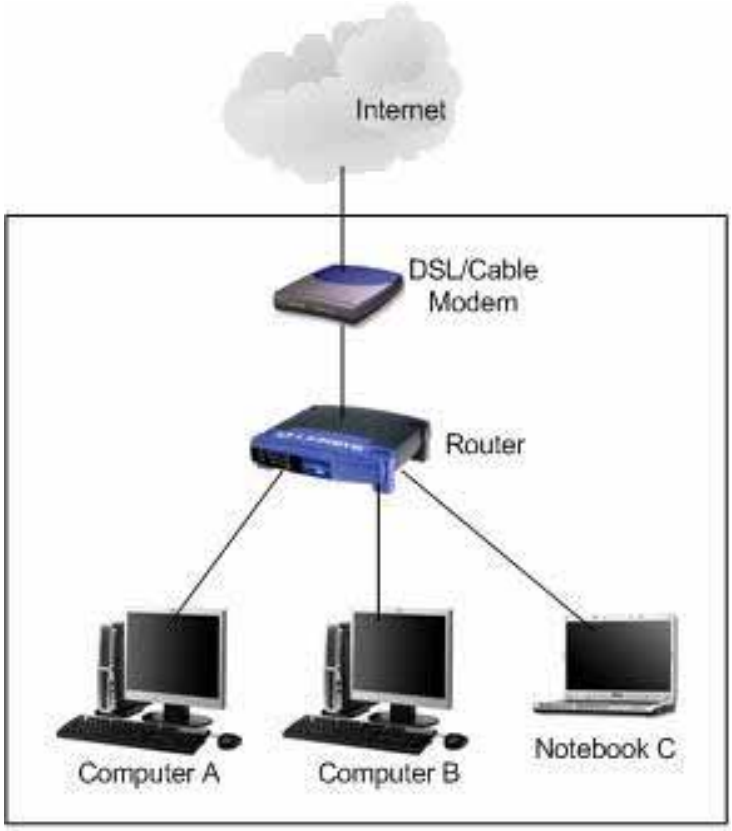
+ Chế độ không bảo mật thì theo chu kỳ thời gian Access Point gửi Broadcast SSID của mình đến các máy trạm dùng card mạng wireless.Mô hình này thường dùng cho các điểm internet công cộng (Hot Post)

+ Chế độ thứ 2 là chế độ bảo mật, Access Point không gửi SSID của mình cho máy trạm mà máy trạm phải có cùng thông số SSID (được cấu hình trong card wireless trên máy trạm) với Access Point. Mô hình này thường sử dụng cho hệ thống mạng công ty)

http://www.ebook.edu.vn

3.3.3. Cấu hình một mạng WLAN đơn giản

Sinh viên thực hiện bài lab cấu hình mạng Wireless cho văn phòng một công ty nhỏ



Yêu cầu thiết bị

- Một Modem ADSL
- Một đường Internet
- Một AccessPoint
- PC có card Wireless

Cấu hình hệ thống

- Cấu hình sơ đồ hệ thống theo hình
- Cấu hình AccessPoint Wireless cho các PC có card mạng không dây kết nối được Internet

http://www.ebook.edu.vn

Bài 4: Cơ bản về cấu hình định tuyến

4.1. Các giao thức định tuyến

Trong ngành mạng máy tính, định tuyến (tiếng Anh: routing hay routeing) là quá trình chọn lựa các đường đi trên một mạng máy tính để gửi dữ liệu qua đó. Việc định tuyến được thực hiện cho nhiều loại mạng, trong đó có mạng điện thoại, liên mạng, Internet, mạng giao thông.

Routing chỉ ra hướng, sự di chuyển của các gói (dữ liệu) được đánh địa chỉ từ mạng nguồn của chúng, hướng đến đích cuối thông qua các node trung gian; thiết bị phần cứng chuyên dùng được gọi là router (bộ định tuyến). Tiến trình định tuyến thường chỉ hướng đi dựa vào bảng định tuyến, đó là bảng chứa những lộ trình tốt nhất đến các đích khác nhau trên mạng. Vì vậy việc xây dựng bảng định tuyến, được tổ chức trong bộ nhớ của router, trở nên vô cùng quan trọng cho việc định tuyến hiệu quả.

Routing khác với bridging (bắc cầu) ở chỗ trong nhiệm vụ của nó thì các cấu trúc địa chỉ gợi nên sự gần gũi của các địa chỉ tương tự trong mạng, qua đó cho phép nhập liệu một bảng định tuyến đơn để mô tả lộ trình đến một nhóm các địa chỉ. Vì thế, routing làm việc tốt hơn bridging trong những mạng lớn, và nó trở thành dạng chiếm ưu thế của việc tìm đường trên mạng Internet.

Các mạng nhỏ có thể có các bảng định tuyến được cấu hình thủ công, còn những mạng lớn hơn có topo mạng phức tạp và thay đổi liên tục thì xây dựng thủ công các bảng định tuyến là vô cùng khó khăn. Tuy nhiên, hầu hết mạng điện thoại chuyển mạch chung (public switched telephone network - PSTN) sử dụng bảng định tuyến được tính toán trước, với những tuyến dự trữ nếu các lộ trình trực tiếp đều bị nghẽn. Định tuyến động (dynamic routing) cố gắng giải quyết vấn đề này

http://www.ebook.edu.vn

bằng việc xây dựng bảng định tuyến một cách tự động, dựa vào những thông tin được giao thức định tuyến cung cấp, và cho phép mạng hành động gần như tự trị trong việc ngăn chặn mạng bị lỗi và nghẽn.

Định tuyến động chiếm ưu thế trên Internet. Tuy nhiên, việc cấu hình các giao thức định tuyến thường đòi hỏi nhiều kinh nghiệm; đừng nên nghĩ rằng kỹ thuật nối mạng đã phát triển đến mức hoàn thành tự động việc định tuyến. Cách tốt nhất là nên kết hợp giữa định tuyến thủ công và tự động.
Những mạng trong đó các gói thông tin được vận chuyển, ví dụ như Internet, chia dữ liệu thành các gói, rồi dán nhãn với các đích đến cụ thể và mỗi gói được lập lộ trình riêng biệt. Các mạng xoay vòng, như mạng điện thoại, cũng thực hiện định tuyến để tìm đường cho các vòng (ví dụ như cuộc gọi điện thoại) để chúng có thể gửi lượng dữ liệu lớn mà không phải tiếp tục lặp lại địa chỉ đích.
Định tuyến IP truyền thống vẫn còn tương đối đơn giản vì nó dùng cách định tuyến bước kế tiếp (next-hop routing), router chỉ xem xét nó sẽ gửi gói thông tin đến đâu, và không quan tâm đường đi sau đó của gói trên những bước truyền còn lại. Tuy nhiên, những chiến lược định tuyến phức tạp hơn có thể được, và thường được dùng trong những hệ thống như MPLS, ATM hay Frame Relay, những hệ thống này đôi khi được sử dụng như công nghệ bên dưới để hỗ trợ cho mạng IP.

Thuật toán vector (distance-vector routing protocols)

Thuật toán này dùng thuật toán Bellman-Ford. Phương pháp này chỉ định một con số, gọi là chi phí (hay trọng số), cho mỗi một liên kết giữa các node trong mạng. Các node sẽ gửi thông tin từ điểm A đến điểm B qua đường đi mang lại tổng chi phí thấp nhất (là tổng các chi phí của các kết nối giữa các node được dùng).

http://www.ebook.edu.vn

Thuật toán hoạt động với những hành động rất đơn giản. Khi một node khởi động lần đầu, nó chỉ biết các node kề trực tiếp với nó, và chi phí trực tiếp để đi đến đó (thông tin này, danh sách của các đích, tổng chi phí của từng node, và bước kế tiếp để gửi dữ liệu đến đó tạo nên bảng định tuyến, hay bảng khoảng cách). Mỗi node, trong một tiến trình, gửi đến từng "hàng xóm" tổng chi phí của nó để đi đến các đích mà nó biết. Các node "hàng xóm" phân tích thông tin này, và so sánh với những thông tin mà chúng đang "biết"; bất kỳ điều gì cải thiện được những thông tin chúng đang có sẽ được đưa vào các bảng định tuyến của những "hàng xóm" này. Đến khi kết thúc, tất cả node trên mạng sẽ tìm ra bước truyền kế tiếp tối ưu đến tất cả mọi đích, và tổng chi phí tốt nhất.

Khi một trong các node gặp vấn đề, những node khác có sử dụng node hỏng này trong lộ trình của mình sẽ loại bỏ những lộ trình đó, và tạo nên thông tin mới của bảng định tuyến. Sau đó chúng chuyển thông tin này đến tất cả node gần kề và lặp lại quá trình trên. Cuối cùng, tất cả node trên mạng nhận được thông tin cập nhật, và sau đó sẽ tìm đường đi mới đến tất cả các đích mà chúng còn tới được.

Thuật toán trạng thái kết nối (Link-state routing protocols)

Khi áp dụng các thuật toán trạng thái kết nối, mỗi node sử dụng dữ liệu cơ sở của nó như là một bản đồ của mạng với dạng một đồ thị. Để làm điều này, mỗi node phát đi tới tổng thể mạng những thông tin về các node khác mà nó có thể kết nối được, và từng node góp thông tin một cách độc lập vào bản đồ. Sử dụng bản đồ này, mỗi router sau đó sẽ quyết định về tuyến đường tốt nhất từ nó đến mọi node khác.

Thuật toán đã làm theo cách này là Dijkstra, bằng cách xây dựng cấu trúc dữ liệu khác, dạng cây, trong đó node hiện tại là gốc, và chứa mọi noded khác trong mạng. Bắt đầu với một cây ban đầu chỉ chứa chính nó. Sau đó lần lượt từ tập các

http://www.ebook.edu.vn

node chưa được thêm vào cây, nó sẽ thêm node có chi phí thấp nhất để đến một node đã có trên cây. Tiếp tục quá trình đến khi mọi node đều được thêm.
Cây này sau đó phục vụ để xây dựng bảng định tuyến, đưa ra bước truyền kế tiếp tốt ưu, … để từ một node đến bất kỳ node khác trên mạng.

So sánh các thuật toán định tuyến

Các giao thức định tuyến với thuật toán vector tỏ ra đơn giản và hiệu quả trong các mạng nhỏ, và đòi hỏi ít (nếu có) sự giám sát. Tuy nhiên, chúng không làm việc tốt, và có tài nguyên tập hợp ít ỏi, dẫn đến sự phát triển của các thuật toán trạng thái kết nối tuy phức tạp hơn nhưng tốt hơn để dùng trong các mạng lớn. Giao thức vector kém hơn với rắc rối về đếm đến vô tận.

Ưu điểm chính của định tuyến bằng trạng thái kết nối là phản ứng nhanh nhạy hơn, và trong một khoảng thời gian có hạn, đối với sự thay đổi kết nối. Ngoài ra, những gói được gửi qua mạng trong định tuyến bằng trạng thái kết nối thì nhỏ hơn những gói dùng trong định tuyến bằng vector. Định tuyến bằng vector đòi hỏi bảng định tuyến đầy đủ phải được truyền đi, trong khi định tuyến bằng trạng thái kết nối thì chỉ có thông tin về "hàng xóm" của node được truyền đi. Vì vậy, các gói này dùng tài nguyên mạng ở mức không đáng kể. Khuyết điểm chính của định tuyến bằng trạng thái kết nối là nó đòi hỏi nhiều sự lưu trữ và tính toán để chạy hơn định tuyến bằng vector.

Giao thức được định tuyến và giao thức định tuyến

Sự nhầm lẫn thường xảy ra giữa "giao thức được định tuyến" và "giao thức định tuyến" ("routed protocols" và "routing protocols").

http://www.ebook.edu.vn

Giao thức được định tuyến (routed protocols hay routable protocols)

Một giao thức đã được định tuyến là bất kỳ một giao thức mạng nào cung cấp đầy đủ thông tin trong địa chỉ tầng mạng của nó để cho phép một gói tin được truyền đi từ một máy chủ (host) đến máy chủ khác dựa trên sự sắp xếp về địa chỉ, không cần biết đến đường đi tổng thể từ nguồn đến đích. Giao thức đã được định tuyến định nghĩa khuôn dạng và mục đích của các trường có trong một gói. Các gói thông thường được vận chuyển từ hệ thống cuối đến một hệ thống cuối khác. Hầu như tất cả giao thức ở tầng 3 các giao thức khác ở các tầng trên đều có thể được định tuyến, IP là một ví dụ. Nghĩa là gói tin đã được định hướng (có địa chỉ rõ ràng)giống như lá thư đã được ghi địa chỉ rõ chỉ còn chờ routing (tìm đường đi đến địa chỉ đó)

Các giao thức ở tầng 2 như Ethernet là những giao thức không định tuyến được, vì chúng chỉ chứa địa chỉ tầng liên kết, không đủ để định tuyến: một số giao thức ở tầng cao dựa trực tiếp vào đây mà không có thêm địa chỉ tầng mạng, như NetBIOS, cũng không định tuyến được.

Giao thức định tuyến (routing protocols)

Giao thức định tuyến được dùng trong khi thi hành thuật toán định tuyến để thuận tiện cho việc trao đổi thông tin giữa các mạng, cho phép các router xây dựng bảng định tuyến một cách linh hoạt. Trong một số trường hợp, giao thức định tuyến có thể tự chạy đè lên giao thức đã được định tuyến: ví dụ, BGP chạy đè trên TCP: cần chú ý là trong quá trình thi hành hệ thống không tạo ra sự lệ thuộc giữa giao thức định tuyến và đã được định tuyến.

Danh sách các giao thức định tuyến

Giao thức định tuyến trong

http://www.ebook.edu.vn

- Router Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)

Hai giao thức sau đây thuộc sở hữa của Cisco, và được hỗ trợ bởi các router Cisco hay những router của những nhà cung cấp mà Cisco đã đăng ký công nghệ:

- Interior Gateway Routing Protocol (IGRP)
- Enhanced IGRP (EIGRP)

Giao thức định tuyến ngoài

- Exterior Gateway Protocol (EGP)
- Border Gateway Protocol (BGP)
- Constrained Shortest Path First (CSPF)

Thông số định tuyến (Routing metrics)

Một thông số định tuyến bao gồm bất kỳ giá trị nào được dùng bởi thuật toán định tuyến để xác định một lộ trình có tốt hơn lộ trình khác hay không. Các thông số có thể là những thông tin như băng thông (bandwidth), độ trễ (delay), đếm bước truyền, chi phí đường đi, trọng số, kích thước tối đa gói tin (MTU - Maximum transmission unit), độ tin cậy, và chi phí truyền thông. Bảng định tuyến chỉ lưu trữ những tuyến tốt nhất có thể, trong khi cơ sở dữ liệu trạng thái kết nối hay topo có thể lưu trữ tất cả những thông tin khác.

Router dùng tính năng phân loại mức tin cậy (administrative distance -AD) để chọn đường đi tốt nhất khi nó "biết" hai hay nhiều đường để đến cùng một đích theo các giao thức khác nhau. AD định ra độ tin cậy của một giao thức định tuyến. Mỗi giao thức định tuyến được ưu tiên trong thứ tự độ tin cậy từ cao đến

http://www.ebook.edu.vn

thấp nhất có một giá trị AD. Một giao thức có giá trị AD thấp hơn thì được tin cậy hơn, ví dụ: OSPF có AD là 110 sẽ được chọn thay vì RIP có AD là 120.

Bảng sau đây cho biết sự sắp xếp mức tin cậy được dùng trong các router Cisco

Giao thức	Administrative distance
Nối trực tiếp	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Không xác định	255

Các lớp giao thức định tuyến

Dựa vào quan hệ của các dòng router với các hệ thống tự trị, có nhiều lớp giao thức định tuyến như sau:

http://www.ebook.edu.vn

- **Giao thức định tuyến trong mạng Ad-hoc** xuất hiện ở những mạng không có hoặc ít phương tiện truyền dẫn.
- **Interior Gateway Protocols (IGPs)** trao đổi thông tin định tuyến trong một AS. Các ví dụ thường thấy là:
  - IGRP (Interior Gateway Routing Protocol)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - OSPF (Open Shortest Path First)
  - RIP (Routing Information Protocol)
  - IS-IS (Intermediate System to Intermediate System)

Chú ý: theo nhiều tài liệu của Cisco, EIGRP không phân lớp như giao thức trạng thái kết nối.

- Exterior Gateway Protocols (EGPs) định tuyến giữa các AS. EGPs gồm:
  - EGP (giao thức cũ để nối mạng Internet trước đây, bây giờ đã lỗi thời)
  - BGP (Border Gateway Protocol: phiên bản hiện tại, BGPv4, có từ khoảng năm 1995)

4.2. Giao thức định tuyến nội vùng RIP

RIP (tiếng Anh: Routing Information Protocol) là một giao thức định tuyến nội vùng sử dụng thuật toán định tuyến Distance-vector.

Các đặc điểm:

- Là giao thức định tuyến theo vector khoảng cách (Distance Vector) , tức là RIP sẽ cập nhật toàn bộ hoặc 1 phần bảng định tuyến của mình cho các Router láng giềng kết nối trực tiếp với nó . Bảng định tuyến gồm các thông

http://www.ebook.edu.vn

tin như : địa chỉ của router kế tiếp trên đường đi , tổng chi phí từ chính router đó đến mạng đích…

- Là giao thức định tuyến theo kiểu classful (tức định tuyến theo lớp địa chỉ) vì rip k mang theo thông tin subnet mask đi kèm (FLSM)
- Chọn đường đi dựa vào thông số định tuyến là hop count (số router) hay còn nói metric của RIP là hop count, dùng simple routing metric. Chính vì thế mà đôi lúc có 1 số đường mà rip chọn k phải là đường tối ưu nhất đến mạng đích. Nếu 1 packet đến mạng đích có số lượng hop vượt quá 15 thì nó sẽ bị drop. Do cái tính khó chịu này của RIP nên mới nó được cho là khó mở rộng , phù hợp với mạng nhỏ (nhưng mèo thấy nó không nhỏ đâu đối với vn)
- Update định kì 30s (thay đổi bằng câu lệnh update-timers) . Ngoài ra RIP còn các giá trị thời gian khác như invalid , holdown và flush timer set bằng câu lệnh sau timers basic update invalid holdown flush
- Administrative Distance (AD) = 120 , thông số này càng nhỏ thì càng ưu tiên
- Load balacing (chia tải) maximum là 6 đường , default là 4 đường có thể set lại bằng câu lệnh maximum-paths . Việc chia tải ở đây đòi hỏi các đường phải có chi phí (cost)bằng nhau mới được nhé hay còn gọi là equal-cost mà cost của rip là hop count vì thế nếu tốc độ của 2 đường khác nhau như 1 đường là dial-up và 1 đường là T1 thì cũng như vậy thôi.

Các cơ chế chống Loop

- Count to infinity (định nghĩa giá trị tối đa) khi trong mạng xảy ra loop , gói tin chạy lòng vòng hoài trong mạng cho đến khi có tiến trình nào đó cắt đứt vòng lặp gọi là đếm vô hạn .Với rip metric là hop count vì thế mỗi khi thông tin cập nhật được “đi qua” 1 router thì số lượng hop sẽ tăng lên 1. Bản thân

http://www.ebook.edu.vn

rip sẽ khắc phục tình trạng đếm đến vô hạn bằng cách cứ thông số định tuyến mà vượt quá 15 thì packet đó sẽ bị drop

- Route poisioning (poison reverse): thường thì khi 1 đường mạng nào đó có thông số định tuyến tăng dần lên thì đã bị tình nghi là loop rồi nhé . Lúc đó router sẽ phát đi 1 thông tin poison reverse để xóa đi đường đó và cho nó vào trạng thái holddown .

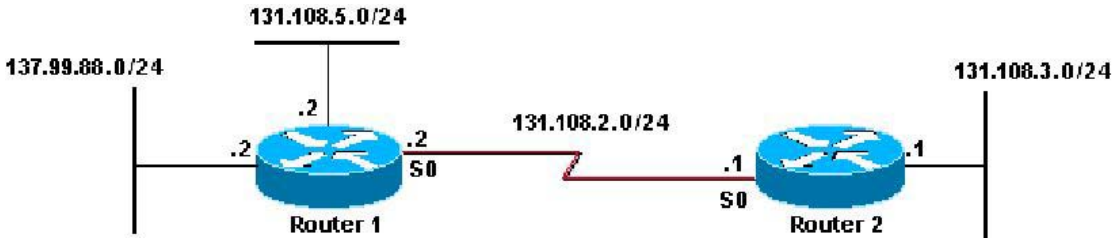
  Triggered update (câu lệnh ip rip triggered) : vì rip cập nhật thông tin định tuyến 30s 1 lần vì thế khi có 1 mạng thay đổi thì phải chờ đến hết 1 chu kỳ 30s thì các router khác trong mạng mới biết được sự thay đổi đó. Cơ chế triggered update này giúp router cập nhật ngay sự thay đổi trong mạng mà k cần phải đợi hết chu kỳ đó. Kết hợp cơ chế này cùng poison reverse là ok.
- Holdown timer :khi router A nhận được 1 thông tin về 1 mạng X từ 1 router B nói rằng mạng X bị đứt thì router A sẽ set holddown timer. Trong suốt thời gian holddown này , router sẽ không cập nhật bất kì thông tin định tuyến nào về mạng X từ các router khác trong mạng , chẳng hạn router C cập nhật cho A nói , mạng X còn sống thì router A sẽ phớt lờ thông tin đó đi. Trừ phi router B nói với nó là mạng X sống lại rồi thì router A mới cập nhật nhé
- Split Horizon tức là khi router gửi thông tin định tuyến ra 1 interface , thì router sẽ k gửi ngược trở lại các thông tin định tuyến mà nó học được từ cổng đó . Cơ chế này chỉ tránh được loop giữa 2 router
- Kết hợp Split horizon với poision reverse : nếu đọc phớt qua , các bạn sẽ thấy 2 anh này trái ngược nhau , chắc là 2 cơ chế này đố kị nhau đây . Nhưng thực ra khi kết hợp lại sẽ hữu dụng trong khi mạng gặp sự cố , hình như mặc định là nó k dùng cơ chế này hay nói cách khác 2 cơ chế này tách riêng không làm chung vì sợ làm tăng kích thước của bảng định tuyến. Khi router A học được

http://www.ebook.edu.vn

1 mạng X bị die từ router B từ cổng S0/0 chẳng hạn , thì A sẽ advertise lại mạng X đó ra cổng s0/0 tiếp tục với hop count là 16

Quá trình gửi và nhận thông tin định tuyến

Mô hình minh họa



Lúc gửi thông tin định tuyến: Trước khi gửi update (về đường mạng 131.108 và 131.99) cho router 2 thì router 1 phải check rằng

- Đường mạng 131.108.5.0/24 có cùng major net với 131.108.2.0/24 hay không?
- Trong trường hợp này là có, Router 1 mới check típ 131.108.5.0 và 131.108.2.0 có cùng subnet mask hay không?
- Nếu trùng, Router 1 sẽ quảng bá đường mạng này.
- Nếu k trùng , router 1 sẽ drop packet đó
- Đường mạng 137.99.88.0/24 có cùng major net với 131.108.2.0/24 hay không?
- Nếu không thì router 1 sẽ làm động tác là tổng hợp (summarize) 137.99.88.0/24 tại major net boundary thành 137.99.0.0 và quảng bá nó.

Trong mô hình này thì ta nhận được kết quả như thế này trong khi thi hành lệnh debug ip rip

http://www.ebook.edu.vn

```
RIP: sending v1 update to 255.255.255.255 via Serial0 (131.108.2.2)
     subnet 131.108.5.0, metric 1
     network 137.99.0.0, metric 1
```

Nhận update :

Lúc này debug ip rip ngay trên router 2 thì ta thấy như thế này

```
RIP: received v1 update from 131.108.2.2 on Serial0
     131.108.5.0 in 1 hops
     137.99.0.0 in 1 hops
```

Router 2 sẽ check để xem nên apply mask nào cho đường mạng 131 và 137 này đây

131.108.5.0 và 131.108.2.0(xét trên interface mà nhận update vào) có cùng 1 major net k?

Nếu có thì apply thẳng mask của interface mà nó nhận update, trong trường hợp này là apply /24). Nếu mạng được quảng bá tức 131.108 mà /32 thì router 2 sẽ apply /32 và típ tục quảng bá cho các router khác là /32(điều này nó khác với IGRP nhé)

131.108.5.0 và 137.99.0.0 có cùng major net k?

Nếu không xét tiếp, trong bảng định tuyến có subnet nào hay mạng con của major net này mà nó học từ các interface khác không?

Nếu không thì router 2 sẽ apply thẳng classful subnet mask là /16 luôn vì 137 là mạng lớp B. Chú ý ở đây nó sẽ apply host mask nếu như giữa 2 router là 1 unnumbered link và chứa thông tin về subnet (tức là khi đó các bit trong phần portion của network được set).

Ngược lại thì router sẽ ignore thông tin định tuyến này đi

Lúc này show ip route thử xem

http://www.ebook.edu.vn

```
R       137.99.0.0/16 [120/1] via 131.108.2.2, 00:00:07, Serial0
     131.108.0.0/24 is subnetted, 3 subnets
R       131.108.5.0 [120/1] via 131.108.2.2, 00:00:08, Serial0
C       131.108.2.0 is directly connected, Serial0
C       131.108.3.0 is directly connected, Ethernet0
```

Do ripv2 phát triển từ ripv1 nên nó cũng còn thừa hưởng những đặc điểm của ripv1 như :

- Là giao thức định tuyến theo vector khoảng cách
- Cost của nó là hop count . Ở đây cho mèo sử dụng từ cost thay cho metric nhé . Vì nếu lỡ có ai xem qua BGP rùi thì sẽ bị lộn 1 tí . Maximum hop count vẫn là 15
- Cũng sử dụng các cơ chế chống lặp vòng như ripv1

Nhưng Ripv2 có các điểm cải tiến khác version 1 như

- Nhiều thông tin định tuyến hơn như có gửi subnet mask đi kèm với địa chỉ mạng trong thông tin mà nó update.
- Hỗ trợ VLSM (Variable length subnet mask) subnet mask khác nhau, CIDR (Classless Interdomain Routing) và route summarization
- Có cơ chế xác thực thông tin khi nhận được bằng plaintext hoặc mã hóa MD5
- Gởi thông tin định tuyến theo địa chỉ multicast là 224.0.0.9 bằng với 01-00-5E-00-00-09

http://www.ebook.edu.vn

4.3. Giao thức định tuyến động OSPF

Tổng Quan Về OSPF

OSPF là một giao thức định tuyến theo trạng thái đường liên kết được triển khai dựa trên các chuẩn mở. OSPF được mô tả trong nhiều chuẩn của IETF (Internet Engineering Task Force). Chuẩn mở ở đây có nghĩa là OSPF hoàn toàn mở với công cộng, không có tính độc quyền.

Nếu so sánh với RIPv1 và RIPv2 là một giao thức nội thì IGP tốt hơn vì khả năng mở rộng của nó. RIP chỉ giới hạn trong 15 hop, hội tụ chậm và đôi khi còn chọn đường có tốc độ chậm vì khi quyết định chọn đường nó không quan tâm đến các yếu quan trọng khác như băng thông chẳng hạn. OSPF khắc phục được các nhược điểm của RIP vì nó là một giao thức định tuyến mạnh, có khả năng mởi rộng, phù hợp với các hệ thống mạng hiện đại. OSPF có thể cấu hình đơn vùng để sử dụng cho các mạng nhỏ.

So Sánh OSPF Với Giao Thức Định Tuyến Theo Distance Vector

Router định tuyến theo trạng thái đường liên kết có một cơ sở đầy đủ về cấu trúc hệ thống mạng. Chúng chỉ thực hiện trao đổi thông tin về trạng thái đường liên kết lúc khởi động và khi hệ thống mạng có sự thay đổi. Chúng không phát quảng bá bảng định tuyến theo định kỳ như các router định tuyến theo distance vector. Do đó, các router định tuyến theo trạng thái đường liên kết sử dụng ít băng thông hơn cho hoạt động duy trì bảng định tuyến.

RIP phù hợp với các mạng nhỏ và đường tốt nhất đối với RIP là đường có số hop ít nhất. OSPF thì phù hợp với mạng lớn, có khả năng mở rộng, đường đi tốt nhất của OSPF được xác định dựa trên tốc độ của đường truyền. RIP cũng như các giao thức định tuyến theo distance vector khác đều sử dụng thuật toán chọn

http://www.ebook.edu.vn

đường đơn giản. Còn thuật toán SPF thì phức tạp. Do đó, nếu router chạy theo giao thức định tuyến theo distance vector thì sẽ ít tốn bộ nhớ và cần năng lực xử lý thấp hơn so với khi chạy OSPF.

- OSPF chọn đường dựa trên chi phí được tính từ tốc độ của đường truyền. Đường truyền có tốc độ càng cao thì chi phí OSPF tương ứng càng thấp.
- OSPF chọn đường tốt nhất từ cây SPF.
- OSPF bảo đảm không bị định tuyến lặp vòng. Còn giao thức định tuyến theo distance vector vẫn có thể bị loop.

Nếu một kết nối không ổn định, chập chờn, việc phát liên tục các thông tin về trạng thái của đường kiên kết này sẽ dẫn đén tình trạng các thông tin quảng cáo không đồng bộ làm cho kết quả chọn đường của các router bị đảo lộn.

OSPF giải quyết được các vấn đề sau:

- Tốc độ hội tụ.
- Hỗ trợ VLSM (Variable Length Subnet Mask).
- Kích cỡ mạng.
- Chọn đường.
- Nhóm các thành viên.

Trong một hệ thống mạng lớn, RIP phải mất ít nhất vài phút mới có thể hội tụ được vì mỗi router chỉ trao đổi bảng định tuyến với các router láng giềng kết nối trực tiếp với mình mà thôi. Còn đối với OSPF sau khi đã hội tụ vào lúc khởi động, khi có thay đổi thì việc hội tụ sẽ rất nhanh vì chỉ có thông tin về sự thay đổi được phát ra cho mọi router trong vùng.

OSPF có hỗ trợ VLSM nên nó được xem là một giao thức định tuyến không theo lớp địa chỉ. RIPv1 không hỗ trợ VLSM, nhưng RIPv2 thì có.

http://www.ebook.edu.vn

Đối với RIP, một mạng đích cách xa hơn 15 router xem như không thể đến được vì RIP có số lượng hop giới hạn là 15. Điều này làm kích thước mạng của RIP bị giới hạn trong phạm vi nhỏ. OSPF thì không giới hạn về kích thước mạng, nó hoàn toàn có thể phù hợp với mạng vừa và lớn.

Khi nhận được từ router láng giềng các báo cáo về số lượng hop đến mạng đích, RIP sẽ cộng thêm 1 vào thông số hop này và dựa vào số lượng hop đó để chọn đường đến mạng đích. Đường nào có khoảng cách ngắn nhất hay nói cách khác là có số lương hop ít nhất sẽ là đường tốt nhất đối với RIP. Nhận xét thấy thuật toán chọn đường như vậy là rất đơn giản và không đòi hỏi nhiều bộ nhớ và năng lực xử lý của router. RIP không hề quan tâm đến băng thông đường truyền khi quyết định chọn đường.

OSPF thì chọn đường dựa vào chi phí được tính từ băng thông của đường truyền. Mọi OSPF đều có thông tin đầy đủ về cấu trúc của hệ thống mạng và dựa vào đó để chọn đường đi tốt nhất. Do đó, thuật toán chọn đường này rất phức tạp, đòi hỏi nhiều bộ nhớ và năng lực xử lý của router cao hơn so với RIP.

RIP sử dụng cấu trúc mạng dạng ngang hàng. Thông tin định tuyến được truyền lần lượt cho mọi router trong cùng một hệ thống RIP. Còn OSPF sử dụng khái niệm về phân vùng. Một mạng OSPF có thể chia các router thành nhiều nhóm. Bằng cách này, OSPF có thể giới hạn lưu thông trong từng vùng. Thay đổi trong vùng này không ảnh hưởng đến hoạt động của các vùng khác. Cấu trúc phân lớp như vậy cho phép hệ thống mạng có khả năng mở rộng một cách hiệu quả.

Thuật Toán Chọn Đường Ngắn Nhất

Theo thuật toán này, đường tốt nhất là đường có chi phí thấp nhất. Thuật toán được sử dụng là Dijkstra, thuật toán này xem hệ thống mạng là mọt tập hợp các nodes được kết nối với nhau bằng kết nối point-to-point. Mỗi kết nối này có một

http://www.ebook.edu.vn

chi phí. Mỗi nodes có một tên. Mỗi nodes có đầy đủ cơ sở dữ liệu về trạng thái của các đường liên kết. Do đó, chúng có đầy đủ thông tin về cấu trúc vật lý của hệ thống mạng. Tất cả các cơ sở dữ liệu này điều giống nhau cho mọi router trong cùng một vùng.

Các Loại Mạng OSPF

Các OSPF phải thiết lập mối quan hệ láng giềng để trao đổi thông tin định tuyến. Trong mỗi mạng IP kết nối vào router. Nó đều cố gắng ít nhất là trở thành một láng giềng hoặc là một láng giềng thân mật với một router khác, router OSPF quyết định chọn router nào làm láng giềng thân mật là tùy thuộc vào từng loại mạng kết nối với nó. Có một số router có thể cố gắng trở thành láng giềng thân mật với mọi router láng giềng khác. Có một số router khác lại có thể chỉ cố gắng trở thành láng giềng thân mật với một hoặc hai router láng giềng thôi. Một khi mối quan hệ láng giềng thân mật đã được thiết lập giữa hai láng giềng với nhau thì thông tin về trạng thái đường liên kết mới được trao đổi.

Giao thức OSPF nhận biết các loại mạng sau:

- Mạng quảng bá đa truy cập, ví dụ mạng Ethernet.
- Mạng point-to-point.
- Mạng không quảng bá đa truy cập (NBMA – NonBroadcast Multil-Access), ví dụ Frame Relay.
- Mạng Point-to-Multipoint có thể được nhà quản trị mạng cấu hình cho một cổng của router.

Trong mạng đa truy cập không thể biết được là có bao nhiêu router sẽ có thể được kết nối vào mạng.

Trong mạng point-to-point thì chỉ có hai router được kết nối với nhau.

http://www.ebook.edu.vn

Trong mạng quảng bá đa truy cập có rất nhiều router kết nối vào. Nếu mỗi router đều thiết lập mối quan hệ thân mật với mọi router khác và thực hiện trao đổi thông tin về trạng thái đường liên kết với mọi router láng giềng thì sẽ quá tải. Nếu có 10 router thì sẽ cần 45 mối liên hệ thân mật, nếu có n router thì sẽ có n*(n-1)/2 mối quan hệ láng giềng cần thiết lập.

Giải pháp cho vấn đề quá tải trên là bầu ra một router làm đại diện (DR-Designated Router). Router này sẽ thiết lập mối quan hệ thân mật với mọi router khác trong mạng quản bá. Mọi router còn lại sẽ chỉ gởi thông tin về trạng thái đường liên kết cho DR. Sau đó DR sẽ gởi các thông tin này cho mọi router khác trong mạng bằng địa chỉ multicast 224.0.0.5 DR đóng vai trò như một người phát ngôn chung.

Việc bầu DR rất có hiệu quả nhưng cũng có một nhược điểm. DR trở thành một tâm điểm nhạy cảm đối với sự cố. Do đó, cần có một router thứ hai được bầu ra để làm đại diện dự phòng (BDR – Backup Designated Router), router này sẽ đảm trách vai trò của DR nếu DR bị sự cố. Để đảm bảo cả DR và BDR đều nhận được thông tin về trạng thái đường liên kết từ mọi router khác trong cùng một mạng, địa chỉ multicast 224.0.0.6 cho các router đại diện.

Trong mạng point-to-point chỉ có 2 router kết nối với nhau nên không cần bầu ra DR và DBR. Hai router này sẽ thiết lập mối quan hệ láng giềng thân mật với nhau.

Loại Mạng Các Đặc Tính Bầu DR

Broadcast, Multi-Access Ethernet,ToKen Ring,FĐI	Có
NonBroadcast Multi-Access Frame Relay,X25,SMDS	Có
Point-to-Point PPP,HDLC	Không
Point-to-Multipoint Được cấu hình bởi Administrator	Không

http://www.ebook.edu.vn

Giao Thức OSPF Hello

Khi router bắt đầu khởi động tiến trình định tuyến OSPF trên một cổng nào đó thì nó sẽ gởi một gói hello ra cổng đó và tiếp tục gởi hello theo định kỳ. Giao thức hello đưa ra các nguyên tắc quản lý việc trao đổi các gói OSPF hello.

Ở lớp 3 của mô hình OSI, gói hello mang địa chỉ multicast 224.0.5.0 địa chỉ này chỉ đến tất cả các OSPF router. OSPF router sử dụng gói hello để thiết lập một quan hệ láng giềng thân mật mới và để xác định là router láng giềng có còn hoạt động hay không. Mặc định hello được gởi đi 10 giây một lần trong mạng quảng bá đa truy cập và mạng Point-to-Point. Trên cổng nói vào mạng NBMA, ví dụ như Frame Relay, chu trình mặc định của hello là 30 giây.

Trong mạng đa truy cập, giao thức hello tiến hành bầu DR và BDR.

Mặc dù gói hello rất nhỏ nhưng nó cũng bao gồm cả phần header của gói OSPF. Cấu trúc của phần header trong gói OSPF được thể hiện như hình sau. Nếu gói hello thì trường Type sẽ có giá trị là một.

Các thông điệp Hello trong OSPF thực hiện ba chức năng chính:

- Tìm ra những router chạy OSPF khác trên cùng một mạng chung.
- Kiểm tra sự tương thích trong các thông số cấu hình.
- Giám sát tình trạng của láng giềng để phản ứng nếu láng giềng bị fail.

Để tìm ra những router láng giềng, OSPF lắng nghe những thông điệp Hello được gửi đến 224.0.0.5. Đây là địa chỉ multicast tượng trưng cho tất cả các router OSPF, trên bất cứ cổng nào đã bật OSPF. Các gói Hello sẽ lấy nguồn từ địa chỉ primary trên cổng, nói cách khác, Hello không dùng địa chỉ phụ. (OSPF

http://www.ebook.edu.vn

router sẽ quảng bá các địa chỉ phụ nhưng nó sẽ không gửi Hello từ những địa chỉ này và không bao giờ hình thành mối quan hệ dùng địa chỉ phụ.

Khi hai router tìm ra nhau thông qua các gói Hello, các router thực hiện các phép kiểm tra các thông số như sau:

- Các router phải vượt qua tiến trình xác thực.
- Các router phải trong cùng địa chỉ mạng primary, phải có cùng subnetmask.
- Phải trong cùng OSPF area.
- Phải có cùng kiểu vùng OSPF.
- Không có trùng RID.
- OSPF Hello và Deadtimer phải bằng nhau.

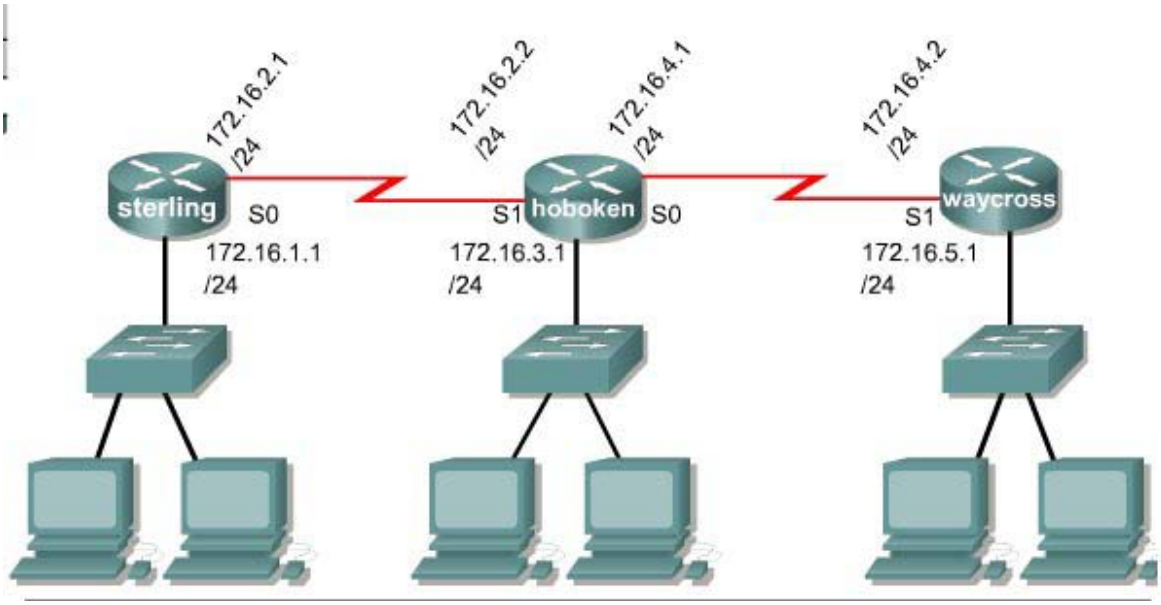
Nếu bất kỳ điều kiện nào nêu trên không thỏa mãn, hai router đơn giản sẽ không hình thành quan hệ láng giềng. Cũng lưu ý rằng một trong những điều kiện quan trọng nhất mà hai bên không cần giống là chỉ số ID của tiến trình OSPF, như được cấu hình trong câu lệnh router ospf process-id. Bạn cũng nên lưu ý rằng giá trị MTU phải bằng nhau để các gói tin DD được gửi thành công giữa những láng giềng nhưng thông số này không được kiểm tra trong tiến trình Hello.

Chức năng thứ ba của Hello là để duy trì liên lạc giữa những láng giềng. Các láng giềng gửi Hello ở mỗi chu kỳ hello interval; nếu router không nhận được Hello trong khoảng thời gian dead interval sẽ làm cho router tin rằng láng giềng của nó đã fail. Khoảng thời gian hello interval mặc định bằng 10 giây trên những cổng LAN và 30 giây trong những đường T1 hoặc đường thấp hơn T1. Thời gian dead interval mặc định bằng bốn lần thời gian hello interval.

http://www.ebook.edu.vn

Bài 5:Thực hành về định tuyến

Thiết kế sơ đồ hệ thống mạng như trong hình



Yêu cầu

- Sử dụng giao thức định tuyến tĩnh cấu hình định tuyến giữa các LAN
- Sửu dụng giao thức IGRP với AS=100 cấu hình định tuyến giữa các LAN

Kết quả

- Các PC thuộc các LAN ping được đến nhau

http://www.ebook.edu.vn

Bài 6: Cấu hình NAT trên Router

6.1. Khái niệm chung về NAT

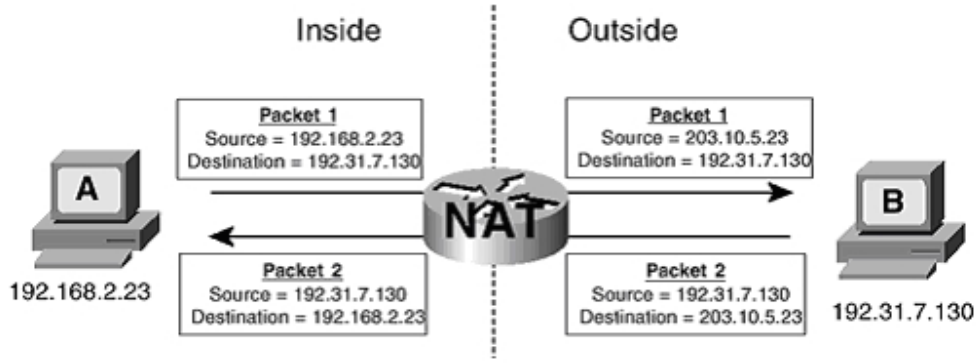
Hai mươi năm trước đây, IPv4 đưa ra một mô hình địa chỉ và cũng đáp ứng được một trong khoảng thời gian, nhưng trong tương lai gần không đáp ứng đủ. Trong khi đó, IPv6 được xem là một không gian địa chỉ không giới hạn, thì được triển khai thử nghiệm chậm chạp và chắc chắn sẽ thay thế IPv4 trong tương lai gần. Trong thời gian chờ đợi sự thay đổi đó, một số kỹ thuật để có thể sử dụng để sử dụng có hiệu quả tài nguyên IP đó là: NAT (Network Address Translation); PAT (Port address translation); VLSM (Variable-Length Subnet Mask).

Nat là chữ viết tắt của chữ Network Address Translate (Dịch địa chỉ IP). NAT có 02 mục đích

- Ẩn địa chỉ IP trong hệ thống mạng nội bộ trước khi gói tin đi ra Internet giằm giảm thiểu nguy cơ tấn công trên mạng
- Tiết kiệm không gian địa chỉ IP

Có 03 phương án NAT

- Nat tĩnh (Static Nat)
- Nat động (Dynamic Nat)
- Nat overload – PAT (Port Address Translate)



http://www.ebook.edu.vn

Host A sử dụng 1 địa chỉ dành riêng 192.168.2.23, host B sử dụng 1 địa chỉ công cộng 192.31.7.130. Khi Host A gửi một packet đến host B, backet sẽ được truyền qua router và router thực hiên qúa trình NAT. NAT sẽ thay thế địa chỉ nguồn private ip address (192.168.2.23) thành một public IP address (203.10.5.23) và forwards the packet., với địa chỉ này packet sẽ được định tuyến trên internet tới destination address (192.31.7.130). Khi host B gửi gói tin hồi đáp tới host A, destination address của gói tin sẽ là 203.10.5.23. gói tin này đi qua router và sẽ được NAT thành địa chỉ 192.168.2.23

Inside local address - Địa chỉ IP được gán cho một host của mạng trong. Đây là địa chỉ được cấu hình như là một tham số của hệ điều hành trong máy tính hoặc được gán một cách tự động thông qua các giao thức như DHCP. Địa chỉ này không phải là những địa chỉ IP hợp lệ được cấp bởi NIC (Network Information Center) hoặc nhà cung cấp dịch vụ Internet.

Inside global address - Là một địa chỉ hợp lệ được cấp bởi NIC hoặc một nhà cung cấp dịch vụ trung gian. Địa chỉ này đại diện cho một hay nhiều địa chỉ IP inside local trong việc giao tiếp với mạng bên ngoài

Outside local address - Là địa chỉ IP của một host thuộc mạng bên ngoài, các host thuộc mạng bên trong sẽ nhìn host thuộc mạng bên ngoài thông qua địa chỉ này. Outside local không nhất thiết phải là một địa chỉ hợp lệ trên mạng IP (có thể là địa chỉ private).

http://www.ebook.edu.vn

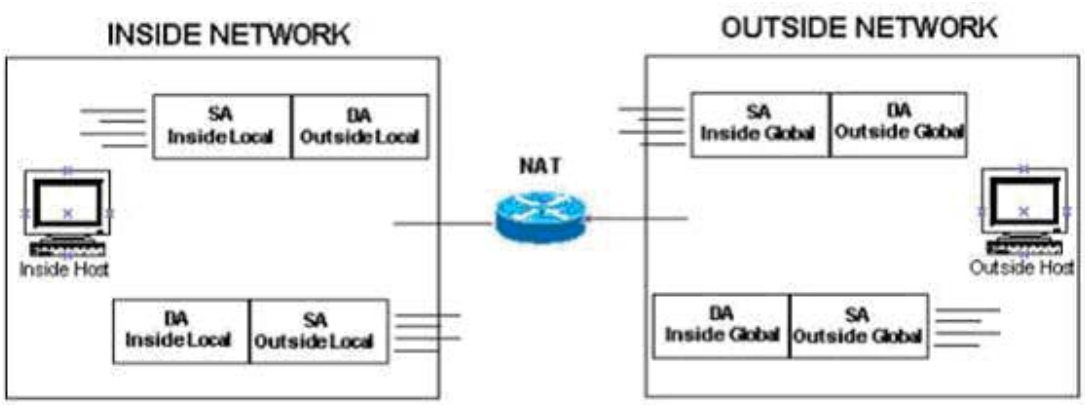
Outside global address - Là địa chỉ IP được gán cho một host thuộc mạng ngoài bởi người sở hữu host đó. Địa chỉ này được gán bằng một địa chỉ IP hợp lệ trên mạng Internet.

Với sơ đồ mạng (Hình 6.1) ta có NAT Table

- Inside local address 192.168.2.23
- Inside global address 205.10.5.23
- Outside globaladdress 197.31.7.130

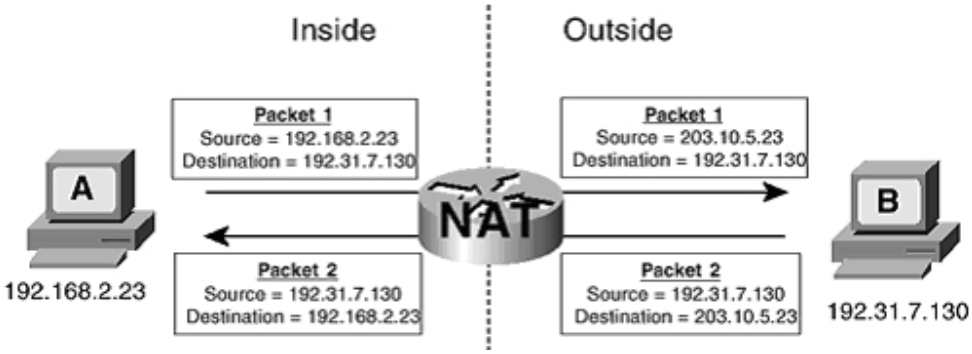
Các gói tin bắt nguồn từ phần mạng “inside” sẽ có địa chỉ source IP là địa chỉ kiểu “inside local” và destination IP là “ouside local” khi nó còn ở trong phần mạng “inside”. Cũng gói tin đó, khi được chuyển ra mạng “outside” source IP address sẽ được chuyển thành "inside global address" và địa destination IP của gói tin sẽ là “outside global address”.

Ngược lại, khi một gói tin bắt nguồn từ một mạng “outside”, khi nó còn đang ở mạng “outside” đó, địa chỉ source IP của nó sẽ là "outside global address", địa chỉ destination IP sẽ là "inside global address". Cũng gói tin đó khi được chuyển vào mạng “inside”, địa chỉ source sẽ là "outside local address" và địa chỉ destination của gói tin sẽ là "inside local address".



http://www.ebook.edu.vn

6.2 Nat tĩnh – Static NAT



Nat tĩnh hay còn gọi là Static NAT là phương thức NAT một đổi một. Nghĩa là một địa chỉ IP cố định trong LAN sẽ được ánh xạ ra một địa chỉ IP Public cố định trước khi gói tin đi ra Internet. Phương pháp này không nhằm tiết kiệm địa chỉ IP mà chỉ có mục đích ánh xạ một IP trong LAN ra một IP Public để ẩn IP nguồn trước khi đi ra Internet làm giảm nguy cơ bị tấn công trên mạng.

Ví dụ: chuyển đổi một địa chỉ IP riêng 165.10.1.2 255.255.255.0 sang dải địa chỉ IP công cộng từ 169.10.1.50 dến 169.10.1.100. Dùng (Netsim) để cấu hình. Sau khi cấu hình song ta dùng lệnh show ip nat translations sẽ có kế quả như sau.

```
r1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp169.10.1.50:9392      165.10.1.2:9392       170.10.1.2:9392       170.10.1.2:9392
icmp169.10.1.50:9393      165.10.1.2:9393       170.10.1.2:9393       170.10.1.2:9393
icmp169.10.1.50:9394      165.10.1.2:9394       170.10.1.2:9394       170.10.1.2:9394
icmp169.10.1.50:9395      165.10.1.2:9395       170.10.1.2:9395       170.10.1.2:9395
icmp169.10.1.50:9396      165.10.1.2:9396       170.10.1.2:9396       170.10.1.2:9396
```

Phương án này có nhược điểm là nếu trong LAN có bao nhiêu IP muốn đi ra Internet thì ta phải có từng đó IP Public để ánh xạ. Do vậy phương án NAT tĩnh chỉ được dúng với các máy chủ thuộc vùng DMZ với nhiệm vụ Public các Server này lên Internet.

http://www.ebook.edu.vn

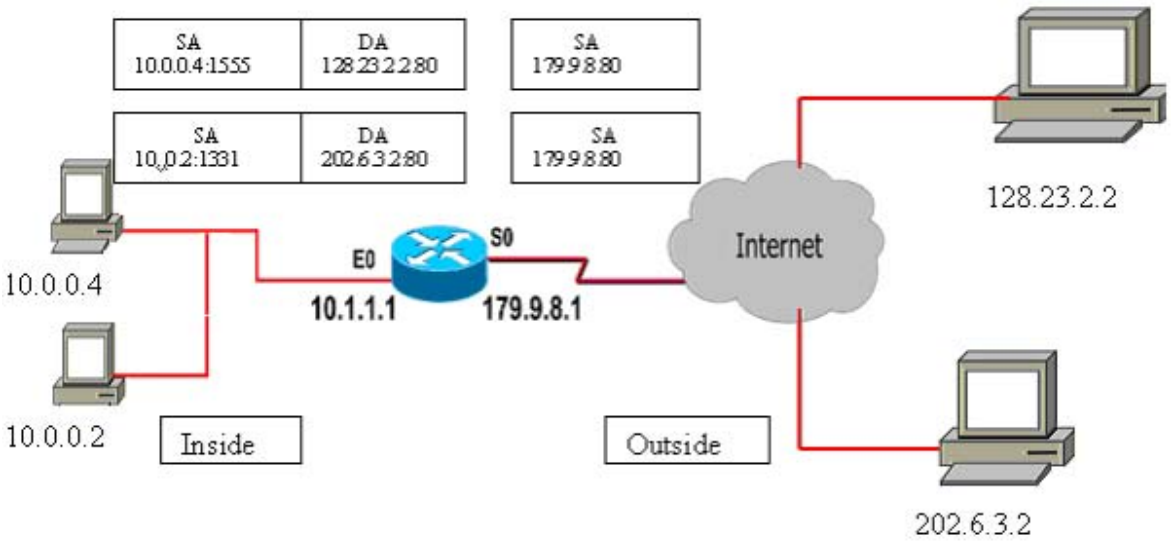
6.3. Nat động – Dynamic NAT

Nat động (Dynamic NAT) là một giải pháp tiết kiệm IP Public cho NAT tĩnh. Thay vì ánh xạ từng IP cố định trong LAN ra từng IP Public cố định. LAN động cho phép NAT cả dải IP trong LAN ra một dải IP Public cố định ra bên ngoài.

Ví dụ:

Hệ thống LAN trong công ty có 100 IP, nếu muốn 100 IP này truy cập Internet thì theo phương án NAT tĩnh công ty sẽ phải thuê từ ISP 100 IP Public. Điều này quá tốn kém, giải pháp NAT động cho phép chỉ cần thuê từ ISP 10 IP Public nếu tại cùng một thời điểm chỉ có 10 IP trong LAN truy cập Internet. Tuy nhiên giải pháp NAT động vẫn có hạn chế vì nếu tại một thời điểm công ty cần 20 IP trong LAN truy cập Internet thì mười IP truy cập sau sẽ phải đợi đến khi nào có IP rỗi (các IP trước không chiếm dụng IP Public nữa) thì mới có thể truy cập Internet được. Chính vì thế giải pháp NAT động ít khi được sử dụng.

6.4. Nat Overload – PAT



http://www.ebook.edu.vn

Nat overload – PAT là giải pháp được dùng nhiều nhất đặc biệt là trong các Modem ADSL, đây là giải pháp mang lại cả hai ưu điểm của NAT đó là:

- Ẩn địa chỉ IP trong hệ thống mạng nội bộ trước khi gói tin đi ra Internet giằm giảm thiểu nguy cơ tấn công trên mạng
- Tiết kiệm không gian địa chỉ IP

Bản chất PAT là kết hợp IP Public và số hiệu cổng (port) trước khi đi ra Internet. Lúc này mỗi IP trong LAN khi đi ra Internet sẽ được ánh xạ ra một IP Public kết hợp với số hiệu cổng

Ví dụ:

Inside local Ip address	Inside global Ip address	outside local Ip address	outside global Ip address
10.0.0.2 : 1331	179.9.8.80:1331	202.6.3.2:80	202.6.3.2:80
10.0.0.4 : 1555	179.9.8.80: 1555	128.23.2.2:80	128.23.2.2:80

Trong ví dụ trên PAT sử dụng số port nguồn cùng với địa chỉ IP riêng bên trong để phân biệt khi chuyển đổi. Router thực hiện chuyển đổi địa chỉ ip nguồn từ 10.0.0.4 sang 179.9.8.80. port nguồn 1331. tương tự ip nguồn từ 10.0.0.2 sang 179.9.8.80. port nguồn là 1555

Giải pháp PAT thực sự tiết kiệm không gian địa chỉ IP vì với mỗi IP Public có thể đại diện cho 65.536 IP trong LAN theo lý thuyết, tuy nhiên thực tế mỗi IP Public đại diện cho khoảng 4000 IP trong LAN. Đây cũng là một con số địa chỉ IP khổng lồ thừa sức cung cấp cho bất kỳ một công ty nào lớn nhất thế giới.

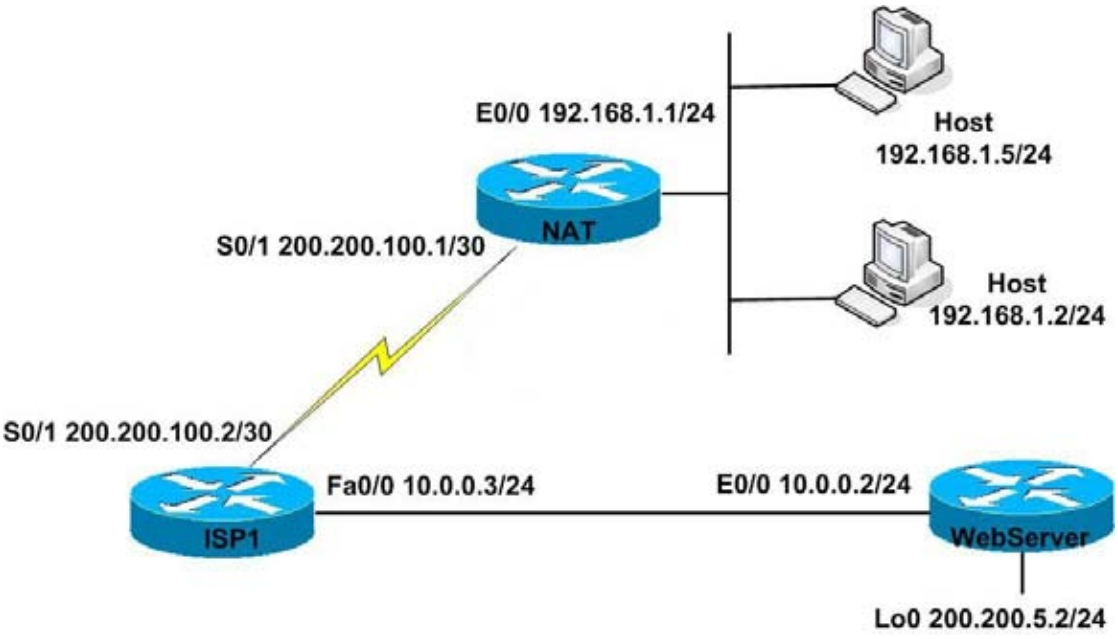
http://www.ebook.edu.vn

Bài 7:Thực hành Cấu hình NAT trên Router

Thực hành cấu hình NAT tĩnh, động, Overload

Công ty du lịch ABC cần khoảng 100 địa chỉ IP riêng dịch sang một dãy địa chỉ IP thật để có thể định tuyến ra ISP. ABC đã thực hiện điều này bằng cách sử dụng NAT, dịch các địa chỉ riêng thành các địa chỉ công cộng được cấp bởi các nhà cung cấp dịch vụ ISP.

Sử dụng phần mềm giả lập thiết kế mạng Boson thiết kế sơ đồ hệ thống mạng như hình vẽ.



Thực hiện

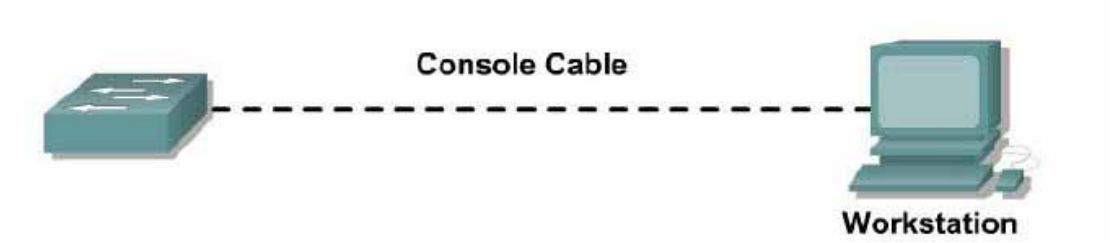
1. Cấu hình các địa chỉ IP trên các router theo sơ đồ trên, kiểm tra các kết nối trực tiếp bằng lệnh show cdp neighbor. Kiểm tra bằng cách ping giữa các workstation và router NAT, giữa WebServer và router ISP1.

http://www.ebook.edu.vn

Bài 8:Cấu hình chuyển mạch (Switching)

8.1. Cấu hình Switch và VLAN

Switch (tiếng Anh), hay còn gọi là thiết bị chuyển mạch, là một thiết bị dùng để kết nối các đoạn mạng với nhau theo mô hình mạng hình sao (star). Theo mô hình này, switch đóng vai trò là thiết bị trung tâm, tất cả các máy tính đều được nối về đây. Trong mô hình tham chiếu OSI, switch hoạt động ở tầng liên kết dữ liệu, ngoài ra có một số loại switch cao cấp hoạt động ở tầng mạng.



Cấu hình các thông số cơ bản cho Catalys Switch với giao diện dòng lệnh CLI. Các tác vụ cần thực hiện bao gồm đặt tên cho switch, cấu hình các interface vlan, cấu hình để telnet vào switch….Dùng máy trạm kết nối với switch qua kết nối console, giao diện tương tác người dùng sử dụng trình HyperTerminal. Đây là một công cụ được MS Windows hỗ trợ.

Thực hiện

- **Khởi động nguồn của switch.**

Trên giao diện Hyper Terminal hiện ra các thông số khởi tạo trong quá trình khởi động Switch.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

http://www.ebook.edu.vn

Người dùng sẽ được hỏi nếu muốn vào các hộp thoại để cấu hình tự động, trả lời NO (vì mục đích của người dùng là muốn vào chế độ CLI (command line interface).

- **Vào enable mode xem cấu hình mặc định của switch**

Switch>enable
Switch#show running-config

- **Thiết lập các thông số cho switch như hostname, enable password, console password và virtual terminal password.**

Các loại password sử dụng có phân biệt chữ thường và chữ hoa. Do đó người dùng cần phân biết các ký tự sử dụng chữ viết hoa khác với chữ viêt thường. Ví dụ Cisco khác với cisco.

Switch#config terminal
Switch(config)#hostname Vnpro
Vnpro(config)#enable password cisco
Vnpro(config)#enable secret class
Vnpro(config)#line console 0
Vnpro(config-line)#password console
Vnpro(config-line)#login
Vnpro(config-line)#^Z

Switch hỗ trợ các Virtual Line dùng cho các phiên telnet. Cần cấu hình password cho các line này mới có thể telnet vào Switch (trình tự cấu hình hỗ trợ telnet sẽ trình bày sau). Để xem thông tin về các Virtual Line trên Switch: dùng lệnh "show line".

http://www.ebook.edu.vn

Vnpro#show line

- **Cấu hình password cho các line vty**

Vnpro#config terminal
Vnpro(config)#line vty 0 4
Vnpro(config-line)#password cisco
Vnpro(config-line)#login

Cấu hình trên thiết bị Cisco, mỗi dòng lệnh do người dùng gõ vào. Sau khi nhấn phím "enter" cấu hình hệ thống sẽ lập tức thay đổi. Vì vậy, đối với các hệ thống mạng thật, trước khi thay đổi một thông số nào đó của thiết bị, cần phải sao lưu lại cấu hình ban đầu để có thể khôi phục lại khi cần thiết.

- **Cấu hình Vlan.**

Kiểm tra cấu hình Vlan mặc định trên Switch
Vnpro#show vlan
Mặc định trên Switch chỉ có Vlan 1 với tất cả các port đều nằm trong Vlan này, Vlan 1002 dành riêng cho FDDI, Vlan 1003 dành riêng cho TOKEN-RING…

- **Có hai cách tạo thêm Vlan**

Cách 1:Thao tác trên Vlan database
Vnpro#vlan database
Vnpro(vlan)#vtp domain Chuyenviet
Vnpro(vlan)#vtp server
Vnpro(vlan)#vlan 10 name Admin
Vnpro(vlan)#vlan 20 name User
Cách 2: Tương tác trực tiếp đến Vlan cần tạo ra
Vnpro(config)#interface vlan 10

http://www.ebook.edu.vn

Vnpro(config-if)#exit

Vnpro(config)#

Vnpro(config)#interface vlan 20

Vnpro(config-if)#exit

Vnpro(config)#

- **Để gán các port vào các Vlan, thực hiện các bước sau:**

Ví dụ ta cần gán các port fastethernet 2 vào Vlan 10, port fastetehnet 3 vào Vlan 20

Vnpro(config)#interface fastethernet0/2

Vnpro(config-if-range)#switchport access vlan 10

Vnpro(config-if-range)#exit

Vnpro(config)#interface fastethernet0/3

Vnpro(config-if-range)#switchport access vlan 20

Vnpro(config-if-range)#exit

Kiểm tra lại cấu hình Vlan

Vnpro#show vlan

Cấu hình IP cho interface Vlan: các interface Vlan được cấu hình IP chỉ mang tính chất luận lý. IP này phục vụ cho việc quản lý, địa chỉ IP luận lý này còn có thể dùng để telnet vào Switch từ xa và chạy các ứng dụng SNMP.

Vnpro#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Vnpro(config)#interface vlan 10

Vnpro(config-if)#ip address 10.0.0.1 255.255.255.0

Vnpro(config-if)#no shutdown

- **Lưu cấu hình vào NVRAM**

Vnpro#copy running-config startup-config

http://www.ebook.edu.vn

Cần chú ý gán default-gateway cho switch bằng câu lệnh

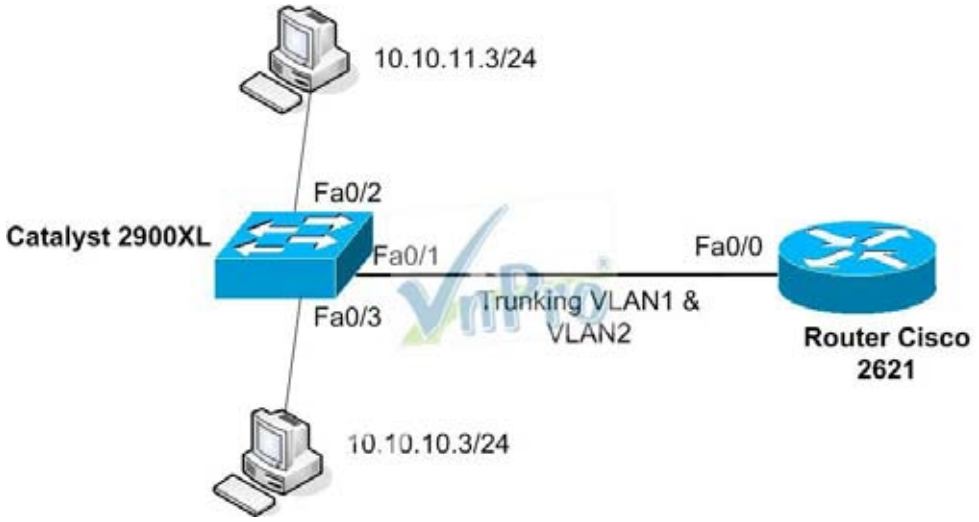
VnPro#ip default-gateway 10.0.0.100

Địa chỉ 10.0.0.100 có thể dùng là địa chỉ của PC được dùng để telnet vào switch.

http://www.ebook.edu.vn

Bài 9:Thực hành Cấu hình chuyển mạch và VLAN

Thực hiện định tuyến giữa các VLAN theo sơ đồ sau đây.



Các bước thực hiện trên Switch2900

1. Vào chế độ privileged mode, cấu hình mật khẩu telnet cho switch

2. Gán địa chỉ IP và default gateway cho VLAN1 cho tiện việc quản trị

3. Thiết lập vtp transparent mode

4. Tạo mới VLAN2 trong cơ sở dữ liệu VLAN của switch. VLAN1 mặc định đã có sẵn

5. Kích hoạt trunking trên cổng giao tiếp Fa0/1

6. Encapsulation trunking bằng sử dụng isl hay dot1q

7. Cho phép tất cả các VLAN được chuyển qua kết nối trunk:

8. Gán cổng Fa0/2 và VLAN 2.

http://www.ebook.edu.vn

Cấu hình trên Router 2600 Series

1. Vào privileged mode cấu hình mật khẩu telnet cho router

2. Chọn cổng fa0/0 để cấu hình trunk,

3. Kích hoạt trunking trên sub-interface Fa0/0.1 và encapsulation bằng isl

4. Cấu hình thông tin lớp 3 cho sub-interface Fa0/0.1

5. Kích hoạt trunking trên sub-interface Fa0/0.2 và encapsulation bằng isl

6. Cấu hình thông tin Layer 3 cho sub-interface Fa0/0.2

http://www.ebook.edu.vn

Bài 10: Thảo luận

Một số chủ đề thảo luận

- Các nguy cơ tiềm tàng trên mạng
  - Viruses, Worms, Trojan Horses.
  - Denial of Service (DoS) và Brute Force Attack
- Các kỹ năng cần có của một kỹ sư trong vai trò HelpDesk
- Quy trình thiết kế và nâng cấp hệ thống mạng đã có
- Tìm hiểu các giao thức mã hoá trong mạng WLAN

http://www.ebook.edu.vn

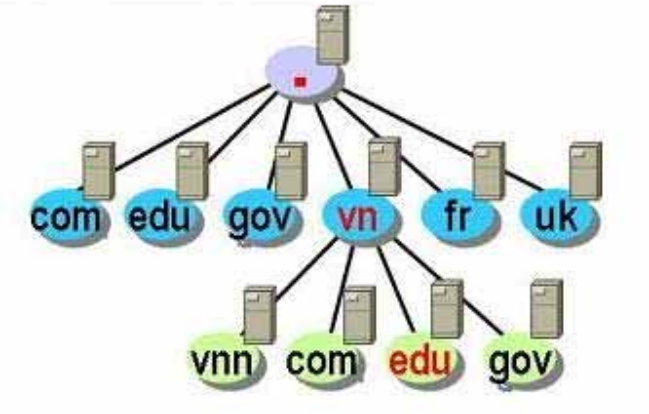
Bài 11: Cấu hình các Web Server, DNS Server

11.1. Dịch vụ phân giải tên miến – DNS Server

11.1.1. Nguyên lý phân giải tên miền

Chức năng của DNS

Mỗi Website có một tên (là tên miền hay đường dẫn URL:Universal Resource Locator) và một địa chỉ IP. Địa chỉ IP gồm 4 nhóm số cách nhau bằng dấu chấm. Khi mở một trình duyệt Web và nhập tên website, trình duyệt sẽ đến thẳng website mà không cần phải thông qua việc nhập địa chỉ IP của trang web. Quá trình "dịch" tên miền thành địa chỉ IP để cho trình duyệt hiểu và truy cập được vào website là công việc của một DNS server. Các DNS trợ giúp qua lại với nhau để dịch địa chỉ "IP" thành "tên" và ngược lại. Người sử dụng chỉ cần nhớ "tên", không cần phải nhớ địa chỉ IP (địa chỉ IP là những con số rất khó nhớ).



Nguyên tắc làm việc của DNS

Mỗi nhà cung cấp dịch vụ vận hành và duy trì DNS server riêng của mình, gồm các máy bên trong phần riêng của mỗi nhà cung cấp dịch vụ đó trong Internet.

http://www.ebook.edu.vn

Tức là, nếu một trình duyệt tìm kiếm địa chỉ của một website thì DNS server phân giải tên website này phải là DNS server của chính tổ chức quản lý website đó chứ không phải là của một tổ chức (nhà cung cấp dịch vụ) nào khác.

INTERNIC (Internet Network Information Center) chịu trách nhiệm theo dõi các tên miền và các DNS server tương ứng. INTERNIC là một tổ chức được thành lập bởi NFS (National Science Foundation), AT&T và Network Solution, chịu trách nhiệm đăng ký các tên miền của Internet. INTERNIC chỉ có nhiệm vụ quản lý tất cả các DNS server trên Internet chứ không có nhiệm vụ phân giải tên cho từng địa chỉ.

DNS có khả năng tra vấn các DNS server khác để có được một cái tên đã được phân giải. DNS server của mỗi tên miền thường có hai việc khác biệt. Thứ nhất, chịu trách nhiệm phân giải tên từ các máy bên trong miền về các địa chỉ Internet, cả bên trong lẫn bên ngoài miền nó quản lý. Thứ hai, chúng trả lời các DNS server bên ngoài đang cố gắng phân giải những cái tên bên trong miền nó quản lý. - DNS server có khả năng ghi nhớ lại những tên vừa phân giải. Để dùng cho những yêu cầu phân giải lần sau. Số lượng những tên phân giải được lưu lại tùy thuộc vào quy mô của từng DNS.

http://www.ebook.edu.vn

Cách sử dụng DNS

Do các DNS có tốc độ biên dịch khác nhau, có thể nhanh hoặc có thể chậm, do đó người sử dụng có thể chọn DNS server để sử dụng cho riêng mình. Có các cách chọn lựa cho người sử dụng. Sử dụng DNS mặc định của nhà cung cấp dịch vụ (internet), trường hợp này người sử dụng không cần điền địa chỉ DNS vào network connections trong máy của mình. Sử dụng DNS server khác (miễn phí hoặc trả phí) thì phải điền địa chỉ DNS server vào network connections. Địa chỉ DNS server cũng là 4 nhóm số cách nhau bởi các dấu chấm

11.1.2. Xây dựng máy chủ phân giải tên miền cho mạng doanh nghiệp

Máy chủ phân giải tên miền DNS là gì ?

Mỗi máy tính, thiết bị mạng tham gia vào mạng Internet đều "nói chuyện " với nhau bằng địa chỉ IP (Internet Protocol). Để thuận tiện cho việc sử dụng và dễ nhớ ta dùng tên (Domain name) để xác định thiết bị đó. Hệ thống tên miễn DNS

http://www.ebook.edu.vn

(Domain Name System) được sử dụng để ánh xạ tên miễn thành địa chỉ IP. Vì vậy, khi muốn liên hệ tới các máy, chúng chỉ cần sử dụng chuỗi ký tự dễ nhớ (domain name) như: www.microsoft.com, www.ibm.com..., thay vì sử dụng địa chỉ IP là một dãy số dài khó nhớ.

Máy chủ phân giải tên miền (DNS server) là những máy chủ được cài đặt, và cung cấp dịch vụ phân giải tên miền DNS. Máy chủ DNS được phân ra thành 2 loại như sau:

- Primary DNS Server (PDS)

Primary DNS Server (PDS) là nguồn xác thực thông tin chính thức cho các tên miền mà nó được phép quản lý. Thông tin về một tên miền do PDS được phân cấp quản lý thì được lưu trữ tại đây và sau đó có thể được chuyển sang các Secondary DNS Server (SDS). Các tên miền do PDS quản lý thì được tạo, và sửa đổi tại PDS và sau đó được cập nhật đến các SDS.

- Secondare DNS Server(SDS).

DNS được khuyến nghị nên sử dụng ít nhất là hai DNS server để lưu địa chỉ cho mỗi một vùng (zone). PDS quản lý các vùng và SDS được sử dụng để lưu trữ dự phòng cho vùng, và cho cả PDS. SDS không nhất thiết phải có những khuyến khích hãy sử dụng. SDS được phép quản lý tên miền nhưng dữ liệu về tên miền không phải được tạo ra từ SDS mà được lấy về từ PDS.

SDS có thể cung cấp các hoạt động ở chế độ không tải trên mạng. Khi lượng truy vấn vùng tăng cao, PDS sẽ chuyển bớt tải sang SDS (quá trình này còn được gọi là cân bằng tải), hoặc khi PDS bị sự cố thì SDS hoạt động thay thế cho đến khi PDS hoạt động trở lại, SDS thường được sử dụng tại nơi gần với các máy trạm (client) để có thể phục vụ cho các truy vấn một cách dễ dàng. Tuy nhiên, cài đặt SDS trên cùng một subnet hoặc dùng một kết nối với PDS là không nên.

http://www.ebook.edu.vn

Điều đó sẽ là một giải pháp tốt để dự phòng cho PDS, vì khi kết nối đến PDS bị hỏng thì cũng không ảnh hưởng gì tới đến SDS.

Ngoài ra PDS luôn duy trì một lượng lớn dữ liệu và thường xuyên thay đổi hoặc thêm các địa chỉ mới vào các vùng. Do đó, DNS server sử dụng một cơ chế cho phép chuyển các thông tin từ PDS sang SDS và lưu giữ trên đĩa. Khi cần phục hồi dữ liệu về các vùng, chúng ta có thể sử dụng giải pháp lấy toàn bộ hoặc chỉ lấy phần thay đổi.

Thay đổi DNS.

Thông thường khi kết nối Internet, tất cả mọi dấu hiệu cho thấy cuộc kết nối suôn sẻ. Thế nhưng, sau khi đã gõ địa chỉ website vào trình duyệt rồi mà đợi mãi vẫn chẳng thấy website hiện ra.

Thanh Status (màu xanh lục) trên IE cũng không thấy xuất hiện. Kiểm tra lại mọi thứ thì vẫn thấy bình thường... Mãi một lúc lâu sau mới thấy trình duyệt thông báo Connecting to 64.128.xxx.xxx rồi sau đó vào website bình thường. Nhưng mỗi lần click vào link nào trên trang thì vẫn lặp lại tình trạng cũ.

DNS, Domain Name Server, hay còn gọi là máy chủ tên miền - là một trong những khâu vô cùng quan trọng trong tiến trình duyệt web của bạn.

Mỗi máy tính trên Internet được đánh dấu bằng một địa chỉ IP, là một mớ số đó, nhất là trong tương lai địa chỉ IP sẽ dài gấp bốn lần địa chỉ hiện nay.

DNS chính là giải pháp. Thay vì bắt con người nhớ số, mỗi số IP sẽ được đổi thành chữ và DNS có nhiệm vụ đổi chữ thành số tương ứng khi có yêu cầu.

Địa chỉ của DNS thường được cung cấp tự động trực tiếp mỗi khi bạn thiết lập kết nối với ISP (nhà cung cấp dịch vụ Internet). Ở Việt Nam, mỗi ISP thường có hai hoặc nhiều DNS để phục vụ số lượng khách hàng của mình.

http://www.ebook.edu.vn

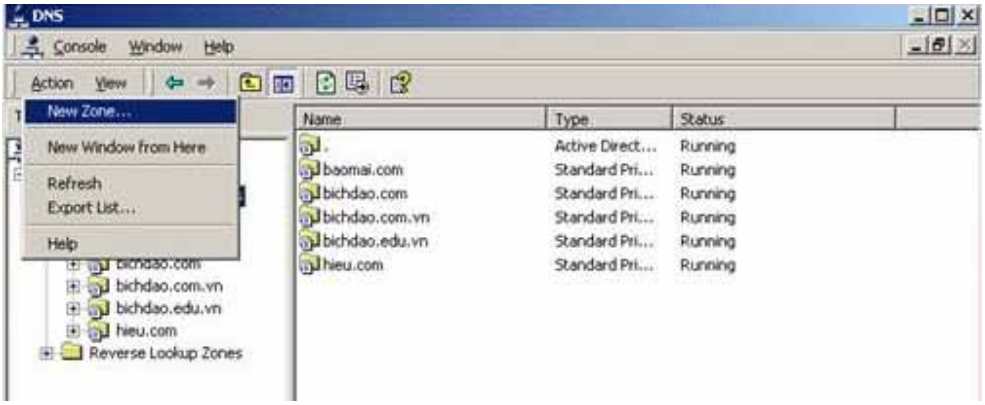
Thế nhưng thường cũng không đủ dùng. Vì vậy không ai cấm việc xài dịch vụ của ISP này nhưng thiết lập DNS của ISP khác, hoặc một DNS nào đó tốt hơn trong các giờ cao điểm.

Thao tác thay DNS cũng rất dễ dàng. Bạn mở cửa sổ Network/properties để vào Internet Protocol(TCP/IP) Properties. Nếu bạn dùng mặc định DNS do ISP cung cấp thì chọn "Obtain DNS server address automatically"

Nếu muốn dùng DNS theo ý mình thì chọn dòng " User the following DNS server addresses", sau đó điền địa chỉ IP của DNS vào 2 dòng bên dưới. Preferrer DNS server là địa chỉ được trình duyệt tìm đến đầu tiên. Alternate DNS server dành cho server dự phòng, trong trường hợp server đầu tiên quá bận. <Network > chính là tên của kết nối Internet của bạn.

Cấu hình cho dịch vụ DNS.

Để tạo một Zone mới kích chuột vào Action chọn NewZone như hình trên.



http://www.ebook.edu.vn

Sau đó chọn Next.

Chọn Standard Primary nếu bạn muốn thiết lập một zone mới, còn nếu bạn đã có một zone nào đó rồi thì bạn có thể chọn Secondary để tạo một bản sao lưu.

Kích chuột chọn Next để tiếp tục.

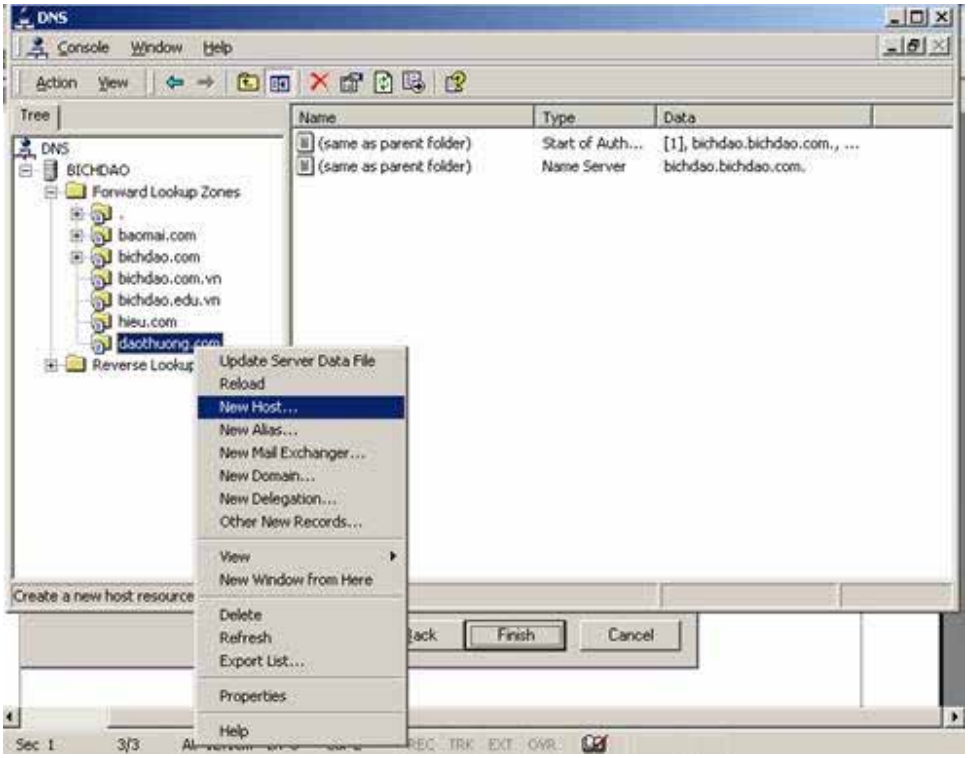
http://www.ebook.edu.vn

Nhập vào nội dung của Zone bạn muốn thiết lập rồi chọn Next.

Chọn Next.

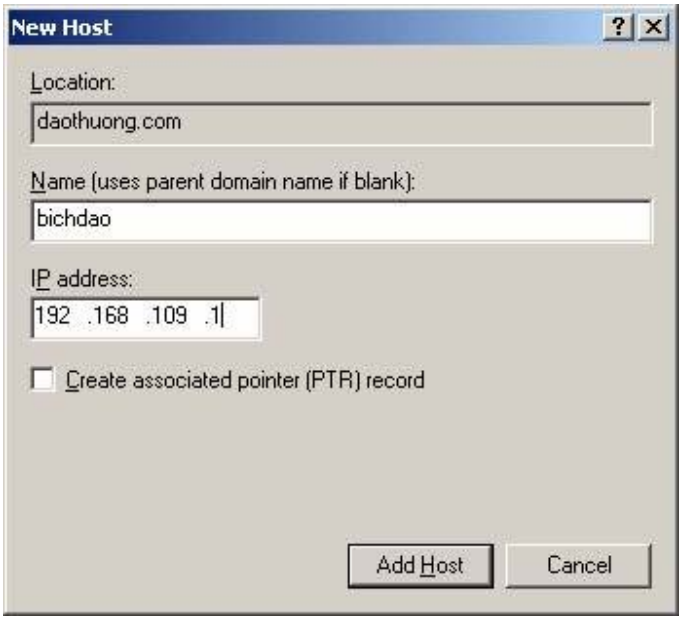
http://www.ebook.edu.vn

Sau đó chọn Finish.



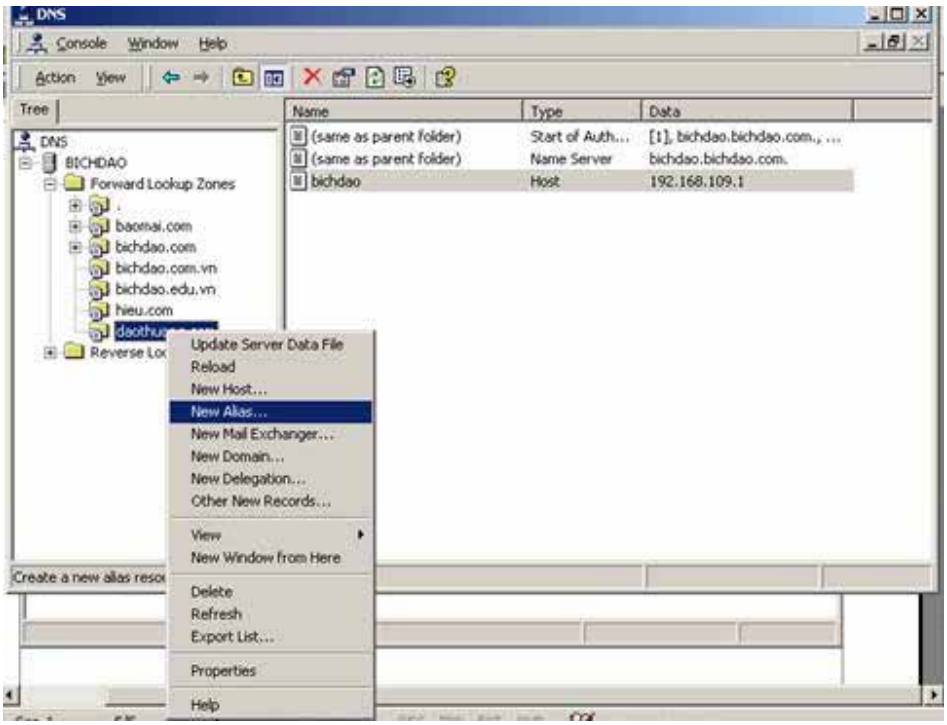
Chuột phải vào phần mà bạn vừa tạo và chọn NewHost để tạo ra một Host mới.

http://www.ebook.edu.vn



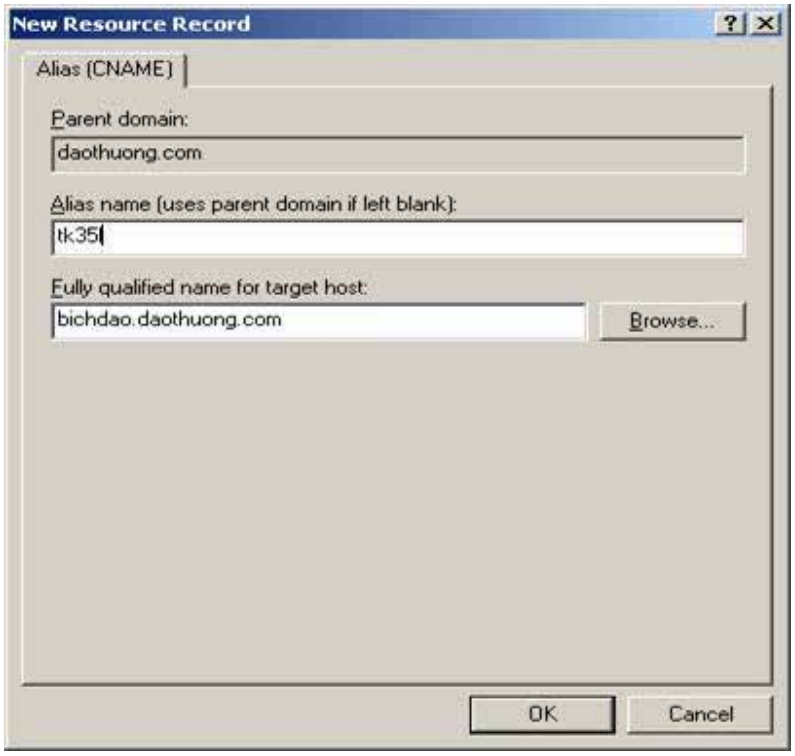
Chọn tuỳ ý một cái tên và chọn địa chỉ IP của Host.

Nhấn Add Host -> Ok -> Done.



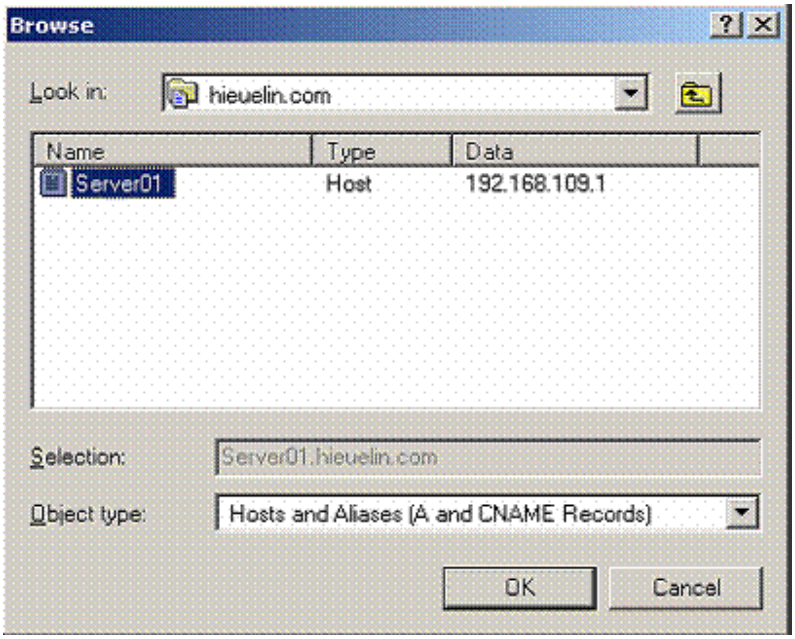
Tiếp tục thiết lập Alias, đây là một định danh của Site mà bạn cần thiết lập.

http://www.ebook.edu.vn



Chọn một tên để thay thế cho định danh mạng. Kế tiếp chọn Browse…

Tìm đúng Zone mà bạn đã tạo Host và chọn Host đó - nhấn OK.



Lúc này bạn đã có thông tin đầy đủ về một tên miền mà mình sẽ tạo ra.

http://www.ebook.edu.vn

Nhấn OK để tiếp tục.

Để có thể thử nghiệm việc phận giải một tên miền với DNS ta hãy sử dụng một dịch vụ ISS để kiểm tra.

11.2. Dịch vụ Web Server

11.2.1. Giao thức HTTP và HTTPS

Giao thức HTTP

HTTP (HyperText Transfer Protocol), tiếng Việt gọi là Giao Thức Truyền Siêu Văn Bản. HTTP là một giao thức chuẩn trực thuộc lớp ứng dụng trong mô hình 7 lớp OSI và được dùng để liên hệ thông tin giữa máy cung cấp dịch vụ (Web Server) và máy dùng dịch vụ (Client). HTTP tương thích với nhiều định dạng thông tin, media và hồ sơ.

Giao thức HTTPS

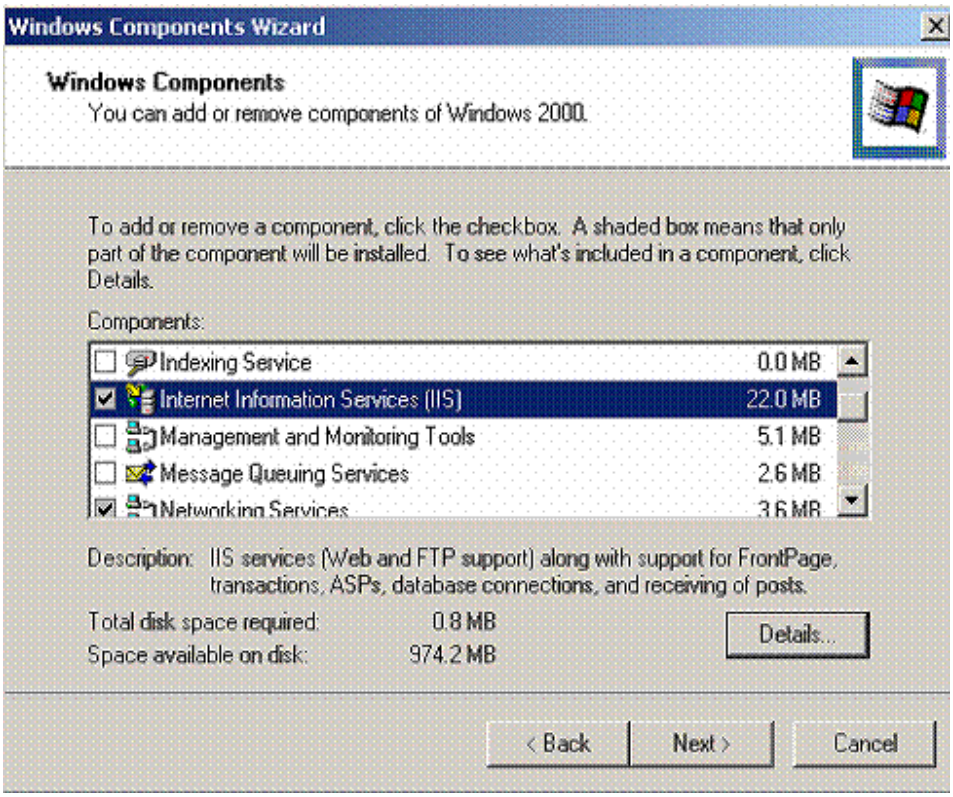
HTTPS(Secure HTTP), là một sự kết hợp giữa giao thức HTTP và giao thức bảo mật SSL hay TLS cho phép trao đổi thông tin một cách bảo mật trên Internet. Giao thức HTTPS thường được dùng trong các giao dịch cần sự bảo mật như e-commerce, e-banking ... trên Internet.

11.2.2. Triển khai Website doanh nghiệp trên Server

Để triển khai một website doanh nghiệp trên Server ta phải cài dịch vụ Web Server lên máy chủ đó. Tuỳ thuộc vào Hệ điều hành và ngôn ngữ lập trình Web mà bạn sẽ quyết định cài lên Server dịch vụ Web Server IIS cho Window hay Apache cho Linux. Sau đây là các bước triển khai dịch vụ Webserver IIS trên máy chủ Window.

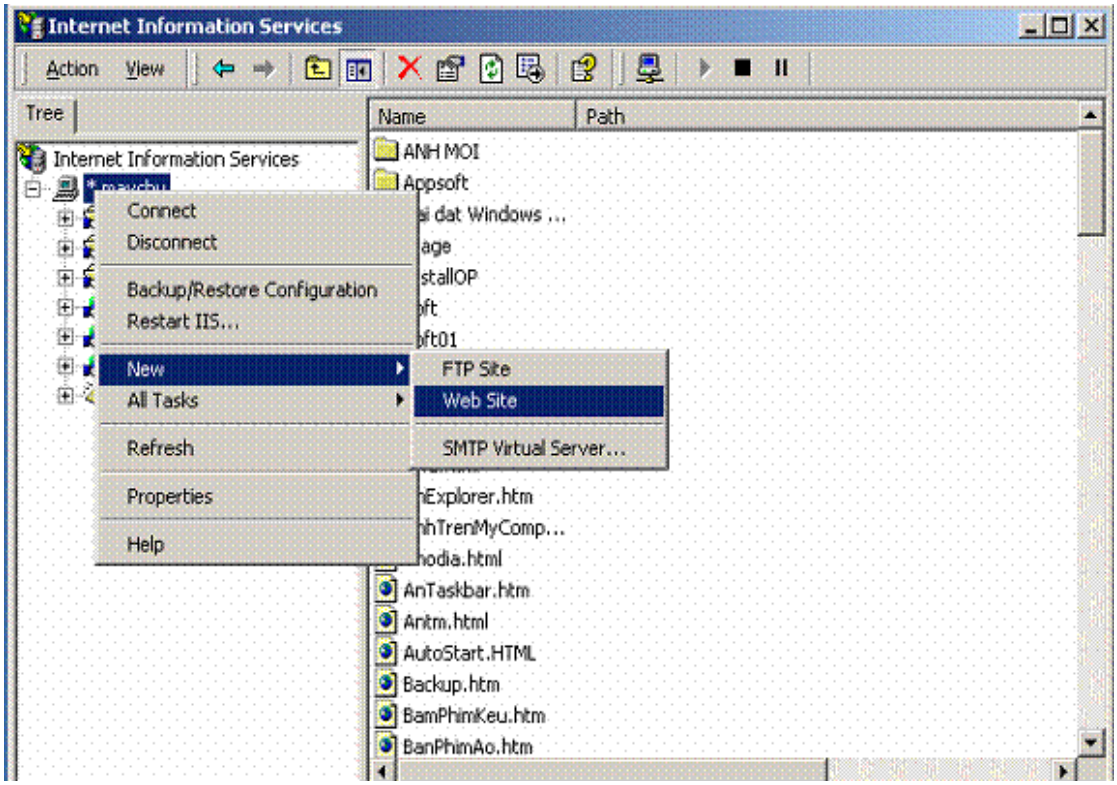
http://www.ebook.edu.vn

Các bước cài đặt ISS khá dễ dàng các bạn có thể cài các mục như với cài DNS, chỉ khác là trong hộp thoại chọn các bạn chọn:



Như trên hình hoặc có thể tuỳ chọn trong mục Details.

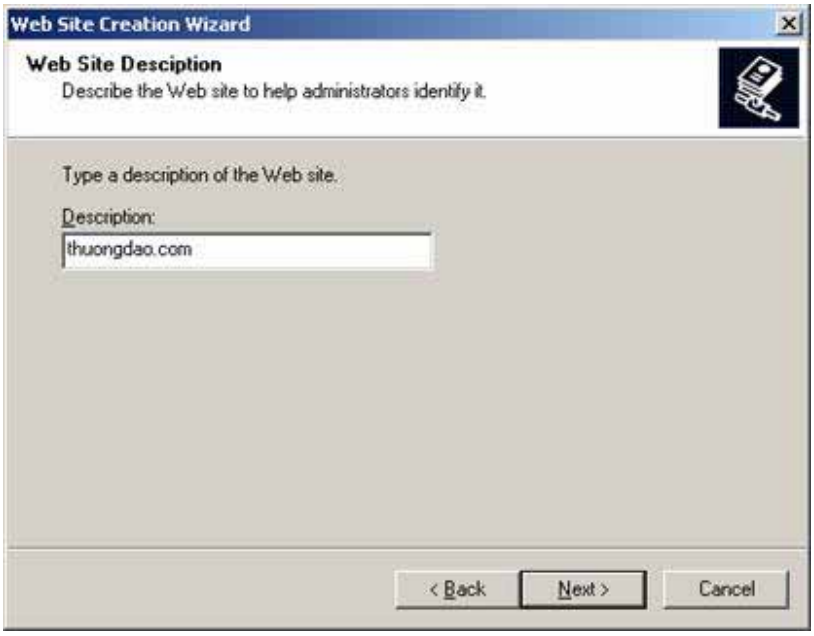
http://www.ebook.edu.vn



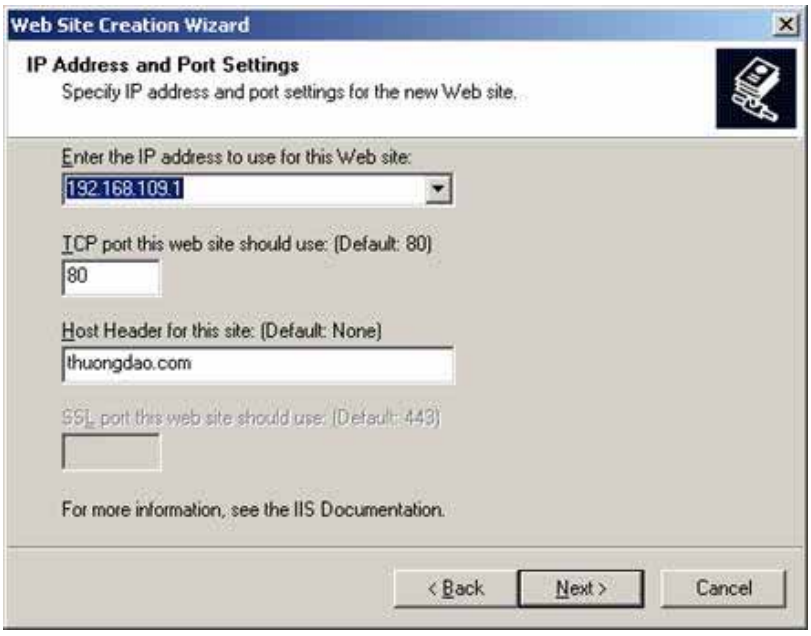
Xuất hiện bảng sau, chúng ta chọn Next.

http://www.ebook.edu.vn

đặt tên mô tả cho Website này và chọn Next.



Chọn các thiết lập:



http://www.ebook.edu.vn

Nhập địa chỉ IP của máy chủ vào mục IP nếu như bạn muốn chỉ định các máy khác địa chỉ web được chỉ tới là địa chỉ nào.
Chọn cổng truy cập trên máy chủ, thông thường chúng ta để cổng 80 nhưng tuỳ vào người quản trị mạng mà chúng ta có thể chọn cổng bất kỳ để tránh sự dòm ngó từ bên ngoài.

Chọn Next.

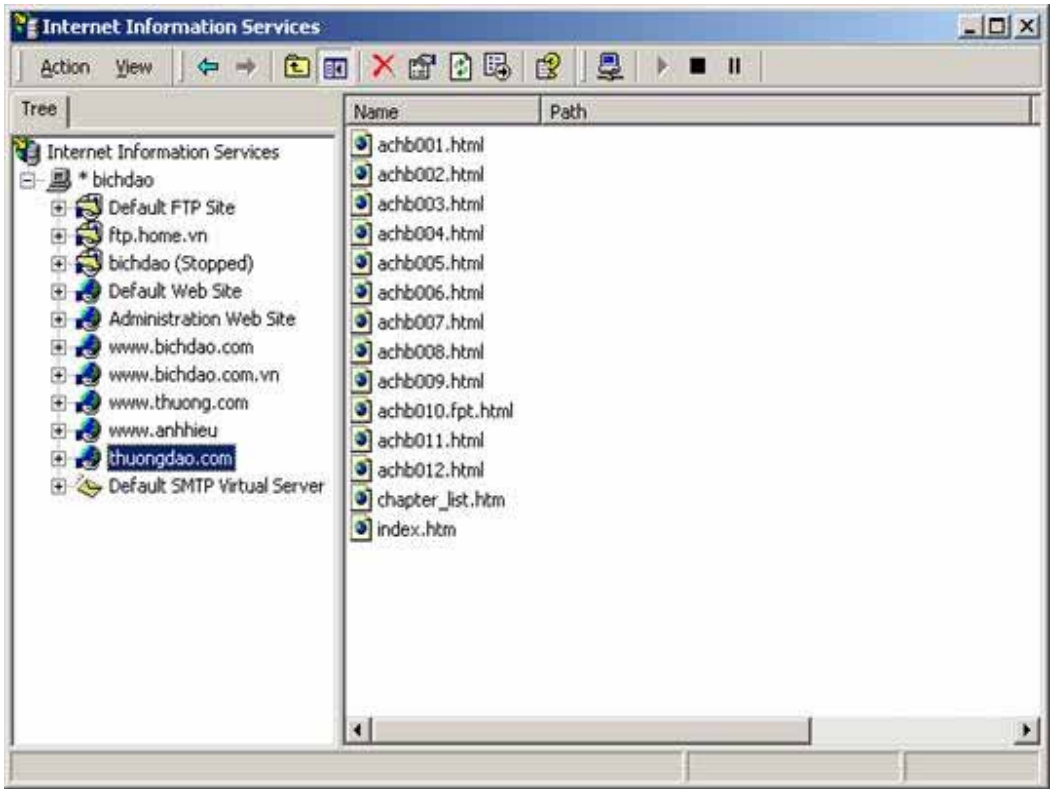
Trong mục này bạn hãy chọn đường dẫn lưu trang web của bạn và chọn Next.

http://www.ebook.edu.vn

Thiết lập các chế độ ghi đọc của người dùng trên Site này và chọn Next.

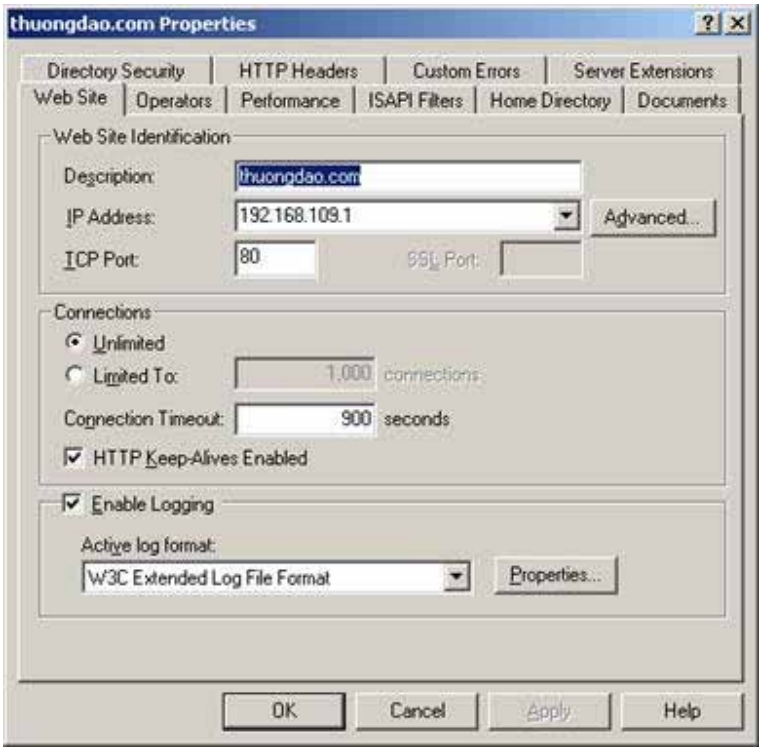
Click vào Finish để kết thúc chọn.

http://www.ebook.edu.vn



Click chuột phải vào trang web mà bạn vừa tạo và cấu hình các thuộc tính cho chúng.

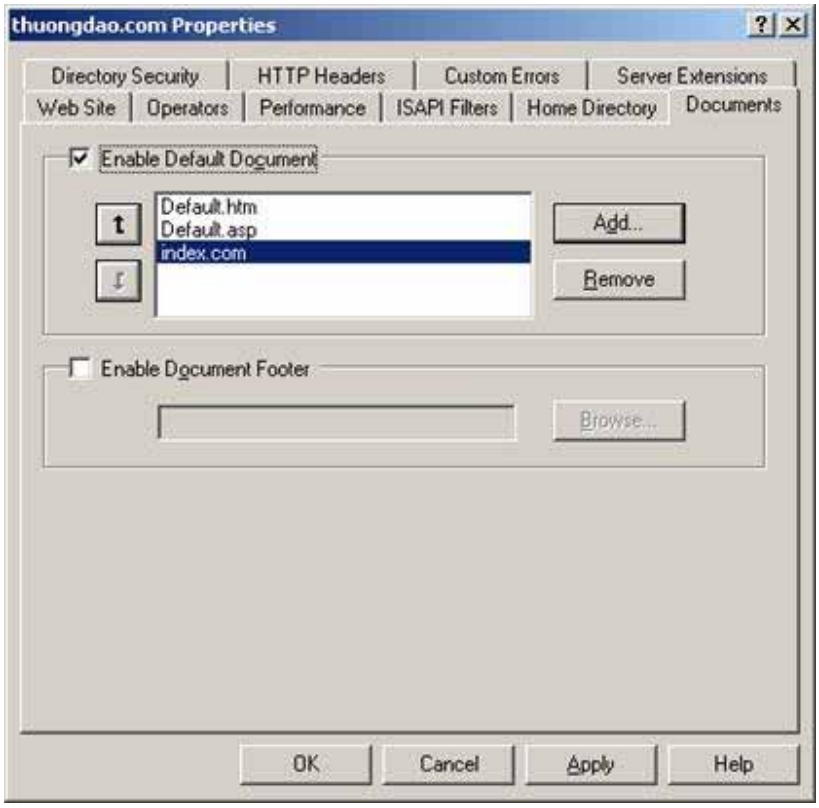
http://www.ebook.edu.vn



Trên trang tuỳ chọn này bạn có thể cấu hình lại các thông số mà trước đó bạn đã tạo ra.

Để thiết lập trang chỉ định khi trình duyệt web của máy Client yêu cầu sẽ được mở ra. Đầu tiên bạn chọn Add để thêm mới tên trang và chọn ,ví dụ tên trang chủ của tôi là index.com thì tôi gõ vào là index.com và Add vào

http://www.ebook.edu.vn



Nhấn Apply rồi OK.

Khi đó trên trình duyệt của máy khách bạn chỉ cần gõ thuongdao.com mà không cần phải gõ địa chỉ IP của trang web vào.

Nếu bạn không để cổng mặc định là 80 thì ngay sau địa chỉ bạn gõ: và tên cổng vào.

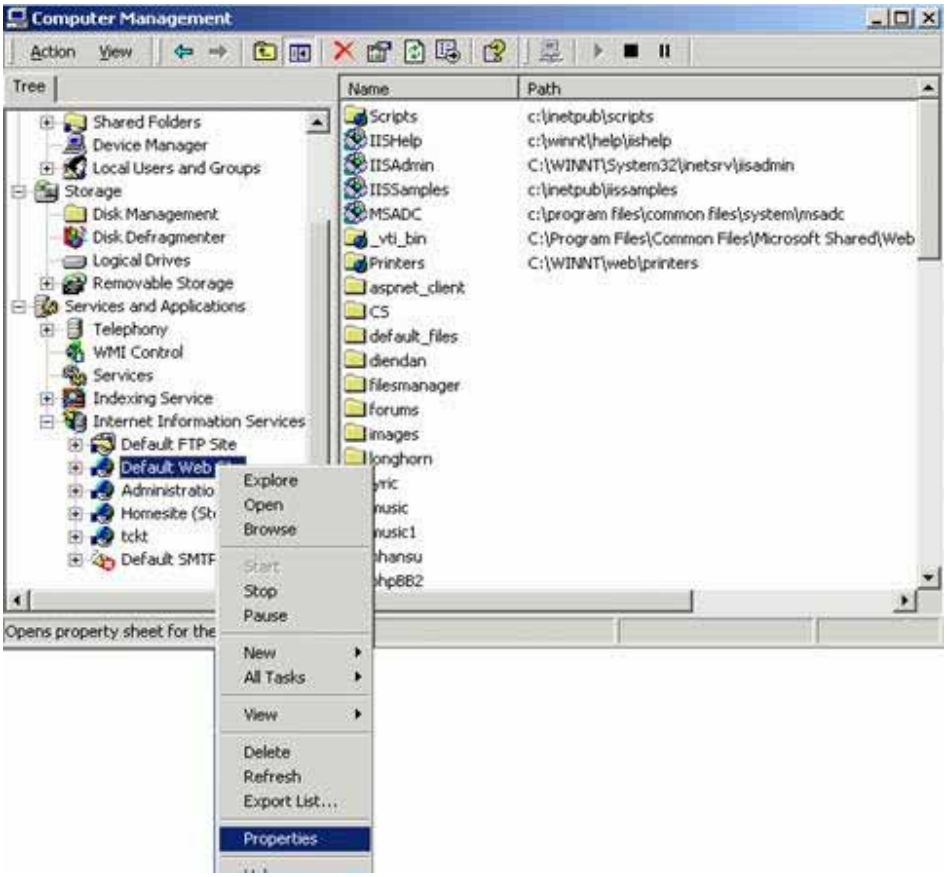
Ví dụ nếu tôi để cổng là 8080 thì tôi gõ trong trình duyệt là

http://thuongdao.com:8080

2. Cấu hình dịch vụ IIS

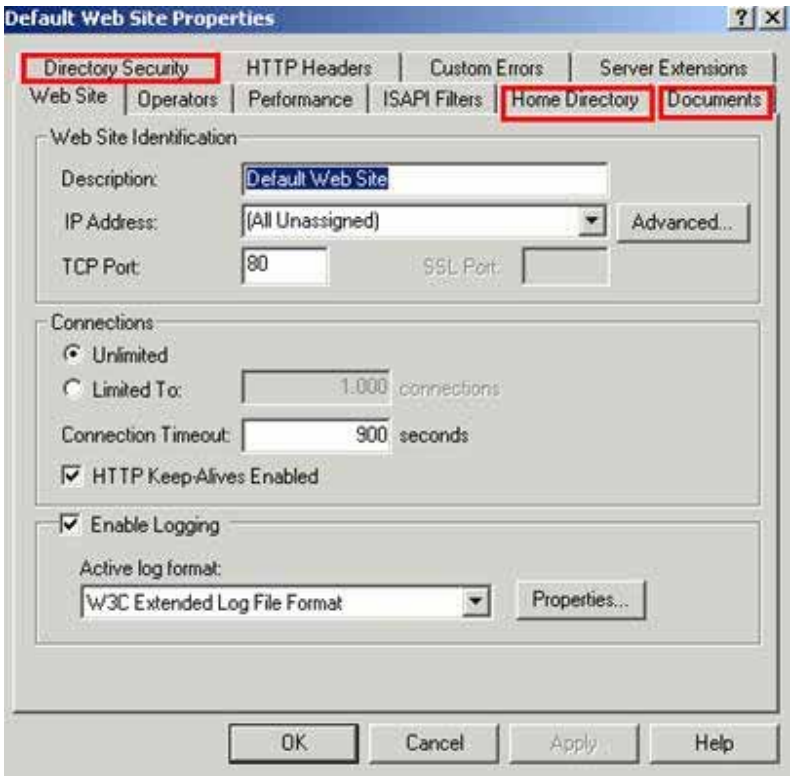
Để cấu hình dịch vụ web cho IIS bạn vào My Computer > Control Panel > Administrative Tool > Internet Services Manager. Sau đó làm như hình minh hoạ.

http://www.ebook.edu.vn



Sau khi nhấp vào properties sẽ hiện lên bảng website.

http://www.ebook.edu.vn



Description: Mô tả tên của Website.

Ip Address: Phần này cho phép chúng ta gắn địa chỉ IP cho Website.

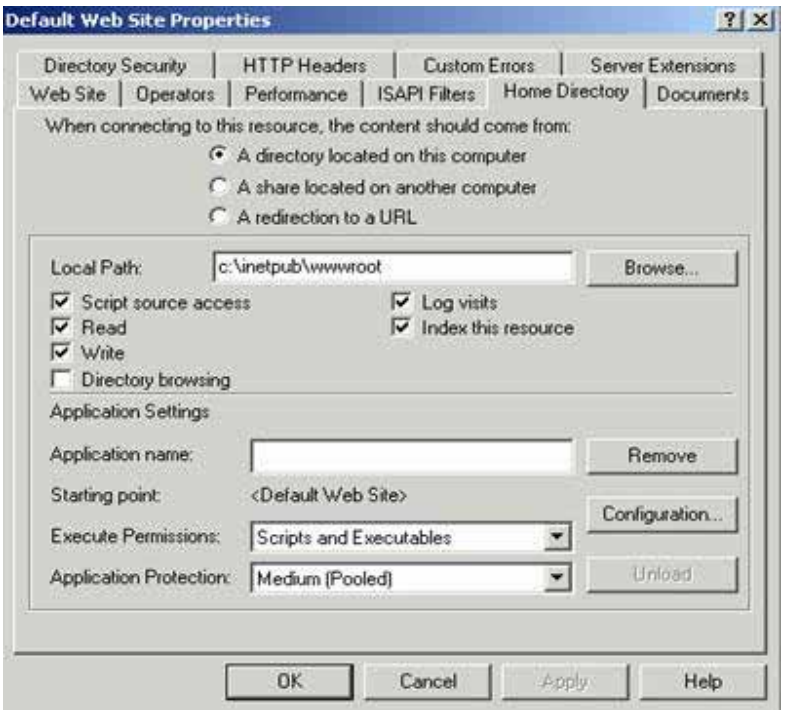
TCP Port: Cổng cho phép kết nối vào Website mặc định là cổng 80

Unlimited: Cho phép kết nối không giới hạn thời gian.

Limited To: Giới hạn thời gian kết nối với Website.

Thẻ tiếp theo là Home Directory.

http://www.ebook.edu.vn

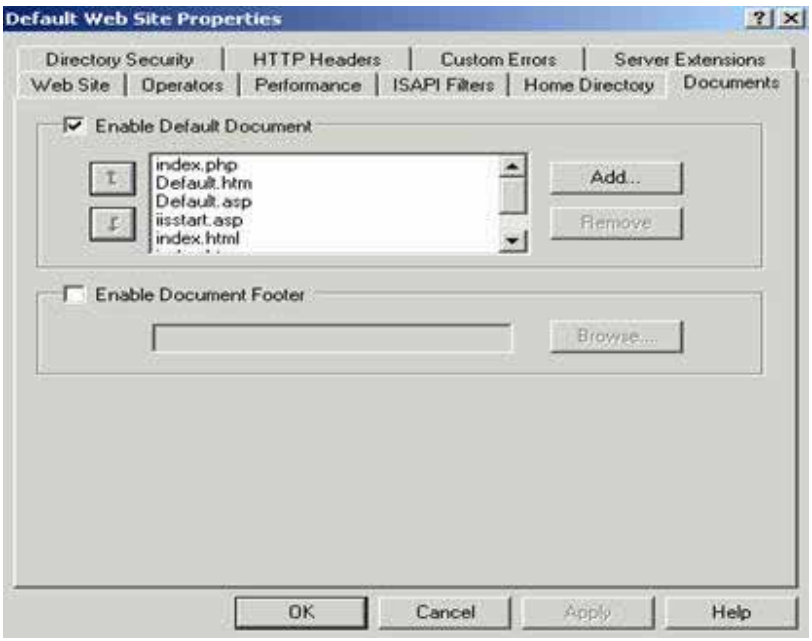


Directory Browsing: Chức năng cho phép hiển thị Browser khi không có trang chủ mặc định.

A redirection a URl: Là tính năng cho phép ta chuyển tiếp đến một trang nào đó (dùng bằng URL)

Thẻ tiếp theo là Document.

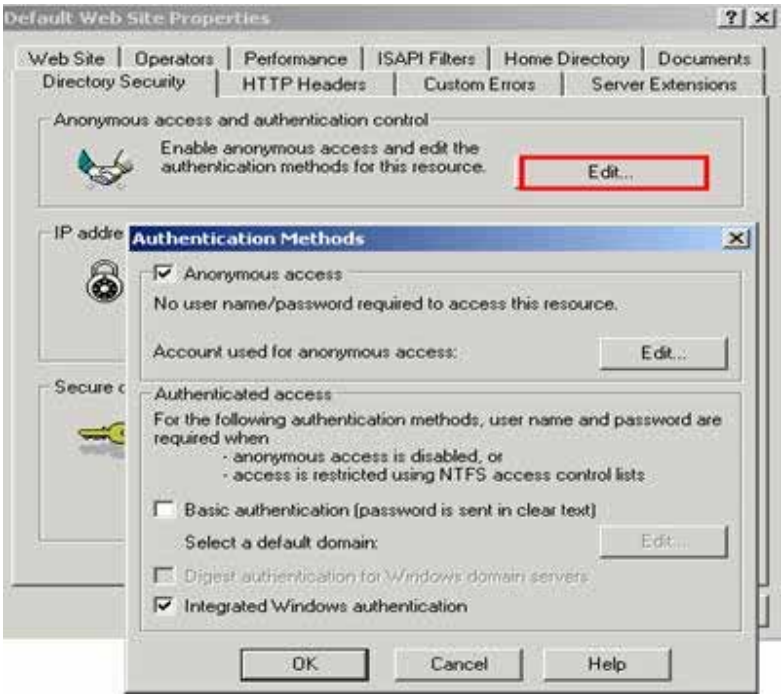
http://www.ebook.edu.vn



Phần này cho phép ta thêm chỉ mục Index cho website của mình. Tức là nếu bạn muốn website của mình mặc định là chạy files index.php. Thì bạn vào phần add sau đó đánh vào index.php. Rồi dùng dấu mũi tên bên trái đưa index.php lên trên đầu tiên như hình minh hoạ. Nhớ rằng chỉ mục document này nó sẽ tự tìm từ trên xuống dưới(sau index.php không có nó sẽ tự tìm Default.htm…)

Thẻ tiếp theo là Directory Security.

http://www.ebook.edu.vn



Trong phần này bạn nhớ để ý mặc định là cho phép chế độ truy cập nặc danh tức là ai cũng có thể vào website của mình. Ta tick vào như hình minh hoạ trên. Còn nếu muốn khi truy cập vào site của mình phải có Username và password (tức là Uer trong computer) thì bỏ tick ở phần Anonymous access thay bằng Basic authentication .Khi đó bất cứ ai truy cập vào site của bạn cũng cần phải có username và password trên server của bạn.

http://www.ebook.edu.vn

Bài 12: Thực hành cấu hình các dịch vụ mạng cơ bản

- Cấu hình Active Directory (AD)
- Cấu hình IIS
- Cấu hình DNS
- Cấu hình DHCP

http://www.ebook.edu.vn

Bài 13. Xây dựng một Mail Server

13.1. Giao thức SMTP, POP3, IMAP

SMTP (tiếng Anh: Simple Mail Transfer Protocol - giao thức truyền tải thư tín đơn giản) là một chuẩn truyền tải thư điện tử qua mạng Internet. SMTP được định nghĩa trong bản RFC 821 (STD 10) và được chỉnh lý bằng bản RFC 1123 (STD 3). Giao thức hiện dùng được là ESMTP (extended SMTP - SMTP mở rộng), được định nghĩa trong bản RFC 2821.

Lịch sử

SMTP là một giao thức dùng nền văn bản và tương đối đơn giản. Trước khi một thông điệp được gửi, người ta có thể định vị một hoặc nhiều địa chỉ nhận cho thông điệp - những địa chỉ này thường được kiểm tra về sự tồn tại trung thực của chúng) . Việc kiểm thử một trình chủ SMTP là một việc tương đối dễ dàng, dùng chương trình ứng dụng "telnet" (xem dưới đây).

SMTP dùng cổng 25 của giao thức TCP. Để xác định trình chủ SMTP của một tên miền nào đấy (domain name), người ta dùng một mẫu tin MX (Mail eXchange - Trao đổi thư) của DNS (Domain Name System - Hệ thống tên miền).

SMTP bắt đầu được sử dụng rộng rãi vào những năm đầu thập niên kỷ 1980. Tại thời điểm đó, SMTP chỉ là một phần mềm bổ sung của bộ trình ứng dụng đồng giao thức UUCP (Unix to Unix CoPy - Sao chép từ máy Unix sang máy Unix) nhưng tiện lợi hơn trong việc truyền tải thư điện tử giữa các máy vi tính - những máy này thỉnh thoảng mới lại được kết nối với nhau một lần, để truyền thông dữ

http://www.ebook.edu.vn

liệu. Thực ra, SMTP sẽ làm việc tốt hơn nếu các máy gửi và máy nhận được kết nối liên tục.

Sendmail là một trong những phần mềm đặc vụ truyền tải thư tín (mail transfer agent) đầu tiên (nếu không phải là cái trước tiên nhất) thực thi giao thức SMTP. Tính đến năm 2001, người ta đã thấy có ít nhất là 50 chương trình ứng dụng thực thi giao thức SMTP, bao gồm cả trình khách (phần mềm dùng để gửi thông điệp) và trình chủ (phần mềm dùng để nhận thông điệp). Một số trình chủ SMTP nổi tiếng có thể liệt kê bao gồm: exim, Postfix, qmail, và Microsoft Exchange Server.

Do thiết kế của giao thức dùng dạng thức văn bản thường của bộ mã ASCII, khi bản thiết kế được khởi công, chức năng của SMTP giải quyết tập tin có dạng thức nhi phân rất kém. Những tiêu chuẩn như MIME đã được xây dựng để mã hóa những tập tin nhị phân, cho phép chúng được truyền tải dùng giao thức SMTP. Hiện nay, phần lớn các trình chủ SMTP hỗ trở phần mở rộng 8BITMIME của SMTP, cho phép các tập tin ở dạng thức nhị phân được truyền thông qua đường dây, dễ như việc truyền tải văn bản thường vậy.

SMTP là một giao thức "đẩy" thông điệp và không cho phép ai "rút" thông điệp từ máy chủ ở xa, theo yêu cầu của mình, một cách tùy tiện. Để lấy được thông điệp, một trình khách thư điện tử phải dùng POP3 (Post Office Protocol - Giao thức bưu điện tử) hoặc IMAP (Internet Message Access Protocol - Giao thức truy cập thông điệp Internet). Chúng ta còn có thể dùng phần mềm ETRN (Extended Turn) để khởi động một trình chủ SMTP phân phát thông điệp mà nó đang lưu trữ.

http://www.ebook.edu.vn

Ví dụ về truyền thông của SMTP

Sau khi kết nối giữa người gửi (trình khách) và người nhận (trình chủ) đã được thiết lập, những việc làm sau đây là những việc hoàn toàn hợp lệ, đối với một phiên giao dịch dùng giao thức SMTP. Trong cuộc hội thoại dưới đây, những gì trình khách gửi được đánh dấu bằng chữ C: đứng trước, còn những gì trình chủ gửi được đánh dấu bằng S:. Các hệ thống máy tính đều có thể thiết lập một kết nối, bằng cách dùng những dòng lệnh của phần mềm telnet, trên một máy khách. Chẳng hạn:

telnet www.example.com 25

khởi động một kết nối SMTP từ máy gửi thông điệp đến máy chủ site www.example.com.

```
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM:<sender@mydomain.com>
S: 250 Ok
C: RCPT TO:<friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: test message
C: From: sender@mydomain.com
C: To: friend@example.com
C:
C: Hello,
C: This is a test.
C: Goodbye.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```


http://www.ebook.edu.vn

Bảo vệ trong SMTP và thư rác

Một trong những giới hạn của bản thiết kế SMTP gốc là việc nó không cung cấp một phương tiện nào để chứng thực (authentication) người gửi khi chúng ta cần. Chính vì thế mà phần mở rộng SMTP-AUTH đã được thiết kế và bổ sung.

Mặc dầu đã có phần chứng thực người gửi bổ sung, nhũng lạm thư điện tử vẫn còn là một vấn đề lớn, khó giải quyết. Việc sửa đổi giao thức SMTP một cách triệt để, hoặc thay thế giao thức toàn bằng một cái khác, là một việc không dễ gì thực hiện được, vì sự thay đổi sẽ gây ảnh hưởng đến mạng lưới truyền thông của những máy chủ SMTP khổng lồ, đã và đang được dùng. Internet Mail 2000 là một trong những bản dự thảo đề cập đến vấn đề này.

Vì lý do trên, một số đề nghị về việc dùng các giao thức bên lề để hỗ trợ hoạt động của SMTP đã được công bố. Nhóm nghiên cứu chống thư nhũng lạm (Anti-Spam Research Group) của Lực lượng chuyên trách nghiên cứu liên mạng (Internet Research Task Force - viết tắt là IRTF) hiện đang làm việc trên một số dự thảo về chứng thực thư điện tử (E-mail authentication) và một số những dự thảo khác liên quan đến việc cung cấp một cơ chế chứng thực nguồn gửi với tính năng: tuy đơn giản song linh hoạt, tuy ở mức độ hạng nhẹ song có khả năng khuếch trương. Những hoạt động gần đây của Lực lượng chuyên trách nghiên cứu liên mạng (Internet Engineering Task Force - viết tắt là IETF), bao gồm MARID (2004) (cộng với sự tiến tới hai cuộc thử nghiệm được IETF chấp thuận trong năm 2005 sau đó), và DKIM (DomainKeys - tạm dịch là "Chìa khóa tại vùng") trong năm 2006.

http://www.ebook.edu.vn

POP3

Post Office Protocol phiên bản 3 (POP3) là một giao thức tầng ứng dụng, dùng để lấy thư điện tử từ server mail, thông qua kết nối TCP/IP. POP3 và IMAP4 (Internet Message Access Protocol) là 2 chuẩn giao thức Internet thông dụng nhất dùng để lấy nhận email. Hầu như các máy tính hiện nay đều hỗ trợ cả 2 giao thức

Trước POP3, đã có 2 phiên bản là POP1 và POP2. Khi POP3 ra đời, đã ngay lập tức thay thế hoàn toàn các phiên bản cũ. Vì vậy, ngày nay, nhắc đến POP thì thường là ám chỉ POP3.

Thiết kế của POP3 hỗ trợ chức năng cho người dùng có kết nối internet không thường trực (như kết nối dial-up), cho phép người dùng kết nối với server, tải mail về, sau đó có thể xem, thao tác với mail offline. Mặc dù trong giao thức hỗ trợ leave mail on server (để nguyên mail trên server), nhưng hầu hết người dùng đều thực hiện mặc định, tức là: kết nối, tải mail về, xóa mail trên server rồi ngắt kết nối.

IMAP

Internet Message Access Protocol (IMAP) cung cấp lệnh để phần mềm thư điện tử trên máy khách và máy chủ dùng trong trao đổi thông tin. Đó là phương pháp để người dùng cuối truy cập thông điệp thư điện tử hay bảng tin điện tử từ máy chủ về thư trong môi trường cộng tác. Nó cho phép chương trình thư điện tử dùng cho máy khách - như Netscape Mail, Eudora của Qualcomm, Lotus Notes hay Microsoft Outlook - lấy thông điệp từ xa trên máy chủ một cách dễ dàng như trên đĩa cứng cục bộ.

http://www.ebook.edu.vn

Chuẩn về thư điện tử được ủng hộ

IMAP là cơ chế cho phép lấy thông tin về thư điện tử của bạn, hay chính các thông điệp từ mail server của môi trường cộng tác.

Giao thức thư điện tử này cho phép người dùng kết nối bằng đường điện thoại vào máy chủ Internet từ xa, xem xét phần tiêu đề và người gửi của thư điện tử trước khi tải những thư này về máy chủ của mình.

Với IMAP người dùng có thể truy cập các thông điệp như chúng được lưu trữ cục bộ trong khi thực tế lại là thao tác trên máy chủ cách xa hàng ki lô mét.

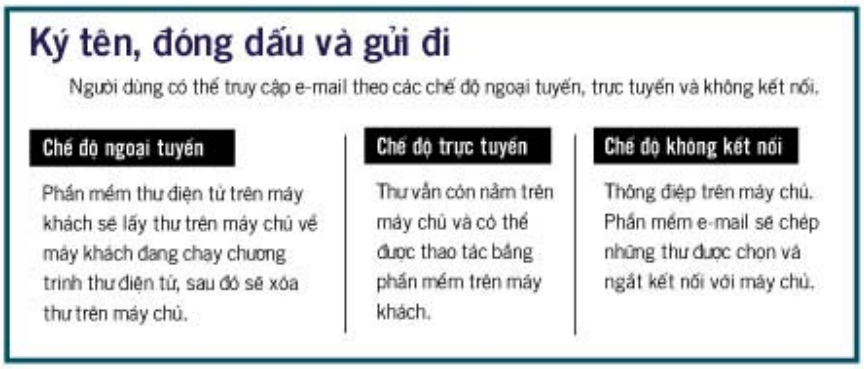
Với khả năng truy cập từ xa này, IMAP dễ được người dùng cộng tác chấp nhận vì họ coi trọng khả năng làm việc lưu động.

Khả năng truy cập là chìa khóa

Người dùng thường xuyên đi lại muốn lưu thông điệp của họ trên máy chủ để đến bất kỳ đầu cuối nào cũng có thể đọc và làm việc được. IMAP cho phép thực hiện điều đó.

IMAP khác với giao thức truy cập thư điện tử Post Office Protocol (POP). POP lưu trữ toàn bộ thông điệp trên máy chủ. Người dùng kết nối bằng đường điện thoại vào máy chủ và POP sẽ đưa các thông điệp vào in-box của người dùng, sau đó xóa thư trên máy chủ. Hai giao thức này đã được dùng từ hơn 10 năm nay. Theo một nhà phân tích thì khác biệt chính giữa POP (phiên bản hiện hành 3.0) và IMAP (phiên bản hiện hành 4.0) là POP3 cho người dùng ít quyền điều khiển hơn trên thông điệp.

http://www.ebook.edu.vn



IMAP mang lại cho người dùng một phương thức lưu trữ thư điện tử thông minh và nhờ đó có thể xem những thông điệp này trước khi tải chúng xuống, bao gồm cả việc có tải xuống những file đính kèm thư hay không. Người dùng cũng có thể áp dụng các bộ lọc và cơ chế tìm kiếm trên máy chủ và có thể lấy thư từ bất kỳ máy nào, bất cứ ở đâu.

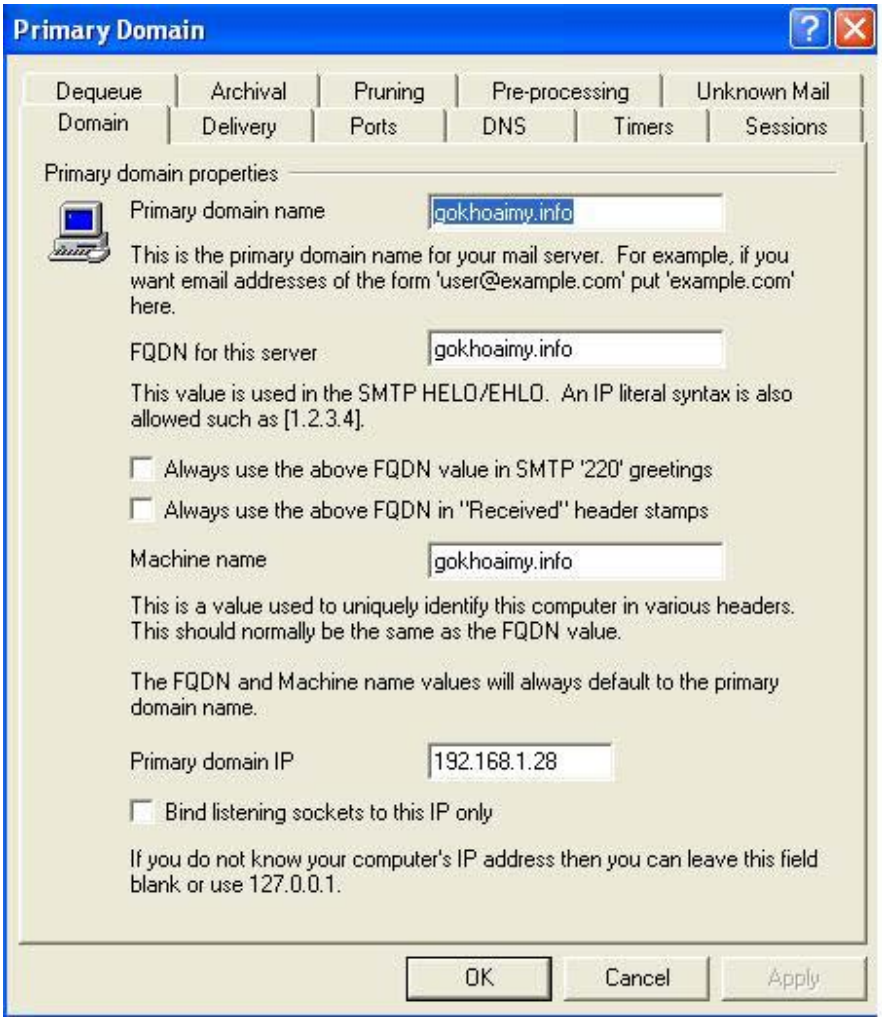
Tuy nhiên, các nhà sản xuất đã thông dịch các đặc tả mơ hồ của IMAP 4 theo nhiều cách khác nhau và điều đó dẫn đến sự không nhất quán trong chương trình thư dành cho máy khách và máy chủ, chẳng hạn người dùng có thể sẽ không đọc được file đính kèm trong Netscape Mail bằng chương trình Eudora Pro. Tuy nhiên, theo dự đoán những vấn đề này sẽ nhanh chóng được giải quyết trong thời gian tới.

13.2. Triển khai Mail Server cho doanh nghiệp

Có nhiều Mail Server để triển khai một hệ thống Mail cho doanh nghiệp. Trong phần này tôi xin giới thiệu Mdaemon là một mail Server dễ triển khai và có đầy đủ các tính năng thông dụng phục vụ cho một doanh nghiệp.

http://www.ebook.edu.vn

Cài đặt và cấu hình Mdaemon

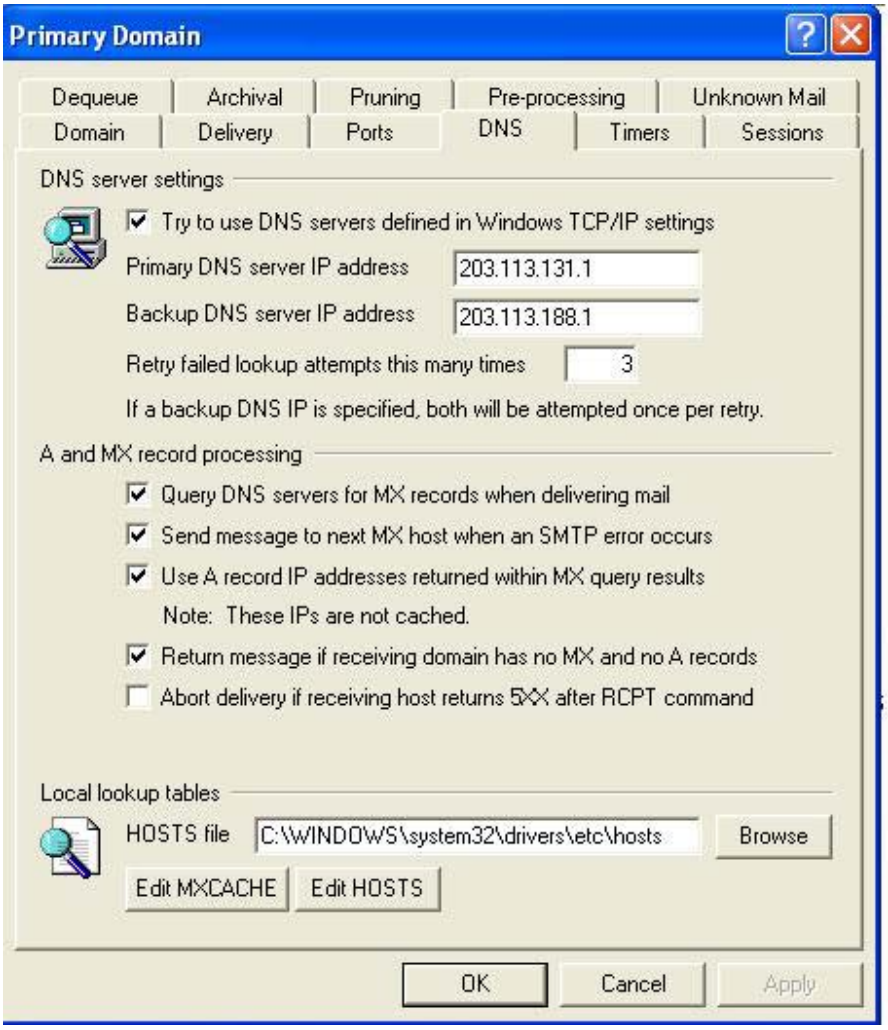


Setup > Primary Domain

Primary domain, FQDN domain, machine name: tên domain của bạn

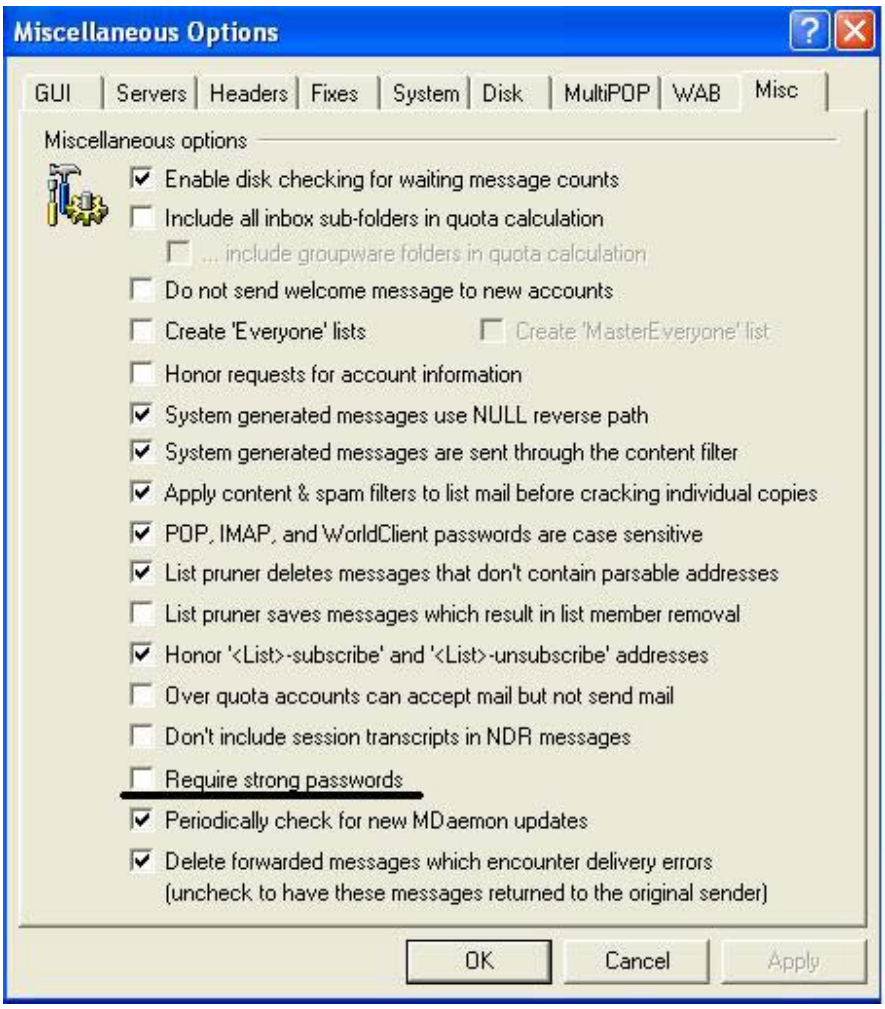
Primary Domain IP: IP máy bạn

http://www.ebook.edu.vn



Qua tab DNS : chỉnh về IP mà ISP bạn đang dùng (ở đây tôi dùng Viettel)

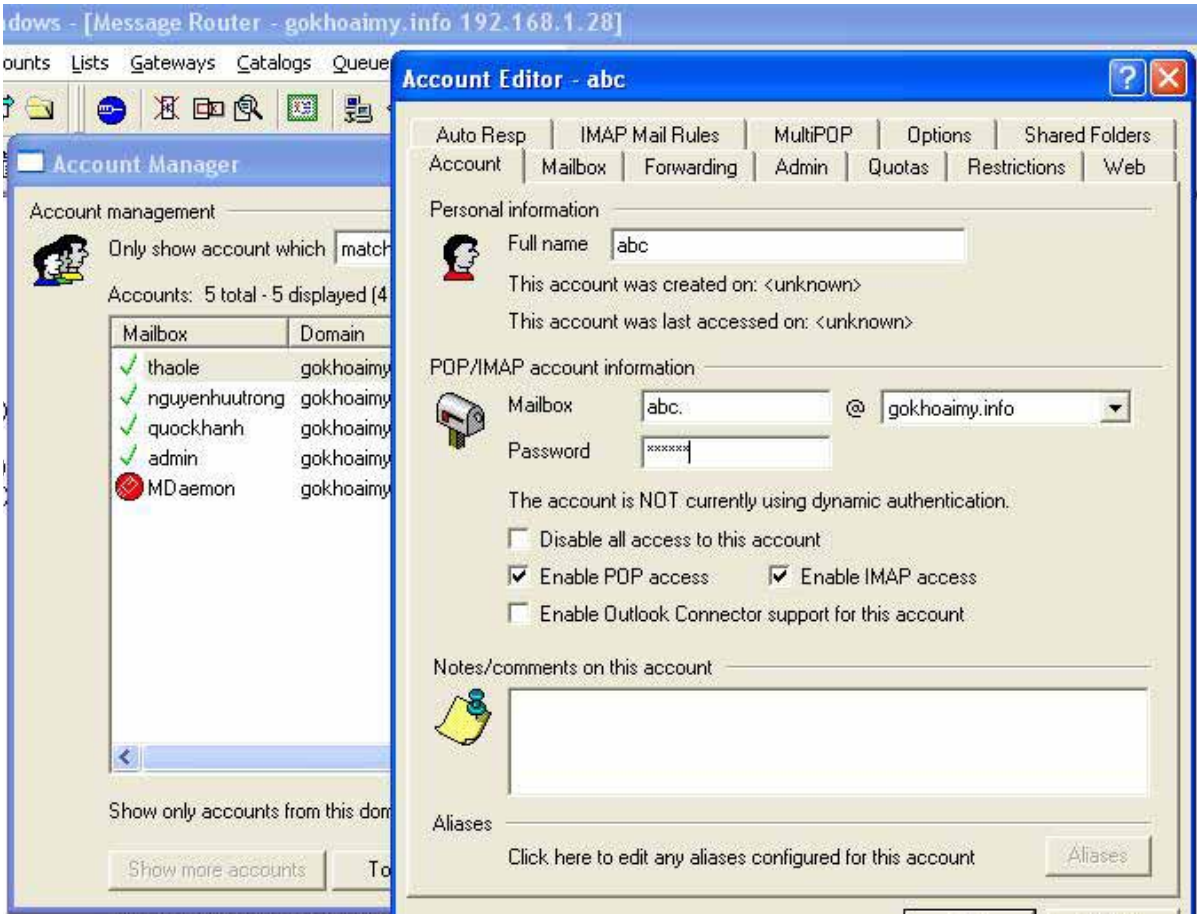
http://www.ebook.edu.vn



Để tạo mailbox với password đơn giản, vào Menu Setup > Miscellaneous Options > Tab Misc > bỏ chọn "Require strong passwords"

http://www.ebook.edu.vn

Tạo Account



http://www.ebook.edu.vn

Bài 14. Thực hành Xây dựng một Mail Server

Chuẩn bị

- Một Server đã cài dịch vụ DNS, IIS
- Mail Server Mdeamon hoặc Exchange

Yêu cầu:

- Cấu hình mail Server và tạo account cho các thành viên trong lớp sử dụng để gửi và nhận mail

http://www.ebook.edu.vn

Bài 15: Thực hành Proxy và Firewall

15.1. Nguyên lý hoạt động của Proxy

Khái niệm Proxy

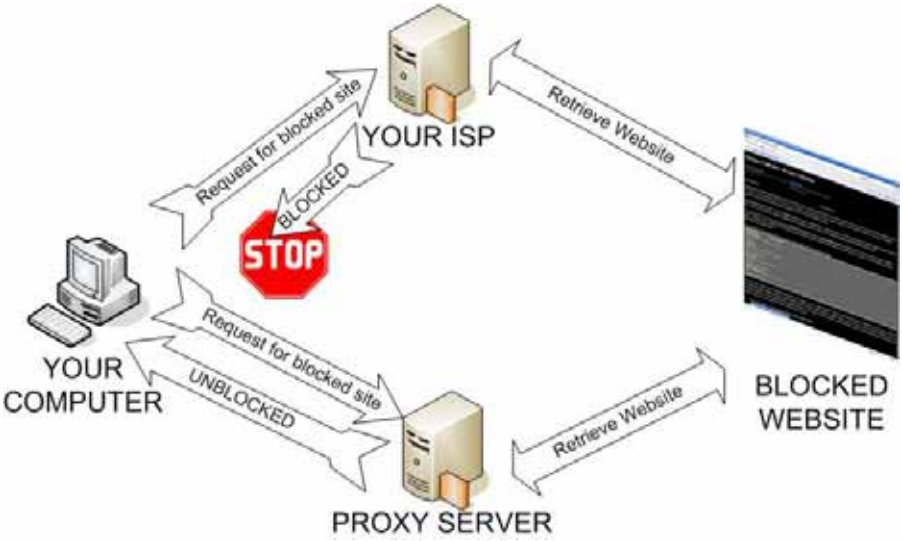
Proxy là một Internet server làm nhiệm vụ chuyển tiếp thông tin và kiểm soát tạo sự an toàn cho việc truy cập Internet của các máy khách, còn gọi là khách hàng sử dụng dịch vụ internet. Trạm cài đặt proxy gọi là proxy server. Proxy hay trạm cài đặt proxy có địa chỉ IP và một cổng truy cập cố định. Ví dụ: 123.234.111.222:80 Địa chỉ IP của proxy trong ví dụ là 123.234.111.222 và cổng truy cập là 80.

Chức năng của proxy

Đối với một só hãng, công ty người ta sử dụng proxy vào việc:

-Proxy chia sẽ đường truyền: giúp nhiều máy truy cập Internet thông qua 1 máy, mà máy này gọi là Proxy server. Chỉ duy nhất máy Proxy này cần modem và account truy cập internet, các máy client (các máy trực thuộc) muốn truy cập internet qua máy này chỉ cần nối mạng LAN tới máy Proxy và truy cập địa chỉ yêu cầu.Những yêu cầu của người sử dung sẽ qua trung gian proxy server thay thế cho server thật sự mà người sử dụng cần giao tiếp, tại điểm trung gian này công ty kiểm soát được mọi giao tiếp từ trong công ty ra ngoài intrnet và từ internet vào máy của công ty. Sử dụng Proxy, công ty có thể cấm nhân viên truy cập những địa chỉ web không cho phép, cải thiện tốc độ truy cập nhờ sự lưu trữ cục bộ các trang web trong bộ nhớ của proxy server và giấu định danh địa chỉ của mạng nội bộ gây khó khăn cho việc thâm nhập từ bên ngoài vào các máy của công ty.

http://www.ebook.edu.vn



Hình 15.1

Đối với các nhà cung cấp dịch vụ đường truyền internet:

-Do trên mạng internet có lượng thông tin rất phong phú, theo quan điểm của từng quốc gia, của từng chủng tộc hay địa phương, các nhà cung cấp dịch vụ internet khu vực đó sẽ phối hợp proxy với kỹ thuật tường lửa để tạo ra một bộ lọc gọi là firewall proxy nhằm ngăn chặn các thông tin độc hại hoặc trái thuần phong mỹ tục đối với quốc gia, đói với chủng tộc hay địa phương đó. Địa chỉ các websit mà khách hàng yêu cầu truy cập sẽ được lọc tại bộ lọc này, nếu địa chỉ không bị cấm thì yêu cầu của khách hàng tiếp tục được gửi đi, tới các DNS server của các nhà cung cấp dịch vụ. Firewall proxy sẽ lọc tất cả các thông tin từ internet gửi vào máy của khách hàng và ngược lại.

Ý nghĩa của proxy

Proxy không chỉ có giá trị bởi nó làm được nhiệm vụ của một bộ lọc thông tin, nó còn tạo ra được sự an toàn cho các khách hàng của nó, firewal Proxy ngăn chặn hiệu quả sự xâm nhập của các đối tượng không mong muốn vào máy của

http://www.ebook.edu.vn

khách hàng. Proxy lưu trữ dược các thông tin mà khách hàng cần trong bộ nhớ, do đó làm giảm thời gian truy tìm làm cho việc sử dụng băng thông hiệu quả.

Proxy server giống như một vệ sĩ bảo vệ khỏi những rắc rối trên Internet. Một Ps thường nằm bên trong tường lửa, giữa trình duyệt web và server thật, làm chức năng tạm giữ những yêu cầu Internet của các máy khách để chúng không giao tiếp trực tiếp Internet. Người dùng sẽ không truy cập được những trang web không cho phép (bị công ty cấm).

Mọi yêu cầu của máy khách phải qua Ps, nếu địa chỉ IP có trên proxy, nghĩa là Website này được lưu trữ cục bộ, thì trang này sẽ đươc truy cập mà không cần phải kết nối Internet, nếu không có trên Ps và trang này không bị cấm yêu cầu sẽ được chuyển đến server thật, DNS server... và ra Internet. Ps lưu trữ cục bộ các trang Web thường truy cập nhất trong bộ đệm giảm chi phí, tốc độ hiển thị trang Web nhanh.

Proxy server bảo vệ mạng nội bộ khỏi bị xác định bởi bên ngoài bằng cách mang lại cho mạng hai định danh: một cho nội bộ, một cho bên ngoài. Điều này tạo ra một "bí danh" đối với thế giới bên ngoài gây khó khăn đối với nếu người dùng "tự tung tự tác" hay các tay bẻ khóa muốn xâm nhập trực tiếp máy nào đó.

Cách sử dụng proxy hiệu quả

Do các proxy có quy mô bộ nhớ khác nhau và số lượng người đang sử dụng proxy nhiều-ít khác nhau, Proxy server hoạt động quá tải thì tốc độ truy cập internet của khách hàng có thể bị chậm. Mặt khác một số websit khách hàng có đầy đủ điều kiện nhân thân để đọc, nghiên cứu nhưng bị tường lửa chặn không truy cập được thì biện pháp đổi proxy để truy cập là điều cần thiết nhằm đảm bảo công việc. Do đó người sử dụng có thể chọn proxy server để sử dụng cho riêng

http://www.ebook.edu.vn

mình. Có các cách chọn lựa cho người sử dụng. Sử dụng proxy mặc định của nhà cung cấp dịch vụ (internet), trường hợp này người sử dụng không cần điền địa chỉ IP của proxy vào cửa sổ internet option của trình duyệt trong máy của mình. Sử dụng proxy server khác (phải trả phí hoặc miễn phí) thì phải điền địa chỉ IP của proxy server vào cửa sổ internet option của trình duyệt.

Một số Proxy miễn phí tham khảo

IP address	Anonymity level	Checked time	Country
203.252.226.215:8001	transparent	Dec-26, 18:26	Korea, Republic of
81.20.173.65:3128	transparent server	Dec-26, 10:08	Russian Federation
81.92.147.62:3128	transparent	Dec-26, 18:15	Czech Republic
189.15.68.99:3128	transparent	Dec-26, 16:14	Brazil
141.223.175.140:8080	transparent proxy server	Dec-26, 15:57	Korea, Republic of
85.226.20.158:3128	transparent proxy	Dec-26, 14:49	Sweden
66.29.36.95:554	hight-anonymous ($)	Dec-27, 06:01	United States
88.243.48.144:3128	transparent	Dec-26, 18:22	Turkey
213.144.14.66:3128	transparent server	Dec-26, 20:44	Germany
212.62.102.247:80	transparent proxy	Dec-26, 14:43	Saudi Arabia
61.19.237.202:8080	transparent	Dec-26, 09:55	Thailand
61.50.217.230:1080	transparent proxy	Dec-26, 09:55	China
202.206.100.39:3128	transparent proxy	Dec-26, 15:59	China
61.142.249.116:8080	transparent proxy	Dec-26, 09:59	China
118.98.212.242:3128	transparent proxy	Dec-26, 19:05	Indonesia
203.73.180.16:3128	transparent	Dec-25, 18:26	Taiwan
200.129.25.3:8080	transparent proxy	Dec-26, 18:29	Brazil
203.190.51.206:8080	transparent server	Dec-25, 14:21	Indonesia
212.62.102.134:80	transparent server	Dec-25, 14:23	Saudi Arabia

http://www.ebook.edu.vn

15.2. Nguyên lý hoạt động của Firewall

Khái niệm tường lửa (Firewall)

Trong ngành mạng máy tính, bức tường lửa (tiếng Anh: firewall) là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

Tường lửa là một thiết bị phần cứng và/hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các tòa nhà. Tường lửa còn được gọi là Thiết bị bảo vệ biên giới (Border Protection Device - BPD), đặc biệt trong các ngữ cảnh của NATO, hay bộ lọc gói tin (packet filter) trong hệ điều hành BSD - một phiên bản Unix của Đại học California, Berkeley.

Nhiệm vụ cơ bản của tường lửa là kiểm soát giao thông dữ liệu giữa hai vùng tin cậy khác nhau. Các vùng tin cậy (zone of trust) điển hình bao gồm: mạng Internet (vùng không đáng tin cậy) và mạng nội bộ (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc quyền tối thiểu (principle of least privilege).
Cấu hình đúng đắn cho các tường lửa đòi hỏi kĩ năng của người quản trị hệ thống. Việc này đòi hỏi hiểu biết đáng kể về các giao thức mạng và về an ninh

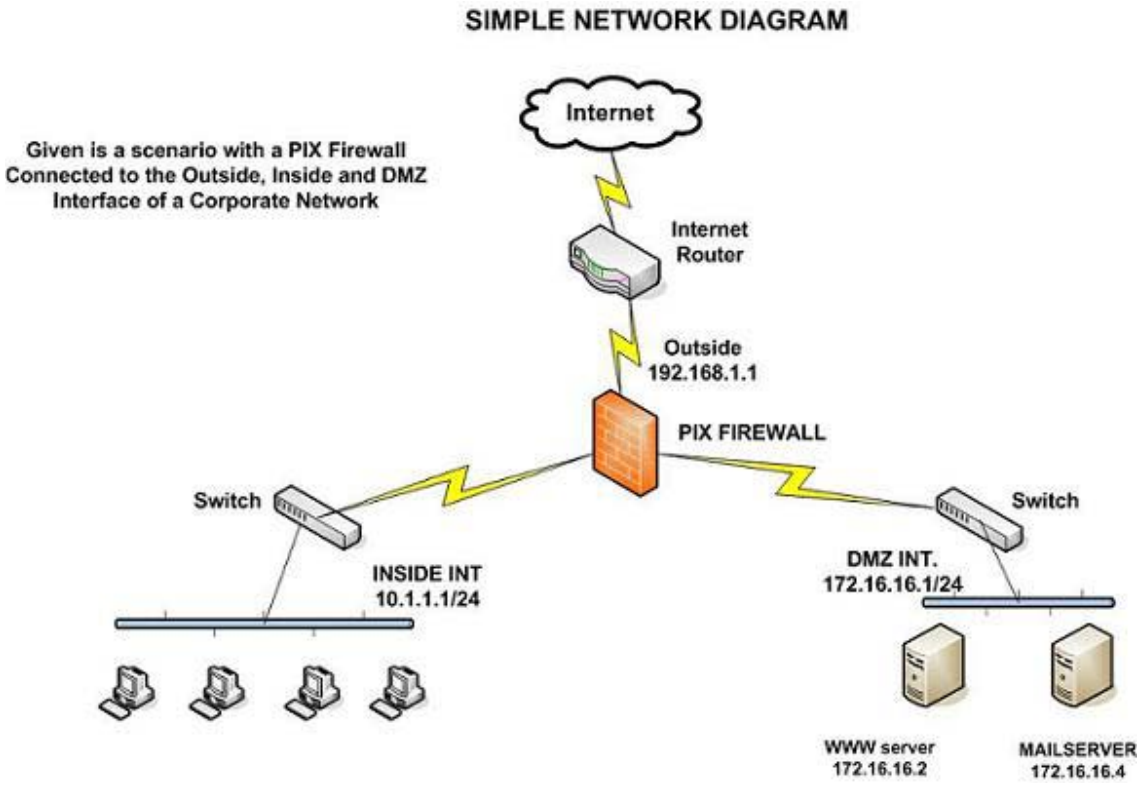
http://www.ebook.edu.vn

máy tính. Những lỗi nhỏ có thể biến tường lửa thành một công cụ an ninh vô dụng.

Lịch sử phát triển Firewall

Công nghệ tường lửa bắt đầu xuất hiện vào cuối những năm 1980 khi Internet vẫn còn là một công nghệ khá mới mẻ theo khía cạnh kết nối và sử dụng trên toàn cầu. Ý tưởng đầu tiên được đã hình thành sau khi hàng loạt các vụ xâm phạm nghiêm trọng đối với an ninh liên mạng xảy ra vào cuối những năm 1980. Năm 1988, một nhân viên tại trung tâm nghiên cứu NASA Ames tại California gửi một bản ghi nhớ qua thư điện tử tới đồng nghiệp rằng: "Chúng ta đang bị một con VIRUS Internet tấn công! Nó đã đánh Berkeley, UC San Diego, Lawrence Livermore, Stanford, và NASA Ames." Con virus được biết đến với tên Sâu Morris này đã được phát tán qua thư điện tử và khi đó đã là một sự khó chịu chung ngay cả đối với những người dùng vô thưởng vô phạt nhất. Sâu Morris là cuộc tấn công diện rộng đầu tiên đối với an ninh Internet. Cộng đồng mạng đã không hề chuẩn bị cho một cuộc tấn công như vậy và đã hoàn toàn bị bất ngờ. Sau đó, cộng đồng Internet đã quyết định rằng ưu tiên tối cao là phải ngăn chặn không cho một cuộc tấn công bất kỳ nào nữa có thể xảy ra, họ bắt đầu cộng tác đưa ra các ý tưởng mới, những hệ thống và phần mềm mới để làm cho mạng Internet có thể trở lại an toàn.

http://www.ebook.edu.vn



Năm 1988, bài báo đầu tiên về công nghệ tường lửa được công bố, khi Jeff Mogul thuộc Digital Equipment Corp. phát triển các hệ thống lọc đầu tiên được biết đến với tên các tường lửa lọc gói tin. Hệ thống khá cơ bản này đã là thế hệ đầu tiên của cái mà sau này sẽ trở thành một tính năng kỹ thuật an toàn mạng được phát triển cao. Từ năm 1980 đến năm 1990, hai nhà nghiên cứu tại phòng thí nghiệm AT&T Bell, Dave Presetto và Howard Trickey, đã phát triển thế hệ tường lửa thứ hai, được biến đến với tên các tường lửa tầng mạch (circuit level firewall). Các bài báo của Gene Spafford ở Đại học Purdue, Bill Cheswick ở phòng thí nghiệm AT&T và Marcus Ranum đã mô tả thế hệ tường lửa thứ ba, với tên gọi tường lửa tầng ứng dụng (application layer firewall), hay tường lửa dựa proxy (proxy-based firewall). Nghiên cứu công nghệ của Marcus Ranum đã khởi đầu cho việc tạo ra sản phẩn thương mại đầu tiên. Sản phẩm này đã được

http://www.ebook.edu.vn

Digital Equipment Corporation's (DEC) phát hành với tên SEAL. Đợt bán hàng lớn đầu tiên của DEC là vào ngày 13 tháng 9 năm 1991 cho một công ty hóa chất tại bờ biển phía Đông của Mỹ.

Tại AT&T, Bill Cheswick và Steve Bellovin tiếp tục nghiên cứu của họ về lọc gói tin và đã phát triển một mô hình chạy được cho công ty của chính họ, dựa trên kiến trúc của thế hệ tường lửa thứ nhất của mình. Năm 1992, Bob Braden và Annette DeSchon tại Đại học Nam California đã phát triển hệ thống tường lửa lọc gói tin thế hệ thứ tư. Sản phẩm có tên "Visas" này là hệ thống đầu tiên có một giao diện với màu sắc và các biểu tượng, có thể dễ dàng cài đặt thành phần mềm cho các hệ điều hành chẳng hạn Microsoft Windows và Mac/OS của Apple và truy nhập từ các hệ điều hành đó. Năm 1994, một công ty Israel có tên Check Point Software Technologies đã xây dựng sản phẩm này thành một phần mềm sẵn sàng cho sử dụng, đó là FireWall-1. Một thế hệ thứ hai của các tường lửa proxy đã được dựa trên công nghệ Kernel Proxy. Thiết kế này liên tục được cải tiến nhưng các tính năng và mã chương trình cơ bản hiện đang được sử dụng rộng rãi trong cả các hệ thống máy tính gia đình và thương mại. Cisco, một trong những công ty an ninh mạng lớn nhất trên thế giới đã phát hành sản phẩm này năm 1997.

Thế hệ FireWall-1 mới tạo thêm hiệu lực cho động cơ kiểm tra sâu gói tin bằng cách chia sẻ chức năng này với một hệ thống ngăn chặn xâm nhập.

Các loại tường lửa

Có ba loại tường lửa cơ bản tùy theo:

- Truyền thông được thực hiện giữa một nút đơn và mạng, hay giữa một số mạng.
- Truyền thông được chặn tại tầng mạng, hay tại tầng ứng dụng.

http://www.ebook.edu.vn

- Tường lửa có theo dõi trạng thái của truyền thông hay không.

Phân loại theo phạm vi của các truyền trông được lọc, có các loại sau:

- Tường lửa cá nhân, một ứng dụng phần mềm với chức năng thông thường là lọc dữ liệu ra vào một máy tính đơn.
- Tường lửa mạng, thường chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các khu phi quân sự (mạng con trung gian nằm giữa mạng nội bộ và mạng bên ngoài). Một tường lửa thuộc loại này lọc tất cả giao thông dữ liệu vào hoặc ra các mạng được kết nối qua nó.

Loại tường lửa mạng tương ứng với ý nghĩa truyền thống của thuật ngữ "tường lửa" trong ngành mạng máy tính.

Khi phân loại theo các tầng giao thức nơi giao thông dữ liệu có thể bị chặn, có ba loại tường lửa chính:

- Tường lửa tầng mạng. Ví dụ iptables.
- Tường lửa tầng ứng dụng. Ví dụ TCP Wrappers.
- Tường lửa ứng dụng. Ví dụ: hạn chế các dịch vụ ftp bằng việc định cấu hình tại tệp /etc/ftpaccess.

Các loại tường lửa tầng mạng và tường lửa tầng ứng dụng thường trùm lên nhau, mặc dù tường lửa cá nhân không phục vụ mạng, nhưng một số hệ thống đơn đã cài đặt chung cả hai.

Cuối cùng, nếu phân loại theo tiêu chí rằng tường lửa theo dõi trạng thái của các kết nối mạng hay chỉ quan tâm đến từng gói tin một cách riêng rẽ, có hai loại tường lửa:

- Tường lửa có trạng thái (Stateful firewall)
- Tường lửa phi trạng thái (Stateless firewall)

http://www.ebook.edu.vn

Lý do sử dụng tường lửa

Mạng internet ngày càng phát triển và phổ biến rộng khắp mọi nơi, lợi ích của nó rất lớn. Tuy nhiên cũng có rất nhiều ngoại tác không mong muốn đối với các cá nhân là cha mẹ hay tổ chức, doanh nghiệp, cơ quan nhà nước... như các trang web không phù hợp lứa tuổi, nhiệm vụ, lợi ích, đạo đức, pháp luật hoặc trao đổi thông tin bất lợi cho cá nhân, doanh nghiệp... Do vậy họ (các cá nhân, tổ chức, cơ quan và nhà nước) sử dụng tường lửa để ngăn chặn.

Một lý do khác là một số quốc gia theo chế độ độc tài, độc đảng áp dụng tường lửa để ngăn chận quyền trao đổi, tiếp cận thông tin của công dân nước mình không cho họ truy cập vào các trang web hoặc trao đổi với bên ngoài, điều mà nhà cầm quyền cho rằng không có lợi cho chế độ đó.

Cách thức ngăn chặn

Để ngăn chặn các trang web không mong muốn, các trao đổi thông tin không mong muốn người ta dùng cách lọc các địa chỉ web không mong muốn mà họ đã tập hợp được hoặc lọc nội dung thông tin trong các trang thông qua các từ khóa để ngăn chặn những người dùng không mong muốn truy cập vào mạng và cho phép người dùng hợp lệ thực hiện việc truy xuất.

Bức tường lửa có thể là một thiết bị định hướng (Router, một thiết bị kết nối giữa hai hay nhiều mạng và chuyển các thông tin giữa các mạng này) hay trên một máy chủ (Server), bao gồm phần cứng và/hoặc phần mềm nằm giữa hai mạng (chẳng hạn mạng Internet và mạng liên kết các gia đình, điểm kinh doanh internet, tổ chức, công ty, hệ thống Ngân hàng, cơ quan nhà nước.

Cơ quan nhà nước có thể lập bức tường lửa ngay từ cổng Internet quốc gia hoặc yêu cầu các nhà cung cấp dịch vụ đường truyền (IXP) và cung cấp dịch vụ Internet (ISP) thiết lập hệ thống tường lửa hữu hiệu hoặc yêu cầu các đại lý kinh

http://www.ebook.edu.vn

doanh internet thực hiện các biện pháp khác như Thông tư liên tịch số 02/2005/TTLT về quản lý đại lý Internet có hiệu lực vào đầu tháng 8-2005 ở Việt Nam.

Vượt tường lửa

Các trang web bị chặn nhất là các trang web sex thường rất linh động thay đổi địa chỉ để tránh sự nhận diện hoặc nhanh chóng thông báo địa chỉ mới một cách hạn chế với các đối tượng dùng đã định.

Người dùng ở các nước có hệ thống tường lửa có thể tiếp cận với nội dung bị chặn qua các ngõ khác bằng cách thay đổi địa chỉ Proxy, DNS hoặc qua vùng nhớ đệm cached của trang tìm kiếm thông dụng như Google, Yahoo..., hoặc sử dụng phần mềm miễn phí Tor. Nói chung người dùng mạng hiểu biết nhiều về máy tính thì biết nhiều kỹ xảo vượt tường lửa.

Hiệu quả khi sử dụng tường lửa

Bức tường lửa chỉ có hiệu quả tốt một thời gian sau đó các trang web bị chặn cũng như người sử dụng dùng mưu mẹo, kỹ xảo, kỹ thuật để né và vượt tường, vì vậy phải luôn luôn cập nhật kỹ thuật, nhận điện các địa chỉ mới để thay đổi phương thức hoạt động, điều này làm tốc độ truy cập chung bị giảm và đòi hỏi phải nâng cấp trang thiết bị, kỹ thuật.

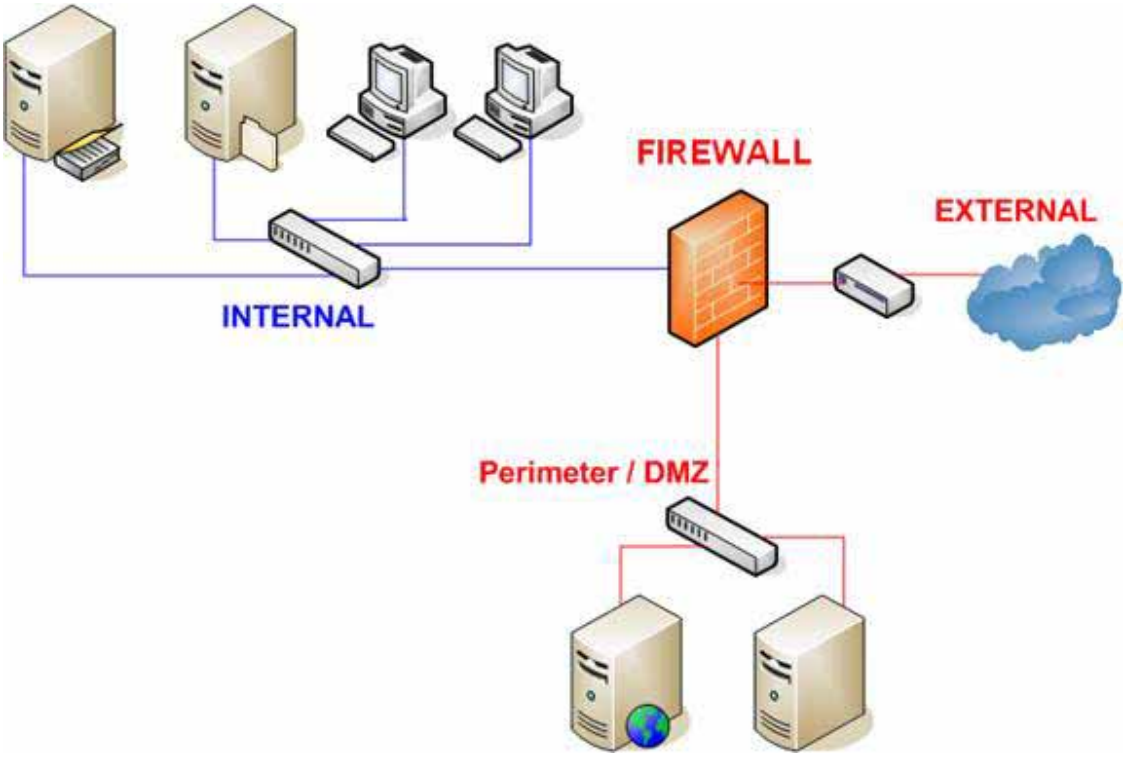
Nhược điểm khi sử dụng tường lửa

Sử dụng tường lửa cần phải xử lý một lượng lớn thông tin nên việc xử lý lọc thông tin có thể làm chậm quá trình kết nối của người kết nối.

Việc sử dụng tường lửa chỉ hữu hiệu đối với những người không thành thạo kỹ thuật vượt tường lửa, những người sử dụng khác có hiểu biết có thể dễ dàng vượt qua tường lửa bằng cách sử dụng các proxy không bị ngăn chặn.

http://www.ebook.edu.vn

15.3. Triển khai xây dựng hệ thống tường lửa cho doanh nghiệp



Mô tả sơ đồ hệ thống:

- Gồm 01 PC đóng vai trò Domain Controller (DC)
- Mạng LAN thuộc dải IP 192.168.1.0/24
- DMZ thuộc dải IP 172.16.1.0/24
- External có dải IP 10.0.0.0/30
- Firewall có 03 Fast Ethernet tương ứng 03 phân vùng LAN (Internal), DMZ và External

Yêu cầu:

- Các PC join vào Domain (DC)
- File Server và Web Server thuộc vùng DMZ cho phép các PC thuộc LAN truy cập vào
- Các PC thuộc LAN có thể truy cập Internet theo sự cho phép của Firewall

http://www.ebook.edu.vn

Bài 16: Cơ bản về bảo mật

16.1. Một số nguy cơ tấn công trên mạng

Những nguy cơ bảo mật đe dọa mất mát dữ liệu nhạy cảm luôn là mối lo ngại của những doanh nghiệp vừa và nhỏ. Sau đây là 10 nguy cơ bảo mật được đánh giá là nguy hiểm nhất mà doanh nghiệp phải đối mặt.

Những nhân viên bất mãn với công ty

Trong một số doanh nghiệp vừa và nhỏ, những dữ liệu kinh doanh quan trọng hay thông tin khách hàng thường được giao phó cho một cá nhân. Điều này tạo nên tình trạng "lệ thuộc quyền hạn" nguy hiểm. Khi cá nhân đó bất mã vì một lý do nào đó với công ty và ban điều hành công ty. Lúc này vấn đề chỉ còn là thời gian và quyền hạn kiểm soát thông tin của anh ta mà thôi.

Không có kế hoạch xử lý rủi ro

Hệ thống máy tính, mạng của doanh nghiệp luôn phải đối mặt với nhiều nguy cơ bảo mật, từ việc hư hỏng vật lý cho đến các trường hợp bị tấn công từ tin tặc hay virus đều có khả năng gây tổn hại cho dữ liệu. Khá nhiều doanh nghiệp vừa và nhỏ thiếu hẳn chính sách phản ứng với việc thất thoát dữ liệu hay kế hoạch khắc phục sự cố. Đại đa số đều lúng túng và bắt đầu các hoạt động mang tính ứng phó.

Những thiết lập mặc định không được thay đổi

http://www.ebook.edu.vn

Tin tặc hiện nay thường dùng các tập tin chứa đựng hàng trăm ngàn tài khoản mặc định (username và password) của các thiết bị kết nối mạng để dò tìm quyền hạn truy xuất khả năng đăng nhập vào hệ thống mạng. Nếu các tài khoản, thiết lập mặc định không được thay đổi, tin tặc sẽ dễ dàng chiếm quyền điều khiển tài nguyên mạng.

Môi trường mạng tại gia không an toàn

Đối với một vài doanh nghiệp nhỏ, các nhân viên thường đem máy tính xách tay (laptop) của mình đến văn phòng để làm việc. Trong môi trường mạng tại gia đình, chế độ bảo mật thường rất kém hay thậm chí không có những thiết lập bảo vệ. Do đó, những chiếc laptop của nhân viên có thể là nguồn gốc phát tán virus, malware hay trở thành zombie trung gian để tin tặc tấn công vào hệ thống mạng của doanh nghiệp.

Thiếu cảnh giác với mạng công cộng

Một thủ đoạn chung tin tặc hay sử dụng để dẫn dụ những nạn nhân là đặt một thiết bị trung chuyển wireless access-point không cài đặt mật khẩu (unsecured) rồi gán một cái nhãn như "Mạng Wi-Fi miễn phí" và rung đùi ngồi chờ những kết nối "ngây thơ" rơi vào bẫy. Tin tặc sẽ dùng các công cụ thâu tóm gói dữ liệu mạng giúp nhận biết cả những văn bản hay bất kỳ những gì mà nhân viên doanh nghiệp gõ rồi gửi ra ngoài.

Mất mát thiết bị di động

Rất nhiều doanh nghiệp, thậm chí gần đây còn có cả một vài hãng lớn bị thất thoát dữ liệu quan trọng do mất cắp máy tính xách tay, thất lạc điện thoại di động hay các đĩa flash USB lưu trữ. Dữ liệu trong các thiết bị này thường ít được mã hóa hay bảo vệ bằng mật khẩu, rất dễ dàng xử lý một khi đã sở hữu chúng.

Lỗi từ máy chủ web

Hiện còn khá nhiều doanh nghiệp không coi trọng việc đặt website của mình tại máy chủ nào, mức độ bảo mật ra sao. Do đó, website kinh doanh của doanh nghiệp sẽ là mồi ngon của các đợt tấn công SQL Injection hay botnet.

Duyệt web tràn lan

http://www.ebook.edu.vn

Không phải nhân viên văn phòng nào cũng đủ am hiểu tường tận về những hiểm họa rình rập trên mạng Internet như malware, spyware, virus, trojan... Họ cứ vô tư truy cập vào các website không xác định hoặc bị dẫn dụ click vào những website được tin tặc bày cỗ chào đón và thế là máy tính của nhân viên sẽ là cánh cửa giúp tin tặc xâm nhập vào trong mạng của doanh nghiệp.

Email chứa đựng mã độc

Những cuộc giội bom thư rác sẽ làm tràn ngập hộp thư của bạn với những tiêu đề hấp dẫn như những vụ scandal tình ái, hình ảnh nóng bỏng hay các lời mời chào kinh doanh... chỉ một cú nhấp chuột sai lầm thì ngay lập tức máy tính sẽ tải về các đoạn mã độc làm tiền đề cho hàng loạt phần mềm độc hại đi sau xâm nhập vào máy tính.

Không vá lỗi bảo mật

Hơn 90% các cuộc tấn công vào hệ thống mạng đều cố gắng khai thác các lỗi bảo mật đã được biết đến. Mặc dù các bản vá lỗi vẫn thường xuyên được những hãng sản xuất cung cấp ngay sau khi lỗi được phát hiện nhưng một vài doanh nghiệp lại không coi trọng việc cập nhật lỗi thường nhật dẫn đến việc các lỗi bảo mật mở toang cổng chào đón những cuộc tấn công.

16.2. Các phương thức tấn công

16.2.1 Viruses, Worms, Trojan Horses.

Trong khoa học máy tính, virus máy tính (thường được người sử dụng gọi tắt là virus) là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác (file, ổ đĩa, máy tính ..).

Trước đây, virus thường được viết bởi một số người am hiểu về lập trình muốn chứng tỏ khả năng của mình nên thường virus có các hành động như: cho một chương trình không hoạt động đúng, xóa dữ liệu, làm hỏng ổ cứng,... hoặc gây ra những trò đùa khó chịu.

Những virus mới được viết trong thời gian gần đây không còn thực hiện các trò đùa hay sự phá hoại đối máy tính của nạn nhân bị lây nhiễm nữa, mà đa phần

http://www.ebook.edu.vn

hướng đến việc lấy cắp các thông tin cá nhân nhạy cảm (các mã số thẻ tín dụng) mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển hoặc các hành động khác nhằm có lợi cho người phát tán virus.

Chiếm trên 90% số virus đã được phát hiện là nhắm vào hệ thống sử dụng hệ điều hành họ Windows chỉ đơn giản bởi hệ điều hành này được sử dụng nhiều nhất trên thến giới. Do tính thông dụng của Windows nên các tin tặc thường tập trung hướng vào chúng nhiều hơn là các hệ điều hành khác. (Cũng có quan điểm cho rằng Windows có tính bảo mật không tốt bằng các hệ điều hành khác (như Linux) nên có nhiều virus hơn, tuy nhiên nếu các hệ điều hành khác cũng thông dụng như Windows hoặc thị phần các hệ điều hành ngang bằng nhau thì cũng lượng virus xuất hiện có lẽ cũng tương đương nhau).

Lược sử của virus

Có nhiều quan điểm khác nhau về lịch sử của virus điện toán. Ở đây chỉ nêu rất vắn tắt và khái quát những điểm chung nhất và, qua đó, chúng ta có thể hiểu chi tiết hơn về các loại virus:

- Năm 1949: John von Neuman (1903-1957) phát triển nền tảng lý thuyết tự nhân bản của một chương trình cho máy tính.
- Vào cuối thập niên 1960 đầu thập niên 1970 đã xuất hiện trên các máy Univax 1108 một chương trình gọi là "Pervading Animal" tự nó có thể nối với phần sau của các tập tin tự hành. Lúc đó chưa có khái niệm virus.
- Năm 1981: Các virus đầu tiên xuất hiện trong hệ điều hành của máy tính Apple II.
- Năm 1983: Tại Đại Học miền Nam California, tại Hoa Kỳ, Fred Cohen lần đầu đưa ra khái niệm computer virus như định nghĩa ngày nay.
- Năm 1986: Virus "the Brain", virus cho máy tính cá nhân (PC) đầu tiên, được tạo ra tại Pakistan bởi Basit và Amjad. Chương trình này nằm trong phần khởi động (boot sector) của một dĩa mềm 360Kb và nó sẽ lây nhiễm tất cả các ổ dĩa mềm. Đây là loại "stealth virus" đầu tiên.

http://www.ebook.edu.vn

- Cũng trong tháng 12 năm này, virus cho DOS được khám phá ra là virus "VirDem". Nó có khả năng tự chép mã của mình vào các tệp tự thi hành (executable file) và phá hoại các máy tính VAX/VMS.
- Năm 1987: Virus đầu tiên tấn công vào command.com là virus "Lehigh".
- Năm 1988: Virus Jerusalem tấn công đồng loạt các đại học và các công ty trong các quốc gia vào ngày thứ Sáu 13. Đây là loại virus hoạt động theo đồng hồ của máy tính (giống bom nổ chậm cài hàng loạt cho cùng một thời điểm).
- Tháng 11 cùng năm, Robert Morris, 22 tuổi, chế ra worm chiếm cứ các máy tính của ARPANET, làm liệt khoảng 6.000 máy. Morris bị phạt tù 3 năm và 10.000 dollar. Mặc dù vậy anh ta khai rằng chế ra virus vì "chán đời" (boresome).
- Năm 1990: Chương trình thương mại chống virus đầu tiên ra đời bởi Norton.
- Năm 1991: Virus đa hình (polymorphic virus) ra đời đầu tiên là virus "Tequilla". Loại này biết tự thay đổi hình thức của nó, gây ra sự khó khăn cho các chương trình chống virus.
- Năm 1994: Những người thiếu kinh nghiệm, vì lòng tốt đã chuyển cho nhau một điện thư cảnh báo tất cả mọi người không mở tất cả những điện thư có cụm từ "Good Times" trong dòng bị chú (subject line) của chúng. Đây là một loại virus giả (hoax virus) đầu tiên xuất hiện trên các điện thư và lợi dụng vào "tinh thần trách nhiệm" của các người nhận được điện thư này để tạo ra sự luân chuyển.
- Năm 1995: Virus văn bản (macro virus) đầu tiên xuất hiện trong các mã macro trong các tệp của Word và lan truyền qua rất nhiều máy. Loại virus này có thể làm hư hệ điều hành chủ. Macro virus là loại virus viết ra bằng ngôn ngữ lập trình Visual Basic cho các ứng dụng (VBA) và tùy theo khả năng, có thể lan nhiễm trong các ứng dụng văn phòng của Microsoft như Word, Excel, PowerPoint, OutLook,.... Loại macro này, nổi tiếng có virus Baza và virus Laroux, xuất hiện năm 1996, có thể nằm trong cả Word hay

http://www.ebook.edu.vn

Excel. Sau này, virus Melissa, năm 1997, tấn công hơn 1 triệu máy, lan truyền bởi một tệp đính kèm kiểu Word bằng cách đọc và gửi đến các địa chỉ của Outlook trong các máy đã bị nhiễm virus. Virus Tristate, năm 1999, có thể nằm trong các tệp Word, Excel và Power Point.

- Năm 2000: Virus Love Bug, còn có tên ILOVEYOU, đánh lừa tính hiếu kì của mọi người. Đây là một loại macro virus. Đặc điểm là nó dùng đuôi tập tin dạng "ILOVEYOU.txt.exe". Lợi dụng điểm yếu của Outlook thời bấy giờ: theo mặc định sẵn, đuôi dạng .exe sẽ tự động bị dấu đi. Ngoài ra, virus này còn có một đặc tính mới của spyware: nó tìm cách đọc tên và mã nhập của máy chủ và gửi về cho tay hắc đạo. Khi truy cứu ra thì đó là một sinh viên người Philippines. Tên này được tha bổng vì Philippines chưa có luật trừng trị những người tạo ra virus cho máy tính.
- Năm 2002: Tác giả của virus Melissa, David L. Smith, bị xử 20 tháng tù.
- Năm 2003: Virus Slammer, một loại worm lan truyền với vận tốc kỉ lục, truyền cho khoảng 75 ngàn máy trong 10 phút.
- Năm 2004: Đánh dấu một thế hệ mới của virus là worm Sasser. Với virus này thì người ta không cần phải mở đính kèm của điện thư mà chỉ cần mở lá thư là đủ cho nó xâm nhập vào máy. Cũng may là Sasser không hoàn toàn hủy hoại máy mà chỉ làm cho máy chủ trở nên chậm hơn và đôi khi nó làm máy tự khởi động trở lại. Tác giả của worm này cũng lập một kỉ lục khác: tay hắc đạo (hacker) nổi tiếng trẻ nhất, chỉ mới 18 tuổi, Sven Jaschan, người Đức. Tuy vậy, vì còn nhỏ tuổi, nên vào tháng 7 năm 2005 nên tòa án Đức chỉ phạt anh này 3 năm tù treo và 30 giờ lao động công ích.

Với khả năng của các tay hacker, virus ngày ngay có thể xâm nhập bằng cách bẻ gãy các rào an toàn của hệ điều hành hay chui vào các chổ hở của các phần mềm nhất là các chương trình thư điện tử, rồi từ đó lan tỏa khắp nơi theo các nối kết mạng hay qua thư điện tử. Do dó, việc truy tìm ra nguồn gốc phát tán virus sẽ càng khó hơn nhiều. Chính Microsoft, hãng chế tạo các phần mềm phổ biến, cũng là một nạn nhân. Họ đã phải nghiên cứu, sửa chữa và phát hành rất nhiều

http://www.ebook.edu.vn

các phần mềm nhằm sửa các khuyết tật của phần mềm cũng như phát hành các thế hệ của gói dịch vụ (service pack) nhằm giảm hay vô hiệu hóa các tấn công của virus. Nhưng dĩ nhiên với các phần mềm có hàng triệu dòng mã nguồn thì mong ước chúng hoàn hảo theo ý nghĩa của sự an toàn chỉ có trong lý thuyết. Đây cũng là cơ hội cho các nhà sản xuất các loại phần mềm bảo vệ có đất dụng võ.

Tương lai không xa có lẽ virus sẽ tiến thêm các bước khác như: nó bao gồm mọi điểm mạnh sẵn có (polymorphic, sasser hay tấn công bằng nhiều cách thức, nhiều kiểu) và còn kết hợp với các thủ đoạn khác của phần mềm gián điệp (spyware). Đồng thời nó có thể tấn công vào nhiều hệ điều hành khác nhau chứ không nhất thiết nhắm vào một hệ điều hành độc nhất như trong trường hợp của Windows hiện giờ. Và có lẽ virus sẽ không hề (thậm chí là không cần) thay đổi phương thức tấn công: lợi dụng điểm yếu của máy tính cũng như chương trình.

Các khái niệm có liên quan

Sâu máy tính(worm): là các chương trình cũng có khả năng tự nhân bản tự tìm cách lan truyền qua hệ thống mạng (thường là qua hệ thống thư điện tử). Điểm cần lưu ý ở đây, ngoài tác hại thẳng lên máy bị nhiễm, nhiệm vụ chính của worm là phá các mạng (network) thông tin, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này. Nhiều nhà phân tích cho rằng worm khác với virus, họ nhấn mạnh vào đặc tính phá hoại mạng nhưng ở đây worm được là một loại virus đặc biệt.

Worm nổi tiếng nhất được tạo bởi Robert Morris vào năm 1988. Nó có thể làm hỏng bất kì hệ điều hành UNIX nào trên Internet. Tuy vậy, có lẽ worm tồn tại lâu nhất là virus happy99, hay các thế hệ sau đó của nó có tên là Trojan. Các worm này sẽ thay đổi nội dung tệp wsok32.dll của Windows và tự gửi bản sao của chính chúng đi đến các địa chỉ cho mỗi lần gửi điện thư hay message.

Phần mềm ác tính (malware): (chữ ghép của maliciuos và software) chỉ chung các phần mềm có tính năng gây hại như virus, worm và Trojan horse.

Trojan Horse: đây là loại chương trình cũng có tác hại tương tự như virus chỉ khác là nó không tự nhân bản ra. Như thế, cách lan truyền duy nhất là thông qua

http://www.ebook.edu.vn

các thư dây chuyền Để trừ loại này người chủ máy chỉ việc tìm ra tập tin Trojan horse rồi xóa nó đi là xong. Tuy nhiên, không có nghĩa là không thể có hai con Trojan horse trên cùng một hệ thống. Chính những kẻ tạo ra các phần mềm này sẽ sử dụng kỹ năng lập trình của mình để sao lưu thật nhiều con trước khi phát tán lên mạng. Đây cũng là loại virus cực kỳ nguy hiểm. Nó có thể hủy ổ cứng, hủy dữ liệu.

Phần mềm gián điệp (spyware): Đây là loại virus có khả năng thâm nhập trực tiếp vào hệ điều hành mà không để lại "di chứng". Thường một số chương trình diệt virus có kèm trình diệt spyware nhưng diệt khá kém đối với các đợt "dịch".

Phần mềm quảng cáo (adware): Loại phần mềm quảng cáo, rất hay có ở trong các chương trình cài đặt tải từ trên mạng. Một số phần mềm vô hại, nhưng một số có khả năng hiển thị thông tin kịt màn hình, cưỡng chế người sử dụng.

Botnet: Trước đây, loại này thường dùng để nhắm vào các hệ thống điều khiển máy tính từ xa, nhưng hiện giờ lại nhắm vào người dùng.

Điều đặc biệt nguy hiểm là các botnet được phơi bày từ các hacker không cần kỹ thuật lập trình cao. Nó được rao bán với giá từ 20USD trở lên cho các hacker. Hậu quả của nó để lại không nhỏ: mất tài khoản. Nếu liên kết với một hệ thống máy tính lớn, nó có thể tống tiền cả một doanh nghiệp.

Nhóm của Sites ở Sunbelt cùng với đội phản ứng nhanh của công ty bảo mật iDefense Labs đã tìm ra một botnet chạy trên nền web có tên là Metaphisher. Thay cho cách sử dụng dòng lệnh, tin tặc có thể sử dụng giao diện đồ họa, các biểu tượng có thể thay đổi theo ý thích, chỉ việc dịch con trỏ, nhấn chuột và tấn công.

Theo iDefense Labs, các bot do Metaphisher điều khiển đã lây nhiễm hơn 1 triệu PC trên toàn cầu. Thậm chí trình điều khiển còn mã hóa liên lạc giữa nó và bot "đàn em" và chuyển đi mọi thông tin về các PC bị nhiễm cho người chủ bot như vị trí địa lý, các bản vá bảo mật của Windows và những trình duyệt đang chạy trên mỗi PC.

Những công cụ tạo bot và điều khiển dễ dùng trên góp phần làm tăng vọt số PC bị nhiễm bot được phát hiện trong thời gian gần đây. Thí dụ, Jeanson James

http://www.ebook.edu.vn

Ancheta, 21 tuổi, người Mỹ ở bang California, bị tuyên án 57 tháng tù vì đã vận hành một doanh nghiệp "đen" thu lợi bất chính dựa vào các botnet điều khiển 400.000 "thành viên" và 3 tay điều khiển bot bị bắt ở Hà Lan mùa thu năm trước chính là trung tâm "đầu não" điều khiển hơn 1,5 triệu PC!

Mặc dù đã có luật để bắt những tội phạm kiểu này, nhưng do dễ dàng có được những công cụ phá hoại nên luôn có thêm người mới gia nhập hàng ngũ hacker vì tiền hay vì tò mò.

Keylogger: là phần mềm ghi lại chuỗi phím gõ của người dùng. Nó có thể hữu ích cho việc tìm nguồn gốc lỗi sai trong các hệ thống máy tính và đôi khi được dùng để đo năng suất làm việc của nhân viên văn phòng. Các phần mềm kiểu này rất hữu dụng cho ngành luật pháp và tình báo - ví dụ, cung cấp một phương tiện để lấy mật khẩu hoặc các khóa mật mã và nhờ đó qua mắt được các thiết bị an ninh. Tuy nhiên, các phần mềm keylogger được phổ biến rộng rãi trên Internet và bất cứ ai cũng có thể sử dụng cho mục đích lấy trộm mật khẩu và chìa khóa mã hóa.

Phishing: là một hoạt động phạm tội dùng các kỹ thuật lừa đảo. Kẻ lừa đảo cố gắng lừa lấy các thông tin nhạy cảm, chẳng hạn như mật khẩu và thông tin về thẻ tín dụng, bằng cách giả là một người hoặc một doanh nghiệp đáng tin cậy trong một giao dịch điện tử. Phishing thường được thực hiện bằng cách sử dụng thư điện tử hoặc tin nhắn, đôi khi còn sử dụng cả điện thoại.

Rootkit: là một bộ công cụ phần mềm dành cho việc che dấu làm các tiến trình đang chạy, các file hoặc dữ liệu hệ thống. Rootkit có nguồn gốc từ các ứng dụng tương đối hiền, nhưng những năm gần đây, rootkit đã bị sử dụng ngày càng nhiều bởi các phần mềm ác tính, giúp kẻ xâm nhập hệ thống giữ được đường truy nhập một hệ thống trong khi tránh bị phát hiện. Người ta đã biết đến các rootkit dành cho nhiều hệ điều hành khác nhau chẳng hạn Linux, Solaris và một số phiên bản của Microsoft Windows. Các rootkit thường sửa đổi một số phần của hệ điều hành hoặc tự cài đặt chúng thành các driver hay các môdule trong nhân hệ điều hành (kernel module).

http://www.ebook.edu.vn

Khi hay tin CD nhạc của Sony cài đặt rookit để giấu file chống sao chép xuất hiện vào tháng 11 năm ngoái, giới tin tặc hân hoan và nhanh chóng khai thác ứng dụng của Sony. Phần mềm của Sony giấu bất kỳ file hay tiến trình bắt đầu với "sys", những kẻ viết phần mềm độc hại đã đổi tên file để lợi dụng đặc điểm này .

Vào tháng 3, nhà sản xuất phần mềm chống virus ở Tây Ban Nha là Panda Software cho biết họ đang tìm biến thể của sâu Bagle cực kỳ độc hại có trang bị khả năng của rootkit. Trầm trọng hơn, tương tự như các "nhà sản xuất" chương trình botnet, những kẻ tạo phần mềm rootkit còn bán hoặc phát tán miễn phí các công cụ, giúp những tay viết phần mềm độc hại dễ dàng bổ sung chức năng rootkit cho các virus cũ như Bagle hay tạo loại mới. Một dự án do Microsoft và các nhà nghiên cứu của đại học Michigan thực hiện thật sự mở đường cho nghiên cứu rootkit, tạo ra một phương thức mới gần như "đặt" HĐH chạy trên phần mềm có tên SubVirt (tên của dự án nghiên cứu). HĐH vẫn làm việc bình thường, nhưng "máy ảo" điều khiển mọi thứ HĐH nhìn thấy và có thể dễ dàng giấu chính nó.

May mắn là kỹ thuật này không dễ thực hiện và người dùng dễ nhận ra vì làm chậm hệ thống và làm thay đổi những file nhất định. Hiện giờ, loại siêu rootkit này chỉ mới ở dạng ý tưởng, cần nhiều thời gian trước khi tin tặc có thể thực hiện phương thức tấn công này.

Phần mềm tống tiền (Ransomware): là loại phần mềm ác tính sử dụng một hệ thống mật mã hóa yếu (phá được) để mã hóa dữ liệu thuộc về một cá nhân và đòi tiền chuộc thì mới khôi phục lại.

Cửa hậu (Backdoor): trong một hệ thống máy tính, cửa hậu là một phương pháp vượt qua thủ tục chứng thực người dùng thông thường hoặc để giữ đường truy nhập từ xa tới một máy tính, trong khi cố gắng không bị phát hiện bởi việc giám sát thông thường. Cửa hậu có thể có hình thức một chương trình được cài đặt (ví dụ Back Orifice hoặc cửa hậu rookit Sony/BMG rootkit được cài đặt khi một đĩa bất kỳ trong số hàng triệu đĩa CD nhạc của Sony được chơi trên một máy

http://www.ebook.edu.vn

tính chạy Windows), hoặc có thể là một sửa đổi đối với một chương trình hợp pháp - đó là khi nó đi kèm với Trojan.

Virus lây qua passport: Loại virus này lây qua các thẻ RFID cá nhân để thay đổi nội dung của thẻ, buộc tội người dùng và có thể ăn cắp passport. Vì sóng RFID không lây qua kim loại nên khi không cần dùng, bạn nên để trong hộp kim loại.

Virus điện thoại di động: chỉ riêng hệ thống PC đã đủ làm người dùng đau đầu, nay lại có virus điện thoại di động. Loại này thường lây qua tin nhắn. Một vài virus ĐTDĐ cũng đánh sập HĐH và làm hỏng thiết bị. Một số khác chỉ gây khó chịu như thay đổi các biểu tượng làm thiết bị trở nên khó sử dụng. Một số ít còn nhằm vào tiền. Ví dụ, một Trojan lây lan các điện thoại ở Nga gửi tin nhắn tới những dịch vụ tính tiền người gửi.

Danh sách các đuôi tệp có khả năng di truyền và bị lây nhiễm

Các tập tin trên hệ điều hành Windows mang đuôi mở rộng sau có nhiều khả năng bị virus tấn công.

- .bat: Microsoft Batch File (Tệp xử lí theo lô)
- .chm: Compressed HTML Help File (Tệp tài liệu dưới dạng nén HTML)
- .cmd: Command file for Windows NT (Tệp thực thi của Windows NT)
- .com: Command file (program) (Tệp thực thi)
- .cpl: Control Panel extension (Tệp của Control Panel)
- .doc: Microsoft Word (Tệp của chương trình Microsoft Word)
- .exe: Executable File (Tệp thực thi)
- .hlp: Help file (Tệp nội dung trợ giúp người dùng)
- .hta: HTML Application (Ứng dụng HTML)

http://www.ebook.edu.vn

- .js: JavaScript File (Tệp JavaScript)
- .jse: JavaScript Encoded Script File (Tệp mã hoá JavaScript)
- .lnk: Shortcut File (Tệp đường dẫn)
- .msi: Microsoft Installer File (Tệp cài đặt)
- .pif: Program Information File (Tệp thông tin chương trình)
- .reg: Registry File
- .scr: Screen Saver (Portable Executable File)
- .sct: Windows Script Component
- .shb: Document Shortcut File
- .shs: Shell Scrap Object
- .vb: Visual Basic File
- .vbe: Visual Basic Encoded Script File
- .vbs: Visual Basic File
- .wsc: Windows Script Component
- .wsf: Windows Script File
- .wsh: Windows Script Host File
- .{*}: Class ID (CLSID) File Extensions

Các hình thức lây nhiễm của virus máy tính

Virus lây nhiễm theo cách cổ điển

Cách cổ điển nhất của sự lây nhiễm, bành trướng của các loai virus máy tính là thông qua các thiết bị lưu trữ di động: Trước đây đĩa mềm và đĩa CD chứa chương trình thường là phương tiện bị lợi dụng nhiều nhất để phát tán. Ngày nay khi đĩa mềm rất ít được sử dụng thì phương thức lây nhiễm này chuyển qua các ổ USB, các đĩa cứng di động hoặc các thiết bị giải trí kỹ thuật số.

http://www.ebook.edu.vn

Virus lây nhiễm qua thư điện tử

Khi mà thư điện tử (e-mail) được sử dụng rộng rãi trên thế giới thì virus chuyển hướng sang lây nhiễm thông qua thư điện tử thay cho các cách lây nhiễm truyền thống.

Khi đã lây nhiễm vào máy nạn nhân, virus có thể tự tìm ra danh sách các địa chỉ thư điện tử sẵn có trong máy và nó tự động gửi đi hàng loạt (mass mail) cho những địa chỉ tìm thấy. Nếu các chủ nhân của các máy nhận được thư bị nhiễm virus mà không bị phát hiện, tiếp tục để lây nhiễm vào máy, virus lại tiếp tục tìm đến các địa chỉ và gửi tiếp theo. Chính vì vậy số lượng phát tán có thể tăng theo cấp số nhân khiến cho trong một thời gian ngắn hàng hàng triệu máy tính bị lây nhiễm, có thể làm tê liệt nhiều cơ quan trên toàn thế giới trong một thời gian rất ngắn.

Khi mà các phần mềm quản lý thư điện tử kết hợp với các phần mềm diệt virus có thể khắc phục hành động tự gửi nhân bản hàng loạt để phát tán đến các địa chỉ khác trong danh bạ của máy nạn nhân thì chủ nhân phát tán virus chuyển qua hình thức tự gửi thư phát tán virus bằng nguồn địa chỉ sưu tập được trước đó.

Phương thực lây nhiễm qua thư điển tử bao gồm:

Lây nhiễm vào các file đính kèm theo thư điện tử (attached mail). Khi đó người dùng sẽ không bị nhiễm virus cho tới khi file đính kèm bị nhiễm virus được kích hoạt (do đặc diểm này các virus thường được "trá hình" bởi các tiêu đề hấp dẫn như sex, thể thao hay quảng cáo bán phần mềm với giá vô cùng rẻ.)

Lây nhiễm do mở một liên kết trong thư điện tử Các liên kết trong thư điện tử có thể dẫn đến một trang web được cài sẵn virus, cách này thường khai thác các lỗ hổng của trình duyệt và hệ điều hành. Một cách khác, liên kết dẫn tới việc thực thi một đoạn mã, và máy tính bị có thể bị lây nhiễm virus.

Lây nhiễm ngay khi mở để xem thư điện tử: Cách này vô cùng nguy hiểm bởi chưa cần kích hoạt các file hoặc mở các liên kết, máy tính đã có thể bị lây nhiễm virus. Cách này cũng thường khai thác các lỗi của hệ điều hành.

Virus lây nhiễm qua mạng Internet

http://www.ebook.edu.vn

Theo sự phát triển rộng rãi của Internet trên thế giới mà hiện nay các hình thức lây nhiễm virus qua Internet trở thành các phương thức chính của virus ngày nay.

Có các hình thức lây nhiễm virus và phần mềm độc hại thông qua Internet như sau:

Lây nhiễm thông qua các file tài liệu, phần mềm: Là cách lây nhiễm cổ điển, nhưng thay thế các hình thức truyền file theo cách cổ điển (đĩa mềm, đĩa USB...) bằng cách tải từ Internet, trao đổi, thông qua các phần mềm...

Lây nhiễm khi đang truy cập các trang web được cài đặt virus (theo cách vô tình hoặc cố ý): Các trang web có thể có chứa các mã hiểm độc gây lây nhiễm virus và phần mềm độc hại vào máy tính của người sử dụng khi truy cập vào các trang web đó.

Lây nhiễm virus hoặc chiếm quyền điều khiển máy tính thông qua các lỗi bảo mật hệ điều hành, ứng dụng sẵn có trên hệ điều hành hoặc phần mềm của hãng thứ ba: Điều này có thể khó tin đối với một số người sử dụng, tuy nhiên tin tặc có thể lợi dụng các lỗi bảo mật của hệ điều hành, phần mềm sẵn có trên hệ điều hành (ví dụ Winidow Media Player) hoặc lỗi bảo mật của các phần mềm của hãng thứ ba (ví dụ Acrobat Reader) để lây nhiễm virus hoặc chiếm quyền kiểm soát máy tính nạn nhân khi mở các file liên kết với các phần mềm này.

Biến thể

Một hình thức trong cơ chế hoạt động của virus là tạo ra các biến thể của chúng. Biến thể của virus là sự thay đổi mã nguồn nhằm các mục đích tránh sự phát hiện của phần mềm diệt virus hoặc làm thay đổi hành động của nó.

Một số loại virus có thể tự tạo ra các biến thể khác nhau gây khó khăn cho quá trình phát hiện và tiêu diệt chúng. Một số biến thể khác xuất hiện do sau khi virus bị nhận dạng của các phần mềm diệt virus, chính tác giả hoặc các tin tặc khác (biết được mã của chúng) đã viết lại, nâng cấp hoặc cải tiến chúng để tiếp tục phát tán.

Virus có khả năng vô hiệu hoá phần mềm diệt virus

http://www.ebook.edu.vn

Một số virus có khả năng vô hiệu hoá hoặc can thiệp vào hệ điều hành làm tê liệt (một số) phần mềm diệt virus. Sau hành động này chúng mới tiến hành lây nhiễm và tiếp tục phát tán. Một số khác lây nhiễm chính vào phần mềm diệt virus (tuy khó khăn hơn) hoặc ngăn cản sự cập nhật của các phần mềm diệt virus.

Các cách thức này không quá khó nếu như chúng nắm rõ được cơ chế hoạt động của các phần mềm diệt virus và được lây nhiễm hoặc phát tác trước khi hệ thống khởi động các phần mềm này. Chúng cũng có thể sửa đổi file hots của hệ điều hành Windows để người sử dụng không thể truy cập vào các website và phần mềm diệt virus không thể liên lạc với server của mình để cập nhật.

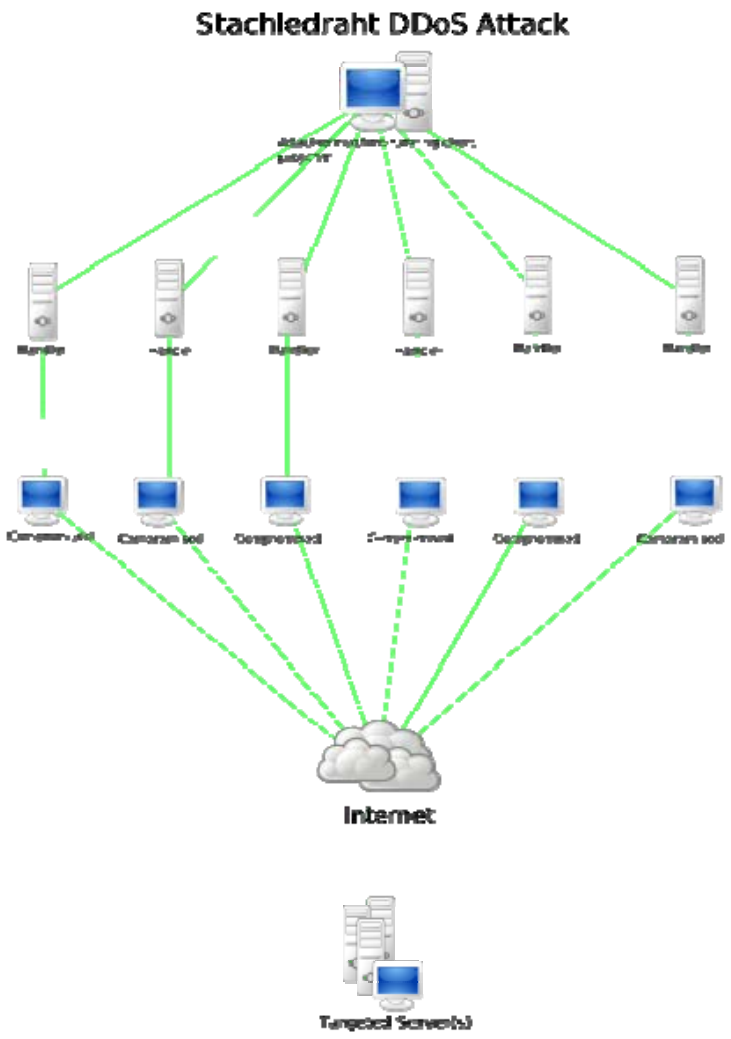
16.2.2 Denial of Service (DoS) và Brute Force Attack

Một cuộc tấn công từ chối dịch vụ (tấn công DoS) hay tấn công từ chối dịch vụ phân tán (tấn công DDoS) là sự cố gắng làm cho tài nguyên của một máy tính không thể sử dụng được nhằm vào những người dùng của nó. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ là khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để chống lại Internet site hoặc service (dịch vụ Web) vận hành hiệu quả hoặc trong tất cả, tạm thời hay một cách không xác định. Thủ phạm tấn công từ chối dịch vụ nhằm vào các mục tiêu site hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

Một phương thức tấn công phổ biến kéo theo sự bão hoà máy mục tiêu với các yêu cầu liên lạc bên ngoài, đến mức nó không thể đâp ứng giao thông hợp pháp, hoặc dáp ứng quá chậm. Trong điều kiện chung, các cuộc tấn công DoS được bổ sung bởi ép máy mục tiêu khởi động lại hoặc tiêu thụ hết tài nguyên của nó đến mức nó không cung cấp dịch vụ, hoặc làm tắc nghẽn liên lạc giữa người sử dụng và nạn nhân.

Tấn công từ chối dịch vụ đươc lưu ý sự vi phạm chính sách sử dụng đúng internet của IAB(Internet Architecture Board). Chúng cũng cấu thành sự vi phạm luật dân sự.

http://www.ebook.edu.vn



Nhận diện

US-CERT xác định dấu hiệu của một vụ tấn cống từ chối dịch vụ gồm có :

- Mạng thực thi chậm khác thường (mở file hay truy cập Website).
- Không thể dùng một Website cụ thể.
- Không có thể truy cập bất kỳ Website nào
- Tăng lượng thư rác nhận được (như một trận "boom mail")
- Không phải tất các các dịch vụ ngừng chạy,thậm chí đó là kết quả của một hoạt động nguy hại, tất yếu của tấn công DoS.

http://www.ebook.edu.vn

Tấn công từ chối dịch cũng có thể dẫn tới vấn đề về nhánh mạng của máy đang bị tấn công. Ví dụ băng thông của router giữa Internet và Lan có thể bị tiêu thụ bởi tấn công, làm tổn hại không chỉ máy tính ý định tấn công mà còn là toàn thể mạng. Nếu cuộc tấn công dẫn tới tỉ lệ lớn thích đáng, toàn bộ vùng địa lý của kết nối Internet có thể bị tổn hại nằm ngoài sự hiểu biết của kẻ tấn công cấu hình chính xác, trang thiết bị mong manh.

Các phương thức tấn công

Tấn công từ chối dịch vụ là một loại hình tấn công nhằm ngăn chặn những người dùng hợp lệ được sử dụng một dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm là tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS.

Tấn công từ chối dịch vụ có thể được thực hiện theo một số cách nhất định. Có năm kiểu tấn công cơ bản sau đây:

- Nhằm tiêu tốn tài nguyên tính toán như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý
- Phá vỡ các thông tin cấu hình như thông tin định tuyến
- Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.
- Phá vỡ các thành phần vật lý của mạng máy tính
- Làm tắc nghẽn thông tin liên lạc có chủ đích giữa các người dùng và nạn nhân dẫn đến việc liên lạc giữa hai bên không được thông suốt.

Một cuộc tấn công từ chối dịch vụ có thể bao gồm cả việc thực thi malware nhằm:

- Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.
- Những lỗi gọi tức thì trong microcode của máy tính.
- Những lỗi gọi tức thì trong chuỗi chỉ thị, dẫn đến máy tính rơi vào trạng thái hoạt động không ổn định hoặc bị đơ.

http://www.ebook.edu.vn

- Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu thốn tài nguyên hoặc bị thrashing. VD: như sử dụng tất cả các năng lực có sẵn dẫn đến không một công việc thực tế nào có thể hoàn thành được.
- Gây crash hệ thống.
- Tấn công từ chối dịch vụ iFrame: trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web đó bị quá hạn.

Các vụ tấn công

Ngày 10 tháng 10 năm 2008, trang web 5giay.vn chính thức công nhận bị tấn công DDOS

16.3. Các chính sách bảo mật

Cách phòng chống virus và ngăn chặn tác hại của nó

Có một câu nói vui rằng Để không bị lây nhiễm virus thì ngắt kết nối khỏi mạng, không sử dụng ổ mềm, ổ USB hoặc copy bất kỳ file nào vào máy tính. Nhưng nghiêm túc ra thì điều này có vẻ đúng khi mà hiện nay sự tăng trưởng số lượng virus hàng năm trên thế giới rất lớn.

Không thể khẳng định chắc chắn bảo vệ an toàn 100% cho máy tính trước hiểm hoạ virus và các phần mềm hiểm độc, nhưng chúng ta có thể hạn chế đến tối đa có thể và có các biện pháp bảo vệ dữ liệu của mình.

http://www.ebook.edu.vn

Sử dụng phần mềm diệt virus

Bảo vệ bằng cách trang bị thêm một phần mềm diệt virus có khả năng nhận biết nhiều loại virus máy tính và liên tục cập nhật dữ liệu để phần mềm đó luôn nhận biết được các virus mới.

Trên thị trường hiện có rất nhiều phần mềm diệt virus. Một số hãng nổi tiếng viết các phần mềm virus được nhiều người sử dụng có thể kể đến là: McAfee, Symantec, Kaspersky

Sử dụng tường lửa

Tường lửa (Firewall) không phải một cái gì đó quá xa vời hoặc chỉ dành cho các nhà cung cấp dịch vụ internet (ISP) mà mỗi máy tính cá nhân cũng cần phải sử dụng tường lửa để bảo vệ trước virus và các phần mềm độc hại. Khi sử dụng tường lửa, các thông tin vào và ra đối với máy tính được kiểm soát một cách vô thức hoặc có chủ ý. Nếu một phần mềm độc hại đã được cài vào máy tính có hành động kết nối ra Internet thì tường lửa có thể cảnh báo giúp người sử dụng loại bỏ hoặc vô hiệu hoá chúng. Tường lửa giúp ngăn chặn các kết nối đến không mong muốn để giảm nguy cơ bị kiểm soát máy tính ngoài ý muốn hoặc cài đặt vào các chương trình độc hại hay virus máy tính.

Sử dụng tường lửa bằng phần cứng nếu người sử dụng kết nối với mạng Internet thông qua một modem có chức năng này. Thông thường ở chế độ mặc định của nhà sản xuất thì chức năng "tường lửa" bị tắt, người sử dụng có thể truy cập vào modem để cho phép hiệu lực (bật). Sử dụng tường lửa bằng phần cứng không

http://www.ebook.edu.vn

phải tuyệt đối an toàn bởi chúng thường chỉ ngăn chặn kết nối đến trái phép, do đó kết hợp sử dụng tường lửa bằng các phần mềm.

Sử dụng tường lửa bằng phần mềm: Ngay các hệ điều hành họ Windows ngày nay đã được tích hợp sẵn tính năng tường lửa bằng phần mềm, tuy nhiên thông thường các phần mềm của hãng thứ ba có thể làm việc tốt hơn và tích hợp nhiều công cụ hơn so với tường lửa phần mềm sẵn có của Windows. Ví dụ bộ phần mềm ZoneAlarm Security Suite của hãng ZoneLab là một bộ công cụ bảo vệ hữu hiệu trước virus, các phần mềm độc hại, chống spam, và tường lửa.

Cập nhật các bản sửa lỗi của hệ điều hành

Hệ điều hành Windows (chiếm đa số) luôn luôn bị phát hiện các lỗi bảo mật chính bởi sự thông dụng của nó, tin tặc có thể lợi dụng các lỗi bảo mật để chiếm quyền điều khiển hoặc phát tán virus và các phần mềm độc hại. Người sử dụng luôn cần cập nhật các bản vá lỗi của Windows thông qua trang web Microsoft Update (cho việc nâng cấp tất cả các phần mềm của hãng Microsoft) hoặc Windows Update (chỉ cập nhật riêng cho Windows). Cách tốt nhất hãy đặt chế độ nâng cấp (sửa chữa) tự động (Automatic Updates) của Windows. Tính năng này chỉ hỗ trợ đối với các bản Windows mà Microsoft nhận thấy rằng chúng hợp pháp.

Vận dụng kinh nghiệm sử dụng máy tính

Cho dù sử dụng tất cả các phần mềm và phương thức trên nhưng máy tính vẫn có khả năng bị lây nhiễm virus và các phần mềm độc hại bởi mẫu virus mới chưa được cập nhật kịp thời đối với phần mềm diệt virus. Người sử dụng máy tính cần sử dụng triệt để các chức năng, ứng dụng sẵn có trong hệ điều hành và các kinh nghiệm khác để bảo vệ cho hệ điều hành và dữ liệu của mình. Một số kinh nghiệm tham khảo như sau:

Phát hiện sự hoạt động khác thường của máy tính: Đa phần người sử dụng máy tính không có thói quen cài đặt, gỡ bỏ phần mềm hoặc thường xuyên làm hệ điều hành thay đổi - có nghĩa là một sự sử dụng ổn định - sẽ nhận biết được sự thay đổi khác thường của máy tính. Ví dụ đơn giản: Nhận thấy sự hoạt động chậm chạp của máy tính, nhận thấy các kết nối ra ngoài khác thường thông qua tường

http://www.ebook.edu.vn

lửa của hệ điều hành hoặc của hãng thứ ba (thông qua các thông báo hỏi sự cho phép truy cập ra ngoài hoặc sự hoạt động khác của tường lửa). Mọi sự hoạt động khác thường này nếu không phải do phần cứng gây ra thì cần nghi ngờ sự xuất hiện của virus. Ngay khi có nghi ngờ, cần kiểm tra bằng cách cập nhật dữ liệu mới nhất cho phần mềm diệt virus hoặc thử sử dụng một phần mềm diệt virus khác để quét toàn hệ thống.

Kiểm soát các ứng dụng đang hoạt động: Kiểm soát sự hoạt động của các phần mềm trong hệ thống thông qua Task Manager hoặc các phần mềm của hãng thứ ba (chẳng hạn: ProcessViewer) để biết một phiên làm việc bình thường hệ thống thường nạp các ứng dụng nào, chúng chiếm lượng bộ nhớ bao nhiêu, chiếm CPU bao nhiêu, tên file hoạt động là gì...ngay khi có điều bất thường của hệ thống (dù chưa có biểu hiện của sự nhiễm virus) cũng có thể có sự nghi ngờ và có hành động phòng ngừa hợp lý. Tuy nhiên cách này đòi hỏi một sự am hiểu nhất định của người sử dụng.

Loại bỏ một số tính năng của hệ điều hành có thể tạo điều kiện cho sự lây nhiễm virus: Theo mặc định Windows thường cho phép các tính năng autorun giúp người sử dụng thuận tiện cho việc tự động cài đặt phần mềm khi đưa đĩa CD hoặc đĩa USB vào hệ thống. Chính các tính năng này được một số loại virus lợi dụng để lây nhiễm ngay khi vừa cắm ổ USB hoặc đưa đĩa CD phần mềm vào hệ thống (một vài loại virus lan truyền rất nhanh trong thời gian gần đây thông qua các ổ USB bằng cách tạo các file autorun.ini trên ổ USB để tự chạy các virus ngay khi cắm ổ USB vào máy tính). Cần loại bỏ tính năng này bằng các phần mềm của hãng thứ ba như TWEAKUI hoặc sửa đổi trong Registry.

Sử dụng thêm các trang web cho phép phát hiện virus trực tuyến: Xem thêm phần "Phần mềm diệt virus trực tuyến" tại bài phần mềm diệt virus

Bảo vệ dữ liệu máy tính

Nếu như không chắc chắn 100% rằng có thể không bị lây nhiễm virus máy tính và các phần mềm hiểm độc khác thì bạn nên tự bảo vệ sự toàn vẹn của dữ liệu của mình trước khi dữ liệu bị hư hỏng do virus (hoặc ngay cả các nguy cơ tiềm tàng khác như sự hư hỏng của các thiết bị lưu trữ dữ liệu của máy tính). Trong

http://www.ebook.edu.vn

phạm vi về bài viết về virus máy tính, bạn có thể tham khảo các ý tưởng chính như sau:

Sao lưu dữ liệu theo chu kỳ là biện pháp đúng đắn nhất hiện nay để bảo vệ dữ liệu. Bạn có thể thường xuyên sao lưu dữ liệu theo chu kỳ đến một nơi an toàn như: các thiết bị nhớ mở rộng (ổ USB, ổ cứng di động, ghi ra đĩa quang...), hình thức này có thể thực hiện theo chu kỳ hàng tuần hoặc khác hơn tuỳ theo mức độ cập nhật, thay đổi của dữ liệu của bạn.

Tạo các dữ liệu phục hồi cho toàn hệ thống không dừng lại các tiện ích sẵn có của hệ điều hành (ví dụ System Restore của Windows Me, XP...) mà có thể cần đến các phần mềm của hãng thứ ba, ví dụ bạn có thể tạo các bản sao lưu hệ thống bằng các phần mềm ghost, các phần mềm tạo ảnh ổ đĩa hoặc phân vùng khác.

Thực chất các hành động trên không chắc chắn là các dữ liệu được sao lưu không bị lây nhiễm virus, nhưng nếu có virus thì các phiên bản cập nhật mới hơn của phần mềm diệt virus trong tương lai có thể loại bỏ được chúng.

http://www.ebook.edu.vn