LỜI CẢM ƠN

Trong thời gian qua, để xây dựng và hoàn thành được đồ án này thì không thể thiếu được sự hướng dẫn, chỉ dạy của các thầy cô bộ môn khoa Công nghệ thông tin và đặc biệt là thầy giáo **TS. Nguyễn Hoài Thu** đã trực tiếp hướng dẫn để em có thể hoàn thành tốt được đồ án do nhà trường và khoa đưa ra.

Em xin trân trọng gửi lời cảm ơn tới:

- Các thầy cô bộ môn khoa Công Nghệ Thông Tin trường Đại Học Dân Lập Hải Phòng.
- Cảm ơn thầy giáo TS. Nguyễn Hoài Thu.
- Cảm ơn Gia đình, bạn bè đã giúp đỡ em hoàn thành đồ án này.

Mặc dù đã cố gắng xong với kinh nghiệm và kiến thức còn hạn chế không tránh khỏi những thiếu xót, em rất mong nhận được những nhận xét chỉ đạo của các thầy cô giáo để em có thêm kinh nghiệm phát triển tốt hơn khi ra trường.

Kính chúc toàn thể các thầy cô luôn mạnh khoẻ, hạnh phúc!

Hải phòng, ngày 05 tháng 07 năm 2010.

Sinh viên

Trương Đức Phúc

MỤC LỤC

LỜI NÓI ĐẦU

Ngày nay, với sự phát triển mạnh mẽ của khoa học kỹ thuật. Đặc biệt, trong lĩnh vực công nghệ thông tin đã tạo nên một động lực thúc đẩy và phát triển các ngành công nghiệp khác nhằm phục vụ và đáp ứng được nhu cầu của con người trong cuộc sống.

Mạng máy tính là một lĩnh vực nghiên cứu, phát triển và ứng dụng cốt lõi trong ngành công ngệ thông tin. Nhờ có mạng máy tính , thông tin được truyền đi một cách nhanh chóng làm cho con người ở khắp mọi nơi trên thế giới có thể giao lưu hợp tác trao đổi thông tin với nhau thuận tiện hơn trước đây.

Hầu hết các tổ chức hay công ty hiện nay đều triển khai xây dựng mạng LAN để phục vụ cho việc quản lý dữ liệu nội bộ cơ quan mình được thuận lợi, đảm bảo tính an toàn dữ liệu cũng như tính bảo mật dữ liệu. Mặt khác mạng Lan còn giúp các nhân viên trong tổ chức hay công ty truy nhập dữ liệu một cách thuận tiện với tốc độ cao. Đây cũng là lĩnh vực mà em rất quan tâm, hoc hỏi và tìm hiểu trong suốt thời gian qua. Và cũng là lý do em chọn đề tài: Thiết lập mạng LAN sử dụng hệ điều hành Windows Server 2003 và đánh giá, đề xuất phương án bảo đảm an toàn mạng.

Trong đồ án này em xin trình bày những vấn đề sau:

- Tìm hiểu về mạng máy tính.
- Tìm hiểu về bảo mật, an toàn mạng
- Tìm hiểu về hệ điều hành Windows Server 2003.
- Tìm hiểu thiết kế mạng.
- Đề xuất giải pháp bảo mật mạng.

CHƯƠNG I
KIẾN THỨC CHUNG VỀ MẠNG MÁY TÍNH

1.1. Tổng quan về mạng máy tính

1.1.1. Giới thiệu mạng máy tính và mục đích của việc kết nối mạng

Mạng máy tính (Network) là một tập hợp các máy tính được kết nối với nhau theo một cách nào đó sao cho chúng có thể trao đổi thông tin qua lại với nhau.

Các máy tính được kết nối thành mạng cho phép các khả năng:

+ Sử dụng chung các công cụ tiện ích
+ Chia sẻ kho dữ liệu dùng chung
+ Tăng độ tin cậy của hệ thống
+ Trao đổi thông điệp, hình ảnh
+ Dùng chung các thiết bị ngoại vi(máy in, máy vẽ, Fax, modem...)
+ Giảm thiểu chi phí và thời gian đi lại

1.1.2. Phân loại mạng

1.1.2.1. Mạng LAN

Mạng LAN là một nhóm các máy tính và các thiết bị truyền thông mạng được kết nối với nhau trong một không gian hẹp như một toà nhà, một khu vực...

Đặc điểm của mạng LAN:

- Băng thông lớn, có khả năng chạy các ứng dụng trực tuyến như xem phim, hội thảo qua mạng.
- Kích thước mạng bị giới hạn bởi các thiết bị.
- Chi phí các thiết bị mạng LAN tương đối rẻ.
- Quản trị đơn giản.

1.1.2 2. Mạng đô thị MAN

Mạng MAN gần giống như mạng LAN nhưng giới hạn của nó là một thành phố hay một quốc gia. Mạng MAN nối kết các mạng LAN lại với nhau thông qua các phương tiện truyền dẫn khác nhau (cáp quang, cáp đồng, sóng...) và các phương thức truyền thông khác nhau.

Đặc điểm của mạng MAN:

- Băng thông mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng...

- Do MAN nối kết nhiều LAN với nhau nên độ phức tạp cũng tăng đồng thời công tác quản trị sẽ khó khăn hơn.

- Chi phí các thiết bị mạng MAN tương đối đắt tiền.

1.1.2.3. Mạng WAN

Mạng WAN bao phủ vùng địa lý rộng lớn có thể là mạng của một công ty đa quốc gia, một lục địa hay toàn cầu. Do phạm vi rộng lớn của mạng WAN nên thông thường mạng WAN là tập hợp các mạng LAN, MAN nối lại với nhau bằng các phương tiện như: vệ tinh (**satellites**), sóng viba (**microwave**), cáp quang,cáp điện thoại...

Đặc trưng của mạng WAN:

- Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng offline như e-mail, web, ftp...

- Phạm vi hoạt động rộng lớn không giới hạn.

- Do kết nối của nhiều LAN, MAN lại với nhau nên mạng rất phức tạp và có tính toàn cầu nên thường là có tổ chức quốc tế đứng ra quản trị.

- Chi phí cho các thiết bị và các công nghệ mạng WAN rất đắt tiền.

WAN có thể chia thành nhiều loại như:

- WAN cho một doanh nghiệp (Enterprise WAN): kết nối các LAN của cùng một doanh nghiệp nằm ở các vị trí khác nhau.

- WAN toàn cầu (Global WAN): kết nối mạng của nhiều tổ chức khác nhau.

1.1.2.4. Mạng INTERNET

Mạng Internet là trường hợp đặc biệt của mạng WAN, nó cung cấp các dịch vụ toàn cầu như mail, web, chat, ftp và phục vụ miễn phí cho mọi người.

Mạng Internet là sở hữu của nhân loại, là sự kết hợp của rất nhiều mạng dữ liệu khác chạy trên nền tảng giao thức TCP/IP.

1.1.2.5. Mạng INTRANET

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

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

1.1.3. Các mô hình quản lý mạng

1.1.3.1. Workgroup

Trong mô hình này các máy tính có quyền hạn ngang nhau và không có các máy tính chuyên dụng làm nhiệm vụ cung cấp dịch vụ hay quản lý. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình. Đồng thời các máy tính cục bộ này cũng tự chứng thực cho người dùng cục bộ.

1.1.3.2. Domain

Ngược lại với mô hình Workgroup, trong mô hình Domain thì việc quản lý và chứng thực người dùng mạng tập trung tại máy tính Primary Domain Controller. Các tài nguyên mạng cũng được quản lý tập trung và cấp quyền hạn cho từng người dùng. Lúc đó trong hệ thống có các máy tính chuyên dụng làm nhiệm vụ cung cấp các dịch vụ và quản lý các máy trạm.

1.1.4. Các mô hình ứng dụng mạng

1.1.4.1. Peer-to-Peer

Mạng Peer to Peer được thiết lập trong đó các thành viên hay các trạm làm việc (Workstations) có vai trò ngang quyền nhau, mỗi máy gọi là một nút. Các trạm làm việc này có thể vừa đóng vai trò máy chủ vừa đóng vai trò máy khách tức là các thành viên có thể truy cập vào các máy trạm nào đó trên mạng để sử dụng chung tài nguyên (các tập tin, máy in...) nếu tài nguyên đó được chia sẻ để dùng chung.

- Ưu điểm: Do mô hình mạng ngang hàng đơn giản nên dễ cài đặt, tổ chức và quản trị, chi phí thiết bị cho mô hình này thấp.
- Khuyết điểm: Không cho phép quản lý tập trung nên dữ liệu phân tán, khả năng bảo mật thấp, rất dễ bị xâm nhập. Các tài nguyên không được sắp xếp nên rất khó định vị và tìm kiếm.

Mạng ngang hàng thích hợp với những mạng nhỏ và tính bảo mật không cao.

1.1.4.2. Client-Server

Là mạng trong đó có ít nhất một máy đóng vai trò máy chủ (Server) các máy còn lại gọi là các máy khách (Client), các máy này sinh ra các yêu cầu dịch vụ đối với máy chủ hay máy phục vụ.

- Ưu điểm: Do các dữ liệu được lưu trữ tập trung nên dễ bảo mật, backup và đồng bộ với nhau. Tài nguyên và dịch vụ được tập trung nên dễ chia sẻ và quản lý và có thể phục vụ cho nhiều người dùng.

- Khuyết điểm: Các server chuyên dụng rất đắt tiền, phải có nhà quản trị cho hệ thống.

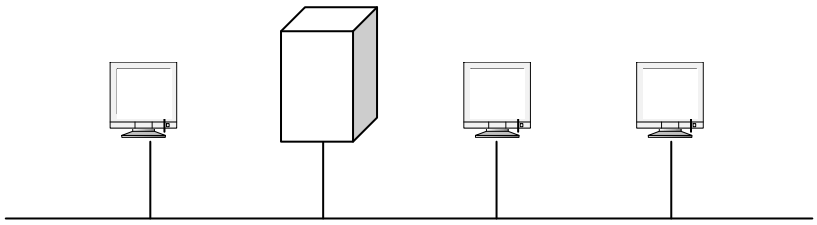
1.2. Network topology và các giao thức truy cập phương tiện truyền

1.2.1. Network topology

Topo (network topology) của mạng LAN là kiến trúc hình học thể hiện cách bố trí các đường dây cáp, sắp xếp các máy tính để kết nối thành mạng hoàn chỉnh. Có các loại cấu trúc topo mạng điển hình sau:

1.2.1.1. Bus topology

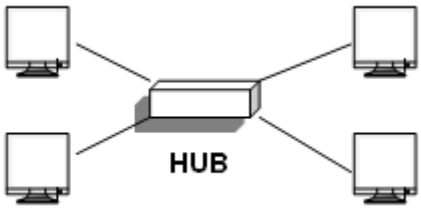
Tất cả các trạm phân chia chung một đường truyền chính. Trên đường truyền chính được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối vào bus thông qua một đầu nối chữ T (T- connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được quảng bá trên 2 chiều của bus và mọi trạm đều có thể nhận được tín hiệu.



Hình 1 : Mô hình kiểu kết nối dạng Bus

- Ưu điểm: Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt.
- Nhược điểm: Sẽ có sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn và khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.

1.2.1.2. Star topology



Hình 2 : Mô hình kết nối dang Star với Hub ở trung tâm

Trong mô hình này, một máy tính được nối vào mạng thông qua một cổng trên thiết bị trung tâm. Thiết bị trung tâm có bao nhiêu cổng thì hỗ trợ bấy nhiêu máy. Thiết bị trung tâm có đặc điểm khi một cổng có tín hiệu thì tín hiệu đó được lặp lại trên các cổng còn lại của Hub. Như vậy, tín hiệu được truyền từ máy tính gửi dữ liệu đến toàn bộ các máy tính khác trên toàn mạng. Tuỳ theo yêu cầu truyền thông trên mạng thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ định tuyến (router), một bộ tập trung (hub).

• Ưu điểm:

- Lắp đặt đơn giản, rễ cấu hình lại khi thêm, bớt trạm, dễ kiểm soát và khắc phục sự cố. tận dụng tối đa tốc độ đường truyền vật lý do sử dụng liên kết điểm - điểm.

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.

- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.

- Mạng có thể mở rộng hoặc thu hẹp tuỳ theo yêu cầu của người sử dụng.

• Nhược điểm:

- Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế.

- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm . Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.

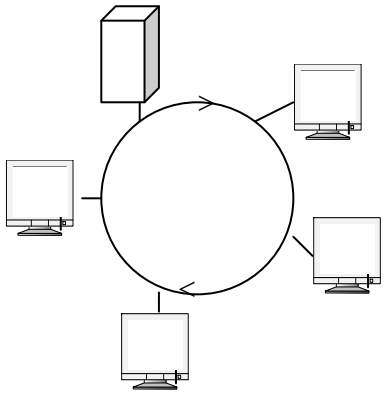
- Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).

Mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cáp xoắn, giải pháp này cho phép nối trực tiếp máy tính với HUB không cần

thông qua trục BUS, tránh được các yếu tố gây ngưng trệ mạng. Gần đây, cùng với sự phát triển switching hub, mô hình này ngày càng trở nên phổ biến và chiếm đa số các mạng mới lắp.

1.2.1.3. Ring topology

Tín hiệu được luân chuyển trên một vòng theo một chiều duy nhất. Mỗi trạm trên mạng được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển kế tiếp theo vòng. Cần thiết phải có giao thức điều khiển việc cấp quyền để truyền dữ liệu trên vòng cho các trạm có nhu cầu. Phương pháp truyền dữ liệu trên mạng ring là chuyển thẻ bài (token).



Hình 3: Mô hình kết nối dạng Ring

Để tăng độ tin cậy của vòng người ta có thể lắp đặt thêm một vòng dự phòng. Khi đường truyền trên đường chính bị sự cố thì dùng vòng dự phòng truyền dữ liệu.

- Ưu điểm: Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên.
- Nhược điểm: Là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

1.2.2. Các giao thức truy cập phương tiện truyền

1.2.2.1. Giao thức CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection). Giao thức này thường dùng cho mạng có cấu trúc hình tuyến, các máy trạm cùng chia sẻ một kênh truyền chung, các trạm đều có cơ hội thâm nhập đường truyền như nhau (Multiple Access). Tuy nhiên tại một thời điểm thì chỉ có một trạm được truyền dữ liệu mà thôi. Trước khi truyền dữ liệu, mỗi trạm phải lắng nghe đường truyền

để chắc chắn rằng đường truyền rỗi (Carrier Sense).

Trong trường hợp hai trạm thực hiện việc truyền dữ liệu đồng thời, xung đột dữ liệu sẽ xảy ra, các trạm tham gia phải phát hiện được sự xung đột và thông báo tới các trạm khác gây ra xung đột (Collision Detection), đồng thời các trạm phải ngừng thâm nhập, chờ đợi lần sau trong khoảng thời gian ngẫu nhiên nào đó rồi mới tiếp tục truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc xung đột có thể xẩy ra với số lượng lớn dẫn đến làm chậm tốc độ truyền tin của hệ thống. Giao thức này còn được trình bày chi tiết thêm trong phần công Ethernet.

1.2.2.2.Giao thức token bus

Nguyên lý: Để cấp phát quyền truy cập cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm nhận thẻ bài thì nó có quyền sử dụng đường truyền trong một thời đoạn định trước (có thể nhận hoặc truyền một hoặc nhiều đơn vị dữ liệu). Khi dữ liệu hết hoặc hết thời đoạn xác định đó trạm chuyển thẻ bài đến trạm tiếp theo.

Với phương pháp này việc đầu tiên là thiết lập vòng logic xác định bởi các trạm có nhu cầu truyền dữ liệu. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu thì ở ngoài vòng logic. Như vậy cần xử lý một số vấn đề sau:

- Bổ xung một trạm vào vòng logic (những trạm có yêu cầu truyền dữ liệu).
- Loại bỏ một trạm ra khỏi vòng logic (trạm không có nhu cầu truyền dữ liệu).
- Quản lý lỗi: có thể xảy ra ví dụ khi 2 trạm đều nghĩ rằng đến lượt mình hoặc không trạm nào nghĩ đến lượt mình truyền dữ liệu...
- Khởi tạo vòng logic.

1.2.2.3. Giao thức token ring

Phương pháp cũng dựa trên nguyên lý dùng thẻ bài truy cập đường truyền tuy nhiên ở đây thẻ bài không luân chuyển theo vòng logic mà luân chuyển theo vòng vật lý. Thẻ bài có chứa một bit biểu diễn trạng thái bân hoặc rỗi. Khi một trạm nhận được một thẻ bài đang ở trạng thái rỗi thì trạm đó có quyền sử dụng thẻ bài (truyền dữ liệu) và nó đổi bit trạng thái của thẻ bài thành bận. Thẻ bài được truyền đi đến trạm đích để trạm đích sao dữ liệu và vẫn ở trạng thái bận cho đến khi nó trở về

trạm nguồn. Lúc này trạm nguồn xoá bỏ dữ liệu và đổi bit trạng thái thành rỗi, thẻ bài tiếp tục luân chuyển trên vòng để đến trạm khác có nhu cầu truyền dữ liệu.

Phương pháp này cần xử lý 2 vấn đề sau: Mất thẻ bài trên vòng và thẻ bài bận lưu chuyển không dừng trên vòng.

1.3. Mô hình 7 mức OSI

1.3.1. Giới thiệu mô hình 7 mức OSI

Để các máy tính và các thiết bị mạng có thể truyền thông với nhau phải có những qui tắc giao tiếp được các bên chấp nhận. Trong mô hình OSI có bảy mức, mỗi mức mô tả một phần chức năng độc lập. Sự tách mức của mô hình này mang lại những lợi ích sau:

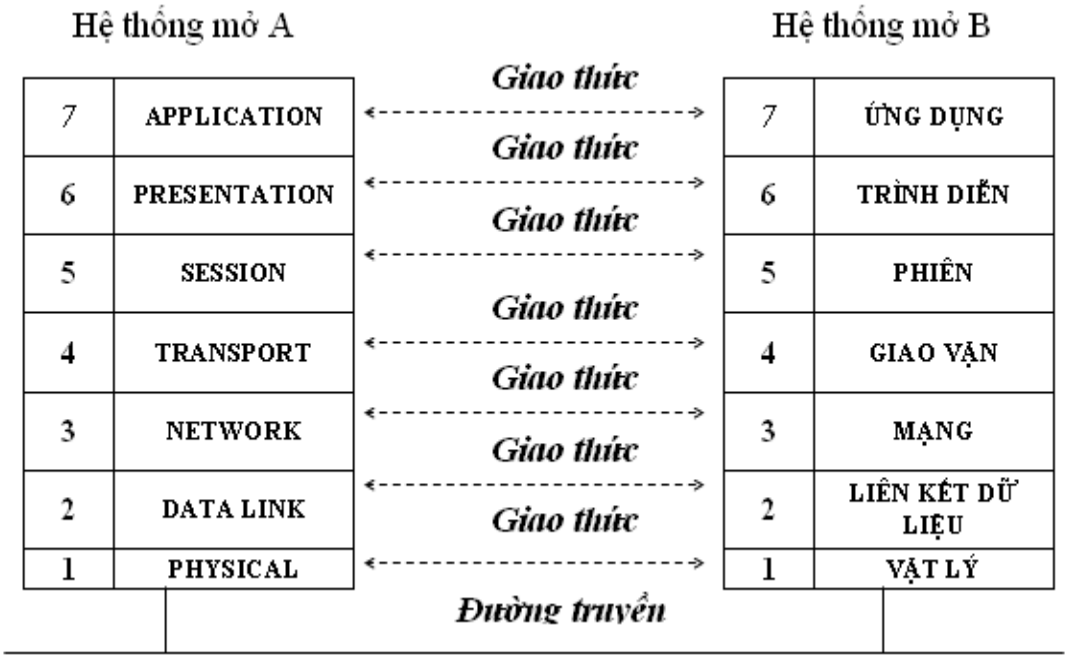
- Chia hoạt động thông tin mạng thành những phần nhỏ hơn, đơn giản hơn giúp chúng ta dễ khảo sát và tìm hiểu hơn.
- Chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà cung cấp sản phẩm.
- Ngăn chặn được tình trạng sự thay đổi của một mức làm ảnh hưởng đến các mức khác, như vậy giúp mỗi mức có thể phát triển độc lập và nhanh chóng hơn.

Mô hình 7 mức OSI cho chúng ta biết:

- Cách thức các thiết bị giao tiếp và truyền thông được với nhau.
- Các phương pháp để các thiết bị trên mạng khi nào thì được truyền dữ liệu, khi nào thì không được.
- Các phương pháp để đảm bảo truyền đúng dữ liệu và đúng bên nhận.
- Cách thức vận tải, truyền, sắp xếp và kết nối với nhau.
- Cách thức đảm bảo các thiết bị mạng duy trì tốc độ truyền dữ liệu thích hợp.
- Cách biểu diễn một bit thiết bị truyền dẫn.

Đây là mô hình dùng làm cơ sở cho nối kết các hệ thống mở phục vụ cho ứng dụng phân tán.

1.3.2. Mô hình và chức năng



Hình 4 : Mô hình 7 mức OSI

- ***Physical layer***

Mức vật lý định nghĩa tất cả các đặc tả về điện và vật lý cho các thiết bị. Trong đó bao gồm bố trí của các chân cắm, các hiệu điện thế, và các đặc tả về cáp nối. Các thiết bị tầng vật lí bao gồm Hub, repeater, thiết bị tiếp hợp mạng (network adapter) và thiết bị tiếp hợp kênh máy chủ (Host Bus Adapter)- (HBA dùng trong mạng lưu trữ (Storage Area Network)). Chức năng và dịch vụ căn bản được thực hiện bởi mức vật lý bao gồm:

Thiết lập hoặc ngắt mạch kết nối điện (electrical connection) với một phương tiện truyền thông (transmission medium).

Tham gia vào quy trình mà trong đó các tài nguyên truyền thông được chia sẻ hiệu quả giữa nhiều người dùng. Chẳng hạn giải quyết tranh chấp tài nguyên (contention) và điều khiển lưu lượng.

Điều biến (modulation), hoặc biến đổi giữa biểu diễn dữ liệu số (digital data) của các thiết bị người dùng và các tín hiệu tương ứng được truyền qua kênh truyền thông (communication channel).

- ***Data link layer***

Cung cấp các phương tiện để truyền thông tin qua liên kết vật lý đảm bảo tin cậy: gửi các khối dữ liệu (frame) với các cơ chế đồng bộ hoá, kiểm soát lỗi và

kiểm soát luồng dữ liệu cần thiết.

- ***Network layer***

Mức mạng cung cấp các chức năng và quy trình cho việc truyền các chuỗi dữ liệu có độ dài đa dạng, từ một nguồn tới một đích, thông qua một hoặc nhiều mạng, trong khi vẫn duy trì chất lượng dịch vụ mà mức giao vận yêu cầu. Mức mạng thực hiện chức năng định tuyến.Các thiết bị định tuyến (*router*) hoạt động tại mức này gửi dữ liệu ra khắp mạng mở rộng, làm cho liên mạng trở nên khả thi.

- ***Transport layer***

Mức này cung cấp dịch vụ chuyên dụng chuyển dữ liệu giữa các người dùng tại đầu cuối, nhờ đó các tầng trên không phải quan tâm đến việc cung cấp dịch vụ truyền dữ liệu đáng tin cậy và hiệu quả. Mức giao vận kiểm soát độ tin cậy của một kết nối được cho trước.

- ***Session layer***

Mức này kiểm soát hội thoại giữa các máy tính, thiết lập, quản lý và kết thúc các kết nối giữa trình ứng dụng địa phương và trình ứng dụng ở xa. Thiết lập các qui trình đánh dấu điểm hoàn thành (checkpointing) - giúp việc phục hồi truyền thông nhanh hơn khi có lỗi xảy ra, vì điểm đã hoàn thành đã được đánh dấu - trì hoãn (adjournment), kết thúc (termination) và khởi động lại (restart). Mô hình OSI uỷ nhiệm cho mức này trách nhiệm "ngắt mạch nhẹ nhàng" (graceful close) các phiên giao dịch (một tính chất của giao thức kiểm soát giao vận TCP) và trách nhiệm kiểm tra và phục hồi phiên, đây là phần thường không được dùng đến trong bộ giao thức TCP/IP.

- ***Presentation layer***

Mức presentation biến đổi dữ liệu để cung cấp một giao diện tiêu chuẩn cho mức ứng dụng.

- ***Application layer***

Mức này có nhiệm vụ phục vụ trực tiếp cho người sử dụng, cung cấp tất cả các yêu cầu cần thiết cho người sủ dụng, yêu cầu phục vụ chung như chuyển file... Mức này là giao diện chính để người dùng tương tác với chương trình ứng dụng, và qua đó với mạng. Một số ví dụ về các ứng dụng trong mức này bao gồm Telnet, Giao thức truyền tập tin FTP và Giao thức truyền thư điện tử SMTP, remote.

1.4. Bộ giao thức TCP/IP

1.4.1. Giới thiệu bộ giao thức TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) là một bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu.

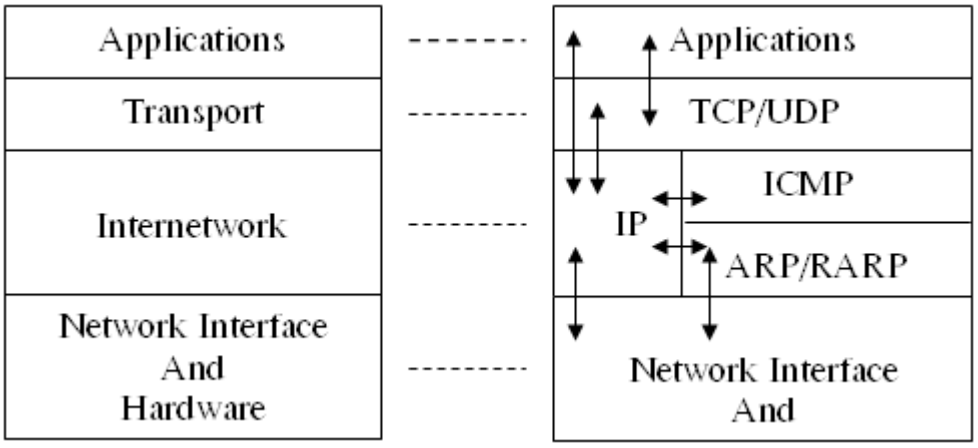
Máy nào hỗ trợ giao thức TCP/IP đều có thể truy cập vào Internet.

TCP/IP thực chất là một họ giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng.

1.4.2. Các mức trong giao thức TCP/IP

Bộ giao thức TCP/IP được phân làm 4 mức

- Application Layer
- Transport Layer
- Internet Layer
- Network access Layer



Hình 6 : Các mức trong giao thức TCP/IP

- ***Network Access layer***

Miêu tả các nối kết vật lý giữa các máy chủ trong mạng. Bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp thông tin cần thiết để có thể hoạt động, truy cập đương truyền vật lý qua các thiết bị giao tiếp đó.

- ***Internet layer***

Xử lý quá trình truyền gói tin trên mạng. Các giao thức trong tầng này gồm

: IP(Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol)

- ***Transport layer***

Transport layer kết hợp các khả năng truyền thông điệp trực tiếp (end-to-end) không phụ thuộc vào mạng bên dưới, kèm theo kiểm soát lỗi (error control), phân mảnh (fragmentation) và điều khiển lưu lượng. Tầng này có hai giao thức chính TCP và UDP.

TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin, đặt hạn chế thời gian time- out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng . Nó chỉ gửi các gói dữ liệu từ trạm này đến trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

- ***Application layer***

Application layer là nơi các chương trình mạng thường dùng nhất làm việc nhằm liên lạc giữa các nút trong một mạng.

Bao gồm các tiến trình và các ứng dụng cung cấp cho người sủ dụng để truy cập mạng. Mức này tương đương với các mức 5,6,7 trong mô hình OSI. Các ứng dụng phổ biến : Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, www (World Wide Web).

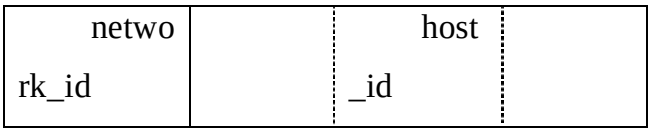
1.4.3. Giới thiệu địa chỉ IPv4

Địa chỉ IP (IPv4) có độ dài 32 bit và được tách thành 4 vùng, mỗi vùng (mỗi vùng 1 byte) thường được biểu diễn dưới dạng thập phân và được cách nhau bởi dấu chấm (.). Ví dụ: 203.162.7.92.

Địa chỉ IPv4 được chia thành 5 lớp A, B, C, D, E; trong đó 3 lớp địa chỉ A, B, C được dùng để cấp phát. Các lớp này được phân biệt bởi các bit đầu tiên trong địa chỉ.

1.4.3.1. Lớp A

Dành một byte cho phần **network_id** và ba byte cho phần **host_id**.

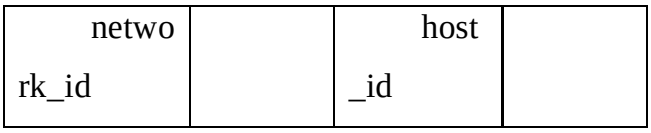


Để nhận diện ra lớp A, bit đầu tiên của byte đầu tiên phải là bit 0. Dưới dạng nhị phân, byte này có dạng 0xxxxxxx. Vì vậy, những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 đến 127 sẽ thuộc lớp A.

Cho phép định danh 126 mạng với tối đa 16 triệu host trên mỗi mạng. Lớp này dùng cho mạng có số trạm cực lớn: 16.777.214

1.43.2. Lớp B

Dành hai byte cho mỗi phần **network_id** và **host_id**.



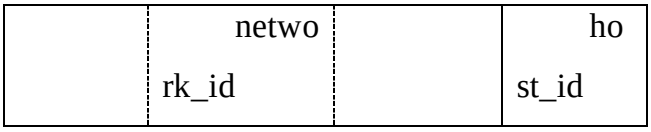
Dấu hiệu để nhận dạng địa chỉ lớp B là byte đầu tiên luôn bắt đầu bằng hai bit 10. Dưới dạng nhị phân, octet có dạng 10xxxxxx. Vì vậy những địa chỉ nằm trong khoảng từ 128 đến 191 sẽ thuộc về lớp B

Phần **network_id** chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16.384 (2^{14}) mạng khác nhau (128.0.0.0 đến 191.255.0.0)

Phần **host_id** dài 16 bit hay có 65536 (2^{16}) giá trị khác nhau. Trừ 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B. Ví dụ, đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.

1.4.3.3. Lớp C

Dành ba byte cho phần **network_id** và một byte cho phần **host_id**.



Byte đầu tiên luôn bắt đầu bằng ba bit 110 và dạng nhị phân của octet này là 110xxxxx. Như vậy những địa chỉ nằm trong khoảng từ 192 đến 233 sẽ thuộc lớp

Phần **network_id** dùng ba byte hay 24 bit, trừ đi 3 bit làm ID của lớp, còn lại 21 bit hay 2.097.152 (2^{21}) địa chỉ mạng (từ **192.0.0**.0 đến **223.255.255**.0).

1.4.3.4. Lớp D và E

Các địa chỉ có byte đầu tiên nằm trong khoảng 224 đến 255 là các địa chỉ thuộc lớp D hoặc E. Do các lớp này không phục vụ cho việc đánh địa chỉ các host nên không trình bày ở đây.

1.4.3.5. Địa chỉ mạng riêng và địa chỉ mạng con

- ***Địa chỉ mạng riêng***

Các địa chỉ IP trong vùng sử dụng trên được gắn cho các máy tính trên mạng Internet. Tuy nhiên các Công ty có nhu cầu sử dụng địa chỉ IP riêng, không kết nối với mạng khác trên Internet, để chỉ định địa chỉ cho các mạng kiểu này ta dựng địa chỉ mạng riêng. Các địa chỉ đó như sau:

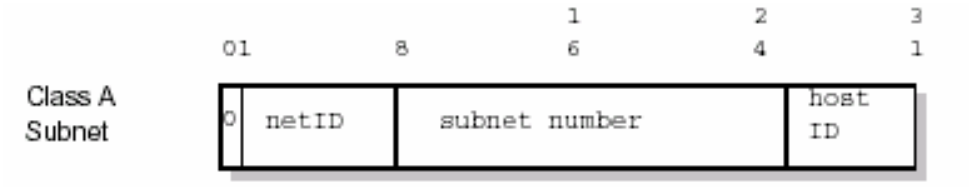
Lớp	Khoảng địa chỉ
A	0.0.0.0 đến 127.255.255.255
B	128.0.0.0 đến 191.255.255.255
C	192.0.0.0 đến 223.255.255.255
D	224.0.0.0 đến 239.255.255.255
E	240.0.0.0 đến 247.255.255.255

Hình 7: Các lớp địa chỉ Internet

Ghi nhớ: *Địa chỉ thực tế không phân trong trường hợp tất cả các bit trong một hay nhiều Octet sử dụng cho địa chỉ mạng hay địa chỉ máy chủ đều bằng 0 hay đều bằng 1. Điều này đúng cho tất cả các lớp địa chỉ.*

- ***IP subnetting***

Đối với các địa chỉ lớp A, B số trạm trong một mạng là quá lớn và trong thực tế thường không có một số lượng trạm lớn như vậy kết nối vào một mạng đơn lẻ. Địa chỉ mạng con cho phép chia một mạng lớn thành các mạng con nhỏ hơn. Người quản trị mạng có thể dùng một số bit đầu tiên của trường hostid trong địa chỉ IP để đặt địa chỉ mạng con. Chẳng hạn đối với một địa chỉ thuộc lớp A, việc chia địa chỉ mạng con có thể được thực hiện như sau:



Hình 8: Cách phân chia địa chỉ mạng con

Việc chia địa chỉ mạng con là hoàn toàn trong suốt đối với các router nằm bên ngoài mạng, nhưng nó là không trong suốt đối với các router nằm bên trong mạng.

- ***Mặt nạ địa chỉ mạng con***

Bên cạnh địa chỉ IP, một trạm cũng cần được biết việc định dạng địa chỉ mạng con: Bao nhiêu bit trong trường hostid được dùng cho phần địa chỉ mạng con(subnetid). Thông tin này được chỉ ra trong mặt nạ địa chỉ mạng con (subnet mask).Subnet mask cũng là một số 32 bit với các bit tương ứng với phần netid và subnetid được đặt bằng 1 còn các bit còn lại được đặt bằng 0.

1.4.4. Địa chỉ thế hệ mới - IPv6

1.4.4.1. Khái quát chung

Địa chỉ thế hệ mới của Internet - IPv6 (IP Address Version 6) được Nhóm chuyên trách về kỹ thuật IETF (Internet Engineering Task Force) của Hiệp hội Internet đề xuất thực hiện kế thừa trên cấu trúc và tổ chức của IPv4. IPv4 có 32 bít địa chỉ với khả năng lý thuyết có thể cung cấp một không gian địa chỉ là 2^{32}. Còn IPv6 có 128 bit địa chỉ dài hơn 4 lần so với IPv4 nhưng khả năng lý thuyết có thể cung cấp một không gian địa chỉ là 2^{128} địa chỉ, số lượng này rất lớn nếu rải đều trên bề mặt quả đất thì mỗi một vùng có khoảng 665 570.10 ^{18} địa chỉ vì diện tích bề mặt quả đất khoảng 511 263 tỷ một vùng. Đây là một không gian địa chỉ cực lớn với mục đích không chỉ cho Internet mà còn cho tất cả các mạng máy tính, hệ thống viễn thông, hệ thống điều khiển và thậm chí cho từng vật dụng trong gia đình. Người ta nói rằng từng chiếc điều hoà, tủ lạnh, máy giặt hay nồi cơm điện v.v... của từng gia đình một cũng sẽ mang một địa chỉ IPv6 để chủ nhân của chúng có thể kết nối và ra lệnh từ xa. Nhu cầu hiện tại chỉ cần 15% không gian địa chỉ IPv6 cũn 85% dự phòng cho tương lai.

1.4.4.2. Cấu trúc địa chỉ IPv6.

Địa chỉ IPv4 được chia ra 5 lớp A,B,C,D,E còn IPv6 lại được phân ra là 3 loại chính sau:

- **Unicast Address**. Địa chỉ đơn hướng. Là địa chỉ dùng để nhận dạng từng Node một (Node - Điểm Nút là tập hợp các thiết bị chuyển mạch nằm ở trung tâm như Router chẳng hạn), cụ thể là một gói số liệu được gửi tới một địa chỉ đơn hướng sẽ được chuyển tới Node mang địa chỉ đơn hướng - Unicast đó.
- **Anycast Address**. Địa chỉ bất kỳ hướng nào. Là địa chỉ dùng để nhận dạng một "Tập hợp Node" bao gồm nhiều Node khác nhau hợp thành, cụ thể là một gói số liệu được gửi tới một địa chỉ "Bất cứ hướng nào" sẽ được chuyển tới một Node gần nhất trong Tập hợp Node mang địa chỉ anycast đó.
- **Multicast Address**. Địa chỉ đa hướng. Là địa chỉ dùng để nhận dạng một "Tập hợp Node" bao gồm nhiều Node khác nhau hợp thành, cụ thể là một gói số liệu được gửi tới một địa chỉ" đa hướng" sẽ được chuyển tới tất cả các Node trong Tập hợp Node mang địa chỉ Multicast đó.

1.5. Môi trường truyền dẫn và các thiết bị mạng thông dụng

1.5.1. Môi trường truyền dẫn

- Liên kết các nút mạng, truyền dẫn các tín hiệu điện hay quang

- Mạng cục bộ sử dụng chủ yếu là các loại cáp, trong đó có hai loại cáp thường được sử dụng: cáp đồng trục, cáp đôi dây xoắn

1.5.1.1. Coaxial cable

Cáp đồng trục bao gồm một sợi dây dẫn ở giữa, bên ngoài bọc một lớp cách điện rồi đến một lớp lưới kim loại, tất cả được đặt trong một lớp vỏ cách điện,

Có hai loại cáp đồng trục phổ biến nhất dung trong mạng là :

- **Thicknet:** Cáp đồng trục dầy có đường kính khoảng 1.3cm và tương đối cứng. Đôi khi người ta xem nó như Ethernet chuẩn và do nó là loại cáp đầu tiên dùng với kiến trúc mạng rất phổ biến-Ethernet. Lõi đồng của loại cáp này dầy hơn lõi cáp mảnh. Lõi đồng càng dầy thì cáp càng mang tín hiệu đi xa hơn. Điều này có

nghĩa là cáp dày có thể mang tín hiệu đi xa hơn cáp mảnh. Cáp dày có thể mang tín hiệu đi được 500m

- ***Thinnet:*** Loại cáp mảnh có đường kính khoảng 0.5 cm. Do loại cáp đồng trục này mềm và dễ kéo dây nên người ta có thể dùng cho gần như bất kỳ kiểu lắp đặt mạng nào. Mạng dùng loại cáp mảnh có cáp nối trực tiếp vào card mạng của máy tính.

Cáp đồng trục mảnh có thể mang tín hiệu đi xa tới 185m trước khi tín hiệu có thể suy yếu.

Cáp đồng trục ít bị ảnh hưởng của nhiễu và sự suy hao tín hiệu cho nên nó cung cấp một đường truyền dài và tốt hơn cáp xoắn.

1.5.1.2. Twisted – Pair Cable

Cáp xoắn đôi gồm hai sợi dây đồng cách ly quấn vào nhau. Một số dây xoắn đôi thường được nhóm chung với nhau và được quấn kín trong vỏ bọc bảo vệ để tạo thành sợi cáp. Số lượng dây xoắn đôi thực tế trong sợi cáp khác nhau. Sự quấn xoắn này làm vô hiệu hoá nhiễu điện từ dây xoắn đôi kế cận và từ những nguồn khác như môtơ, rơle,và máy biến thế.

Cáp xoắn đôi có hai loại:

- Cáp xoắn đôi trần (UTP)

Cắp xoắn đôi trần sử dụng chuẩn 10BaseT, là loại cáp phổ biến nhất và nhanh chóng trở thành loại cáp mạng cục bộ được ưa chuộng nhất. Độ dài tối đa của 1 đoạn cáp là 100m.

Cáp xoắn đôi trần gồm hai dây đồng cách điện. Tuỳ theo mục đích cụ thể mà cáp xoắn đôi trần sẽ khống chế ở bao nhiêu mắt xoắn cho phép trên mỗi mét sợi cáp.

- Cáp xoắn đôi có bọc (STP)

Cáp xoắn đôi có bọc dùng vỏ đồng bện, vốn là loại vỏ bọc bảo vệ có chất lượng cao hơn cáp xoắn đôi trần. Cáp xoắn đôi có bọc cũng dùng lớp cách ly ở giữa và xung quanh các cặp dây và mắt xoắn bên trong của cặp dây. Lớp cách ly này tạo cho cáp xoắn đôi có bọc tính cách ly tuyệt hảo đến dữ liệu truyền. Cáp xoắn đôi có

bọc it bị tác động bởi nhiễu điện và có tốc độ truyền qua khoảng cách xa cao hơn cáp xoắn đôi dây trần.

1.5.1.3. Fiber – Optic Cable

Loại cáp này truyền dẫn tín hiệu đi trên cơ sở truyền tín hiệu quang theo một ống thuỷ tinh nhờ vào định luật phản xạ toàn phần. Cấu trúc gồm một giây dẫn trung tâm là một hoặc một bó sợi thuỷ tinh hoặc plastic có thể truyền dẫn tín hiệu quang , nó được bọc một lớp áo có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất tín hiệu. Lớp ngoài là lớp vỏ để bảo vệ cáp.

Cáp sợi quang có ưu điểm rất lớn là độ suy hao tín hiệu đường truyền thấp do đó có thể đi cáp xa (vài km), có giải thông lớn (đạt 2 Gb/s), không dùng tín hiệu điện nên tránh nhiễu điện từ và các hiệu ứng điện khác, không thể dùng các thiết thu phát điện tử để thu trộm tín hiệu cho nên an toàn thông tin trên đường truyền.

Nhược điểm khó lắp đặt khi đấu nối cáp và giá thành cao.

1.5.2. Các thiết bị mạng thông dụng

1.5.2.1. Hub

Hub là điểm kết nối dây trung tâm của mạng, tất cả các trạm trên mạng LAN được sử dụng thông qua hub. Một hub thường có nhiều cổng nối với người sử dụng để gắn máy tính với các thiết bị ngoại Tất cả các LAN liên kết với nhau qua hub sẽ trở thành một LAN.

Passive Hub chỉ đảm bảo các chức năng kết nối hoàn toàn không xử lý lại tín hiệu.

Active Hub có chức năng khuyếch đại tín hiệu để chống suy hao.

Intelligent Hub là active hub nhưng có khả năng tạo ra các gói tin mang tin tức về hoạt động của mình và gửi lên mạng để người quản trị mạng có thể thực hiện quản trị tự động.

1.5.2.2. Repeater

Làm việc với tầng thứ nhất của mô hình OSI - tầng vật lý. Repeater có hai cổng. Nó thực hiện việc chuyển tiếp tất cả các tín hiệu vật lý đến từ cổng này ra cổng khác sau khi đã khuyếch đại. Tất cả các Lan liên kết với nhau qua repeater trở

thành một LAN. Nó chỉ có khả năng liên kết các LAN có cùng một chuẩn công nghệ.

1.5.2.3. Bridge

Bridge là một thiết bị cho phép nối kết các mạng LAN với nhau. Bridge có chọn lọc và chuyển đi các gói tin có đích ở phần mạng bên kia và dùng để liên kết các LAN có cùng giao thức tầng liên kết dữ liệu, có thể khác nhau về môi trường truyền dẫn vật lý. Không hạn chế về số lượng bridge sử dụng. Cũng có thể được dùng để chia một LAN thành nhiều LAN con → giảm dung lượng thông tin truyền trên toàn LAN.

Làm việc với tầng thứ hai của mô hình OSI: tầng liên kết dữ liệu.

1.5.2.4. Router

Chức năng của Router là gửi đi các gói dữ liệu dựa trên địa chỉ phân lớp của mạng và cung cấp các dịch vụ như bảo mật, quản lý lưu thông. Router có khả năng thực hiện giải thuật chọn đường tối ưu cho các gói tin.

Thường có nhiều hơn 2 cổng. Nó tiếp nhận tín hiệu vật lý từ một cổng, chuyển đổi về dạng dữ liệu, kiểm tra địa chỉ mạng rồi chuyển dữ liệu đến cổng tương ứng.

- Dùng để liên kết các LAN có thể khác nhau về chuẩn LAN nhưng cùng giao thức mạng ở tầng network.

1.5.2.5. Switch

Chức năng chính của switch là cùng một lúc duy trì nhiều kết nối giữa các thiết bị mạng. Switch nhận tín hiệu vật lý, chuyển đổi thành dữ liệu, từ một cổng, kiểm tra địa chỉ đích rồi gửi tới một cổng tương ứng.

CHƯƠNG II

BẢO MẬT MẠNG MÁY TÍNH

2.1. Các vấn đề chung về bảo mật mạng

Do đặc điểm của một hệ thống mạng là có nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên (mất mát, hoặc sử dụng không hợp lệ) trong môi trường mạng phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.

Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đối tượng đồng thời đảm bảo mạng hoạt động ổn định, không bị tấn công bởi những kẻ phá hoại.

Không một hệ thống mạng nào đảm bảo là an toàn tuyệt đối, một hệ thống dù được bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hoá bởi những kẻ có ý đồ xấu.

2.1.1. Đối tượng tấn công mạng

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.

Một số đối tượng tấn công mạng là:

- Hacker: Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.

- Masquerader: Là những kẻ giả mạo thông tin trên mạng. Có một số hình thức như giả mạo địa chỉ IP, tên miền, định danh người dùng ...

- Eavesdropping: Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị.

Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau như: ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có

chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

2.1.2. Các lỗ hổng bảo mật

Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

2.1.3. Chính sách bảo mật

Là tập hợp các qui tắc áp dụng cho mọi đối tượng có tham gia quản lý và sử dụng các tài nguyên và dịch vụ mạng.

Mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng , đồng thời giúp các nhà quản trị thiết lập các biện pháp bảo đảm hữu hiệu trong quá trình trang bị, cấu hình, kiểm soát hoạt động của hệ thống và mạng

Một chính sách bảo mật được coi là hoàn hảo nếu nó xây dựng gồm các văn bản pháp qui, kèm theo các công cụ bảo mật hữu hiệu và nhanh chóng giúp người quản trị phát hiện, ngăn chặn các xâm nhập trái phép.

2.2. Các lỗ hổng và phương thức tấn công mạng chủ yếu

2.2.1. Các lỗ hổng

Các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Windows 95, UNIX hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như

word processing, các hệ databases...

Có nhiều tổ chức khác nhau tiến hành phân loại các dạng lỗ hổng đặc biêt. Theo cách phân loại của Bộ quốc phòng Mỹ, các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

- Lỗ hổng loại C: các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services - Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống; không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.

- Lỗ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ nên có thể dẫn đến mất mát hoặc lộ thông tin yêu cầu bảo mật. Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống.

- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

2.2.2. Một số phương thức tấn công mạng phổ biến

2.2.2.1. Password Cracker

Password cracker là một chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.

Để hiểu cách thức hoạt động của các chương trình bẻ khoá, chúng ta cần hiểu cách thức mã hoá để tạo mật khẩu. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.

2.2.2.2. Virus

Virus máy tính thực chất chỉ là một chương trình máy tính có khả năng tự sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác (đối tượng có thể là các file chương trình, văn bản, đĩa mềm...), và chương trình đó mang tính phá hoại. Virus có nhiều cách lây lan và tất nhiên cũng có nhiều cách phá hoại,

nhưng chỉ cần bạn nhớ rằng đó là một đoạn chương trình và đoạn chương trình đó dùng để phục vụ những mục đích không tốt.

2.2.2.3. Sniffer

Đối với bảo mật hệ thống sniffer được hiểu là các công cụ (có thể là phần cứng hoặc phần mềm) "bắt" các thông tin lưu chuyển trên mạng và từ các thông tin "bắt" được đó để lấy được những thông tin có giá trị trao đổi trên mạng.

Phương thức tấn công mạng dựa vào các hệ thống sniffer là rất nguy hiểm vì nó được thực hiện ở các tầng rất thấp trong hệ thống mạng. Với việc thiết lập hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng. Các thông tin đó có thể là:

- Các tài khoản và mật khẩu truy nhập
- Các thông tin nội bộ hoặc có giá trị cao...

Tuy nhiên việc thiết lập một hệ thống sniffer không phải đơn giản vì cần phải xâm nhập được vào hệ thống mạng đó và cài đặt các phần mềm sniffer. Đồng thời các chương trình sniffer cũng yêu cầu người sử dụng phải hiểu sâu về kiến trúc, các giao thức mạng.

Hạn chế sniffer:

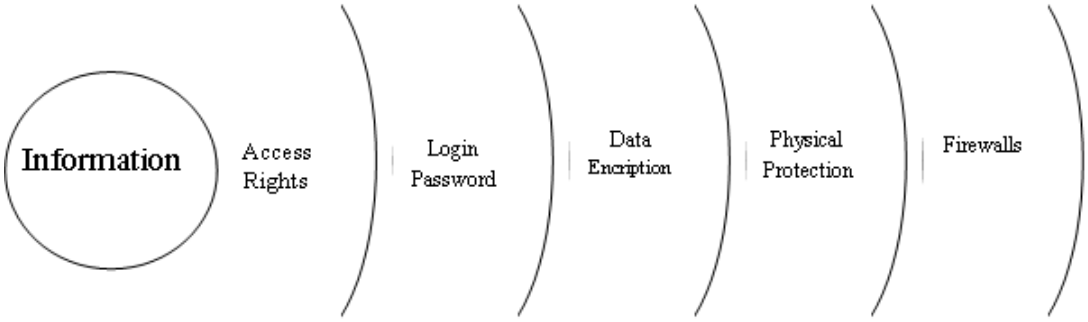
- Không cho người lạ truy nhập vào các thiết bị trên hệ thống
- Quản lý cấu hình hệ thống chặt chẽ
- Thiết lập các kết nối có tính bảo mật cao thông qua các cơ chế mã hoá

2.2.3. Các mức độ bảo vệ an toàn mạng

Do đặc điểm trên mạng với nhiều đối tượng sử dụng, phân tán về mặt địa lý nên việc bảo vệ tài nguyên tránh khỏi mất mát, bị xâm phạm là vấn đề rất phức tạp. Kẻ vi phạm trong thực tế có thể thâm nhập vào bất kỳ điểm nào mà thông tin kẻ đó quan tâm đi qua hoặc được cất giữ. Điểm đó có thể trên đường truyền, tại máy trạm, máy chủ hoặc tại các giao diện kết nối liên mạng (bridge, router, gateway...)

Vì không thể có một giải pháp an toàn tuyệt đối nên người ta phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp rào chắn đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ các thông

tin cất giữ trên máy tính, phần lớn trên Server, bởi thế ngoài các biện pháp bảo vệ vật lý trên đường truyền, người ta xây dựng các biện pháp triển khai trên Server.



Hình 9 : Rào chắn bảo vệ thông tin trên mạng.

2.2.3.1. Access Rights

Lớp bảo vệ trong cùng là quyền truy cập nhằm kiển soát các nguồn tài nguyên của mạng và quyền hạn trên tài nguyên đó. Dĩ nhiên kiểm soát các cấu trúc dữ liệu càng chi tiết càng tốt. Với sự hỗ trợ của hệ điều hành, việc kiểm soát hiện tại thường ở mức tệp. Để truy cập vào một thư mục, tệp tin người dùng phải có được quyền truy xuất các đối tượng đó, các quyền như read, write, modify, read and execute...

2.2.3.2. Login/Password

Đây cũng là kiểm soát quyền truy cập nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống (đăng nhập mạng). Mức kiểm soát này phổ biến vì nó đơn giản, ít phí tổn và rất hiệu quả. Mỗi người sử dụng kể cả người quản trị muốn vào mạng để sử dụng tài nguyên, trước tiên phải đăng ký tên và mật khẩu trước. Người quản trị mạng có trách nhiệm quản lý giám sát mọi hoạt động của mạng. Xác định quyền truy cập của người dùng mạng tuỳ theo thời gian và không gian (đăng nhập mạng tuỳ theo thời điểm và vị trí khác nhau).

Giữ kín được thông tin về tên và mật khẩu của người dùng sẽ tăng cao hiệu quả của lớp kiểm soát này, tuy nhiên thường người dùng quá dễ dãi để lộ tên tài khoản truy cập mạng của mình. Cách khắc phục ví dụ như trao quyền thay đổi mật khẩu cho người dùng, người quản trị chịu trách nhiệm đặt, thay đổi mật khẩu theo thời gian...

2.2.3.3. Data Encription

Để bảo vệ thông tin truyền trên mạng, người ta sử dụng các phương pháp mã hoá. Dữ liệu được biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó (mã hoá) và được biến đổi ngược lại ở nơi nhận (giải mã) để người nhận hiểu được thông tin. Đây là lớp bảo vệ rất quan trọng và được sử dụng rộng rãi trong môi trường mạng.

2.2.3.4. Physical Protection

Nhằm ngăn cản các truy cập vật lý bất hợp pháp vào hệ thống mạng. Có thể ví dụ các phương pháp như ngăn cấm người không phận sự vào phòng máy, sử dụng máy không ổ mềm, hệ thống báo động, bảo vệ đường dây truyền tín hiệu mạng...

2.2.3.5. Firewalls

Để bảo vệ từ xa cho một máy hoặc một hệ thống mạng máy tính người ta thường sử dụng hệ thống bức tường lửa. Bức tường lửa có chức năng ngăn chặn các thâm nhập trái phép (theo danh sách truy nhập xác định trước), và thậm chí có thể lọc bỏ các gói tin mà ta không muốn gửi đi hoặc nhận vào vì lí do nào đó.

2.3. Các biện pháp bảo vệ mạng máy tính.

2.3.1. Kiểm soát hệ thống qua logfile.

Một trong những biện pháp dò tìm các dấu vết hoạt động trên một hệ thống là dựa vào các công cụ ghi logfile. Các công cụ này thực hiện ghi lại nhật ký các phiên làm việc trên hệ thống. Nội dung chi tiết thông tin ghi lại phụ thuộc vào cấu hình người quản trị hệ thống. Ngoài việc rà soát theo dõi hoạt động, đối với nhiều hệ thống các thông tin trong logfile giúp người quản trị đánh giá được chất lượng, hiệu năng của mạng lưới.

a) Logfile lastlog:

Tiện ích này ghi lại những lần truy nhập gần đây đối với hệ thống. Các thông tin ghi lại gồm tên người truy nhập, thời điểm, địa chỉ truy nhập ... Các chương trình login sẽ đọc nội dung file lastlog, kiểm tra theo UID truy nhập vào hệ thống và sẽ thông báo lần truy nhập vào hệ thống gần đây nhất.

b) Logfile UTMP

Logfile này ghi lại thông tin về những người đang login vào hệ thống,

thường nằm ở thư mục /etc/utmp. Để xem thông tin trong logfile có thể sử dụng các tiện ích như who, w, finger, rwho, users.

e) Tiện ích sulog

Bất cứ khi nào người sử dụng dùng lệnh "su" để chuyển sang hoạt động hệ thống dưới quyền một user khác đều được ghi log thông qua tiện ích sulog. Những thông tin logfile này được ghi vào logfile /var/adm/sulog. Tiện ích này cho phép phát hiện các trường hợp dùng quyền root để có được quyền của một user nào khác trên hệ thống.

f) Tiện ích cron

Tiện ích cron sẽ ghi lại logfile của các hoạt động thực hiện bởi lệnh crontabs. Thông thường, logfile của các hoạt động cron lưu trong file /var/log/cron/log. Ngoài ra, có thể cấu hình syslog để ghi lại các logfile của hoạt động cron.

g) Logfile của sendmail

Hoạt động ghi log của sendmail có thể được ghi qua tiện ích syslog. Ngoài ra chương trình sendmail còn có lựa chọn "-L + level security" với mức độ bảo mật từ "debug" tới "crit" cho phép ghi lại logfile. Vì sendmail là một chương trình có nhiều bug, với nhiều lỗ hổng bảo mật nền người quản trị hệ thống thường xuyên nên ghi lại logfile đối với dịch vụ này.

h) Logfile của dịch vụ FTP

Hầu hết các daemon FTP hiện nay đều cho phép cấu hình để ghi lại logfile sử dụng dịch vụ FTP trên hệ thống đó. Hoạt động ghi logfile của dịch vụ FTP thường được sử dụng với lựa chọn "-l".

2.3.2. Thiết lập chính sách bảo mật hệ thống

Trong các bước xây dựng một chính sách bảo mật đối với một hệ thống, nhiệm vụ đầu tiên của người quản trị là xác định được đúng mục tiêu cần bảo mật. Việc xác định những mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp các nhà quản trị thiết lập các biện pháp đảm bảo hữu hiệu trong quá trình trang bị, cấu hình và kiểm soát hoạt động của hệ thống. Những mục tiêu bảo mật bao gồm:

2.3.2.1. Xác định đối tượng cần bảo vệ

Đây là mục tiêu đầu tiên và quan trọng nhất trong khi thiết lập một chính sách bảo mật. Người quản trị hệ thống cần xác định rõ những đối tượng nào là quan trọng nhất trong hệ thống cần bảo vệ và xác định rõ mức độ ưu tiên đối với những đối tượng đó. Ví dụ các đối tượng cần bảo vệ trên một hệ thống có thể là: các máy chủ dịch vụ, các router, các điểm truy nhập hệ thống, các chương trình ứng dụng, hệ quản trị CSDL, các dịch vụ cung cấp ...

Trong bước này cần xác định rõ phạm vi và ranh giới giữa các thành phần trong hệ thống để khi xảy ra sự cố trên hệ thống có thể cô lập các thành phần này với nhau, dễ dàng dò tìm nguyên nhân và cách khắc phục. Có thể chia các thành phần trên một hệ thống theo các cách sau:

- Phân tách các dịch vụ tùy theo mức độ truy cập và độ tin cậy.
- Phân tách hệ thống theo các thành phần vật lý như các máy chủ (server), router, các máy trạm (workstation)...
- Phân tách theo phạm vi cung cấp của các dịch vụ như: các dịch vụ bên trong mạng (NIS, NFS ...) và các dịch vụ bên ngoài như Web, FTP, Mail ...

2.3.2.2. Xác định nguy cơ đối với hệ thống

Các nguy cơ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộc tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn. Thông thường, một số nguy cơ này nằm ở các thành phần sau trên hệ thống:

- ***Các điểm truy nhập:***

Các điểm truy nhập của hệ thống bất kỳ (Access Points) thường đóng vai trò quan trọng đối với mỗi hệ thống vì đây là điểm đầu tiên mà người sử dụng cũng như những kẻ tấn công mạng quan tâm tới. Thông thường các điểm truy nhập thường phục vụ hầu hết người dùng trên mạng, không phụ thuộc vào quyền hạn cũng như dịch vụ mà người sử dụng dùng. Do đó, các điểm truy nhập thường là thành phần có tính bảo mật lỏng lẻo. Mặt khác, đối với nhiều hệ thống còn cho phép người sử dụng dùng các dịch vụ như Telnet, rlogin để truy nhập vào hệ thống, đây là những dịch vụ có nhiều lỗ hổng bảo mật.

- ***Không kiểm soát được cấu hình hệ thống***

Không kiểm soát hoặc mất cấu hình hệ thống chiếm một tỷ lệ lớn trong số các lỗ hổng bảo mật. Ngày nay, có một số lượng lớn các phần mềm sử dụng, yêu cầu cấu hình phức tạp và đa dạng hơn, điều này cũng dẫn đến những khó khăn để người quản trị nắm bắt được cấu hình hệ thống. Để khắc phục hiện tượng này, nhiều hãng sản xuất phần mềm đã đưa ra những cấu hình khởi tạo mặc định, trong khi đó những cấu hình này không được xem xét kỹ lưỡng trong một môi trường bảo mật. Do đó, nhiệm vụ của người quản trị là phải nắm được hoạt động của các phần mềm sử dụng, ý nghĩa của các file cấu hình quan trọng, áp dụng các biện pháp bảo vệ cấu hình như sử dụng phương thức mã hóa hashing code (MD5).

- ***Những bug phần mềm sử dụng***

Những bug phần mềm tạo nên những lỗ hổng của dịch vụ là cơ hội cho các hình thức tấn công khác nhau xâm nhập vào mạng. Do đó, người quản trị phải thường xuyên cập nhật tin tức trên các nhóm tin về bảo mật và từ nhà cung cấp phần mềm để phát hiện những lỗi của phần mềm sử dụng. Khi phát hiện có bug cần thay thế hoặc ngừng sử dụng phần mềm đó chờ nâng cấp lên phiên bản tiếp theo.

- ***Những nguy cơ trong nội bộ mạng***

Một hệ thống không những chịu tấn công từ ngoài mạng, mà có thể bị tấn công ngay từ bên trong. Có thể là vô tình hoặc cố ý, các hình thức phá hoại bên trong mạng vẫn thường xảy ra trên một số hệ thống lớn. Chủ yếu với hình thức tấn công ở bên trong mạng là kẻ tấn công có thể tiếp cận về mặt vật lý đối với các thiết bị trên hệ thống, đạt được quyền truy nhập bất hợp pháp tại ngay hệ thống đó. Ví dụ nhiều trạm làm việc có thể chiếm được quyền sử dụng nếu kẻ tấn công ngồi ngay tại các trạm làm việc đó.

2.3.2.3. Xác định phương án thực thi chính sách bảo mật

Sau khi thiết lập được một chính sách bảo mật, một hoạt động tiếp theo là lựa chọn các phương án thực thi một chính sách bảo mật. Một chính sách bảo mật là hoàn hảo khi nó có tình thực thi cao. Để đánh giá tính thực thi này,có một số tiêu chí để lựa chọn đó là:

- Tính đúng đắn
- Tính thân thiện
- Tính hiệu quả

2.3.2.4. Thiết lập các qui tắc/thủ tục

- ***Các thủ tục đối với hoạt động truy nhập bất hợp pháp***

Sử dụng một vài công cụ có thể phát hiện ra các hành động truy nhập bất hợp pháp vào một hệ thống. Các công cụ này có thể đi kèm theo hệ điều hành, hoặc từ các hãng sản xuất phần mềm thứ ba. Đây là biện pháp phổ biến nhất để theo dõi các hoạt động hệ thống.

- Các công cụ logging: hầu hết các hệ điều hành đều hỗ trợ một số lượng lớn các công cụ ghi log với nhiều thông tin bổ ích. Để phát hiện những hoạt động truy nhập bất hợp pháp, một số qui tắc khi phân tích logfile như sau:

+ So sánh các hoạt động trong logfile với các log trong quá khứ. Đối với các hoạt động thông thường, các thông tin trong logfile thường có chu kỳ giống nhau như thời điểm người sử dụng login hoặc log out, thời gian sử dụng các dịch vụ trên hệ thống...

+ Nhiều hệ thống sử dụng các thông tin trong logfile để tạo hóa đơn cho khách hàng. Có thể dựa vào các thông tin trong hóa đơn thanh toán để xem xét các truy nhập bất hợp pháp nếu thấy trong hóa đơn đó có những điểm bất thường như thời điểm truy nhập, số điện thoại lạ ...

+ Dựa vào các tiện ích như syslog để xem xét, đặc biệt là các thông báo lỗi login không hợp lệ (bad login) trong nhiều lần.

+ Dựa vào các tiện ích kèm theo hệ điều hành để theo dõi các tiến trình đang hoạt động trên hệ thống; để phát hiện những tiến trình lạ, hoặc những chương trình khởi tạo không hợp lệ ...

- Sử dụng các công cụ giám sát khác: Ví dụ sử dụng các tiện ích về mạng để theo dõi các lưu lượng, tài nguyên trên mạng để phát hiện những điểm nghi ngờ.

- ***Các thủ tục bảo vệ hệ thống***

- Thủ tục quản lý tài khoản người sử dụng.
- Thủ tục quản lý mật khẩu.

- Thủ tục quản lý cấu hình hệ thống.
- Thủ tục sao lưu và khôi phục dữ liệu.
- Thủ tục báo cáo sự cố.

2.3.2.5. Kiểm tra, đánh giá và hoàn thiện chính sách bảo mật.

Một hệ thống luôn có những biến động về cấu hình, các dịch vụ sử dụng, và ngay cả nền tảng hệ điều hành sử dụng, các thiết bị phần cứng .... do vậy người thiết lập các chính sách bảo mật mà cụ thể là các nhà quản trị hệ thống luôn luôn phải rà sóat, kiểm tra lại chính sách bảo mật đảm bảo luôn phù hợp với thực tế. Mặt khác kiểm tra và đánh giá chính sách bảo mật còn giúp cho các nhà quản lý có kế hoạch xây dựng mạng lưới hiệu quả hơn.

- *Kiểm tra, đánh giá*

Công việc này được thực hiện thường xuyên và liên tục. Kết quả của một chính sách bảo mật thể hiện rõ nét nhất trong chất lượng dịch vụ mà hệ thống đó cung cấp. Dựa vào đó có thể kiểm tra, đánh giá được chính sách bảo mật đó là hợp lý hay chưa. Ví dụ, một nhà cung cấp dịch vụ Internet có thể kiểm tra được chính sách bảo mật của mình dựa vào khả năng phản ứng của hệ thống khi bị tấn công từ bên ngoài như các hành động spam mail, DoS, truy nhập hệ thống trái phép ...

Hoạt động đánh giá một chính sách bảo mật có thể dựa vào một số tiêu chí sau:

- Tính thực thi.
- Khả năng phát hiện và ngăn ngừa các hoạt động phá hoại.
- Các công cụ hữu hiệu để hạn chế các hoạt động phá hoại hệ thống.

- *Hoàn thiện chính sách bảo mật*

Từ các hoạt động kiểm tra, đánh giá nêu trên, các nhà quản trị hệ thống có thể rút ra được những kinh nghiệm để có thể cải thiện chính sách bảo mật hữu hiệu hơn. Cải thiện chính sách có thể là những hành động nhằm đơn giản công việc người sử dụng, giảm nhẹ độ phức tạp trên hệ thống ...

Những hoạt động cải thiện chính sách bảo mật có thể diễn ra trong suốt thời gian tồn tại của hệ thống đó. Nó gắn liền với các công việc quản trị và duy trì hệ thống. Đây cũng chính là một yêu cầu trong khi xây dựng một chính sách bảo

mật, cần phải luôn luôn mềm dẻo, có những thay đổi phù hợp tùy theo điều kiện thực tế.

2.3.3. Sử dụng hệ thống firewall

2.3.3.1. Giới thiệu Firewall

Firewall là thiết bị nhằm ngăn chặn sự truy nhập không hợp lệ từ mạng ngoài vào mạng trong. Hệ thống firewall thường bao gồm cả phần cứng và phần mềm. Firewall thường được dùng theo phương thức ngăn chặn hay tạo các luật đối với các địa chỉ khác nhau.

Một FireWall bao gồm một hay nhiều thành phần sau :

+ Bộ lọc packet (packet- filtering router).

+ Cổng ứng dụng (Application-level gateway hay proxy server).

+ Cổng mạch (Circuite level gateway).

2.3.3.2. Các chức năng cơ bản của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ (Trusted Network) và Internet thông qua các chính sách truy nhập đã được thiết lập.

- Cho phép hoặc cấm các dịch vụ truy nhập từ trong ra ngoài và từ ngoài vào trong.

- Kiểm soát địa chỉ truy nhập, và dịch vụ sử dụng.

- Kiểm soát khả năng truy cập người sử dụng giữa 2 mạng.

- Kiểm soát nội dung thông tin truyền tải giữa 2 mạng.

- Ngăn ngừa khả năng tấn công từ các mạng ngoài.

Xây dựng firewalls là một biện pháp khá hữu hiệu, nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ do đó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng. Thông thường, một hệ thống firewall là một cổng (gateway) giữa mạng nội bộ giao tiếp với mạng bên ngoài và ngược lại

CHƯƠNG III

TÌM HIỂU VỀ HỆ ĐIỀU HÀNH WINDOWS SERVER 2003

3.1. Giới thiệu hệ điều hành Windows Server 2003

3.1.1. Giới thiệu hệ điều hành Windows Server 2003

Windows Server 2003 là hệ điều hành mạng, chúng ta có thể dùng Windows Server 2003 để triển khai các hệ thống Domain Controller quản trị tài nguyên và người dùng cho một công ty hay xây dựng các Web Server mạnh mẽ, tổ chức các File Server lưu trữ dữ liệu,cung cấp các dịch vụ cho người dùng …

3.1.2. Các phiên bản của họ hệ điều hành Windows Server 2003

- Windows Server 2003 Web Edition: tối ưu dành cho các máy chủ web

- Windows Server 2003 Standard Edition: bản chuẩn dành cho các doanh nghiệp, các tổ chức nhỏ đến vừa.

- Windows Server 2003 Enterprise Edition: bản nâng cao dành cho các tổ chức, các doanh nghiệp vừa đến lớn.

- Windows Server 2003 Datacenter Edittion: bản dành riêng cho các tổ chức lớn, các tập đoàn ví dụ như IBM, DELL….

3.1.3. Những điểm mới của họ hệ điều hành Windows Server 2003

- Khả năng kết chùm các Server để san sẻ tải (Network Load Balancing Clusters) cân bằng lưu lượng IP đến các nút trong một cluster.

- Hỗ trợ tốt hệ điều hành Windows XP như: Hiểu được chính sách nhóm (group policy) được thiết lập trong Windows XP, có bộ công cụ quản trị đầy đủ các tính năng chạy trên Windows XP.

- Tích hợp tính năng cơ bản của Mail Server : Đối với các công ty nhỏ không đủ chi phí mua Exchange để xây dựng Mail Server, có thể sử dụng dịch vụ POP3(Post Office Protocol) và SMTP (Simple Mail Transfer Protocol) được tích hợp sẵn trong Windows Server 2003 để làm hệ thống mail đơn giản phục vụ cho công ty.

- IPSec là một cải tiến mới cho phép các máy bên trong mạng nội bộ thực hiện các kết nối peer-to-peer đến các máy bên ngoài internet, các thông tin được truyền giữa các máy này có thể được mã hóa hoàn toàn.

- Bổ sung tính năng NetBIOS over TCP/IP cho dịch vụ RRAS (Routing and Remote Access) cho phép duyệt các máy tính trong mạng nhưng ở xa thông qua công cụ Network Neughborhood.

- Hỗ trợ công tác quản trị từ xa do Windows Server 2003 cải tiến RDP (Remote Desktop Protocol) có thể truyền trên đường truyền 40Kbps. Web admin giúp người dùng quản trị server từ xa thông qua dịch vụ web một cách trực quan và dễ dàng.

- Internet Information Services (IIS) 6.0: Để tăng an toàn cho Web server, IIS 6.0 được cấu hình cho sự bảo mật tối đa. IIS 6.0 và Windows Server 2003 cung cấp giải pháp Web server đáng tin cậy, hiệu quả, kết nối thông suốt và tích hợp nhất với sự chịu đựng lỗi, yêu cầu hàng đợi, giám sát ứng dụng, vòng lặp chu kỳ ứng dụng tự động, cất giữ (caching). IIS 6.0 cho phép bạn quản lý doanh nghiệp an toàn trên mạng.

- Internet Protocol version 6 (IPv6) : Đây là giao thức Internet phiên bản 6. IPv6 [4] là thế hệ kế tiếp của các giao thức tầng Internet của bộ giao thức TCP/IP. IPv6 giải quyết những vấn đề hiện tại của IPv4, (giao thức Internet đang sử dụng) về vấn đề thiếu hụt địa chỉ, an toàn bảo mật, tự động cấu hình, khả năng mở rộng.

- Những bổ sung cho Group Policy : Những cải tiến mới cho Group Policy (chính sách nhóm) trong Windows Server 2003 giúp người quản trị điều khiển thông qua đa số các thiết lập cấu hình mạng. Chẳng hạn, người quản trị bây giờ có thể cấu hình một số thiết lập DNS client trên các máy tính chạy Windows Server 2003 có sử dụng Group Policy. Tính năng Group Policy có thể được sử dụng để cho phép hay hạn chế sự truy cập cấu hình người dùng tới những thành phần cá nhân của giao diện người dùng mạng.

3.2. Các dịch vụ mạng của hệ điều hành Windows Server 2003

3.2.1 . Active Directory

3.2.1.1. Giới thiệu về Active Directory

Active Directory là nơi lưu trữ các thông tin về tài nguyên khác nhau trên

mạng. Các tài nguyên được Active Directory lưu trữ và theo dõi bao gồm File Server, Printer, Fax Service, Application, Data, User, Group và Web Server. Thông tin nó lưu trữ được sử dụng và truy cập các tài nguyên trên mạng. Sự khác nhau giữa Active Directory và Active Directory Service đó là các hình thức lưu trữ và quản lý thông tin tài nguyên.

Thông qua Active Directory người dùng có thể tìm chi tiết của bất kỳ một tài nguyên nào dựa trên một hay nhiều thuộc tính của nó. Vì vậy mà không cần phải nhớ tất cả đường dẫn và địa chỉ nơi tài nguyên đang được định vị, mỗi thiết bị và tài nguyên trên mạng sẽ được ánh xạ đến một tên có khả năng nhận diện đầy đủ về nó. Tên này sẽ được lưu trữ lại trong Active Directory cùng với vị trí nguyên thuỷ của tài nguyên. Người sử dụng có thể truy cập đến tài nguyên này nếu họ được phép thông qua Active Directory .

3.2.1.2. Chức năng Avtive Directory

- Chức năng chính của Avtive Directory là :

+ Lưu trữ 1 danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.

+ Cung cấp một Server đóng vai trò chứng thực (Authentication Server) hoặc Server quản lý đăng nhập (Logon Server), Server này còn được gọi là Domain Controller (máy điều khiển vùng).

+ Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (Index) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng.

+ Cho phép chúng ta tạo ra các tài khoản người dùng với những mức độ quyền khác nhau.

+ Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (Sub Domain) hay các đơn vị tổ chức OU (Organizational Unit). Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phân nhỏ.

3.2.1.3. Hệ thống Avtive Directory

- Hệ thống Active Dicrectory bao gồm cấu trúc logic và cấu trúc vật lý :

3.2.1.3.1. Cấu trúc Logic

a. Domain

Domain là phương tiện để quy định tập hợp những người dùng, máy tính, tài nguyên, chia sẻ có những quy tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các Server dễ dàng hơn. Tất cả các máy tính trong domain chia sẻ chung một cơ sở dữ liệu Active Directory.

Mục đích chính của việc tạo domain là tạo một ranh giới an toàn trong một mạng windows 2003. Người quản trị domain điều khiển các máy tính trong domain. Chỉ trừ khi được gắn quyền, nếu không thì người quản trị mạng trong domain này không thể điều khiển các domain khác. Mỗi một domain thì có các quền và các chính sách an toàn riêng, nó được thiết lập bởi người quản trị.

Domain đáp ứng 3 chức năng chính như sau:

+ Đóng vai trò như một khu vực quản trị (Administrative Boundary) các đối tượng, là tập hợp các định nghĩa quản trị cho các đối tượng chia sẻ như: có chung 1 cơ sở dữ liệu thư mục, các chính sách bảo mật, các quan hệ ủy quyền với các Domain khác.

+ Cung cấp các Server dự phòng làm chức năng điều khiển vùng (Domain Controller), đồng thời đảm bảo các thông tin trên các Server này được đồng bộ với nhau.

+ Là trung tâm của mạng Windows Server 2000 và Windows Server 2003. Các máy điều khiển vùng (Domain Controller) hoặc là PDC (Primary Domain Controller) hoặc là BDC (Backup Domain Controller), được gọi là DC. Theo mặc định, tất cả Windows Server 2003 khi cài đặt đều là Server độc lập (Stand - Alone Server).

b. Organizational unit

Là những đơn vị tổ chức. Có thể chứa các user, account, group.. Ví dụ, khi thiết kế một hệ thống thì chúng ta khảo sát hệ thống đó có bao nhiêu phòng ban, bộ phận. Dựa trên kết quả khảo sát này sẽ tạo những OU tương ứng với các phòng ban.

- Trong OU, ta sẽ tạo ra các group (có thể là gourp quản lý và group nhân viên, đều thuộc OU). Sau đó ta sẽ tạo ra các user thuộc các group tương ứng.

- Trong OU có thể chứa :

- User: là các tài khoản người dùng.

- Khi cài đặt Active Directory sẽ có một số tài khoản built-in được tạo ra như Administrator là người có toàn quyền quản trị hệ thống. Backup operator là nhóm

và người dùng có khả năng backup và restore dữ liệu của hệ thống mà không cần những quyền hạn hợp lệ đối với những dữ liệu này.

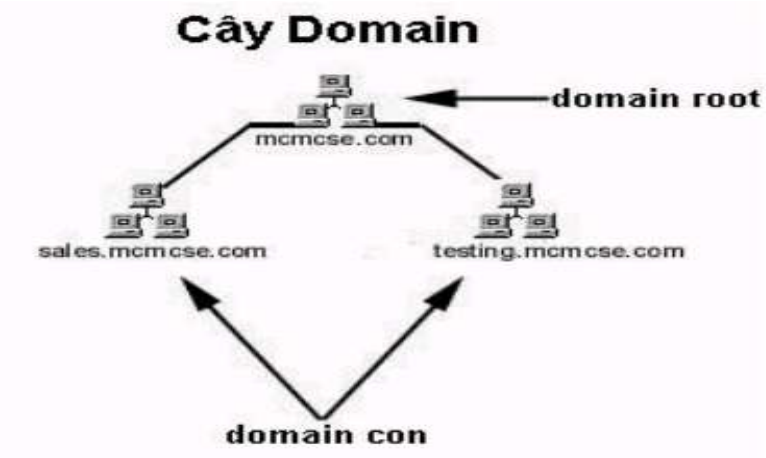
- Tuy nhiên để các nhân viên trong một tổ chức có thể sử dụng tài nguyên và đăng nhập (log-in) vào Domain thì người quản trị cần phải tạo những tài khoản hợp lệ, và cấp phát cho người sử dụng. Các user sẽ dùng những tài khoản được cấp bởi Administrator để log-in và Domain. Và truy cập dữ liệu trên file Server hay các dịch vụ khác.

- Group: là một tập hợp những người dùng có những đặc tính chung, ví dụ như các nhân viên của một phòng ban có quyền truy cập lên cùng một folder hoặc có quyền in cùng một máy in.

- Computer Account : được tạo ra để quản lý một máy tính cụ thể trong mạng.

c. Domain Tree

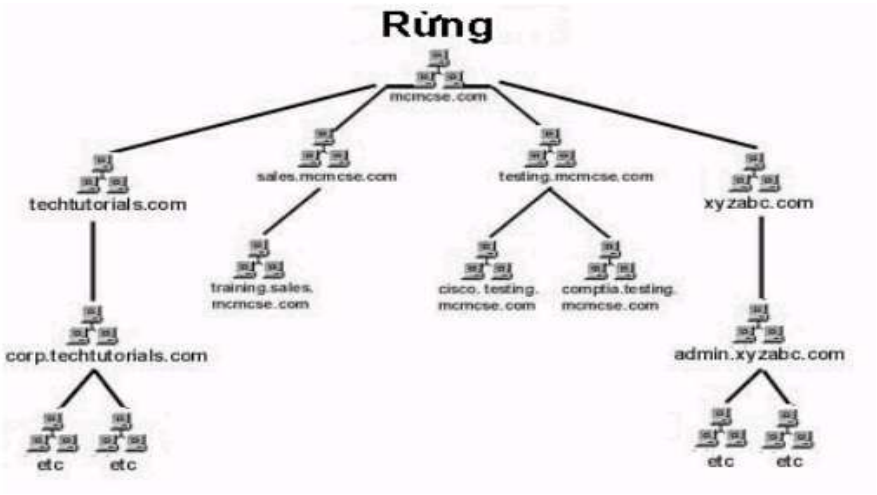
Domain Tree là cấu trúc bao gồm nhiều domain được sắp xếp có cấp bậc theo cấu trúc hình cây.Domain tạo ra đầu tiên được gọi là domain root và nằm ở gốc của cây thư mục. Tất cả các domain tạo ra sau sẽ nằm bên dưới domain root và được gọi là domain con (child domain). Tên của các domain con phải khác biệt nhau. Khi một domain root và ít nhất một domain con được tạo ra thì hình thành một cây domain.



Hinh 10: Mô hình cây domain

d. Domain Forest:

Forest (rừng) được xây dựng trên một hoặc nhiều Domain Tree, nói cách khác Forest là tập hợp các Domain Tree có thiết lập quan hệ và ủy quyền cho nhau.



Hinh 11 : Mô hình Domain Forest

3.2.1.3.2. Cấu trúc vật lý .

a. Sites.

Một site là một sự kết hợp của một hoặc nhiều các subnet IP mà nó được kết nối bởi các đường truyền tốc độ cao. Các site được định nghĩa để tạo ra sự thuận lợi đặc biệt cho chiến lược truy cập và nhân bản một Active Directory. Các mục đích chính của việc định nghĩa có thể kể ra dưới đây:

- Cho phép các kết nối tin cậy và tốc độ cao giữa các domain controller.
- Tối ưu việc truyền tải trên mạng.

Sự khác nhau cơ bản giữa site và domain đó là domain mô tả cấu trúc logic của sự tổ chức mạng trong khi đó site mô tả cấu trúc vật lý mạng. Theo trên thì cấu trúc logic và cấu trúc vật lý của Active Directory là tách rời nhau. Vì thế,

- Không cần có sự tương quan giữa cấu trúc vật lý của mạng và cấu trúc domain của nó.
- Không gian tên của site và domain không cần tương quan.
- Active Directory cho phép nhiều site trong một domain cũng giống như nhiều domain trong một site

Không gian giữa tên logic chứa các Computer, các domain và các OU, không có các site. Một site chứa thông tin về các đối tượng computer và các đối tượng connection

b. Domain Controller.

Domain controller là một máy tính chay windows 2003 server và nó chứa 1 bản sao của Active Directory. Cơ sở dữ liệu chứa các thông tin về domain cục bộ.

Có thể có nhiều hơn một domain controller trong một domain. Tất cả các domain controller trong domain đều duy trì một bản sao active directory.

Các chức năng khác nhau domain controller bao gồm :

- Duy trì một bản sao của cơ sở dữ liêu directory.
- Duy trì các thông tin của Active Directory.
- Nhân bản các thông tin được cập nhật đến các domain controller trong domain.
- Quản lý và giúp đỡ người sử dụng trong việc tìm kiếm các đối tượng trong Active Directory. Nó kiểm tra tích hợp lệ của việc logon của người sử

dụng truy cập tài nguyên được yêu cầu.

- Cung cấp khả năng chịu lỗi trong môi trường đa domain controller

3.2.1.3.3. Những công cụ quản lý Active Director.

Những công cụ quản lý Active Directory thường cung cấp ở dạng Snap-in cho MMC (Microsoft Management Console).

+ Active Directory users and Computer: quản trị người dùng, nhóm, máy tính, và đơn vị tổ chức.

+ Active Directory and Trusts: dùng làm việc với vùng, hệ vùng phân cấp, tập hợp hệ vùng phân cấp.

+ Active Directory Sites and Services : quản lý Site và mạng con.

3.2.2 . Domain Name System (DNS)

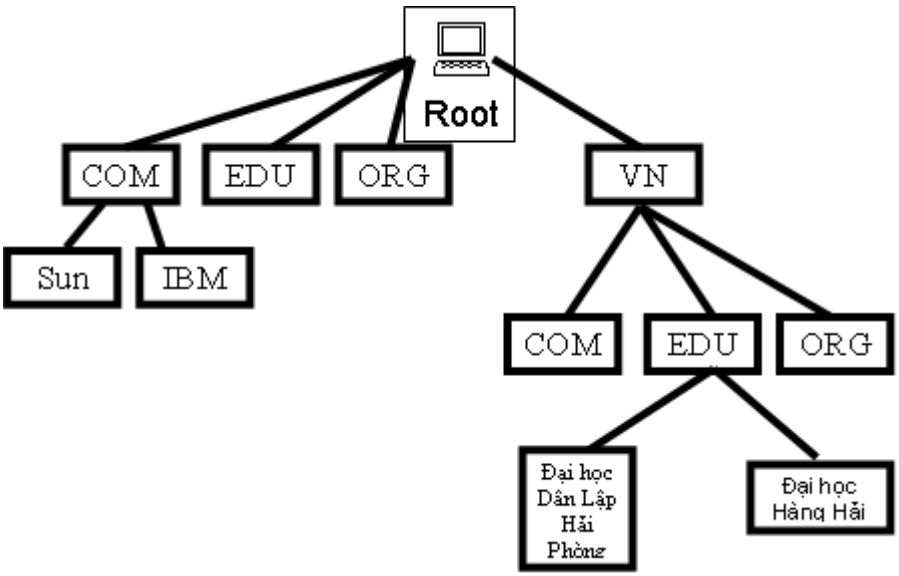
3.2.2.1. Giới thiệu về DNS

DNS là một cơ sở dữ liệu phân tán được dùng để dịch tên máy tính (host name) thành địa chỉ IP trong các mạng TCP/IP. Để cung cấp một cấu trúc phân cấp cho cơ sở dữ liệu DNS người ta cung cấp một lược đồ đánh tên được gọi là không gian tên miền. Miền gốc (root domain) là mức định của cấu trúc tên miền được ký hiệu một dấu chấm (.). Miền mức định được đặt dưới miền gốc và chúng được đại diện cho kiểu của tổ chức, chẳng hạn *com* hay *edu* hay *org* hoặc nó có thể là một định danh địa lý như *vn* (Việt nam). Các miền mức thứ 2 được đăng ký cho tên các tổ chức khác hay các người sử dụng đơn lẻ. Chúng có thể chứa cả hai: các máy tính/tài nguyên (host) và các miền con (subdomains).

Một số loại tên miền:

- *COM – Commercial : Tổ chức thương mại*
- *EDU – Educational : Tổ chức giáo dục*
- *GOV – Government : Cơ quan chính phủ*
- *MIL – Military : Nhóm quân sự*
- *NET – Network : Trung tâm thông tin mạng*
- *ORG – Organizations : Các tổ chức khác*
- *INFO – Information : Cung cấp thông tin*
- *Trong tiêu chuẩn ISO3166 quy định nếu có hai ký tự thì đây được sử*

dụng xác định tên miền thuộc quốc gia nào (vn,sg,ca,uk,jp ...)



Hình 12 : Mô hình minh họa sự phân cấp

3.2.2.2. Quản lý tên miền

Các máy tính thực hiện quản lý tên miền được gọi là DNS Server. Mỗi tên miền khi đăng ký phải được lưu trữ trên một DNS Server. Quản lý tên miền được thực hiện thông qua cơ chế phân cấp. Cấp cao nhất là các Root Server. Trên thế giới hiện nay có khoảng 13 Root Server

Phân loại DNS Server

- Primary server

Nơi xác thực thông tin về địa chỉ IP và tên miền chính thức.

- Secondart server

Nơi lưu trữ dự phòng cơ sở dữ liệu tên miền cho các Primary server

- Caching only server

Nơi lưu trữ các địa chỉ tên miền trên bộ nhớ cache nhằm tăng tốc truy vấn tên miền.

3.2.2.3. Name Resolution

Tiến trình dịch tên máy thành địa chỉ IP tương ứng được gọi là Dịch Tên.Ví dụ khi chúng ta truy cập vào website www.microsoft.com. Địa chỉ website này sẽ được DNS dịch và cung cấp địa chỉ IP tương ứng để định vị máy tính trên mạng. Máy chủ tên trong vùng có trách nhiệm dịch tên này bởi vì nó lưu trữ ánh xa tên - địa chỉ IP. Một máy chủ tên chỉ có thể xử lý truy vấn dịch tên cho vùng mà nó

được cấp quyền trên đó. Máy chủ tên lưu lại kết quả của việc dịch tên để giảm tải trên máy chủ DNS. Các máy chủ tên có thể thực hiện truy vấn sau:

3.2.2.3.1. Forward Lookup Query

Một truy vấn tìm kiếm chuyển tiếp dịch một tên để có được địa chỉ IP liên quan. Máy khách gửi một yêu cầu đến địa chỉ www.microsoft.com đến máy chủ tên địa phương.Máy chủ tên địa phương đầu tiên sẽ kiểm tra trong tập tin cơ sở dữ liệu vùng mà nó đang giữ.Nếu không tìm thấy ánh xạ tên - địa chỉ IP theo yêu cầu nó sẽ chuyển truy vấn đó đến một máy chủ tên gốc.Máy chủ tên gốc kiểm tra ánh xạ đó trong tập tin cơ sở dữ liệu vùng và gửi một tham chiếu máy chủ tên *Com*.Sau đó máy trình tên truy vấn máy chủ tên *Com* để dịch tên.Máy chủ tên *Com* trả về một tham chiếu máy chủ tên Microsoft.Sau đó Máy chủ tên cục bộ sẽ chuyển truy vấn đến máy chủ tên Microsoft và nó trả về địa chỉ IP của www.microsoft.com . Máy chủ tên cục bộ sau đó sẽ chuyển địa chỉ IP này cho máy khách để dùng nó truy cập đến www.microsoft.com.

3.2.2.3.2. Reverse Lookup Query

Tiến trình này dịch một địa chỉ IP thành tên tương ứng.. Một số chú ý với miền :

- Tên của các miền con dựa cơ sở trên địa chỉ IP
- Các octet địa chỉ IP được lưu theo thứ tự ngược lại.
- Việc quản trị của các miền con được thực hiện dựa trên cơ sở của các địa chỉ IP và địa chỉ mạng con.

3.2.3 . Dịch vụ DHCP (Dynamic Host Configuration Protocol)

DHCP tự động gán địa chỉ IP và sẽ đảm bảo việc quản lý các địa chỉ IP này. DHCP sử dụng một tiến trình tạo địa chỉ cho mướn để gán địa chỉ IP cho các máy tính khách chỉ trong một khoảng thời gian xác định. Do DHCP là một tiến trình cung cấp IP động nên các máy khách sẽ cập nhật hoặc làm mới các địa xin cấp của chúng tại các khoảng thời gian đều đặn. TCP/IP có thể được cấu hình tự động hoặc thủ công. Việc cấu hình tự động TCP/IP được thực hiện bằng cách sử dụng DHCP.

3.2.4 . Internet information services (IIS)

IIS là một ứng dụng trên Windows, nó cho phép chạy các ứng dụng như Web sites, FPT sites, và Application Pools trên nó. **IIS** 6.0 có sẵn trên tất cả các phiên của *Windows Server 2003*, IIS 6.0 trên Windows 2003 được nâng cấp từ IIS 5.0 của Windows 2000. **IIS** 6.0 cung cấp một số đặc điểm mới giúp tăng tính năng tin cậy, tính năng quản lý, tính năng bảo mật, tính năng mở rộng và tương thích với hệ thống mới.

3.2.5. FTP Server– File Transfer Protocol Server

File Transfer Protocol là một phương pháp truyền file từ hệ thống mạng máy tính này đến hệ thống mạng máy tính khác giống như ta ngồi trên mạng LAN.

3.2.6. Mail Server

Mail Server là một chương trình phần mềm dùng để quản lý các Mail client. Có hai dạng Mail Server đó là Mail Online và Mail Offline.

Mail Online: Do nhà cung cấp tự quản lý và người sử dụng chỉ cần cấu hình Mail client

Mail Offline: Người quản trị phải quản lý và tạo ra các account cho người dùng, loại mail này sử dụng phổ biến có hai loại là Mdeamon và Exchange Windows Server 2003 mặc định được tích hợp sẵn một ứng dụng quản lý Mail Server đó là dịch vụ POP3. Loại dịch vụ này sử dụng giao thức POP3 và SMTP để gửi và nhận Mail. POP3 có cổng mặc định là 110 và SMTP có cổng mặc định là 25. Người dùng mail client sẽ quản lý và sử dụng Mail client bằng chương trình Outlook Express

3.2.7. Remote access services

Windows 2003 server cho phép các client từ xa để kết nối tới server truy cập từ xa bằng cách sử dụng một số các thiết bị phần cứng modem, Integrated Services Digital Network (ISDN) adapter và Digital Subscriber Line (DSL) modem. Truy cập từ xa chạy Routing and Remote Access có khả năng hỗ trợ các giao thức khác nhau cho truyền tải dữ liệu và giao thức VPN. Một giao thức truy cập từ xa như PPP được sử dụng cho việc kết nối đến các server truy cập từ xa.

Server truy cập từ xa là một máy tính, nó đang chạy Windows 2003 và hỗ trợ RRAS. Nó xác thực các user và các phiên truy cập từ xa cho đến khi user hoàn thành phiên của người quản trị mạng. Vai trò của server truy cập từ xa là một gateway cho việc gửi dữ liệu giữa các clietn và LAN. Client gửi dữ liệu đến và nhận dữ liệu từ server truy cập từ xa. Sử dụng giao thức như TCP/IP dữ liệu được mã hoá và sau đó nó được gói trọn trong giao thức truy cập từ xa. Hai loại kết nối truy cập từ xa được cung cấp bởi Windows 2003 truy cập từ xa.

CHƯƠNG IV
TÌM HIỂU THIẾT KẾ MẠNG LAN

4.1. Các bước thiết kế mạng LAN

4.1.1. Phân tích yêu cầu

– Xác định mục tiêu sử dụng LAN: ai sử dụng LAN và yêu cầu dung lượng trao đổi dữ liệu, loại hình dịch vụ, thời gian đáp ứng,...; yêu cầu phát triển của LAN trong tương lai; xác định chủ sở hữu và quản trị LAN.

– Xác định số lượng nút mạng hiện thời và tương lai (rất lớn trên 1000 nút, vừa trên 100 nút và nhỏ dưới 10 nút). Trên cơ sở số lượng nút mạng, chúng ta có phương thức phân cấp, chọn kỹ thuật chuyển mạch, và chọn thiết bị chuyển mạch.

– Dựa vào mô hình phòng ban để phân đoạn vật lý đảm bảo hai yêu cầu an ninh và đảm bảo chất lượng dịch vụ.

– Dựa vào mô hình topo lựa chọn công nghệ đi cáp.

– Dự báo các yêu cầu mở rộng.

4.1.2. Lựa chọn phần cứng

Dựa trên các phân tích yêu cầu và kinh phí dự kiến cho việc triển khai, chúng ta sẽ lựa chọn nhà cung cấp thiết bị tốt nhất như là Cisco, Nortel, 3COM, Intel ... Các công nghệ có khả năng mở rộng. Phần cứng chia làm 3 phần: hạ tầng kết nối (hệ thống cáp), các thiết bị kết nối (hub, switch, bridge, router), các thiết bị xử lý (các loại server, các loại máy in, các thiết bị lưu trữ,..)

4.1.3. Lựa chọn phần mềm

- Lựa chọn hệ điều hành Unix (AIX, OSF, HP, Solaris, ...), Linux , Windows dựa trên yêu cầu về xử lý số lượng giao dịch, đáp ứng thời gian thực, kinh phí, an ninh an toàn.

- Lựa chọn các công cụ phát triển phần mềm ứng dụng như các phần mềm quản trị cơ sở dữ liệu (Oracle, Informix, SQL, Lotusnote, ...), các phần mềm portal như Websphere, ...

- Lựa chọn các phần mềm mạng như thư điện tử (Sendmail, PostOffice, Netscape, ...), Web server (Apache, IIS, ...),

- Lựa chọn các phần mềm đảm bảo an ninh an toàn mạng như phần mềm tường lửa (PIX, Checkpoint, Netfilter, ...), phần mềm chống virut (VirusWall, NAV, ...), phần mềm chống đột nhập và phần mềm quét lỗ hổng an ninh trên mạng.

- Lựa chọn các phần mềm quản lý và quản trị mạng.

4.1.4. Đánh giá khả năng

- Dựa vào thông tin đã được xác minh của các hãng có uy tín trên thế giới.

- Thực hiện thử nghiệm và kiểm tra trong phòng thí nghiệm của các chuyên gia.

- Đánh giá trên mô hình thử nghiệm.

4.1.5. Tính toán giá thành

Giá thành thấp đảm bảo các chỉ tiêu kỹ thuật, các yêu cầu của ứng dụng, tính khả mở của hệ thống.

4.1.6. Triển khai pilot

Triển khai ở quy mô nhỏ nhưng vẫn minh họa được toàn bộ các yêu cầu về kỹ thuật, yêu cầu về ứng dụng làm cơ sở cho việc đánh giá khả năng và giá thành của mạng trước khi triển khai trên diện rộng.

4.2. Các vấn đề cần lưu ý

Khi thiết kế một hệ thống LAN ta cần chú ý những hạng mục cần thực sau đây, giúp cho việc định hướng đúng tác thiết kế xây dựng 1 hệ thống mạng LAN.

- Chi phí tổng thể cho việc đầu tư trang thiết bị cho toàn hệ thống.
- Những yêu cầu thật cần thiết cho hệ thống mạng tại thời điểm xây dựng và những kế hoạch mở rộng hệ thống trong tương lai.
- Khảo sát hiện trạng địa hình, địa lý, cách bố trí phòng ban.
- Cân nhắc áp dụng kiểu kiến trúc, công nghệ mạng thực sự cần thiết trong thời gian hiện tại và tương lai.
- Khảo sát và lựa chọn ISP hội tụ những điều kiện tốt nhất cho mạng LAN

của mình.

- Lên kế hoạch tiến độ thi công, thực hiện toàn bộ công trình.
- Lập kế hoạch sử dụng tài chính.
- Lập kế hoạch chuẩn bị nhân lực.
- Lập bảng thống kê chi tiết cho việc triển khai đầu tư trang thiết bị.
- Mô hình hóa hệ thống mạng bằng phần mềm Visio.

Triển khai công trình, quyết tâm thực hiện cho bằng được kế hoạch đưa ra với thời gian sớm nhất.

4.3. Những yêu cầu chung của việc thiết kế mạng

Một hệ thống mạng LAN sau khi thiết kế xong phải thỏa mãn các điều kiện sau đây:

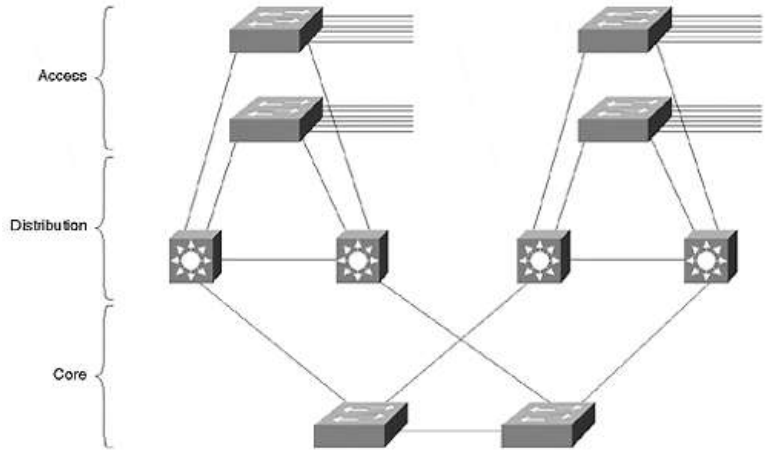
- Phải đảm bảo các máy tính trong công ty trao đổi dữ liệu được với nhau.
- Chia sẻ được máy in, máy Fax, ổ CD-ROM…
- Tổ chức phân quyền truy cập theo từng người dùng.
- Cho phép các nhân viên đi công tác có thể truy cập vào công ty.
- Tổ chức hệ thống Mail nội bộ và Internet.
- Tổ chức Web nội bộ và Internet.
- Cài đặt các chương trình ứng dụng phục vụ cho công việc của các nhân viên.
- Ngoài ra hệ thống mạng còn cung cấp các dịch vụ khác.

4.4. Mô hình cơ bản.

4.4.1. Hierarchical models

Đây là mô hình phân cấp gồm các lớp sau:

- Lớp lõi (Core Layer): Đây là trục xương sống của mạng(backbone) thường dùng các bộ chuyển mạch có tốc độ cao(high-speed switching), thường có các đặc tính như độ tin cậy cao, có công suất dư thừa, có khả năng tự khắc phục lỗi, có khả năng thích nghi cao, đáp ứng nhanh, dễ quản lý, có khả năng lọc gói, hay lọc các tiến trình đang truyền trong mạng.



Hinh 12 : Mô hình phân cấp

- Lớp phân tán (Distribution Layer) : Là ranh giới giữa lớp truy nhập và lớp lõi của mạng. lớp phân tán thực hiện các chức năng như đảm bảo gửi dữ liệu đến từng phân đoạn mạng, đảm bảo an ninh-an toàn, phân đoạn mạng theo nhóm công tác, chia miền Broadcast/multicast, định tuyến giữa các LAN ảo (VLAN), chuyển môi trường truyền dẫn, định tuyến giữa các miền, tạo biên giới giữa các miền trong định tuyến tĩnh và động, thực hiện các bộ lọc gói(theo địa chỉ, theo số hiệu cổng,...), thực hiện các cơ chế đảm bảo chất lượng dịch vụ QoS.
- Lớp truy nhập(Access Layer) Lớp truy nhập cung cấp các khả năng truy nhập cho người dùng cục bộ hay từ xa truy nhập vào mạng. Thường được thực hiện bằng các bộ chuyển mạch(switch) trong môi trường campus, hay các công nghệ WAN.

Đánh giá mô hình

- Giá thành thấp
- Dễ cài đặt
- Dễ mở rộng
- Dễ cô lập lỗi.

4.4.2. Secure models.

4.4.2.1 Giới thiệu mô hình an ninh an toàn

An ninh – an toàn mạng dùng riêng, hay mạng nội bộ là giữ không cho ai làm cái mà mạng nội bộ đó không muốn cho làm.

Khi kết nối LAN phải triển khai cơ chế nào để thực hiện yêu cầu an ninh an toàn. Chúng ta gọi đó là an ninh an toàn mạng.

Tài nguyên mà chúng ta muốn bảo vệ là gì?

• Là các dịch vụ mà mạng đang triển khai

• Là các thông tin quan trọng mà mạng đó đang lưu giữ, hay cần lưu chuyển .

• Là các tài nguyên phần cứng và phần mềm mà hệ thống mạng đó có để cung ứng cho những người dùng mà nó cho phép.

4.4.2.2. Các bước xây dựng

- Xác định cần bảo vệ cái gì?
- Xác định bảo vệ khỏi những loại tấn công nào ?
- Xác định những mối đe doạ an ninh có thể ?
- Xác định các công cụ để đảm bảo an ninh ?
- Xây dựng mô hình an ninh – an toàn.

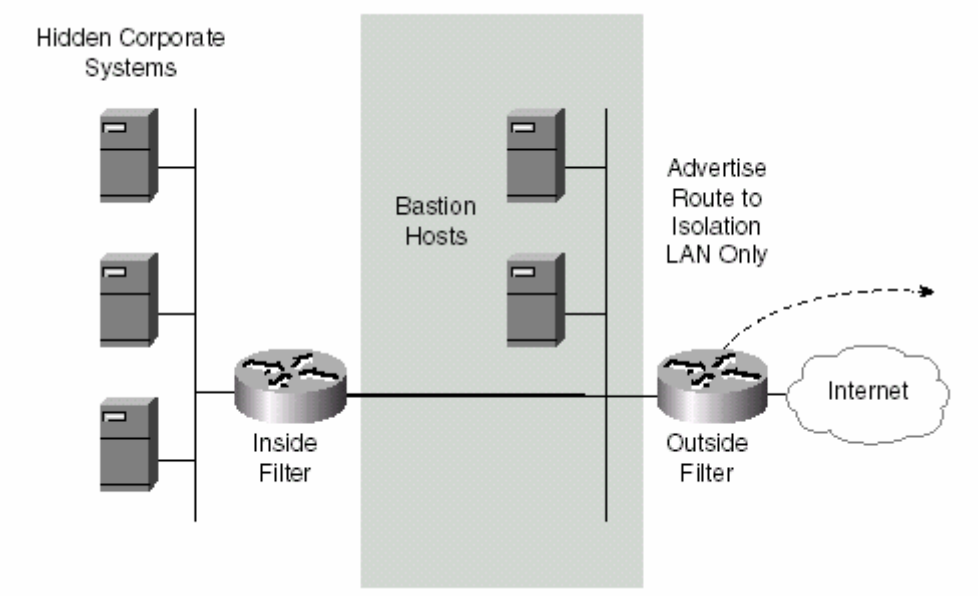
Mục đích của việc xây dụng mô hình an ninh – an toàn khi kết nối LAN là xây dựng các phương án để triển khai vấn đề an ninh – an toàn khi kết nối và đưa LAN vào hoạt động.

Đầu tiên mục đích và yêu cầu về vấn đề an ninh – an toàn hệ thống ứng dụng phải được vạch ra rõ ràng. Chẳng hạn mục tiêu và yêu cầu an ninh – an toàn khi kết nối LAN cho các cơ quan hành chính nhà nước sẽ khác với việc kết nối LAN cho các trường đại học.

Thứ hai, mô hình an ninh – an toàn phải phù hợp với các chính sách, nguyên tặc và luật lệ hiện hành.

Thứ ba, phải giải quyết cá vấn đề liên quan đến an ninh – an toàn một cách toàn cục. Có nghĩa là phải đảm bảo cả về phương tiện kỹ thuật và con người triển khai.

4.4.2.3. Three-Part Firewall System



Hình 13: Mô hình tường lửa 3 phần

– LAN cô lập làm vùng đệm giữa mạng công tác với mạng bên ngoài (LAN cô lập được gọi là khu phi quân sự hay vùng DMZ).

– Thiết bị định tuyến trong có cài đặt bộ lọc gói được đặt giữa DMZ và mạng công tác.

– Thiết bị định tuyến ngoài có cài đặt bộ lọc gói được đặt giữa DMZ và mạng ngoài.

4.5. Mô phỏng thiết lập mạng LAN

4.5.1. Yêu cầu công ty

Em giả sử thiết lập hệ thống mạng của công ty có 3 tầng với 5 phòng ban. Công ty có gồm 32 máy Client được phân phối cho 5 phòng ban như sau:

Phòng Tài Chính – Kế Toán	10 máy Client
Phòng Kinh Doanh	10 máy Client
Phòng Kỹ Thuật	10 máy Client
Phòng Giám Đốc	1 máy Client
Phòng Phó Giám Đốc	1 máy Client

Công ty có yêu cầu như sau: Hê thống mạng được chia thành các nhóm sử dụng tương ứng với mỗi phòng ban, có chia sẻ dữ liệu và dùng chung thiết bị như máy photo, máy fax….. Các user được phân quyền phù hợp với công việc của mình.

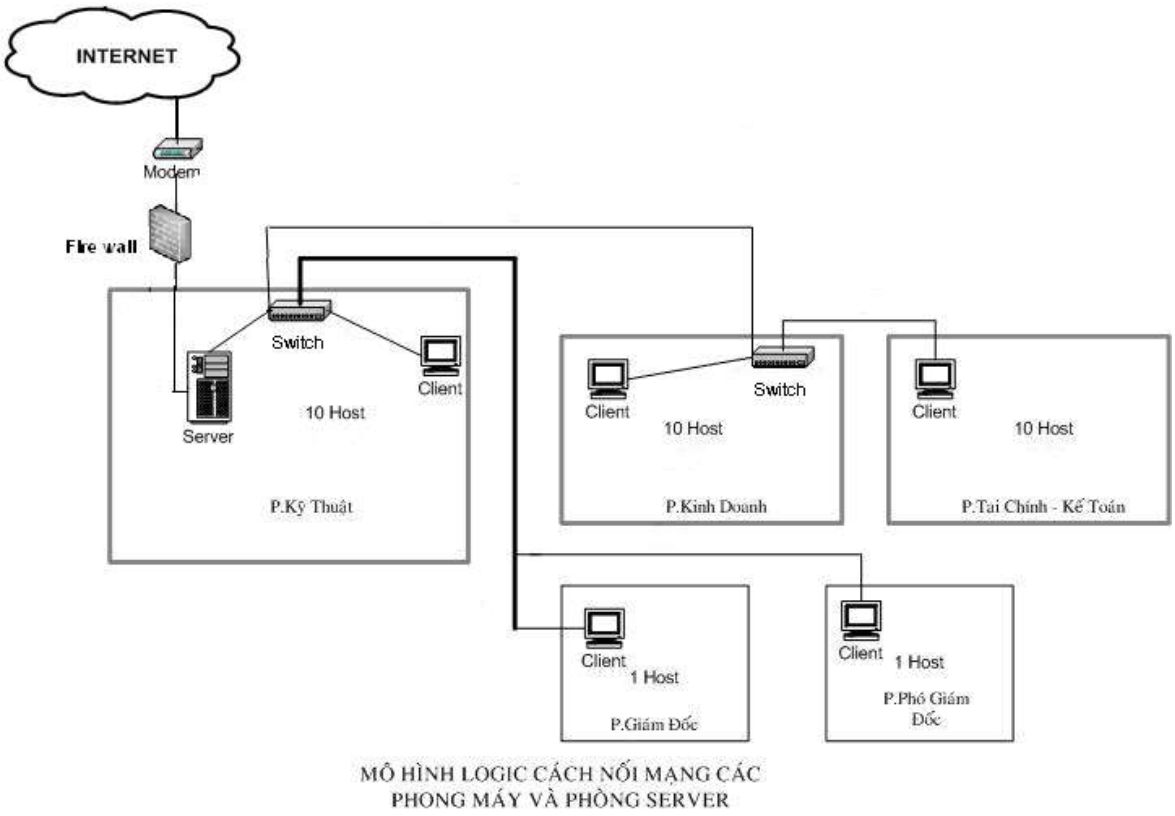
Mạng có kết nối với internet.

4.5.2. Phân tích yêu cầu

- Vì công ty có nhu cầu chia sẻ dữ liệu và dung chung thiết bị và có chính sách quản lý người dùng nên cần có 1 máy server để quản lý.
- Mạng máy tính trên là LAN Campus Network. (Mạng Campus là mạng có nhiều LAN trong một hoặc nhiều tòa nhà).
- Vì là mạng Campus nên mạng này sẽ được xây dựng trên nền tảng công nghệ cao Ethernet / Fast Etherner / Gigabit Ethernet.
- Mạng cần có độ ổn định và khả năng dự phòng để đảm bảo chất lượng cho việc truy cập các dữ liệu quan trọng.
- Mạng của công ty được chia thành các nhóm sử dụng và được phân quyền sử dụng các dữ liệu và chương trình và mạng có kết nối interner nên hệ thống mạng cần có tường lửa để đảm bảo an ninh cho toàn bộ thiết bị nội bộ trước các truy cập trái phép và hạn chế sử dụng internet. Như hạn chế quyền chat, hạn chế quyền sử dụng một số trang web….
- Mạng này cần được cấu thành bởi các switch để hạn chế xung đột dữ liệu truyền tải.

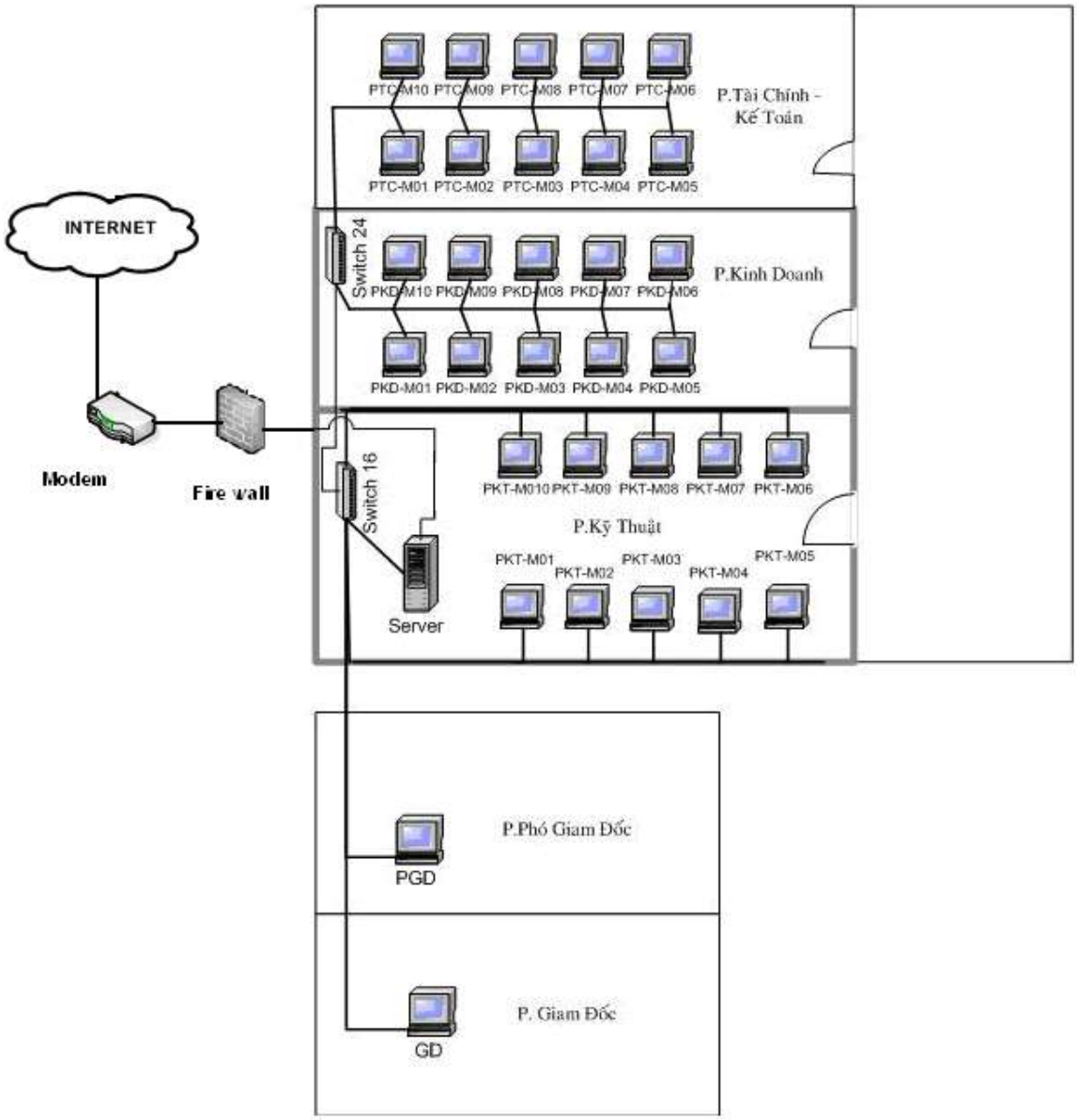
4.5.3. Thiết kế sơ đồ mạng

4.5.3.1. Sơ đồ Logic các phòng máy



Hinh 14 : Sơ đồ Logic các phòng máy

4.5.3.2. Sơ đồ vật lý



Hinh 15 : Sơ đồ vật lý cá phòng máy

4.5.3.3. Giải thích mô hình

Trong cấu hình vẽ mạng máy tính cục bộ toà nhà điều hành có 1 switch phân phối có chức năng định tuyến. Switch này có tác dụng chuyển lưu lượng qua lại giữa các switch truy cập và một nhiệm vụ rất quan trọng là định tuyến giữa các LAN ảo. Bất kỳ một switch truy cập nào được kết nối đến switch phân phối đều đảm bảo cung cấp băng thông cho toàn bộ các máy tính kết nối đến switch truy cập. Switch phân phối sử dụng ở đây là thiết bị có nhiều cổng truy nhập 100Mbps . Các switch truy cập cung cấp 24 cổng 10/100 Mbps đảm bảo băng thông này cho từng máy trạm**.**

Nếu số lượng máy tính trong toàn bộ toàn nhà phát triển lên, các switch truy cập có thể cắm xếp trồng để cung cấp số lượng cổng truy cập nhiều hơn hoặc các phòng ban có thể cắm switch mở rộng để cung cấp thêm số cổng truy nhập.

Phòng kinh doanh và phòng kế toán ta sử dụng chung switch. Phòng kỹ thuật và phòng giám đốc ta sử dụng chung switch.

Switch chính từ phòng kỹ thuật ta kết nối với phân mạng truy cập Internet thông qua Firewall. Firewall sẽ làm nhiệm vụ ngăn chặn và bảo mật các máy tính thuộc phân mạng nội bộ với mạng Internet phía bên ngoài. Như vậy một giao tiếp mạng của firewall sẽ kết nối với phân mạng bên trong và 1 giao tiếp mạng sẽ kết nối với phân mạng Internet công cộng.

4.5.4. Lựa chọn giải pháp

Tùy thuộc vào nhu cầu sử dụng, tầm quan trọng dữ liệu mà mỗi công ty có những yêu cầu chính sách bảo mật khác nhau. Với mô hình và yêu cầu của công ty trên thì em lựa chon những giải pháp sau:

4.5.4.1 . Lựa chọn mô hình mạng

Công ty là một doanh nghiệp thuộc loại vừa và nhỏ, hệ thống mạng gồm 1 server và 32 máy Client nên em chọn giải pháp là mạng LAN với mô hình là Start. Nghĩa là có một phòng đặt các thiết bị trung tâm từ đó dẫn dây đến các phòng còn lại và thuộc loại mô hình Client/Server thường được dùng trong các doanh nghiệp công ty.

4.5.4.2. Lựa chọn hệ điều hành mạng

Nhằm quản lý tốt và tăng cường hệ thống bảo mật dữ liệu cho công ty thì em lựa chọn hệ điều hành : Window Server 2003 Standar Edition, đây là ban chuẩn dung cho doanh nghiệp vừa va nhỏ. Nếu dùng hệ điều hành này thì ngoài những tính năng của Window XP có nó còn có thêm tính năng bảo mật và phân chia quền truy cập chia sẻ tài nguyên cho các máy con khác tốt hơn.

4.5.4.3. Lựa chọn thiết bị mạng

Switch : 1 Switch 24 port và 1 Switch 16 port

Cáp: Em lựa chọn cáp STP CAT5 (thích hợp cho đường truyền 100 Mb/s). Vì loại cáp này có lớp bọc kim loại tác dụng chống nhiễu điện từ.

Đầu nối cáp: sử dụng đầu nối RJ-45

Để kết nối với Internet cần phải có Firewall. Firewall sẽ làm nhiệm vụ ngăn chặn và bảo mật các máy tính thuộc phân mạng nội bộ với mạng Internet từ phía bên ngoài.

Máy tính:

Máy Server: Chạy hệ điều hành Microsoft Windows 2003 Server và cài các dịch vụ phục vụ cho các máy Client như : MS ISA Server…

Máy Client : Chạy hệ điều hành Microsoft Windows XP professional. Chạy các chương trình ứng dụng như : Microsoft Office XP , các phần mềm kế toán , nhân sự …

4.5.5. Đánh giá mô hình

Ưu điểm:

- Dữ liệu được bảo mật an toàn do sử dụng hệ điều hành Windows Server 2003 , dễ backup và diệt virus. Chi phí cho các thiết bị thấp.
- Trong mô hình công ty này thì do lắp đặt mô hình mạng Client/ Server nên có một hệ thống máy chủ sẽ quản lý tất cả các tài nguyên hệ thống và chịu trách nhiệm phân chia quyền sử dụng tài nguyên hệ thống cho các máy con. Mỗi máy con sau khi được hệ thống máy chủ phân quyền sử dụng tài nguyên thì có : Username và Passwword để đăng nhập hệ thống, việc phân quyền này giúp tăng thêm tính năng bảo mật cho hệ thống cơ sở dữ liệu cho công ty hơn.
- Dùng ít cáp, dễ lắp đặt.
- Việc quản trị dễ dàng (do mạng thiết kế theo mô hình xử lý tập trung và được phân chia quyền sử dụng hệ thống).
- Sử dụng Switch (không sử dụng hub) vì Switch có khả năng mở rộng mạng tối ưu hơn Hub ,tốc độ truyền dữ liệu nhanh…Ngoài ra Switch còn hỗ trợ Trunking,VLAN…
- Dùng cáp STP không dùng UTP vì STP chống nhiễu, tốc độ truyền tín hiệu nhanh, không bị nghe trộm.
- Hệ thống có phân tách các phòng ban thành các mạng con riêng để giảm thiểu việc truy xuất dữ liệu trái phép trong nội bộ công ty.

Tồn tại:

- Khó khăn trong việc cài đặt thêm các phần mềm cho client .
- Máy server phải cài nhiều dịch vụ cung cấp cho các máy client.
- Phụ thuộc nhiều vào tốc độ Server.
- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm .
- Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động
- Khó đáp ứng được yêu cầu của nhiều ứng dụng khác nhau.
- Tốc độ truy xuất không nhanh.

CHƯƠNG V
ĐỀ XUẤT PHƯƠNG ÁN BẢO MẬT MẠNG

5.1. Đánh giá hệ điều hành Windows Server 2003

Cũng như các hệ điều hành khác Windows Server 2003 cũng có những ưu, khuyết điểm của nó, tuy nhiên Windows Server 2003 chinh phục được nhiều người dùng bởi những tính năng nổi trội. Hệ điều hành này cho phép tổ chức quản lý một cách chủ động theo nhiều mô hình khác nhau: peer-to-peer, clien/server. Nó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (start), đường thẳng (bus), vòng (ring) và phức hợp. Nó có một số đặc tính ưu việt bảo đảm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows Server 2003 đáp ứng được hầu hết các giao thức phổ biến nhất trên mạng và cũng hỗ trợ được rất nhiều những dịch vụ truyền thông trên mạng. Nó vừa đáp ứng được cho mạng cục bộ (LAN) và cho cả mạng diện rộng (WAN). Windows Server 2003 cho phép dùng giao thức TCP/IP, vốn là một giao thức được sử dụng rất phổ biến trên hầu hết các mạng diện rộng và trên Internet. Windows Server 2003 là hệ điều hành hướng đối tượng, và hệ bảo mật của nó được xây dựng ngay trong cấp thấp nhất của cấu trúc đối tượng. Chính vì thế Window Server dễ bảo vệ an toàn hơn so với hầu hết mọi hệ điều hành khác. Tuy nhiên đây là hệ điều hành khá phức tạp và chế đô bảo mật của nó không thể cung cấp cho ta một giải pháp bảo mật tuyệt đối. Vì vậy những nhà quản trị mạng phải quan tâm khi thực hiện các công tác quản trị và bảo trì hệ thống. Bạn cần phải có một cấp bảo mật phù hợp với nhu cầu của mình và tích hợp những phần mềm bổ trợ vào mô hình của bạn. Các kế hoạch bảo mật gồm cả biện pháp an ninh vật lý. Để xây dựng hệ thống mạng vững chắc không chỉ có ngăn ngừa kể tấn công ngoài mạng mà còn cả trong nội bộ của bạn nữa.

5.2. Chiến lược bảo mật

Để đảm bảo an toàn thông tin, mọi tổ chức cần phải xây dựng một chính sách thông tin. Quá trình xây dựng một chính sách thông tin giống như một vòng tròn trong đó mỗi lần quay trở lại điểm khởi đầu là một lần làm tăng độ an toàn. Việc đầu tiên trong việc phát triển chính sách thông tin là tạo một danh sách các nguồn

lực cần được bảo vệ nghĩa là không chỉ bao gồm máy tính, máy in, bộ chỉ đường, tường lửa mà còn những nơi cần đặt phần cứng và các thiết bị Backup khác. Cần phải xác định rõ những ai được phép xâm nhập vào phần cứng và cấu trúc lô gic của phần mềm máy tính. Sau khi lập danh sách thống kê các nguồn lực ta cần thiết lập một catalo về các mối nguy hiểm đe doạ tới mỗi nguồn lực đó. Sau đó ta mới tiến hành việc phân tích các điểm yếu để tìm ra những phần hay bị đe doạ nhất.

5.3. Bảo mật thông qua hạn chế thông tin

Rất nhiều nơi rất hạn chế trong việc đưa ra thông tin về bảo mật hệ thống mạng. Một số nơi thì cố gắng dấu thông tin ở trên server của họ và chỉ cho phép một số ít người có thẩm quyền được truy cập. Việc bảo mật thông qua hạn chế thông tin là chiến lược đối với rất nhiều nơi. Bằng việc hạn chế thông tin các nhà quản trị mạng còn hy vọng rằng không ai phát hiện được điểm yếu của họ để mà khai thác chúng.

Các phần mềm bảo mật tốt nhất hiện nay đều sử dụng những thuật toán sẵn có nên Hacker có thể tìm ra cách làm việc của các thuật toán hoặc sử dụng các phần mềm trung gian để xem mã và cách thức bảo mật. Điều này buộc các nhà phát triển phần mềm phải luôn phát triển thuật toán, cung cấp các thuật toán mã hoá mạnh.

5.4. Bảo mật phân quyền tài khoản

Để thực hiện một tác vụ thành công trên LAN cần một số yếu tố về bảo mật như:

Cần xác định xem ai là người có quyền truy xuất thông tin , ở nhiều nơi không có danh sách rõ ràng về người có quyền truy xuất thông tin. Danh sách thẩm quyền này thường bao gồm thông tin về quyền mà từng người được cấp để thực hiện tác vụ. Để thiết lập danh sách này cần phải xây dựng và xác lập một tập hợp các quyền được cấp cho những người sử dụng. Danh sách thẩm quyền giúp tránh cho việc truy xuất và sử dụng dịch vụ mà không được phân quyền. Bằng cách sử dụng các quy luật ràng buộc nó cho phép người sử dụng được phép hoặc không được phép sử dụng căn cứ trên độ tin cậy của họ. Hầu như mọi trình ứng dụng đều có cách thức cấp quyền của nó . Do có ngày càng nhiều các chương trình ứng dụng được tải trên LAN, việc thực hiện phân quyền sẽ hạn chế hơn lỗ hổng trong bảo mật.

Danh sách quyền phải được duy trì đối với mỗi nguồn lực như máy in, file dữ liệu, CSDL hay trình ứng dụng và nhóm người sử dụng dịch vụ, những người có quyền truy xuất đối với các đối tượng đặc biệt này. Do vây người quản trị cần chú ý những vấn đề sau:

- Cung cấp tài khoản cho người dùng với mưc phân quyền hợp lý.
- Tài khoản người dùng là chủ đề biến tấu trung tâm của hệ điều hành windows server 2003. Những ai muốn truy cập vào một máy tính đều phải gõ đúng tên người dùng và mật khẩu.
- Không nên để lộ mật khẩu cho bất kỳ ai. Không tạo một mật khẩu (password) dễ dàng. Không dùng một hoặc hai password khi bạn đăng ký làm thành viên với nhiều địa chỉ (site) khác nhau. Không dùng những từ dễ đoán ra, hãy kết hợp các chữ cái, các biểu tượng và con số với nhau, và nhớ phải tạo password dài hơn 7 ký tự. Không nên dùng ngày sinh, tên người yêu, con cái... hoặc đơn giản như ABCD1234. Hãy ghi nhớ password của mình nhưng không nên lưu trên máy tính. Không nên dùng chức năng nhớ password và hãy chịu khó nhập password mỗi lần đăng nhập.
- Cần đặt ra các quy định nhưng phải tránh không gây khó khăn cho nhân viên, nhất là phải tạo điều kiện cho họ thực hiện công việc một cách tốt nhất.
- Cho phép người dùng truy cập mở vào web, nhưng hạn chế truy cập vào những trang mạng xã hội trong giờ làm việc. Nếu có truy cập thì không được tiết lộ địa chỉ, mật khẩu, hay bất cứ thông tin khách hàng nào cho các nguồn không quen biết.
- Đổi tên tài khoản Administrator và dung một mật hiệu khó đoán. Vì kẻ tấn công chỉ có thể vào hệ thống thông qua tài khoản Administrator. Làm như vậy để kẻ tấn công khó có thể đoán được tên tài khoản Admin**.**
- Ẩn định khóa chặn trên các tài khoản user.
- Khi đã thay đổi tên tài khoản Administrator ta có thể tạo 1 tài khoản Administrator giả và không có quyền nào cả. Kẻ tấn công sẽ mất nhiều thời gian vào tài khoản đó.
- Các điều hành viên nên có 2 tài khoản. Một tài khoản thường để sử dụng khi không thực hiện công việc điều hành.

- Che giấu tên người dùng.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System tìm đến khóa **DontDisplayLockedUserId** đổi giá trị là 1.

- Đặt lại đường dẫn cho AD Database.
- Kiểm tra các log file từ các máy chủ và các ứng dụng. Chúng sẽ cung cấp cho ta một số thông tin tốt nhất về hệ thống, các tấn công bảo mật. Trong rất nhiều trường hợp, đó chính là một trong những cách để xác nhận quy mô của một tấn công vào máy chủ.

5.5. Firewall

Mạng LAN có nhiều Server, do đó khả năng bảo mật cũng cần được chú trọng, có nhiều cách bảo mật nhưng thông dụng nhất là tường lửa. Tường lửa là một hệ thống giúp bảo vệ an toàn của mạng bằng cách thực hiện điều khiển xử lý, nhằm kiểm soát khả năng của người sử dụng trong việc truy xuất các nguồn lực giữa mạng này với mạng khác. Các nhà quản trị hệ thống là người cần xác định mức bảo mật cần thiết cho các nguồn lực của mạng. Tường lửa được thiết kế nhằm tránh việc truy xuất tự do các nguồn lực của mạng thông qua kết nối LAN việc điều khiển này sẽ giúp bảo vệ an toàn dữ liệu và phần mềm. Tường lửa sẽ giúp chống lại những kẻ phá hoại và Hacker.

Khi hệ thống được kết nối LAN và thực hiện trao đổi dịch vụ, để bảo vệ những dịch vụ này tường lửa có thể từ chối những yêu cầu từ những máy tính khác thiếu tin cậy. Để bảo vệ những dịch vụ này có một vài cách được áp dụng đó là sử dụng Proxy nhằm đảm bảo cho sự an toàn của dữ liệu truyền do không kết nối trực tiếp đến mạng nội bộ. Đây là cách bảo mật khá tốt nhưng dữ liệu không được cập nhật kịp thời. Một cách nữa là sử dụng tường lửa đa tầng. Tường lửa giữ vai trò trung tâm trong bảo mật hệ thống. Nó giúp cho người sử dụng truy xuất các nguồn lực qua LAN mà không cần phải lo ngại về sự an toàn khi kết nối. Khi kết nối với LAN mạng thành phần sẽ được xử lý như một máy cá nhân thông qua sử dụng Proxy.

Các tường lửa phức tạp đều sử dụng cấu trúc đa tầng. Tường lửa phía ngoài được thiết lập danh giới vùng (DMZ-Demiliteried Zone) và một tường lửa phía trong dùng để bảo vệ mạng. Trong vùng đã được xác định các Web Server, các FTP Server và các Main Getway được thiết lập. Mọi dữ liệu gửi ra ngoài mạng sẽ phải

xuyên qua tường lửa. Xây dựng nhiều mức là một giải pháp tốt bổ xung thêm chức năng mà không làm giảm khả năng bảo mật.

5.6. Hệ thống kiểm tra xâm nhập mạng (IDS)

Một IDS, không liên quan tới các công việc điều khiển hướng đi của các gói tin, mà nó chỉ có nhiệm vụ phân tích các gói tin mà firewall cho phép đi qua, tìm kiếm các chữ kí tấn công đã biết (các chữ kí tấn công chính là các đoạn mã được biết mang tính nguy hiểm cho hệ thống) mà không thể kiểm tra hay ngăn chặn bởi firewall. IDS tương ứng với việc bảo vệ đằng sau của firewall, cung cấp việc chứng thực thông tin cần thiết để đảm bảo chắc chắn cho firewall hoạt động hiệu quả.

5.7. Sử dụng thêm phần mềm.

5.7.1. Phần mềm Anti-Virus (AV)

Phần mềm AV nên được cài trên toàn bộ máy trạm (workstation), máy chủ (server), hệ thống hỗ trợ dịch vụ số, và hầu hết những nơi chứa dữ liệu quan trọng vào ra. Hai vấn đề quan trọng nhất để xem xét khi đặt yêu cầu một nhà sản xuất AV quản lý nhiều máy chủ và máy trạm trên toàn bộ phạm vi của công ty là khả năng nhà cung cấp đó có đối phó được các đe doạ từ virus mới hay không. (nguyên nhân: không bao giờ cho rằng phầm mềm đang chạy, luôn kiểm tả phiên bản của virus và các file cập nhật cho virus mới).

5.7.2. HP Openview

HP OpenView là họ các phần mềm quản trị các tài nguyên công nghệ thông tin từ cơ sở hạ tầng, dịch vụ, phần mềm ứng dụng cho đến các khách hàng, thuê bao của hệ thống. Ưu điểm nổi bật của HP OpenView là một giải pháp quản trị tổng thể với đầy đủ mọi tính năng cần thiết để quản trị một hệ thống thông tin phức tạp bao gồm cả phần cứng, hệ điều hành và các trình ứng dụng, cho phép các sản phẩm có thể tích hợp chặt chẽ với nhau, tạo ra một giải pháp thống nhất trong toàn bộ hệ thống. Khả năng tích hợp của nó không chỉ thể hiện giữa các sản phẩm trong cùng họ HP OpenView mà nó còn có thể tích hợp với các giải pháp quản trị chuyên biệt đối với các sản phẩm phần cứng/phần của các hãng khác nhau như CiscoWorks, Compaq Insight Manager, SUN Management Center, HP TopTools, Oracle Enterprise Manager.

Khi mạng có sự cố HP Openview giúp bạn nhanh chóng biết được lỗi đã xảy ra ở đâu bằng cách chỉ cho bạn thấy tận gốc của vấn đề chi tiết đến từng sự kiện, điều này giúp bạn khắc phục được các lỗi khó và nặng nhất. HP Openview cũng giúp bạn chọn lọc và lập báo cáo về các vấn đề mấu chốt của mạng từ đó bạn có thể vạch ra kế hoạch vận hành mạng 1 cách trơn tru nhất.

Tuy nhiên HP Openview có giá rất cao, nó chỉ thích hợp cho khách hàng có các hệ thống lớn, phức tạp.

5.7.3. Cisco Secure ACS

Cisco Secure ACS là một phần mềm ứng dụng bảo mật mạng cho phép ta điều khiển cách truy cập mạng, các cuộc gọi vào, và truy cập Internet. Cisco Secure ACS chạy trên nền Windows hoạt động giống như một dịch vụ của Windows NT/2000 điều khiển việc xác thực, cấp quyền, và tính cước người dùng truy cập vào mạng.

5.7.4. ZoneAlarm (Firewall mềm)

Zone Alarm Antivirus là phương thức tốt nhất để loại trừ virus khỏi máy tính và ngăn chặn không cho chúng xâm nhập ngay từ lúc ban đầu.

Zone Alarm Antivirus với một tường lửa hiệu quả giúp máy tính của bạn trở nên mạnh mẽ hơn trước sự xâm nhập của các hacker. Zone Alarm Antivirus kết hợp công nghệ tường lửa với bộ máy chống virus và quét virus đột phá, sẽ tiêu diệt mọi virus cứng đầu nhất và xóa bỏ hoàn toàn các mã độc khỏi máy tính một cách an toàn.

KẾT LUẬN

Đồ án này đã trình bày về thiết lập mạng Windows 2003 Server, qua đó chỉ ra các yếu tố cần quan tâm để tối ưu hóa và bảo đảm an toàn cho mạng này. Để thực hiện điều trên thì cần phải nắm được kiến thức về mạng, hệ điều hành cũng như mô hình bảo mật hệ thống. Tuy nhiên, để xây dựng và phát triển một hệ thống mạng hoàn chỉnh thì cần phải có những kiến thức thực tiễn.

Quá trình làm đồ án này đã giúp em hiểu thêm về mạng máy tính, cung cấp thêm kiến thức về xây dựng mô hình, cách thiết kế triển khai hệ thống mạng, cách đi dây dẫn, kết nối các thiết bị mạng và lựa chọn mô hình mạng phù hợp với thực tế triển khai.

Lựa chọn mô hình mạng tối ưu trên cơ sở khả năng thực tiễn sẽ giúp cho việc quản trị hệ thống mạng đơn giản và hiệu quả hơn.

Mặc dù đã cố gắng nhưng chắc chắn đề tài của em không tránh khỏi những thiếu sót, em rất mong nhận được những nhận xét chỉ bảo của các thày, cô để có thêm kinh nghiệm khi ra trường.

TÀI LIỆU THAM KHẢO

I. Sách tham khảo.

1. Giáo trình thiết kế và xây dựng mạng LAN và WAN, Trung tâm khoa học tự nhiên và công nghệ quốc gia – Viện công nghệ thông tin. Tháng 01 năm 2004.

2. Hệ bảo mật Windows NT khai thác và ứng, Nhóm Ngọc Anh Thư Press, NXB giáo dục 2004.

3 . Hỗ trợ kỹ thuật Windows NT, ban biên dich VN- GUIDE, NXB thống kê.

II. Website

1. www.quantrimang.com
2. www.manguon.com
3. www.nhatnghe.com
4. http://www.khkt.net.