LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành nhất tới TS. Lại Minh Tuấn đã hướng dẫn em phát triển đồ án nghiên xây dựng ứng dụng thu thập cảnh báo trong hệ thống mạng cho điện thoại thông minh chạy hệ điều hành androidvà cho em những định hướng và những kiến thức quý báu về an toàn mạng và hiểu biết hơn về hệ điều ahnhf android.

Em cũng xin tỏ lòng biết ơn sâu sắc tới thầy cô, bạn bè cùng khóa đã giúp đỡ em học tập và rèn luyện trong suốt những năm học vừa qua.

Em xin cảm ơn gia đình và bạn bè, những người luôn khuyến khích và tạo mọi điều kiện hỗ trợ tốt nhất cho em trong mọi hoàn cảnh.

Em xin chân thành cảm ơn trường Học viện Kỹ thuật Mật Mã đã cho em một môi trường học tập lành mạnh và vững chắc, tạo cho em những điều kiện tốt nhất trong quá trình học tập và làm đồ án này.

Do thời gian hoàn thành đồ án có hạn cho nên em không tránh khỏi những khiếm khuyết, em rất mong có được những góp ý và giúp đỡ của các thầy cô giáo để em có thể tiếp tục đồ án này ở mức ứng dụng cao hơn trong tương lai.

Em xin chân thành cảm ơn!

*Hà Nội, ngày 01 tháng 06 năm 2018*

**Sinh viên thực hiện**

**Vũ Văn Minh**

**LỜI MỞ ĐẦU**

Hiện nay mạng Internet đã trở thành một phần không thể thiếu của con người. Internet ngày càng phổ biến rộng rãi cho mọi người để trao đổi thông tin trên mạng . Khả năng kết nối trên toàn thế giới đang mang lại thuận tiện cho tất cả mọi người, nhưng nó cũng tiềm ẩn những nguy cơ khó lường đe dọa tới mọi mặt của đời sống xã hội. Việc mất trộm thông tin trên mạng gây ảnh hưởng đến tính riêng tư cho các cá nhân, những vụ lừa đảo, tấn công từ chối dịch vụ gây ảnh hưởng lớn đến hoạt động kinh doanh cho công ti và gây phiền toái cho mọi người dung Internet… làm cho vấn đề bảo mật trên mạng luôn là một vấn đề nong hổi và được quan tâm đến trong mọi thời điểm.

Cho đến nay, các giải pháp bảo mật luôn được chú trọng và đã có những đóng góp lớn trong việc hạn chế và ngăn chặn những vấn đề bảo mật, ví dụ như Firewall ngăn chặn những kết nối không đáng tin cậy, mã hóa tang dộ an toàn cho việc truyền dữ liệu, các chương trình duyệt virus với cơ sở dữ liệu liên tục cập nhập về những loại virus mới nhất. Tuy nhiên hiện nay các vụ vi phạm bảo mật xảy ra càng ngày càng tinh vi hơn cùng với sự gia tang những vụ lạm dụng, dung sai xuất phát từ hệ thống mà những phương pháp bảo mật truyền thống không chống được. Những điều đó yêu cầu phải có một Phuong án kịp thời để sử lý ngăn chặn những cuộc tấn công, và kịp thời bảo vệ hệ thống mạng máy tính.

Nhằm giải quyết vấn đề xử lý phát hiện cảnh báo khi bị tấn công trên mạng dữ liệu. Chính vì vậy, em xin lựa chọn đồ án với tên đề tài là “xây dựng ứng dụng thu thập cảnh báo trong hệ thống mạng cho điện thoại thông minh chạy hệ điều hành android” nhằm mục đích phát hiện và cảnh báo mỗi khi mạng máy tính bị tấn công và gửi thông báo về điện thoại người quản lý mạng dữ liệu đó.

Em xin chân thành cảm ơn các thầy cô hướng dẫn em tận tình để em hoàn thành báo cáo thực tập này!

*Hà Nội ngày 01 tháng 03 năm 2018*

**Sinh viên thực hiện**

**Vũ Văn Minh**

MỤC LỤC

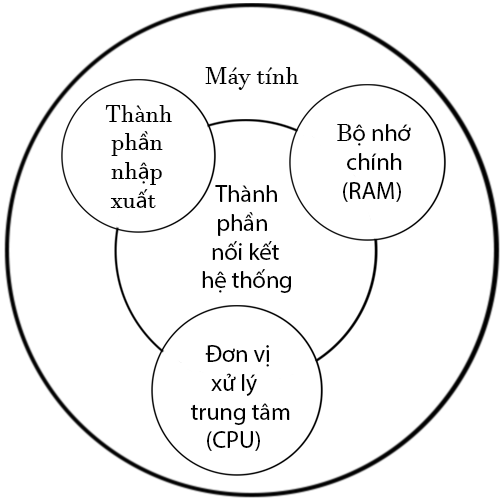
PHẦN I : TỔNG QUAN VỀ MẠNG MÁY TÍNH

**CHƯƠNG 1 : GIỚI THIỆU VỀ MÁY TÍNH VÀ MẠNG MÁY TÍNH**

**1.1.Lịch sử máy tính**

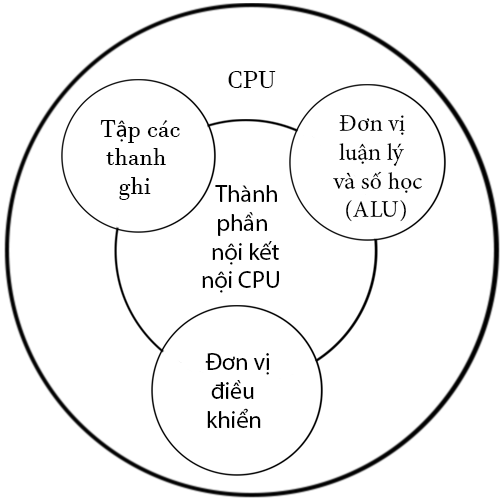
**1.1.1.Cấu trúc tổng quát của máy tính**

Máy tính là một hệ thống phức tạp với hang triệu thành phần điện tử cơ sở. Ở mức đơn giản nhất, máy tính có thể được xem như một thực thể tưởng tác theo mottj cách thức nào đó với môi trường bên ngoài. Một cách tổng quát, các mối quan hệ của nó môi trường bên ngoài có thể phân loại thành các thiết bị ngoại vi hay đường liên lạc.



Hình 1.1.1a: Cấu trúc tổng quát của máy tính

Thành phần chính , quan trọng nhất của máy tính là đơn vị xử lý trung tâm ( CPU – Central Processing Unit): Điều khiển hoạt động của máy tính và thực hiện các chức năng xử lý dữ liệu.



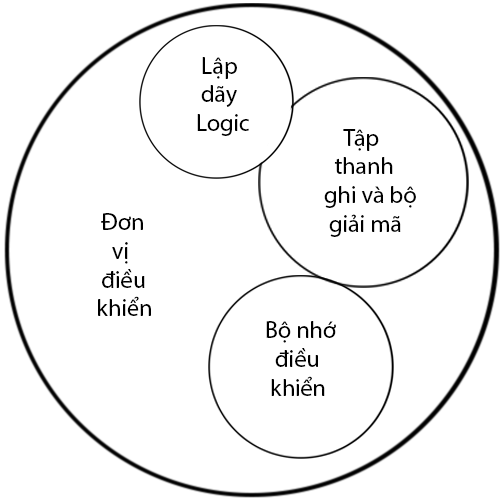
Hình 1.1.1b: Bộ xử lý trung tâm của máy tính (CPU)

CPU thường được đề cập đến với tên gọi bộ xử lý. Máy tính có thể có một hoặc nhiều thành phần nói trên, ví dụ như một hoặc nhiều CPU. Trước đây đa phần các máy tính chỉ có một CPU nhưng gần đây có sự gia tang sử dụng nhiều CPU trong một hệ thống máy đơn. CPU luôn luôn là đối tượng quan trọng vì đây là thành phần phức tạp nhất của hệ thống. Cấu trúc của CPU gồm các thành phần chính:

* Đơn vị điều khiển : Điều khiển hoạt động của CPU và do đó điều khiển hoạt động của máy tính.
* Đơn vị luận lý và số học (ALU – Arithmetic and Logic Unit) : Thực hiện các chức năng xử lý dữ liệu của máy tính.
* Tập thanh ghi : Cung cấp nơi lưu trữ bên trong CPU.
* Thành phần nối kết nội CPU : Cơ chế cung cấp khả năng liên lạc giữa đơn vị điều khiển, ALU và tập thanh ghi.

Trong các thành phần con nói trên của CPU, đơn vị điều khiển lại giữ vai trò quan trọng nhất. Sự cài đặt đơn vị này dẫn đến một khái niệm nền tảng trong chế tạo bộ vi xử lý máy tính. Đó là khái niệm vi lập trình. Hình dưới đây mô tả tổ chức bên trong một đơn vị điều khiển với ba thành phần chính gồm:

* Bộ lập dãy logic.
* Bộ giải mã và tập các thanh ghi điều khiển.
* Bộ nhớ điều khiển.



Hình 1.1.1c : Đơn vị điều khiển của CPU

Các thành phần khác của máy tính:

* Bộ nhớ chính : Dùng để lưu trữ dữ liệu.
* Các thành phần nhập xuất : Dùng để di chuyển dữ liệu giữa máy tính và môi trường bên ngoài.
* Các thành phần nối kết hệ thống : Cung cấp cơ chế liên lạc giữa CPU, bộ nhớ chính và các thành phần nhập xuất.

**1.1.2. Chức năng của máy tính**

Một cách tổng quát, một máy tính có thể thực hiện bốn chức năng cơ bản sau:

* Di chuyển dữ liệu.
* Điều khiển.
* Lưu trữ dữ liệu.
* Xử lý dữ liệu.
* Xử lý dữ liệu : Máy tính phải có khả năng xử lý dữ liệu. Diwx liệu có thể có rất nhiều dạng và phạm vi yêu cầu xử lý cũng rất rộng. Tuy nhiên chỉ có một số phương pháp cơ bản trong xử lý dữ liệu.
* Lưu trữ dữ liệu : Máy tính cũng cần phải có khả năng lưu trữ dữ liệu. Ngay cả khi máy tính đang xử lý . Do vậy cần thiết phải có chức năng lưu trữ ngắn hạn. Tuy nhiên, chwucs năng lưu trữ dài hạn cũng có tầm quan trọng tương đối với dữ liệu cần được lưu trữ trên máy cho những lần cập nhập và tìm kiếm kế tiếp.
* Di chuyển dữ liệu : Máy tính có phải có khả năng di chuyển dữ liệu giữa nó và thế giới bên ngoài. Khả năng này được thể hiện thông qua việc di chuyển dữ liệu giữa máy tính tính với các thiết bị nối kết trực tiếp hay từ xa đến nó. Tùy thuộc vào kiểu kết nối và cự ly di chuyển dữ liệu, mà có tiến trình nhập xuất dữ liệu hay truyền dữ liệu:

**1.2 Mạng máy tính**

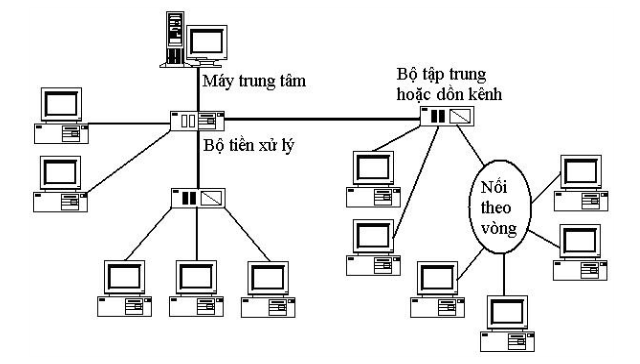
Mạng máy tính là một hệ thống kết nối các máy tính đơn lẻ thông qua các đường truyền vật lý theo một kiến trúc nào đó.

Đường truyền vật lý dung để chuyển các tín hiệu số hay tín hiệu tương tự giữa các máy tính. Đường truyền vật lý thường là:

* Đường dây điện thoại thông thường.
* Cáp đồng trục.
* Sóng vô tuyến điện tử.
* Cáp sợi quang.

**1.2.1. Lịch sử phát triển mạng máy tính**

Từ những năm 60, đã xuất hiện những mạng nối cá máy tính và các Terminal để sử dụng chung nguồn tài nguyên, giảm chi phí khi muốn thông tin, trao đổi số liệu và sử dụng trong công tác văn phòng một cách tiện lợi.



Hình 1.2.1: Mạng máy tính với bộ tiền xử lý.

Việc tăng nhanh các máy tính mini, các máy tính cá nhân làm tăng nhu cầu truyền số liệu giữa các máy tính, các Terminal và giữa các Terminal với các máy tính là một trong những động lực thúc đẩy sự ra đời và phát triển ngày càng mạnh mẽ các mạng máy tính. Quá trình hình thành mạng máy tính có thể tóm tắt qua một số thời điểm chính sau:

Những năm 60: Để tận dụng công suất của máy tính, người ta ghép nối các Terminal vào một máy tính được gọi là máy tính trung tâm (main frame). Máy tính trung tâm làm tất cả mọi việc từ quản lý các thủ tục truyền dữ liệu, quản lý quá trình đồng bộ của các trạm cuối, cho đến việc xử lý các ngắt từ các trạm cuối.

Những năm 70: Các máy tính đã được nối với nhau trực tiếp thành một mạng máy tính nhằm phân tán tài của hệ thống và tăng độ tin cậy và người ta bắt đầu xây dựng mạng truyền thông trong đó các thành phần chính của nó là các nút mạng(node) gọi là bộ chuyển mạch, dung để hướng thông tin tới đích.

Từ thập kỷ 80 trở đi: Việc kết nối mạng máy tính đã bắt đầu dược thực hiện rộng rãi nhờ tỷ lệ giữa giá thành máy tính và chuyển chi phí truyền tin đã giảm đi rõ rệt do sự bùng nổ của các thế hệ máy tính cá nhân.

**1.2.2. Nhu cầu và mục đích của việc kết nối các máy tính thành mạng**

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

- Có rất nhiều công việc về bản chất là phân tán hoạc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.

- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm(ổ cứng, máy in, ổ CD ROM…).

- Nhu cầu liên lạc trao đổi thông tin nhờ phương tiện máy tính.

- Các ứng dụng phần mềm đòi hỏi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

Chính vì vậy, việc kết nối các máy tính thành mạng nhằm mục đích:

* Chia sẻ tài nguyên:
* Chia sẻ dữ liệu: Về nguyên tắc, bất kỳ người sử dụng nào trên mạng đều có quyền truy cập, khai thác và sử dụng những tài nguyên chung của mạng( thường là server).
* Chia sẻ phần cứng: Tài nguyên chung của mạng cũng bao gồm các máy móc, thiết bị như: Máy in(Printer), máy quét(Scanner), ổ đĩa mềm(Floppy), ổ đĩa CD(CD Rom) được nối vào mạng. Thông qua mạng máy tính, người sử dụng có thể sử dụng những tài nguyên phần cứng này ngay cả khi máy tính của họ không có những phần cứng đó.
* Duy trì và bảo vệ dữ liệu: Một mạng máy tính có thể cho phép cá dữ liệu được tự động lưu trữ dự phòng tới một trung tâm nào đó trong mạng. Công việc này là hết sức khó khăn và tốn nhiều thời gian nếu phải làm trên từng máy độc lập. Hơn nữa, mạng máy tính còn cung cấp cơ chế bảo mật(security) bằng mật khẩu (password) đối với người sử dụng, hạn chế được việc sao chép, mất mát thông tin ngoài ý muốn.
* Nâng cao độ tin cậy của hệ thống nhờ kahr năng thay thế cho nhau khi xảy ra sự cố kỹ thuật đối với một máy tính nào đó trong mạng.
* Khai thác có hiệu quả các cơ sở dữ liệu tập trung và phân tán, nâng cao khả năng tích hợp và trao đổi các loại dữ liệu giữa các máy tính trên mạng.

**1.2.3. Đặc trưng kỹ thuật của mạng máy tính**

**1.2.3.1. Đường truyền**

Là thành tố quan trọng của một mạng máy tính, là phương tiện dung để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điện tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân(On-Off), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc song điện từ.

* Các tần số radio có thể truyền bằng cáp điện (dây xoắn đôi hoặc đồng trục) hoặc bằng phương tiện quảng bá (radio broadcasting).
* Sóng cực ngắn (viba) thường được dung để truyền giữa các trạm mặt đất và các vệ tinh. Chúng cũng được dung để truyền các tín hiệu quảng bá từ một trạm phát đến nhiều trạm thu. Mạng điện thoại “tổ ong” là một ví dụ cho cách dung này.
* Tia hồng ngoài là lý tưởng đối với nhiều laoij truyền thông mạng. Tia hồng ngoại và các tần số cao hơn của ánh sáng có thể được truyền qua cáp sợ quang. CÁc đặc trưng cơ bản của đường truyền là giải thông (bandwidth), độ suy hao và độ nhiễu điện tử.
* Dải thông của một đường truyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được, nó biểu thị khả năng truyền tải tín hiệu của đường truyền. Tốc độ truyền dữ liệu trên đường truyền được gọi là thông lượng(throughput) của đường truyền, thường được tính bằng số lượng bit được truyền đi trong một giây(bps). Giải thông của cáp truyền phụ thuộc vào độ dài cáp(nói chung cáp ngắn có thể có giải thông lớn hơn so với cáp dài). Bởi vậy, khi thiết kế cáp cho mạng cần thiết phải chỉ rõ độ dài chạy cáp tối đa vì ngoài giới hạn đó chất lượng truyền tín hiệu không còn được đảm bảo.
* Độ suy hao của một đường truyền là độ đo sự yếu đi của tín hiệu trên đường truyền đó, nó cũng phụ thuộc vào độ dài cáp. Còn độ nhiễn điện từ EMI (Electronmangetic Interference) gây ra bởi tiếng ồn từ bên ngoài làm ảnh hưởng đến tín hiệu trên đường truyền.

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

* Đường truyền hữu tuyến: Cá máy tính được nối với nhau bằng các dây cáp mạng. Đường truyền hữu tuyến gồm có:
* Cáp đồng trục (Coaxial cable).
* Cáp xoắn đôi (Twisted pải cable) gồm 2 loại có bọc kim (stp- shieldel twisted pair) và không bọc kim (utp – Unshieldel twisted pair).
* Cáp sợi quang(Fiber optic cable).
* Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các song vô tuyến với các thiết bị điều chế/ giải điều chế ở các đầu mút. Đường truyền vô tuyến gồm có:
* Radio.
* Sóng cực ngắn (Viba).
* Tia hồng ngoại (Infrared).

**1.2.3.2. Kiến trúc mạng**

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

**1.2.3.2.1. Hình tạng mạng**

Hình trạng mạng là cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là “topology” của mạng.

Có 2 kiểu nối mạng chủ yếu là điểm – điểm (point to point) và điểm – đa điểm (point to multipoint).

* Theo kiểu điểm – điểm: Các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu trữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Một số mạng có cấu trúc điểm – điểm như: mạng hình sao, mạng chu trình…
* Theo kiểu điểm – đa điểm: Tất cả các nút phân chia chung một đường truyền vật lý. Dữ liệu gửi đi từ một nút nào đó sẽ có thể được tiếp nhận bởi tất cả các nút còn lại. Bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi nút căn cứu vào đó kiểm tra xem dữ liệu có phải gửi cho mình hay không. Mạng trực tuyến tính (bú), mạng hình vòng(ring), mạng vệ tinh(satellite) hay radio… là những mạng có cấu trúc điểm – đa điểm phổ biến.

**1.2.3.2.2. Giao thức mạng**

Việc trao đổi thông tin dù là đơn giản nhất, cũng phải tuân theo những quy tắc nhất định. Đơn giản như khi hai người nói chuyện với nhau muốn cho cuộc nói chuyện có kết quả thì ít nhất cả hai cũng phải ngầm hiểu và tuân theo và tuân thủ quy ước : khi một người nói thì người kia phải nghe và ngược lại. Việc truyền thông trên mạng cũng vậy, cần có các quy tắc, quy ước truyền thông về nhiều mặt: khuôn dạng cú pháp của dữ liệu, các thủ tục gửi , nhận dữ liệu , kiểm soát hiệu quả và chất lượng truyền tin … Tập hợp những quy tắc quy ước truyền thông đó được gọi là giao thức của mạng (network protocol).

Có rất nhiều giao thức mạng, các mạng có thê sử dụng cá giao thức khác nhau tùy sự lựa chọn của người thiết kế. Tuy vậy, các giao thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, …

**1.2.3.3. Hệ điều hành mạng**

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

* Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:
* Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ, tìm kiếm , xóa, copy, đặt các thuộc tính cho tệp đều thuộc nhóm công việc này.
* Tài nguyên thiết bị, điều phối việc sử dụng CPU, các ngoại vi… để tối ưu hóa việc sử dụng.
* Quản lý người dung và các công việc trên hệ thống : Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.
* Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi( ví dụ format đĩa, sao chép tệp và thư mục , in ấn chung…)

Các hệ điều hành mạng thông dụng nhất hiện nay là : WindownNT, Windown9x, Windown 2000, Unix, Novell…

**1.2.4. Phân loại mạng máy tính:**

Có nhiều cách phân loại mạng khác nhau tùy thuộc vào yếu tố chính được chọn làm chỉ tiêu phân loại như :

* Khoảng cách địa lý của mạng.
* Kỹ thuật chuyên mạch áp dụng trong mạng.
* Hình trạng mạng
* Giao thức sử dụng.
* Hệ điều hành mạng sử dụng…

**1.2.4.1. Phân loại mạng theo khoảng cách địa lý:**

Mạng máy tính có thể phân bố trên một vùng lãnh thổ nhất định và cũng có thể phân bố trong phạm vi một quốc gia hay rộng hơn nữa là toàn thế giới. Dựa vào phạm vi phân bố của mạng, người ta có thể phân ra các loại mạng như sau:

**1.2.4.1.1. Mạng toàn cầu(GAN – Global Area NetWork)**

Là mạng kết nối các máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

**1.2.4.1.2. Mạng diện rộng(WAN- Wide Area Network)**

Là mạng kết nối các máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường các kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể kết nối với nhau tạo thành GAN hay tự nó cũng có thể xem là một GAN.

**1.2.4.1.3. Mạng đô thị(MAN- Metropolitan Area Network)**

Là mạng kết nối các máy tính trong phạm vi một đo thị , một trung tâm văn hóa xã hội, có bán kính tối đa vào khoảng 100km. Kết nối này được thực hiện thông qua môi trường truyền thông tốc độ cao(50-100Mbps).

**1.2.4.1.4. Mạng cục bộ(LAN-Local Area Network)**

Là mạng kết nối các máy tính trong một khu vực bán kính hẹp, thông thường khoảng vài tram mét đến vài kilomet. Kết nối được thực hiện thông qua môi trường truyền thông tốc độ cao. Ví dụ như cá đồng trục, cáp xoắn đôi hay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan, tổ chức, trong một tòa nhà. Nhiều LAN có thể được kết nối với nhau thành WAN.

**1.2.4.2. Phân loại theo kỹ thuật chuyển mạch áp dụng trong mạng**

Nếu lấy kỹ thuật chuyển mạch làm yếu tố chính để phân loại ta sẽ có:

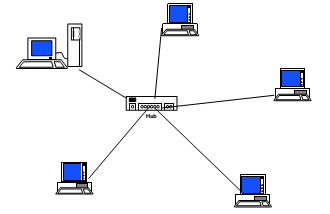
* Mạng chuyển mạch kênh.
* Mạng chuyển mạch thông báo.
* Mạng chuyển mạch gói.

**1.2.4.3. Phân loại theo hình trạng mạng**

Khi phân loại theo hình trạng mạng, người ta thường phân loại thành: Mạng hình sao, hình vòng, trục tuyến tính, hình cây,… Dưới đay là một số hình trạng mạng cơ bản:

**1.2.4.3.1. Mạng hình sao**

MẠng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tùy theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là bộ chuyển mạch(switch), bộ chọn đường (router) hoặc là bộ phân kênh (hub). Vai trò của thiết bị trung tâm này là thực hiện việc thiết lập các liên kết điểm – điểm (point – to – point) giữa các trạm.



Hình 1.2.4.3.1: Mạng hình sao (Star)

* Ưu điểm của topo mạng hình sao.

Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng(them , bớt các trạm), dễ dàng kiểm soát và khác phục sự cố, tận dụng được tối đa tôc độ truyền của đường truyền vật lý.

* Nhược điểm của topo mạng hình sao.

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

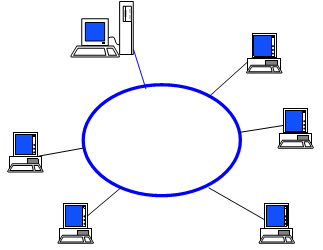
**1.2.4.3.2. Mạng hình vòng**

Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất.

Một trạm của mạng được nối với vòng qua một bộ chuyển tiếp(repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp trên vòng. Như vậy tín hiệu đucợ lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết điểm – điển giữa.

Để tăng độ tin cậy của mạng ta có thể lắp đặt them các vòng dự phòng, nếu vòng chính có sự cố thì vòng phụ sẽ được sử dụng.

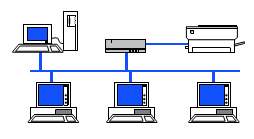
Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.



Hình 1.2.4.3.2: Mạng hình vòng(Ring)

**1.2.4.3.3. Mạng trực tuyến tính(Bus)**

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



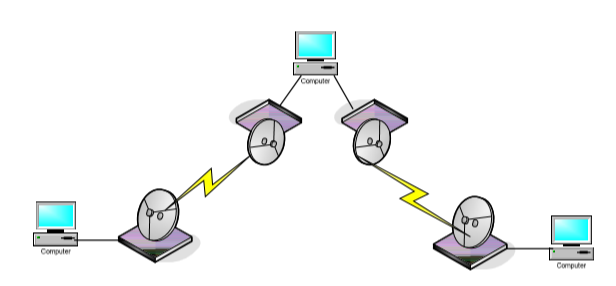
Hình 1.2.4.3.3: Mạng trục tuyến tính (Bus)

Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus, tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp. Đối với cvacs bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho các trạm trên amngj đều có thể thu nhận được tín hiệu đó. Như vậy topo mạng dữ liệu được truyền theo các liên kết điểm – đa điểm(point – to – point) hay quảng bá(broadcast).

**Ưu điểm**: Dễ thiết kế, chi phí thấp.

**Nhược điểm**: Tính ổn định kém, chỉ một nút mạng hỏng là toàn bộ mạng bị ngừng hoạt động.

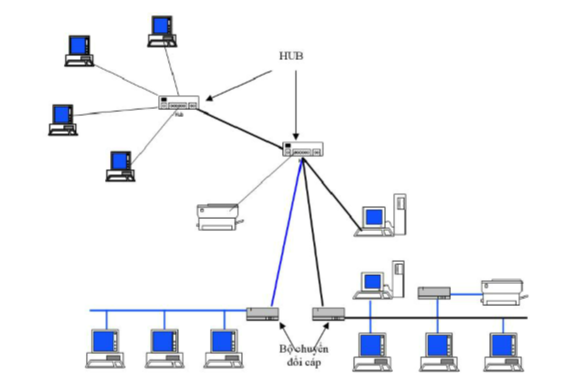
**1.2.4.3.4. Mạng dạng vô tuyến – Satellite(vệ tinh) hoặc Radio**



Hình 1.2.4.3.5: Mạng vô tuyến – Satellite hoạc Radio

**1.2.4.3.5. Mạng kết nối hỗn hợp**

Ngoài các hình trạng cơ bản chuẩn, còn có thẻ kết hợp hai hay nhiều hình trạng cơ bản lại với nhau tạo ra các hình trạng mở rộng nhằm tận dụng những ưu điểm , khắc phục những nhược điểm của từng loại mạng riêng khi chúng chưa được kết hợp với nhau:



Hình 1.2.4.3.5: Mạng kết nối hỡn hợp

**1.2.4.4. Phân loại theo giao thức và theo hệ điều hành mạng sử dụng**

Khi phân loại theo giao thức mà mạng sử dụng người ta phân loại thành: Mạng TCP/TP, mạng NETBOIS…

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

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

**1.2.4.4.1. Mạng khách/chủ(Client – Server)**

Trang mạng có những máy chuyên dụng phục vụ cho những mục đích khác nhau, máy phục vụ này hoạt động như một người phục vụ và không kiêm ai vai trò của trạm làm việc hay máy khách.

Các máy phục vụ chuyên dụng được tối ưu hóa để phục vụ nhanh những yêu cầu của các máy khách.

Các loại thường dung: máy phục vụ tập tin/in ấn(file/print server), máy phục vụ chương trình ứng dụng(application server), máy phục vụ thư tín (mail, server), máy phục vụ fax(fax server), máy phục vụ truyền thông(communication server).

Một trong những ưu điểm quan trọng của mạng dựa trên máy phục vụ đó là: có tính an toàn và bảo mật cao. Hầu hết các mạng trong thực tế(nhất là những mạng lớn) đều dựa trên mô hình khách chủ/này.

**1.2.5. Một số mạng máy tính thông dụng nhất**

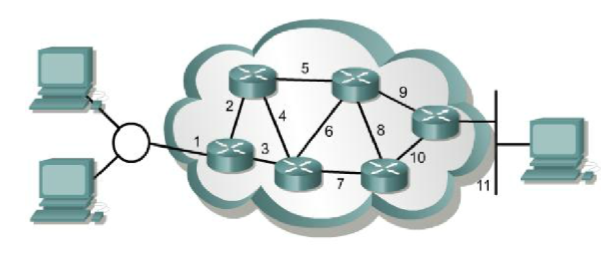
**1.2.5.1. Mạng cục bộ (LAN):**

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

Mạng cục bộ có một số các đặc trưng sau:

* Đặc trưng đại lý: Mạng cục bộ thường được cài đặt trong một phạm vi địa lý tương đối nhỏ như: Trong một tòa nhà, một trường đại học, một căn cứ quân sự,… Với đường kính của mạng có thể là từ vài chục mét, tới vài chục kilomet trong điều kiện công nghệ hiện nay.
* Đặc trưng tốc độ truyền: MẠng cục bộ tốc độ có tốc độ truyền thường cao hơn so với mạng diện rộng. Với công nghệ mạng hiện nay, tốc độ truyền của mạng cục bộ có thể đạt tới 100Mb/s.
* Đặc trưng dộ tin cậy: Tỷ suất lỗi trên mạng cục bộ là thấp hơn nhiều so với mạng diện rộng hoặc các loại mạng khác.
* Đặc trưng quản lý: MẠng cục bộ thường là sở hữu riêng của một tổ chức nào đó.

**1.2.5.2. Mạng diện rộng với kết nối LAN to LAN:**

****

Hình 1.2.5.2: Mạng diện rộng với kết nối LAN to LAN

Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, một quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu.

Mạng diện rộng có một số đặc điểm sau:

* Tốc độ truyền dữ liệu không cao.
* Phạm vi địa lý không giới hạn.
* Thường triển khai dựa vào các công ty truyền thông, bưu điện và dung các hệ thống truyền thông này để tạo dựng đường truyền.
* Một mạng WAN có thể là sở hữu của một tập đoàn, một tổ chức hoặc là mạng kết nối của nhiều tập đoàn, tổ chwucs.

**1.2.5.3. Liên mạng Internet**

Cùng với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng Internet. Nó có những đặc điểm sau:

* Là một mạng toàn cầu.
* Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin.
* Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP.
* Là sở hữu chung của toàn nhân loại.
* Càng ngày càng phát triển mãnh liệt.

**1.2.5.4. Mạng Internet**

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 vào bảo mật thông tin.

Internet được phát triển từ các mạng LAN, WAN dung công nghệ Internet.

**CHƯƠNG 2: CHUẨN HÓA MẠNG MÁY TÍNH, MÔ HÌNH OSI, TCP/IP**

**2.1 Vấnđề chuẩn hóa mạng máy tính và các tổ chức chuẩn hóa mạng:**

Sự phát triển sớm của LAN, WAN , MAN diễn ra rất hỗn loạn theo nhiều phương cách khác nhau.

Vì lý do , hội đồng tiêu chuẩn quốc tế là ISO (International Standards Organization), do các nước thành viên lập nên, công việc ở Bắc Mỹ chịu sự điều hành của ANSI(American National Standards Institude) ở Hoa Kỳ đã ủy thác cho IEEE(Institude ofElectrical and Electronic Engineers)phát triển và đề ra những tiêu chuẩn kỹ thuật cho LAN. Tổ chwucs này đã xây dựng nên mô hình tham chiếu cho việc kết nối các hệ thống mở OSI(reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Có hai loại chuẩn cho mạng đó là:

* Các chuẩn chính thwucs(de jure) do các tổ chức chuẩn quốc gia và quốc tế ban hành.
* Các chuẩn thwucj(de facto) do các hang sản xuất, các tổ chức người sử dụng xây dựng và được dung rộng rãi trong thực tế.

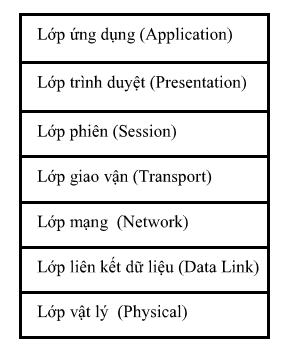
**2.2. Mô hình chiếu OSI 7 lớp**

**2.2.1. Giới thiệu về mô hình OSI**

Vấn đề không tương thích giữa cá mạng máy tính với nhau đã làm trở ngại cho sự tương tác giữa những người sử dụng mạng khác nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng.

Chính vì lý do đó, tổ chức tiêu chuẩn hóa quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán và gồm 7 lớp.

**2.2.2. Các lớp trong mô hình OSI và chức năng của chúng**

****

Hình 2.2.2: Mô hình tham chiếu OSI 7 lớp

**2.2.2.1. Lớp vật lý**

Lớp này bảo đảm các công việc sau:

* Thiết lập, cắt kết nối.
* Truyền tin dạng bit qua kênh vật lý.
* Có thể có nhiều kênh.

**2.2.2.2. Lớp liên kết dữ liệu**

Lớp này đảm bảo việc biến đổi các tin dạng bit nhận được từ lớp dưới(lớp vật lý) sang khung số liệu, thông báo cho hệ phát kết quả thu được sao cho các thông tin truyền lên cho mức 3 không có lỗi. Các thông tin truyền ở mức một có thể làm hỏng các thông tin khung số liệu(frame error). Phần mềm mức hai sẽ thông báo cho mức một truyền lại các thông tin bị mất/lỗi. Đồng bộ các hệ có tốc độ xử lý khác nhau, một trong những phương pháp hay sử dụng là dùng bộ đệm trung gian để lưu giữ số liệu nhận được. Độ lớn của bộ đệm này phụ thuộc vào tương quan xử lý của các hệ thu và phát.

Trong trường hợp đường truyền song công toàn phần, lớp datalink phải đảm bảo việc quản lý các thông tin số liệu và các thông tin trạng thái.

**2.2.2.3. Lớp mạng**

Nhiệm vụ của lớp mạng là đảm bảo chuyển chính xác số liệu giữa cá thiết bị cuối trong mạng. Để làm được việc đó, phải có chiến lược đánh địa chỉ thống nhất trong toàn mạng . Mỗi thiết bị cuối và thiết bị mạng có một địa chỉ mạng xác định. Số liệu cần trao đổi giữa các thiết bị cuối được tổ chức thành các gói(packet) có độ dài thay đổi và được gán đầy đủ địa chỉ nguồn(source address) và địa chỉ đích (destination address).

Lớp mạng đảm bảo việc tmf đường tối ưu cho các gói dữ liệu bằng các giao thức chọn đường dựa trên các thiết bị chọn đường(router). Ngoài ra, lớp mạng có chức năng điều kiển lưu lượng số liệu trong mạng để tránh xảy ra tắc nghẽn bằng cách chọn các chiến lược tìm đường khác nhau để quyết định việc chuyển tiếp các gói số liệu.

**2.2.2.4 Lớp giao vận**

Lớp này thực hiện các chức năng nhận thông tin từ lớp phiên(session) chia thành các gói nhỏ hơn và truyền xuống lớp dưới, hoặc nhận thông tin từ lớp dưới chuyển lên phục hồi theo cách chia của hệ phát(fragmentation and reassembly). Nhiệm vụ quan trọng nhất của lớp vận chuyển là đảm bảo chuyển số liệu chính xác giữa hai thực thể thuộc lớp phiên(end to end control). Để làm được việcđó, ngoài chức năng kiểm tra số tuần tự phát, thu, kiểm tra và phét hiện, xử lý lỗi, lớp vận chuyển còn có chức năng điều khiển lưu lượng số liệu để đồng bộ giữa thể thu và phát và tránh tắc nghẽn số liệu khi chuyển qua lớp mạng. Ngoài ra, nhiều thực thể lớp phiên có thể traoddooir số liệu trên cùng một kết nối lớp mạng(multiplexing).

**2.2.2.5. Lớp phiên**

Liên kết giữa hai thực thể có nhu cầu trao đổi số liệu, ví dụ người dùng và một máy tính ở xa, được gọi là một phiên làm việc. Nhiệm vụ của lớp phiên là quản lý việc trao đổi số liệu, ví dụ: thiết lập giao diện giữa người dùng và máy, xác định thông số điều khiển trao đổi số liệu (tốc độ truyền, số bit trong một byte, có kiểm tra lỗi parity hay không, v.v.), xác định loại giao thức mô phỏng thiết bị cuối (terminal emulation),… Chức năng quan trọng nhất của lớp phiên là đảm bảo đồng bộ số liệu bằng cách thực hiện các điểm kiểm tra. Tại các điểm kiểm tra này, toàn bộ trạng thái và số liệu của phiên làm việc được lưu trữ trong bộ nhớ đệm. Khi có sự cố, có thể khởi tạo lại phiên làm việc từ điểm kiểm tra cuối cùng (không phải khởi tạo lại từ đầu).

**2.2.2.6. Lớp trình diễn**

Nhiệm vụ của lớp trình diễn là thích ứng các cấu trúc dữ liệu khác nhau của người dùng với cấu trúc dữ liệu thống nhất sử dụng trong mạng. Số liệu của người dùng có thể được nén và mã hoá ở lớp trình diễn, trước khi chuyển xuống lớp phiên. Ngoài ra, lớp trình diễn còn chứa các thư viện các yêu cầu của người dùng, thư viện tiện ích, ví dụ thay đổi dạng thể hiện của các tệp, nén tệp...

**2.2.2.7. Lớp ứng dụng**

Lớp ứng dụng cung cấp các phương tiện để người sử dụng có thể truy nhập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân tán. Lớp ứng dụng cho phép người dùng khai thác các tài nguyên trong mạng như là tài nguyên tại chỗ.

**2.2.3. Phương thức hoạt động của mô hình OSI**

Ở mỗi tầng trong mô hình OSI, có hai phương thức hoạt động chính được áp dụng đó là: phương thức hoạt động có liên kết (connection oriented) và không có liên kết (connectionless).

Với phương thức có liên kết, trước khi truyền dữ liệu cần thiết phải thiết lập một liên kết logic giữa các thực thể cùng lớp (layer). Còn với phương thức không có liên kết, thì không cần lập liên kết logic và mỗi đơn vị dữ liệu trước hoặc sau đó.

Phương thức có liên kết, quá trình truyền dữ liệu phải trải qua 3 giai đoạn :

Thiết lập liên kết: Hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ được sử dụng trong giai đoạn về sau.

Truyền dữ liệu: Dữ liệu được truyền với các cơ chế kiểm soát và quản lý.

Hủy bỏ liên kết: Giải phóng các tài nguyên hệ thống đã cấp phát cho liên kết để dùng cho các liên kết khác.

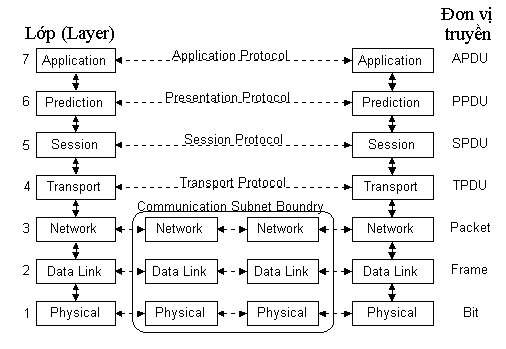
So sánh 2 phương thức hoạt động trên, chúng ta thấy rằng phương thức hoạt động có liên kết cho phép truyền dữ liệu tin cậy, do nó có cơ chế kiểm soát và quản lý chặt chẽ từng liên kết logic. Nhưng mặt khác, nó lại khá phức tạp và khó cài đặt và ngược lại.

Hai lớp kề nhau có thể không nhất thiết phải sử dụng cùng một phương thức hoạt động, mà có thể dùng hai phương thức khác nhau.

**2.2.4. Quá trình truyền dữ liệu trong mô hình OSI**

Tiến trình gửi: Dữ liệu qua lớp ứng dụng (application) được gắn thêm phần tiêu đề AH (Application Header) vào phía trước dữ liệu rồi kết quả đưa xuống lớp trình diễn (presentation). Lớp trình diễn có thể biến đổi mục dữ liệu này theo nhiều cách khác nhau, thêm phần header vào đầu và chuyển xuống lớp phiên. Quá trình này được lặp đi lặp lại cho đến khi dữ liệu đi xuống đến lớp vật lý, ở đấy chúng thật sự được truyền sang máy nhận.

Quá trình nhận diễn ra ngược lại, ở máy nhận, các phần Header khác nhau được loại bỏ từng cái một khi dữ truyền lên theo các lớp cho đến khi khôi phục lại nguyên trạng khối dữ liệu đã truyền đi ở máy truyền.



Hình 2.2.4 : Quá trình truyền dữ liệu trong mô hình OSI

Cụ thể: giả sử bắt đầu chương trình gửi mail vào thời điểm này, lớp application đã nhận biết được sự chọn lựa và chuyển xuống lớp presentation.

Presentation quyết định định dạng hay mã hoá dữ liệu nhận được từ lớp application. Sau đó chuyển xuống tiếp lớp session, tại đây dữ liệu được gán một control frame đặc biệt cho biết là có thể chuyển data xuống lớp tranport.

Tại lớp tranport data được gom lại thành các frame. Tại lớp data link nếu dữ liệu quá lớn, lớp này sẽ phân chia thành những gói nhỏ và đánh thứ tự cho những gói đó và truyền xuống lớp network.

Lớp này them những thông tin địa chỉ vào gói dữ liệu mà nó nhận được và chuyển xuống chính xác cho lớp data link. Tại đây, dữ liệu được chuyển thành các bit đưa xuống cáp và truyền sang máy B.

Máy B nhận dữ liệu và dịch ngược theo thứ tự các lớp:

Physical– Data Link– Network–Transport– Session– Presentation– Application.

**2.3. TCP/IP và mạng Internet**

**2.3.1. Họ giao thức TCP/IP**

**2.3.1.1. Giới thiệu về họ giao thức TCP/IP**

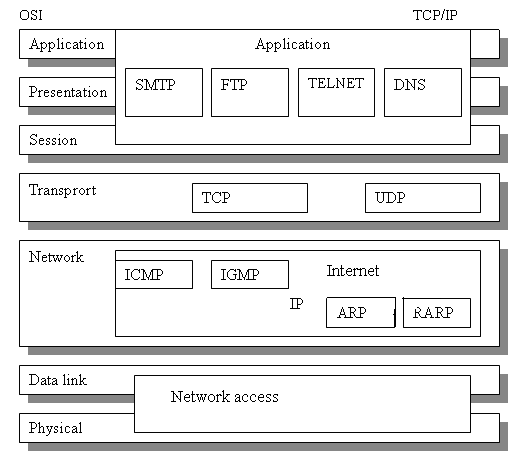
Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng ARPA (Advanced Research Projects Agency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở của nó. Hai giao thức được dùng chủ yếu ở đây là TCP (Transmission Control Protocol) và IP (Internet Protocol). Chúng đã nhanh chóng được đón nhận và phát triển với mục đích xây dựng và phát triển một mạng truyền thông mở rộng khắp thế giới mà ngày nay chúng ta gọi là Internet. Phạm vi phục vụ của Internet không còn dành cho quân sự như ARPAnet nữa mà nó đã mở rộng lĩnh vực cho mọi loại đối tượng sử dụng, trong đó tỷ lệ quan trọng nhất vẫn thuộc về giới nghiên cứu khoa học và giáo dục.

TCP/IP (Transmission Control Protocol/ Internet Protocol) TCP/IP là một họ giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng được hình thành từ những năm 70.

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

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

Các giao thức hỗ trợ ứng dụng phổ biến như truy nhập từ xa (telnet), chuyển tệp (FTP), dịch vụ World Wide Web (HTTP), thư điện tử (SMTP), dịch vụ tên miền (DNS),...



Hình 2.3.1.1a: Mô hình OSI và mô hình kiến trúc của TCP/IP

Như vậy, TCP tương ứng với lớp 4 cộng thêm một số chức năng của lớp 5 trong họ giao thức chuẩn ISO/OSI. Còn IP tương ứng với lớp 3 của mô hình OSI.

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

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

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

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

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

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

|  |  |
| --- | --- |
| Application | Stream |
| Transport | Segment/Datagram |
| Internet | Datagram |
| Network Access | Frame |

Hình 2.3.1.1.b: Cấu trúc dữ liệu tại các lớp của TCP/IP

* **Lớp truy nhập mạng:**

Network access là lớp thấp nhất trong cấu trúc phân bậc của TCP/IP. Những giao thức ở lớp này cung cấp cho hệ thống phương thức để truyền dữ liệu trên các tầng vật lý khác nhau của mạng. So sánh với cấu trúc OSI/OSI, lớp này của TCP/IP tương đương với hai lớp datalink, và physical.

Chức năng định dạng dữ liệu sẽ được truyền ở lớp này bao gồm việc nhúng các gói dữ liệu IP vào các frame sẽ được truyền trên mạng và việc ánh xạ các địa chỉ IP vào địa chỉ vật lý được dùng cho mạng.

* **Lớp liên mạng:**

Internet là lớp ở ngay trên lớp network access trong cấu trúc phân lớp của TCP/IP. Internet protocol là giao thức trung tâm của TCP/IP và là phần quan trọng nhất của lớp internet. IP cung cấp các gói lưu chuyển cơ bản mà thông qua đó các mạng dùng TCP/IP được xây dựng.

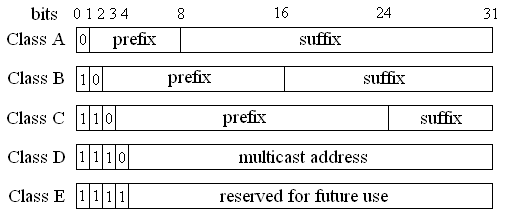
**2.3.1.2. Giao thức IP :**

Mục đích chính của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP cung cấp các chức năng chính sau:

* Định nghĩa cấu trúc các gói dữ liệu là đơn vị cơ sở cho việc truyền dữ liệu.
* Định nghĩa phương thức đánh địa chỉ IP.
* Truyền dữ liệu giữa tầng vận chuyển và tầng mạng .
* Định tuyến để chuyển các gói dữ liệu trong mạng.
* Thực hiện việc phân mảnh và hợp nhất (fragmentation – reassembly) các gói dữ liệu và nhúng/tách chúng trong các gói dữ liệu ở tầng liên kết.

**2.3.1.2.1 Địa chỉ IP:**

Sơ đồ địa chỉ hoá để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP. Mỗi địa chỉ IP có độ dài 32 bits (đối với IP4) được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu thị dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Mục đích của địa chỉ IP là để định danh duy nhất cho một host bất kỳ trên liên mạng.

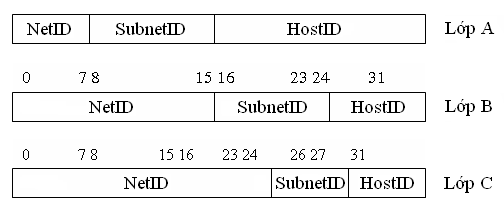


Hình 2.3.1.2.1a: Cách đánh địa chỉ TCP/IP

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

Trong thực tế, do địa chỉ IP là một tài nguyên cần thiết phải tiết kiệm triệt để, tránh lãng phí nên người ta đưa ra cách chia subnet (subneting).

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



Hình 2.3.1.2.1b: Bổ sung vùng subnetid

**2.3.1.2.2. Cấu trúc gói dữ liệu IP:**

IP là giao thức cung cấp dịch vụ truyền thông theo kiểu không liên kết (connectionless). Phương thức không liên kết cho phép cặp trạm truyền nhận không cần phải thiết lập liên kết trước khi truyền dữ liệu và do đó không cần phải giải phóng liên kết khi không còn nhu cầu truyền dữ liệu nữa. Phương thức kết nối không liên kết cho phép thiết kế và thực hiện giao thức trao đổi dữ liệu đơn giản (không có cơ chế phát hiện và khắc phục lỗi truyền). Cũng chính vì vậy độ tin cậy trao đổi dữ liệu của loại giao thức này không cao.

Các gói dữ liệu IP được định nghĩa là các datagram. Mỗi datagram có phần tiêu đề (header) chứa các thông tin cần thiết để chuyển dữ liệu (ví dụ địa chỉ IP của trạm đích). Nếu địa chỉ IP đích là địa chỉ của một trạm nằm trên cùng một mạng IP với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích; nếu địa chỉ IP đích không nằm trên cùng một mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển IP gateway để chuyển tiếp. IP gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau. Cấu trúc gói số liệu IP như sau:

* VER (4 bits): chỉ Version hiện hành của IP được cài đặt.
* IHL (4 bits): chỉ độ dài phần tiêu đề (Internet Header Length) của datagram, tính theo đơn vị word (32 bits).Độ dài mặc định của phần tiêu đề là 5 từ.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Hlength | | T\_o\_S | Total Length | |
| Identification | | | | Flags | Fragment offset |
| Time to live | | Protocol | | Header checksum | |
| Source Address | | | | | |
| Destination Address | | | | | |
| Option +Padding | | | | | |
| Data (max=65.535 byte) | | | | | |

Hình 2.3.1.2a: Cấu trúc gói dữ liệu TCP/IP

* Type of service (8 bits): cho biết các thông tin về loại dịch vụ và mức ưu tiên của gói IP, có dạng cụ thể như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Precedence | D | T | R | Reserved |

* Total Length (16 bits): chỉ độ dài toàn bộ datagram, kể cả phần header (tính theo đơn vị bytes), vùng dữ liệu của datagram có thể dài tới 65535 bytes.
* Identification (16 bits) : cùng với các tham số khác như (source address và destination address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng
* Flags (3 bits) : liên quan đến sự phân đoạn (fragment) các datagram.
* Fragment Offset (13 bits) : chỉ vị trí của đoạn (fragment) ở trong datagram, tính theo đơn vị 64 bits, có nghĩa là mỗi đoạn (trừ đoạn cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội của 64 bits.
* Time To Live (TTL – 8 bits): quy định thời gian tồn tại của một gói dữ liệu trên liên mạng để tránh tình trạng một datagram bị quẩn trên mạng.
* Protocol (8 bits): chỉ giao thức tầng kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP).
* Header checksum (16 bits): mã kiểm soát lỗi sử dụng phương pháp CRC (Cyclic Redundancy Check) dùng để đảm bảo thông tin về gói dữ liệu được truyền đi một cách chính xác (mặc dù dữ liệu có thể bị lỗi).
* Source Address (32 bits): địa chỉ của trạm nguồn.
* Destination Address (32 bits): địa chỉ của trạm đích.
* Option (có độ dài thay đổi) sử dụng trong một số trường hợp, nhưng thực tế chúng rất ít dùng. Option bao gồm bảo mật, chức năng định tuyến đặc biệt.
* Padding (độ dài thay đổi): vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.
* Data (độ dài thay đổi): vùng dữ liệu có độ dài là bội của 8 bits, tối đa là 65535 bytes.

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

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

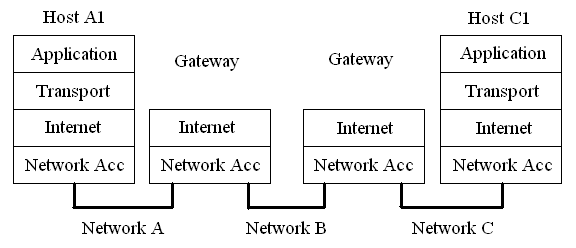


Hình 2.3.1.2.2c: Cổng truy nhập dịch vụ TCP

**2.3.1.2.3. Định tuyến IP :**

Có hai loại định tuyến: Định tuyến trực tiếp và định tuyến không trực tiếp

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



Hình 2.3.1.3: Dùng các gateway để gửi các gói dữ liệu

**2.3.2 Mạng Internet:**

Internet bắt nguồn từ đề án ARPANET (Advanced Research Project Agency Network) khởi sự trong năm 1969 bởi Bộ Quốc phòng Mỹ (American Department of Defense). Cùng với thời gian Internet phát triển nhanh chóng và ngày nay Internet là một phần không thể thiếu trong cuộc sống cũng như trong công việc của mỗi chúng ta. Dựa vào Internet chúng ta có thể giao tiếp với nhau không phụ thuộc vào địa lý, có thể chia sẻ tài nguyên và thực hiện các dịch vụ thương mại như buôn bán ….

**2.3.2.1 Kiếm trúc mạng Internet:**

Internet là một siêu mạng dựa trên sự liên nối trên nhiều lớp khác nhau:

* Mạng liên lục địa: Sử dụng trục cable qua các đại dương, hoặc sử dụng các vệ tinh. Mục đích là nối thông tin giữa các lục địa.
* Mạng lục địa: Gồm các hãng điều tiết quốc gia hay liên quốc gia, cung cấp phương tiện truyền tin cho các khách hàng trên một vùng nhất định của một lục địa
* Mạng truy nhập địa phương: Gồm các hãng bán dịch vụ cổng vào cho khách hàng qua mạng lưới điện thoại hay mạng riêng, và nối vào các mạng lục địa bởi các đường truyền đặc biệt (Specialized links): TRANSPAC–France–Telecom, FranceNet, World Net, Imaginet, ...
* Mạng biệt lập: Các mạng được xây dựng riêng để bán dịch vụ cho khách và có cổng nối với siêu mạng Internet (Computer Serve, IBM, Micronet,Microsoft Network).

Về mặt thiết bị ba thành phần chính tạo nên Internet là:

* Các trạm chủ (host), các trạm làm việc (workstation), máy tính cá nhân (pc), máy chủ, máy lớn, v.v ... trên đó chạy các chương trình ứng dụng. Các máy tính có thể thuộc các loại khác nhau, chỉ cần hiểu được TCP/IP và có phần cứng, phần mềm tương ứng để truy cập và sử dụng các dịch vụ Internet.
* Các mạng diện rộng, mạng cục bộ, đường thuê bao điểm–điểm (Point to Point), liên kết Dial–Up (điện thoại, ISDN, X.25) v.v ... mang tải thông tin trao đổi giữa các máy tính.
* Các bộ dẫn đường (router) phục vụ việc kết nối giữa các mạng.

**2.3.2.2 Các dịch vụ thông tin trên Internet:**

**2.3.2.2.1 Thư điện tử (Mail):**

Dịch vụ thư tín điện tử (Email) giúp ta gửi thông tin đến mọi người nếu ta có địa chỉ thư điện tử của họ. Trên Internet thư điện tử không chỉ đến với những người nối trực tiếp vào Internet mà có thể đến cả với những người không nối trực tiếp vào Internet. Những người không nối trực tiếp vào mạng vào Internet thường là thành viên của một số mạng thương mại như CompuServe, American Online,.... Số lượng người sử dụng thư điện tử lên tới hàng chục triệu người, do vậy dịch vụ thư điện tử đóng một vai trò hết sức quan trọng.

**2.3.2.2.2 Truyền file (FTP):**

FTP (File Tranfer Protocol) là một dịch vụ tốt và có hiệu quả để lấy tệp từ các máy tính khác trên mạng. Việc này cũng giống như việc đăng nhập vào một máy tính nhưng nó giới hạn người sử dụng bằng một số lệnh giới hạn đối với những người sử dụng mạo danh.

FTP hỗ trợ tất cả các dạng tệp, ta có thể tạo ra các văn bản mã ACSII, Portscript hoặc tài liệu PCL, hay các phần mềm dưới dạng nhị phân. FTP giúp cho việc chia sẻ dữ liệu và tài nguyên mạng trở nên dễ dàng.Đây là một dịch vụ hết sức quan trọng trong Internet.

**2.3.2.2.3 Truy cập từ xa (Telnet):**

Telnet là dịch vụ có trong bất cứ hệ điều hành nào do vậy chúng được sử dụng ngay lúc chúng ra đời. Telnet cho phép bạn đăng nhập vào hệ thống từ một thiết bị đầu cuối nào trên mạng. Nó sử dụng để cung cấp các dịch vụ của Internet hoàn toàn giống như bạn quay số để nối trực tiếp vào Internet bằng modem.

**2.3.2.2.4 *World Wide Web:***

World Wide Web (WWW) hay Web là một dịch vụ mới nhất và có hiệu quả nhất trên Internet. WWW với những đặc trưng của riêng nó cùng với tổ hợp các dịch vụ thông tin đã biến nó trở thành một dịch vụ rất hữu ích nhưng lại rất dễ hiểu.

Tài liệu WWW được viết bằng ngôn ngữ HTML (HyperText Markup Language) hay còn gọi là ngôn ngữ siêu văn bản. Dưới dạng nguyên thủy nó giống như văn bản bình thường nhưng nó có thêm một số lệnh định dạng. HTML bao gồm nhiều cách liên kết với các tài nguyên FTP, Gopher server, WAIS server và Web server. Web server trao đổi các tài liệu HTML bằng giao thức HTTP (HyperText Transfer Protocol) hay gọi là giao thức truyền siêu văn bản.

Việc dịch vụ WWW có thể cho phép kết nối các thông tin trên quy mô lớn, sử dụng đơn giản đã giúp nó trở thành một dịch vụ quan trọng trên Internet. Tài liệu HTML có khả năng cung cấp các nội dung có giá trị và các thông tin bổ ích, đơn giản. Chỉ cần một lần kích chuột là có thể truy nhập vào các Server thông tin ở bất cứ đâu.

**PHẦN II : CÁC CHÍNH SÁCH BẢO MẬT**

**CHƯƠNG 3: TỔNG QUAN VỀ BẢO MẬT**

**3.1 Định nghĩa bảo mật mạng:**

Bảo mật mạng là sự đảm bảo an toàn của toàn bộ hệ thống mạng trước những hoạt động nhằm tấn công phá hoại hệ thống mạng cả từ bên trong như bên ngoài.

Hoạt động phá hoại là những hoạt động như xâm nhập trái phép sử dụng tài nguyên trái phép ăn cắp thông tin, các hoạt động giả mạo nhằm phá hoại tài nguyên mạng và cơ sở dữ liệu của hệ thống.

Vấn đề bảo mật mạng luôn là một vấn đề bức thiết khi ta nghiên cứu một hệ thống mạng. Hệ thống mạng càng phát triển thì vấn đề bảo mật mạng càng được đạt lên hàng đầu.

Khi nguyên cứu một hệ thống mạng chúng ta cần phải kiểm soát vấn đề bảo mật mạng ở các cấp độ sau:

* Mức mạng: Ngăn chặn kẻ xâm nhập bất hợp pháp vào hệ thống mạng.
* Mức server: Kiểm soát quyền truy cập, các cơ chế bảo mật, quá trình nhận dạng người dùng, phân quyền truy cập, cho phép các tác vụ
* Mức cơ sở dữ liệu: Kiểm soát ai? được quyền như thế nào? với mỗi cơ sở dữ liệu.
* Mức trường thông tin: Trong mỗi cơ sở dữ liệu kiểm soát được mỗi trường dữ liệu chứa thông tin khác nhau sẽ cho phép các đối tượng khác nhau có quyền truy cập khác nhau.
* Mức mật mã: Mã hoá toàn bộ file dữ liệu theo một phương pháp nào đó và chỉ cho phép người có “ chìa khoá” mới có thể sử dụng được file dữ liệu.

Theo quan điểm hệ thống, một xí nghiệp (đơn vị kinh tế cơ sở) được thiết lập từ ba hệ thống sau:

* Hệ thống thông tin quản lý.
* Hệ thống trợ giúp quyết định.
* Hệ thống các thông tin tác nghiệp.

Trong đó hệ thống thông tin quản lý đóng vai trò trung gian giữa hệ thống trợ giúp quyết định và hệ thống thông tin tác nghiệp với chức năng chủ yếu là thu thập, xử lý và truyền tin.



Hình 3.1 Sơ đồ mạng thông dụng hiện nay.

**3.1.1. Các yếu tố cần quan tâm khi phân tích bảo mật mạng:**

Vấn đề con người: Trong bảo mật mạng yếu tố con người cũng rất quan trọng. Khi nghiên cứu đến vấn đề bảo mật mạng cần quan tâm xem ai tham gia vào hệ thống mạng, họ có tránh nhiệm như thế nào. Ở mức độ vật lý khi một người không có thẩm quyền vào phòng máy họ có thể thực hiện một số hành vi phá hoại ở mức độ vật lý.

Kiến trúc mạng: Kiến trúc mạng cũng là một vấn đề mà chúng ta cần phải quan tâm khi nghiên cứu, phân tích một hệ thống mạng. Chúng ta cần nghiên cứu hiện trạng mạng khi xây dựng và nâng cấp mạng đưa ra các kiểu kiến trúc mạng phù hợp với hiện trạng và cơ sở hạ tầng ở nơi mình đang định xây dựng….

Phần cứng và phần mềm:

Mạng được thiết kế như thế nào. Nó bao gồm những phần cứng và phần mềm nào và tác dụng của chúng. Xây dựng một hệ thống phần cứng và phần mềm phù hợp với hệ thống mạng cũng là vấn đề cần quan tâm khi xây dựng hệ thống mạng. Xem xét tính tương thích của phần cứng và phần mềm với hệ thống và tính tương thích giữu chúng.

**3.1.2. Các yếu tố cần được bảo vệ**

- Bảo vệ dữ liệu (tính bảo mật tính toàn vẹn và tính kíp thời).

- Bảo vệ tài nguyên sử dụng trên mạng để tránh sử dụng tài nguyên này vào mục đính tấn công của kẻ khác.

- Bảo vệ danh tiếng.

**3.2. Các kiểu tấn công mạng**

Cùng với sự phát triển nhanh chóng của mạng thì nó cũng để lại nhiều lỗ hổng để hacker có thể tấn công. Các thủ đoạn tấn công ngày càng trở nên tinh vi hơn. Các phương pháp tấn công thường gặp là :

* + 1. **Thăm dò(reconnaissance):**

Đó chính là hình thức hacker gửi vài thông tin truy vấn về địa chỉ IP hoặc domain name bằng hình thức này hacker có thể lấy được thông tin về địa chỉ IP và domain name từ đó thực hiện các biện pháp tấn công khác…

* + 1. **Packet sniffer:**

Packet sniffer là phần mềm sử dụng NIC card ở chế độ “promisscuous” để bắt tất cả các gói tin trong cùng miền xung đột. Nó có thể khai thác thông tin dưới dạng clear Text.

* + 1. **Đánh lừa (IP spoofing):**

Kỹ thuật này được sử dụng khi hacker giả mạo địa chỉ IP tin cậy trong mạng nhằm thực hiện việc chèn thông tin bất hợp pháp vào trong phiên làm việc hoặc thay đổi bản tin định tuyến để thu nhận các gói tin cần thiết.

* + 1. **Tấn công từ chối dịch vụ (Denial of services):**

Kiểu tấn công này nhằm tắc nghẽn mạng bằng cách hacker gửi các gói tin với tốc độ cao và liên tục tới hệ thống bảo mật nhằm làm tê liện hệ thống chiếm hết băng thông sử dụng.

* + 1. **Tấn công trực tiếp password:**

Đó là kiểu tấn công trực tiếp vào username và password của người sử dụng nhằm ăn cắp tài khoải sử dụng vào mục đích tấn công. Hacker dùng phần mềm để tấn công (vị dụ như Dictionary attacks).

* + 1. **Thám thính(agent):**

Hacker sử dụng các các phần mềm vius, trojan thường dùng để tấn công vào máy trạm làm bước đệm để tấn công vào máy chủ và hệ thống. Kẻ tấn công có thể nhận được các thông tin hữu ích từ máy nạn nhân thông qua các dịch vụ mạng.

* + 1. **. Tấn công vào yếu tố con người:**

Hacker có thể tấn công vào các lỗ hổng do lỗi nhà quản trị hệ thống hoặc liên lạc với nhà quản trị hệ thống giả mạo là người sủ dụng thay đổi username và password.

* 1. **Các mức độ bảo mật:**

Khi phân tích hệ thống bảo mật mạng người ta chia ra làm các muác độ an toàn sau:

**Bức tường lửa (Firewall)**

**Bảo vệ vật lý (Physical Protect)**

**Mã hóa dữ liệu(Data Encryption)**

**Đăng nhập/Mật khẩu(Login/Password)**

**Quyền truy nhập (Access Right)**

**Thông tin (Information)**

Hình 3.3 Các mức độ bảo mật

* + 1. **Quyền truy nhập:**

Đây là lớp bảo vệ sâu nhất nhằm kiểm soát tài nguyên mạng kiểm soát ở mức độ file và việc xác định quyền hạn của người dùng do nhà quản trị quyết định như: chỉ đọc( only read), chỉ ghi (only write), thực thi(execute).

* + 1. **Đăng nhập/Mật khẩu(login/password):**

Đây là lớp bảo vệ mức độ truy nhập thông tin ở mức độ hệ thống. Đây là mức độ bảo vệ được sử dụng phổ biến nhất vì nó đơn giản và ít tốn kém. Nhà quản trị cung cấp cho mỗi người dùng một username và password và kiểm soát mọi hoạt động của mạng thông qua hình thức đó. Mỗi lần truy nhập mạng người dùng phải đăng nhập nhập username và password hệ thống kiểm tra thấy hợp lệ mới cho đăng nhập.

* + 1. **Mã hóa dữ liệu(Data encryption):**

Đó là sử dụng các phương pháp mã hoá dữ liệu ở bên phát và thực hiện giải mã ở bên thu bên thu chỉ có thể mã hóa chính xác khi có khoá mã hóa do bên phát cung cấp.

* + 1. **Bảo vệ vật lý (Physical protect):**

Đây là hình thức ngăn chạn nguy cơ truy nhập vật lý bất hợp pháp vào hệ thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khoá máy tính, hoặc cài đặt cơ chế báo động khi có truy nhập vào hệ thống ...

* + 1. **Bức tường lửa (firewall):**

Đây là hình thức ngăn chặn sự xâm nhập bất hợp pháp vào mạng nội bộ thông qua firewall. Chức năng của tường lửa là ngăn chặn các truy nhập trái phép (theo danh sách truy nhập đã xác định trước) và thậm chí có thể lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó. Phương thức bảo vệ này được dùng nhiều trong môi trường liên mạng Internet.

* 1. **Các biện pháp bảo vệ an toàn hệ thống:**

Đối với mỗi hệ thống mạng, không nên cài đặt và chỉ sử dụng một chế độ an toàn cho dù nó có thể rất mạnh, mà nên lắp đặt nhiều cơ chế an toàn khác nhau để chúng có thể hỗ trợ lẫn nhau và có thể đẳm bảo an toàn ở mức độ cao.

* + 1. **Quyền hạn tối thiểu (Least Privilege):**

Một nguyên tắc cơ bản nhất của an toàn nói chung là trao quyền tối thiểu. Có nghĩa là: Bất kỳ một đối tượng nào trên mạng chỉ nên có những quyền hạn nhất định mà đối tượng đó cần phải có để thực hiện các nhiệm vụ của mình và chỉ có những quyền đó mà thôi. Như vậy, mọi người sử dụng đều không nhất thiết được trao quyền truy nhập mọi dich vụ Internet, đọc và sửa đổi tất cả các file trong hệ thống… Người quản trị hệ thống không nhất thiết phải biết các mật khẩu root hoặc mật khẩu của mọi người sử dụng …

Nhiều vấn đề an toàn trên mạng Internet bị xem là thất bại khi thực hiện nguyên tắc Quyền hạn tối thiểu. Vì vậy, các chương trình đặc quyền phải được đơn giản đến mức có thể và nếu một chương trình phức tạp, ta phải tìm cách chia nhỏ và cô lập từng phần mà nó yêu cầu quyền hạn.

* + 1. **Bảo vệ theo chiều sâu (Defense in Depth):**

Đối với mỗi hệ thống, không nên cài đặt và chỉ sử dụng một chế độ an toàn cho dù nó có thể rất mạnh, mà nên lắp đặt nhiều cơ chế an toàn để chúng có thể hỗ trợ lẫn nhau.

* + 1. **Nút thắt (choke point):**

Một nút thắt bắt buộc những kẻ đột nhập phải đi qua một lối hẹp mà chúng ta có thể kiểm soát và điều khiển được. Trong cơ chế an toàn mạng, Firewall nằm giữa hệ thống mạng của ta và mạng Internet, nó chính là một nút thắt. Khi đó, bất kỳ ai muốn truy nhập vào hệ thống cũng phải đi qua nó, vì vậy, ta có thể theo dõi, quản lý được.

Nhưng một nút thắt cũng sẽ trở nên vô dụng nếu có một đường khác vào hệ thống mà không cần đi qua nó (trong môi trường mạng, còn có những đường Dial–up không được bảo vệ khác có thể truy nhập được vào hệ thống)

* + 1. **Điểm xung yếu nhất (Weakest point):**

Một nguyên tắc cơ bản khác của an toàn là: “Một dây xích chỉ chắc chắn khi mắt nối yếu nhất được làm chắc chắn”. Khi muốn thâm nhập vào hệ thống của chúng ta, kẻ đột nhập thường tìm điểm yếu nhất để tấn công vào đó. Do vậy, với từng hệ thống, cần phải biết điểm yếu nhất để có phương án bảo vệ.

* + 1. **Hỏng trong an toàn (Fail–Safe Stance):**

Nếu một hệ thống chẳng may bị hỏng thì nó phải được hỏng theo một cách nào đó để ngăn chặn những kẻ lợi dụng tấn công vào hệ thống hỏng đó. Đương nhiên, việc hỏng trong an toàn cũng hủy bỏ sự truy nhập hợp pháp của người sử dụng cho tới khi hệ thống được khôi phục lại.

Nguyên tắc này cũng được áp dụng trong nhiều lĩnh vực. Chẳng hạn, cửa ra vào tự động được thiết kế để có thể chuyển sang mở bằng tay khi nguồn điện cung cấp bị ngắt để tránh giữ người bên trong.

Dựa trên nguyên tắc này, người ta đưa ra hai quy tắc để áp dụng vào hệ thống an toàn:

- Default deny Stance: Chú trọng vào những cái được phép và ngăn chặn tất cả những cái còn lại.

- Default permit Stance: Chú trọng vào những cái bị ngăn cấm và cho phép tất cả những cái còn lại. Những gì không bị ngăn cấm thì được phép.

Theo quan điểm về vấn đề an toàn trên thì nên dùng quy tắc thứ nhất, còn theo quan điểm của các nhà quản lý thì lại là quy tắc thứ hai.

* + 1. **Sự tham gia toàn cầu:**

Để đạt được hiệu quả an toàn cao, tất cả các hệ thống trên mạng toàn cầu phải tham gia vào giải pháp an toàn. Nếu tồn tại một hệ thống có cơ chế an toàn kém, người truy nhập bất hợp pháp có thể truy nhập vào hệ thống này và sau đó dùng chính hệ thống này để truy nhập vào các hệ thống khác.

* + 1. **Kết hợp nhiều biện pháp bảo vệ:**

Trên liên mạng, có nhiều loại hệ thống khác nhau được sử dụng, do vậy, phải có nhiều biện pháp bảo vệ để đảm bảo chiến lược bảo vệ theo chiều sâu. Nếu tất cả các hệ thống của chúng ta đều giống nhau và một người nào đó biết cách thâm nhập vào một hệ thống thì cũng có thể thâm nhậo được vào các hệ thống khác.

* + 1. **Đơn giản hóa:**

Nếu ta không hiểu một cái gì đó, ta cũng không thể biết được liệu nó có an toàn hay không. Chính vì vậy, ta cần phải đơn giản hóa hệ thống để có thể áp dụng các biện pháp an toàn một cách hiệu quả hơn.

* 1. **Các chính sách bảo mật:**

Kế hoạch an toàn thông tin phải tính đến các nguy cơ từ bên ngoài và từ trong nội bộ, đồng thời phải kết hợp cả các biện pháp kỹ thuật và các biện pháp quản lý. Sau đây là các bước cần tiến hành:

• Xác định các yêu cầu và chính sách an toàn thông tin: Bước đầu tiên trong kế hoạch an toàn thông tin là xác định các yêu cầu truy nhập và tập hợp những dịch vụ cung cấp cho người sử dụng trong và ngoài cơ quan, trên cơ sở đó có được các chính sách tương ứng.

• Thiết kế an toàn vòng ngoài: Việc thiết kế dựa trên các chính sách an toàn được xác định trước. Kết quả của bước này là kiến trúc mạng cùng với các thành phần phần cứng và phần mềm sẽ sử dụng. Trong đó cần đặc biệt chú ý hệ thống truy cập từ xa và cơ chế xác thực người dùng.

• Biện pháp an toàn cho các máy chủ và máy trạm: Các biện pháp an toàn vòng ngoài, dù đầy đủ đến đâu, cũng có thể không đủ để chống lại sự tấn công, đặc biệt là sự tấn công từ bên trong. Cần phải kiểm tra các máy chủ và máy trạm để phát hiện những sơ hở về bảo mật. Đối với Filewall và các máy chủ ở ngoài cần kiểm tra những dạng tấn công (denial of service).

• Kiểm tra thường kỳ: Cần có kế hoạch kiểm tra định kỳ toàn bộ hệ thống an toàn thông tin, ngoài ra cần kiểm tra lại mỗi khi có sự thay đổi về cấu hình.

* + 1. **Kế hoạch bảo mật mạng:**

Có một chính sách bảo mật mạng đúng đắn và hiệu quả để có thể bảo vệ các thông tin, các tài nguyên của một công ty, tổ chức nói riêng hay của một bộ, ngành, của một quốc gia nói chung là vấn đề hết sức quan trọng. Nếu như các tài nguyên và thông tin mà công ty đó có trên mạng là đáng được bảo vệ thì một chính sách bảo mật mạng là đáng được thực hiện. Hầu hết các cơ quan đều có các thông tin nhạy cảm và các bí mật cạnh tranh trên mạng máy tính của họ, vì vậy chúng ta sẽ cần một chính sách bảo mật mạnng đề bảo vệ tài nguyên và thông tin của công ty.

Để có một chính sách bảo mật mạng hiệu quả thì chúng ta phải trả lời được câu hỏi: loại dịch vụ nào, loại tài nguyên nào người dùng được phép truy nhập và loại nào thì bị cấm?

* + 1. **Chính sách bảo mật nội bộ:**

Một tổ chức có thể có nhiều bộ phận ở nhiều nơi, mỗi bộ phận có mạng riêng. Nếu tổ chức lớn thì mỗi mạng phải có ít nhất một người quản trị mạng. Nếu các nơi không nối với nhau thành mạng nội bộ thì chính sách an ninh cũng có những điểm khác nhau.

Thông thường thì tài nguyên mạng ở mỗi nơi bao gồm:

• Các trạm làm việc

• Các thiết bị kết nối: Gateway, Router, Bridge, Repeater

• Các Server

• Phần mềm mạng và phần mềm ứng dụng

• Cáp mạng

• Thông tin trong các tệp và các CSDL

Chính sách an ninh tại chỗ phải cân nhắc đến việc bảo vệ các tài nguyên này. Đồng thời cũng phải cân nhắc giữa các yêu cầu an ninh với các yêu cầu kết nối mạng bởi vì một chính sách bảo vệ tốt cho mạng này lại bất lợi cho mạng khác.

* + 1. **Phương thức thiết kế:**

Tạo ra một chính sách mạng có nghĩa là lập lên các thủ tục và kế hoạch bảo vệ tài nguyên của chúng ta khỏi mất mát và hư hại. Một hướng tiếp cận khả thi là trả lời các câu hỏi sau :

• Chúng ta muốn bảo vệ tài nguyên nào ?

• Chúng ta cần bảo vệ tài nguyên trên khỏi những người nào ?

• Có các mối đe doạ như thế nào ?

• Tài nguyên quan trọng tới mức nào ?

• Chúng ta sẽ dùng cách nào để bảo vệ tài nguyên theo cách tiết kiệm và hợp lý nhất

• Kiểm tra lại chính sách theo chu kỳ nào để phù hợp với các thay đổi về mục đích cũng như về hiện trạng của mạng ?

* + 1. **Thiết kế chính sách bảo mật mạng:**
       1. **Phân tích nguy cơ mất an ninh:**

Trước khi thiết lập chính sách ta cần phải biết rõ tài nguyên nào cần được bảo vệ, tức là tài nguyên nào có tầm quan trọng lớn hơn để đi đến một giải pháp hợp lý về kinh tế. Đồng thời ta cũng phải xác định rõ đâu là nguồn đe doạ tới hệ thống. Nhiều nghiên cứu cho thấy rằng, thiệt hại do những kẻ “đột nhập bên ngoài” vẫn còn nhỏ hơn nhiều so với sự phá hoại của những “người bên trong”. Phân tích nguy cơ bao gồm những việc :

• Ta cần bảo vệ những gì ?

• Ta cần bảo vệ những tài nguyên khỏi những gì ?

• Làm thế nào để bảo vệ ?

* + - 1. **Xác định tài nguyên cần bảo vệ:**

Khi thực hiện phân tích ta cũng cần xác định tài nguyên nào có nguy cơ bị xâm phạm. Quan trọng là phải liệt kê được hết những tài nguyên mạng có thể bị ảnh hưởng khi gặp các vấn đề về an ninh.

* Phần cứng: Vi xử lý, bản mạch, bàn phím, terminal, trạm làm việc, máy tính các nhân, máy in, ổ đĩa, đường liên lạc, server, router
* Phần mềm: Chương trình nguồn, chương trình đối tượng, tiện ích, chương trình khảo sát, hệ điều hành, chương trình truyền thông.
* Dữ liệu: Trong khi thực hiện, lưu trữ trực tuyến, cất giữ off–line, backup, các nhật ký kiểm tra, CSDL truyền trên các phương tiện liên lạc.
* Con người: Người dùng, người cần để khởi động hệ thống.
* Tài liệu: Về chương trình , về phần cứng, về hệ thống, về thủ tục quản trị cục bộ.
* Nguồn cung cấp: giấy in, các bảng biểu, băng mực, thiết bị từ.
  + - 1. **Xác định các mối đe dọa bảo mật mạng:**

Sau khi đã xác định những tài nguyên nào cần được bảo vệ, chúng ta cũng cần xác định xem có các mối đe doạ nào nhằm vào các tài nguyên đó. Có thể có những mối đe dọa sau:

* **Truy nhập bất hợp pháp:**

Chỉ có những người dùng hợp pháp mới có quyền truy nhập tài nguyên mạng, khi đó ta gọi là truy nhập hợp pháp. Có rất nhiều dạng truy nhập được gọi là bất hợp pháp chẳng hạn như dùng tài khoản của người khác khi không được phép. Mức độ trầm trọng của việc truy nhập bất hợp pháp tuỳ thuộc vào bản chất và mức độ thiệt hại do truy nhập đó gây nên.

* **Để lộ thông tin:**

Để lộ thông tin do vô tình hay cố ý cũng là một mối đe dọa khác. Chúng ta nên định ra các giá trị để phản ánh tầm quan trọng của thông tin. Ví dụ đối với các nhà sản xuất phần mềm thì đó là: mã nguồn, chi tiết thiết kế, biểu đồ, thông tin cạnh tranh về sản phẩm... Nếu để lộ các thông tin quan trọng, tổ chức của chúng ta có thể bị thiệt hại về các mặt như uy tín, tính cạnh tranh, lợi ích khách hàng ...

* **Từ chối cung cấp dịch vụ:**

Mạng thường gồm những tài nguyên quý báu như máy tính, CSDL ... và cung cấp các dịch vụ cho cả tổ chức. Đa phần người dùng trên mạng đều phụ thuộc vào các dịch vụ để thực hiện công việc được hiệu quả.

Chúng ta rất khó biết trước các dạng từ chối của một dịch vụ. Có thể tạm thời liệt kê ra một số lỗi mạng bị từ chối: do một gói gay lỗi, do quá tải đường truyền, router bị vô hiệu hóa, do virus…

* + - 1. **Xác định trách nhiệm người sử dụng mạng:**
  + **Ai được quyền dùng tài nguyên mạng:**

Ta phải liệt kê tất cả người dùng cần truy nhập tới tài nguyên mạng. Không nhất thiết liệt kê toàn bộ người dùng. Nếu phân nhóm cho người dùng thì việc liệt kê sẽ đơn giản hơn. Đồng thời ta cũng phải liệt kê một nhóm đặc biệt gọi là các người dùng bên ngoài, đó là những người truy nhập từ một trạm đơn lẻ hoặc từ một mạng khác.

* + **Sử dụng tài nguyên thế nào cho đúng:**

Sau khi xác định những người dùng được phép truy nhập tài nguyên mạng, chúng ta phải tiếp tục xác định xem các tài nguyên đó sẽ được dùng như thế nào. Như vậy ta phải đề ra đường lối cho từng lớp người sử dụng như: Những nhà phát triển phần mềm, sinh viên, những người sử dụng ngoài.

* + **Ai có quyền cấp phát truy nhập:**

Chính sách an ninh mạng phải xác định rõ ai có quyền cấp phát dịch vụ cho người dùng. Đồng thời cũng phải xác định những kiểu truy nhập mà người dùng có thể cấp phát lại. Nếu đã biết ai là người có quyền cấp phát truy nhập thì ta có thể biết được kiểu truy nhập đó được cấp phát, biết được người dùng có được cấp phát quá quyền hạn không. Ta phải cân nhắc hai điều sau:

* Truy nhập dịch vụ có được cấp phát từ một điểm trung tâm không?
* Phương thức nào được dùng để tạo tài khoản mới và kết thúc truy nhập?

Nếu một tổ chức lớn mà không tập trung thì tất nhiên là có nhiều điểm trung tâm để cấp phát truy nhập, mỗi điểm trung tâm phải chịu trách nhiệm cho tất cả các phần mà nó cấp phát truy nhập.

* + **Người dùng có quyền hạn và trách nhiệm gì:**

Cần phải xác định rõ quyền lợi và nghĩa vụ của người sử dụng nhằm đảm bảo cho việc quản lý và hoạt động bình thường của mạng. Đảm bỏa tính minh bạch và riêng tư cho người dùng, cũng như người dùng phải có trách nhiệm bảo tài khoản của mình.

* + **Người quản trị hệ thống có quyền hạn và trách nhiệm gì:**

Người quản trị hệ thống thường xuyên phải thu thập thông tin về các tệp trong các thư mục riêng của người dùng để tìm hiểu các vấn đề hệ thống. Ngược lại, người dùng phải giữ gìn bí mật riêng tư về thông tin của họ. Nếu an ninh có nguy cơ thì người quản trị phải có khả năng linh hoạt để giải quyết vấn đề.

* + **Làm gì với các thông tin quan trọng:**

Theo quan điểm an ninh, các dữ liệu cực kỳ quan trọng phải được hạn chế, chỉ một số ít máy và ít người có thể truy nhập. Trước khi cấp phát truy nhập cho một người dùng, phải cân nhắc xem nếu anh ta có khả năng đó thì anh ta có thể thu được các truy nhập khác không. Ngoài ra cũng phải báo cho người dùng biết là dịch vụ nào tương ứng với việc lưu trữ thông tin quan trọng của anh ta.

* + - 1. **Kế hoạch hành động khi chính sách bị vi phạm:**

Mỗi khi chính sách bị vi phạm cũng có nghĩa là hệ thống đứng trước nguy cơ mất an ninh. Khi phát hiện vi phạm, chúng ta phải phân loại lý do vi phạm chẳng hạn như do người dùng cẩu thả, lỗi hoặc vô ý, không tuân thủ chính sách...

* + **Phản ứng khi có vi phạm:**

Khi vi phạm xảy ra thì mọi người dùng có trách nhiệm đều phải liên đới. Ta phải định ra các hành động tương ứng với các kiểu vi phạm. Đồng thời mọi người đều phải biết các quy định này bất kể người trong tổ chức hoặc người ngoài đến sử dụng máy. Chúng ta phải lường trước trường hợp vi phạm không cố ý để giải quyết linh hoạt, lập các sổ ghi chép và định kỳ xem lại để phát hiện các khuynh hướng vi phạm cũng như để điều chỉnh các chính sách khi cần.

* + **Phản ứng khi người dùng cục bộ vi phạm:**

Người dùng cục bộ có các vi phạm sau:

* Vi phạm chính sách cục bộ.
* Vi phạm chính sách của các tổ chức khác.

Trường hợp thứ nhất chính chúng ta, dưới quan điểm của người quản trị hệ thống sẽ tiến hành việc xử lý. Trong trường hợp thứ hai phức tạp hơn có thể xảy ra khi kết nối Internet, chúng ta phải xử lý cùng các tổ chức có chính sách an ninh bị vi phạm.

* + **Chiến lược phản ứng:**

Chúng ta có thể sử dụng một trong hai chiến lược sau:

* Bảo vệ và xử lý.
* Theo dõi và truy tố.

Trong đó, chiến lược thứ nhất nên được áp dụng khi mạng của chúng ta dễ bị xâm phạm. Mục đích là bảo vệ mạng ngay lập tức xử lý, phục hồi về tình trạng bình thường để người dùng tiếp tục sử dụng được, như thế ta phải can thiệp vào hành động của người vi phạm và ngăn cản không cho truy nhập nữa. Đôi khi không thể khôi phục lại ngay thì chúng ta phải cách ly các phân đoạn mạng và đóng hệ thống để không cho truy nhập bất hợp pháp tiếp tục.

* + - 1. **Xác định các lỗi an ninh:**

Ngoài việc nêu ra những gì cần bảo vệ, chúng ta phải nêu rõ những lỗi gì gây ra mất an ninh và làm cách nào để bảo vệ khỏi các lỗi đó. Trước khi tiến hành các thủ tục an ninh, nhất định chúng ta phải biết mức độ quan trọng của các tài nguyên cũng như mức độ của nguy cơ.

1. **Lỗi điểm truy nhập:**

Lỗi điểm truy nhập là điểm mà những người dùng không hợp lệ có thể đi vào hệ thống, càng nhiều điểm truy nhập càng có nguy có mất an ninh.

1. **Lỗi cấu hình hệ thống:**

Khi một kẻ tấn công thâm nhập vào mạng, hắn thường tìm cách phá hoại các máy trên hệ thống. Nếu các máy được cấu hình sai thì hệ thống càng dễ bị phá hoại. Lý do của việc cấu hình sai là độ phức tạp của hệ điều hành, độ phức tạp của phần mềm đi kèm và hiểu biết của người có trách nhiệm đặt cấu hình. Ngoài ra, mật khẩu và tên truy nhập dễ đoán cũng là một sơ hở để những kẻ tấn công có cơ hội truy nhập hệ thống.

1. **Lỗi phần mềm:**

Phần mềm càng phức tạp thì lỗi của nó càng phức tạp. Khó có phần mềm nào mà không gặp lỗi. Nếu những kẻ tấn công nắm được lỗi của phần mềm, nhất là phần mềm hệ thống thì việc phá hoại cũng khá dễ dàng. Người quản trị cần có trách nhiệm duy trì các bản cập nhật, các bản sửa đổi cũng như thông báo các lỗi cho người sản xuất chương trình.

1. **Lỗi người dùng nội bộ:**

Người dùng nội bộ thường có nhiều truy nhập hệ thống hơn những người bên ngoài, nhiều truy nhập tới phần mềm hơn phần cứng do đó đễ dàng phá hoại hệ thống. Đa số các dịch vụ TCP/IP như Telnet, tfp, … đều có điểm yếu là truyền mật khẩu trên mạng mà không mã hoá nên nếu là người trong mạng thì họ có khả năng rất lớn để có thể dễ dàng nắm được mật khẩu với sự trợ giúp của các chương trình đặc biệt.

1. **Lỗi an ninh vật lý:**

Các tài nguyên trong các trục xương sống (backbone), đường liên lạc, Server quan trọng ... đều phải được giữ trong các khu vực an toàn về vật lý. An toàn vật lý có nghĩa là máy được khoá ở trong một phòng kín hoặc đặt ở những nơi người ngoài không thể truy nhập vật lý tới dữ liệu trong máy.

1. **Lỗi bảo mật:**

Bảo mật mà chúng ta hiểu ở đây là hành động giữ bí mật một điều gì, thông tin rất dễ lộ ra trong những trường hợp sau:

* + Khi thông tin lưu trên máy tính.
  + Khi thông tin đang chuyển tới một hệ thống khác.
  + Khi thông tin lưu trên các băng từ sao lưu.

**CHƯƠNG 4: TỔNG QUAN VỀ FIREWALL**

* 1. **Firewall:**
     1. **Khái niệm:**

Firewall hiểu một cách chung nhất là cơ cấu để bảo vệ một mạng máy tính chống lại sự truy nhập bất hợp pháp từ các (mạng) máy tính khác. Firewall bao gồm các cơ cấu nhằm:

• Ngăn chặn truy nhập bất hợp pháp.

• Cho phép truy nhập sau khi đã kiểm tra tính xác thực của thực thể yêu cầu truy nhập.

Trên thực tế, Firewall được thể hiện rất khác nhau: bằng phần mềm hoặc phần cứng chuyên dùng, sử dụng một máy tính hoặc một mạng các máy tính. Theo William Cheswick và Steven Beilovin thì bức tường lửa có thể được xác định như là một tập hợp các cấu kiện đặt giữa hai mạng.

Nhìn chung bức tường lửa có những thuộc tính sau :

* Thông tin giao lưu được theo hai chiều.
* Chỉ những thông tin thoả mãn nhu cầu bảo vệ cục bộ mới được đi qua.
* Bản thân bức tường lửa không đòi hỏi quá trình thâm nhập.

**4.1.2. Chức năng:**

**Ưu điểm:**

- Firewall có thể bảo vệ hệ thống máy tính chống lại những kẻ đột nhập qua khả năng ngăn chặn những phiên làm việc từ xa (remote login).

- Ngăn chặn thông tin từ bên ngoài (Internet) vào trong mạng được bảo vệ, trong khi cho phép người sử dụng hợp pháp được truy nhập tự do mạng bên ngoài.

- Firewall ngăn chặn các dịch vụ ít tin cậy.

- Truy nhập có điều khiển đến từng host.

- Tập trung hóa chính sách bảo mật

- Xác nhận người dùng và lưu trữ thông tin.

**Hạn chế:**

• Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

• Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không “đi qua” nó. Một cách cụ thể, Firewall không thể chống lại một cuộc tấn công từ một đường dial–up, hoặc sự mất mát thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

• Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data–drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua Firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

• Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của Firewall (một ví dụ là các virus máy tính).

**4.2. Phân loại**

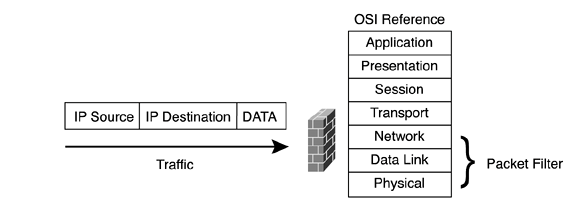
Các công ty như CISCO và các nhà cung cấp khác đã đưa ra vô số sản phẩm Firewall, chúng có khả năng hiển thị các đường truyền với các kỹ thuật khác nhau. Một số loại Firewall ngày nay có khả năng ngăn chặn các gói dữ liệu đẩy lên lớp 4(TCP layer). Một số khác cũng có khả năng ngăn chặn tất cả các lớp và được xem như là *deep packet firewalls.* Có 3 kiểu phương thức ngăn chặn là:

* Packet filtering and stateless filtering
* Stateful filtering
* Deep packet layer inspection

Packet filters (basic access-list filters on routers) là block ngay lập tức.Sau đây giới thiệu về proxy Server no có khả năng kiểm soát các sự tấn công từ thiết bị độc lập. Prixy server là một Server được đặt ở giữa các client ứng dụng như Web browser và real server.

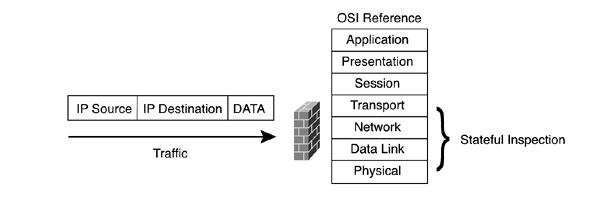
Nó chặn tất cả các request tới realserver với cái nhìn nếu nó có thể đáp ứng các request của bản thân nó. Nếu không, nó chuyển các request tới real server. Proxy yêu cầu kết nối tới internet căn cứ vào các yêu cầu từ nội bộ hoặc các nguồi ẩn. Proxy server là các ứng dụng cơ bản, chậm và khó quản lý đối với một mạng IP lớn. Thế hệ tiếp theo của Packet filter là stateless Firewalls. Vấn đề cơ bản là stateless firewall cho phép chỉ nhận một gói thông tin nó là căn cứ trong địa chỉ và cổng nguồn từ mạng có thật.

Stateless firewall được đưa ra việc cộng thêm sự linh hoạt và cơ động tới khả năng cấu hình mạng. Stateless firewall ngăn chặn các thông tin cơ bản về địa chỉ nguồn và địa chỉ đích. Hìn 4.2 giới thiệu khả năng ngăn chặn chiều sâu của lọc gói tin và stateless Firewall. Các gói tin được ngăn chặn ở lớp 3 trong mô hình OSI mô hình phân lớp mạng. Bởi vậy stateless Firewall có khả năng ngăn chặn các địa chỉ IP nguồn và đích và các giao thức cổng nguồn và đích.



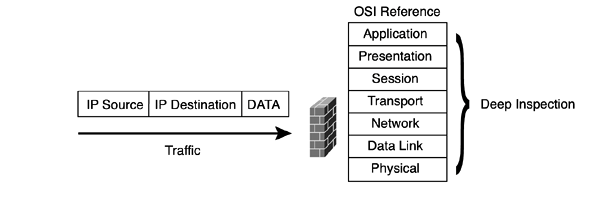
Hình 4.2.a: Stateless Firewall

Statefull firewall giới hạn thông tin mạng từ địa chỉ cơ bản nguồn và đíchtrong địa chỉ IP nguồn, đích, cổng nguồn TCP/UDP, cổng đích TCP/UDP.Statefull firewall cũng có thể ngăn chặn nội dung dữ liệu và kiểm tra các giao thức bất thường về giao thức.Ví dụ như statefull firewall có thể trang bị tốt hơn proxy server hoặc packet filter trong việc phát hiện và dừng các tấn công từ chối dịch vụ. Bởi vì địa chỉ nguồn và đích biến đổi, dữ liệu được cho phép thông qua nơi xát thực hoặc được cố gắng chắn lại trong mạng. Statefull firewall có thể ngăn chặn từ lớp 4 trong mô hình OSI :



Hình 4.2.b: Stateful Firewall

Cùng với sự ngăn chặn lớp gói tin chiều sâu, firewall còn ngăn chặn các thông tin từ nguồn tới đích căn cứ vào địa chỉ IP nguồn đích, cổng TCP/UDP nguồn và đích. Nó cũng có thể ngăn chặn các thích ứng về giao thức, kiểm tra các tấn công vào các ứng dụng cơ bản, sự chắc chắn về bảo toàn luông dữ liệu giữa các thiết bị TCP/IP. Các sản phẩm IDS (Intrusion detection system) và NetScrem firewall hỗ trợ sự ngăn chặn lớp gói tin chiều sâu. Cisco PIX Firewall hỗ trợ hoạt động stateless và statefull:



Hình 4.2.c: Deep Packet Layer Firewall

Đặc biệt, các chức năng này được thực hiện trong phần cứng. Dữ liệu được tính toán theo tiêu chuẩn như là từ chối đối với DoS là loại bỏ ngay lập tức và có thể đưa vào bộ đệm …