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

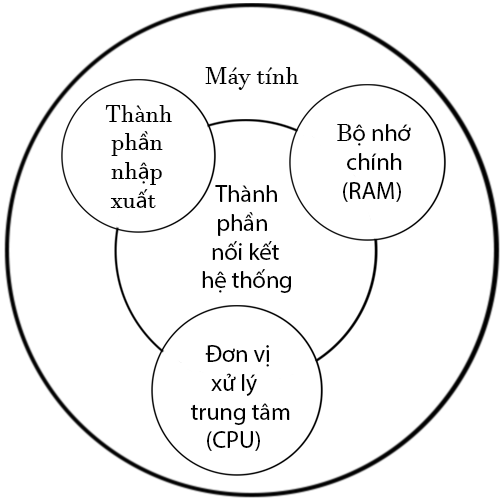
PHẦN I: TỔNG QUAN VỀ MẠNG MÁY TÍNH

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

**1.1. Lịch sử máy tính**

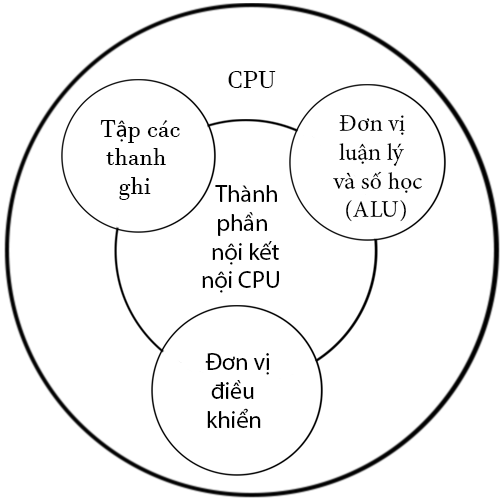
**1.1.1. Cấu trúc tổng quát của máy tính**

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.



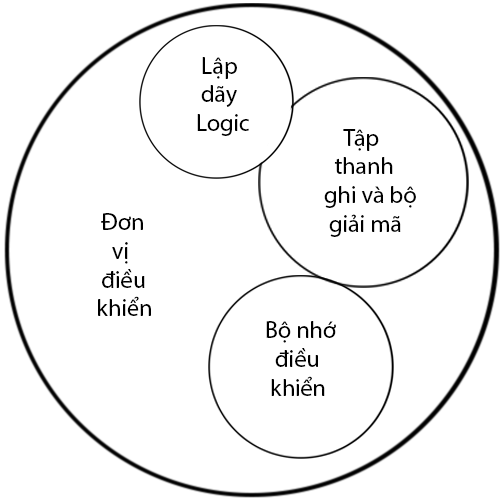
*Hình 1.1.1b: Bộ xử lý trung tâm của máy tính (CPU)*

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**

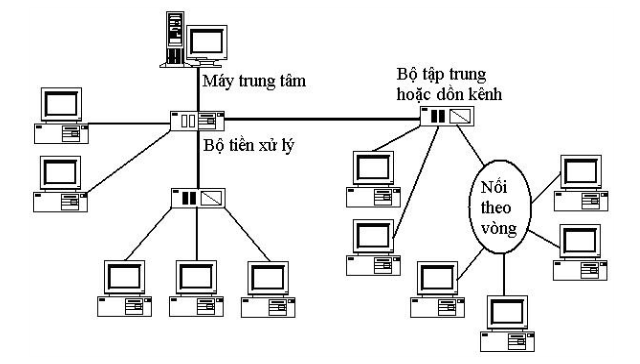
Mạng máy tính là một hệ thống kết nối các máy tính đơn lẻ thông qua các đường truyền vật lý theo một kiến trúc nào đó.

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 loại 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:

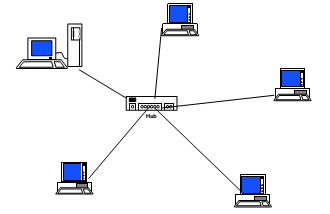
* Mạng chuyển mạch kênh.
* Mạng chuyển mạch thông báo.
* Mạng chuyển mạch gói.

**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 (thêm, 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).

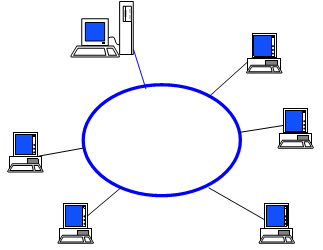
**1.2.4.3.2. Mạng hình vòng**

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.

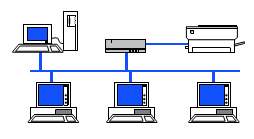
Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.



*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).



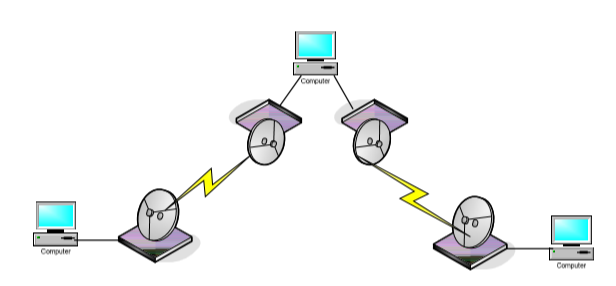
*Hình 1.2.4.3.3: Mạng trục tuyến tính (Bus)*

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 các 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.

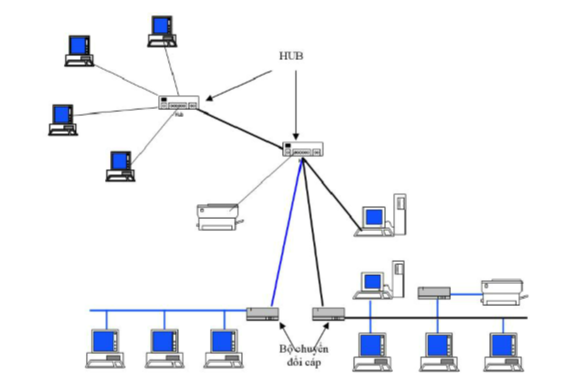
**1.2.4.3.4. Mạng dạng vô tuyến – Satellite (vệ tinh) hoặc Radio**



*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**

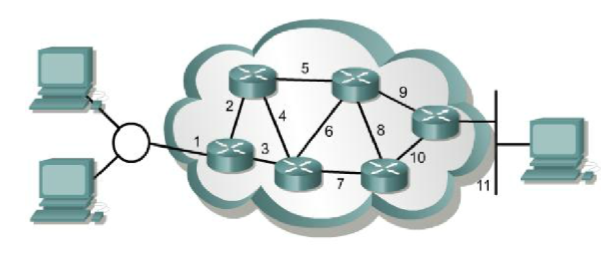
**1.2.5.1. Mạng cục bộ (LAN):**

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

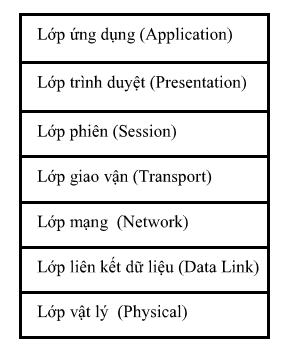
**2.2. Mô hình chiếu OSI 7 lớp**

**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.

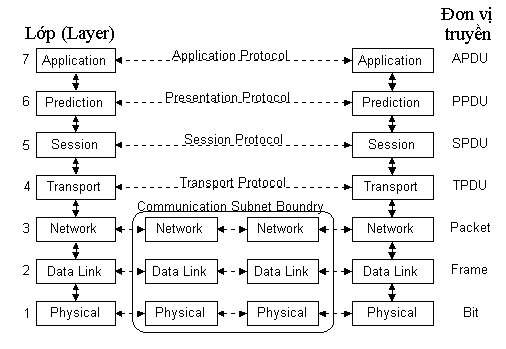
So sánh 2 phương thức hoạt động trên, chúng ta thấy rằng phương thức hoạt động có liên kết cho phép truyền dữ liệu tin cậy, do nó có cơ chế kiểm soát và quản lý chặt chẽ từng liên kết logic. Nhưng mặt khác, nó lại khá phức tạp và khó cài đặt và ngược lại.

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**

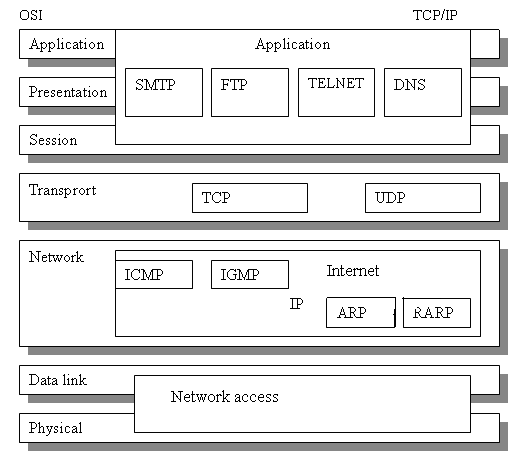
Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng ARPA (Advanced Research Projects Agency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở của nó. Hai giao thức được dùng chủ yếu ở đây là TCP (Transmission Control Protocol) và 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.

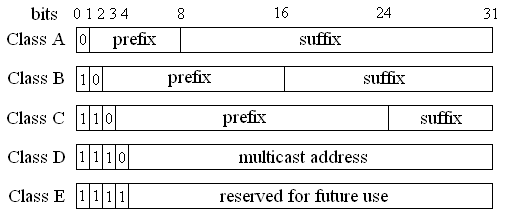
**2.3.1.2. Giao thức IP:**

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.

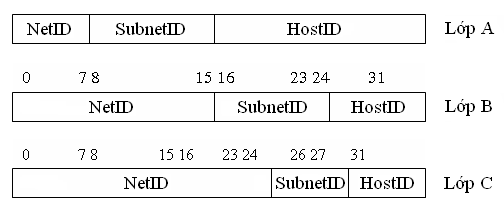


*Hình 2.3.1.2.1a: Cách đánh địa chỉ TCP/IP*

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).

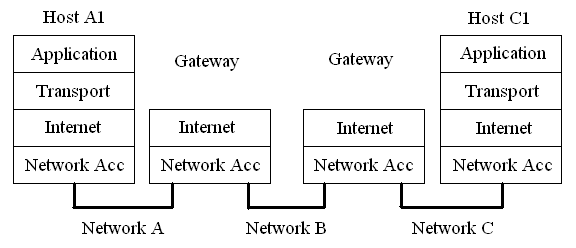


*Hình 2.3.1.2.2c: Cổng truy nhập dịch vụ TCP*

**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: TỔNG QUAN VỀ HỆ THỐNG GIÁM SÁT THÔNG TIN AN NINH MẠNG**

**CHƯƠNG 3: HỆ HỐNG GIÁM SÁT MẠNG**

**3.1. Giám sát mạng là gì?**

Giám sát mạng cho mạng của một công ty là một chức năng quan trọng, nó có thể tiết kiệm tiền thông qua việc làm tăng hiệu quả của mạng lưới, năng suất nhân viên và chi phí cơ sở hạ tầng. Một hệ thống giám sát mạng giám sát cho nhiều vấn đề. Nó có thể tìm và giúp đỡ giải quyết việc tải trang web snail-paced, mất mát email, hoạt động của người truy vấn và truyền tải file, nguyên nhân do quá tải, sự cố server, kết nối mạng delay hoặc các thiết bị khác.

Các hệ thống giám sát mạng (NMSs) thì khác với các hệ thống phát hiện xâm nhập (IDSs) hoặc các hệ thống phòng chống xâm nhập (IPSs). Những hệ thống khác phát hiện break-ins và ngăn chặn người dùng trái phép. Tập chung của NMS không phải cho vấn đề an ninh cho mỗi lần đăng nhập.

Giám sát mạng có thể đạt được bằng cách sử dụng phần mềm khác nhau hoặc kết hợp giữa các plug và play, thiết bị phần cứng và giải pháp phần mềm. Hầu hết bất kì loại mạng nào cũng có thể được giám sát. Nó không quan trọng là có dây hay không có dây, một mạng LAN công ty, VPN hoặc dịch vụ cung cấp WAN. Bạn có thể giám sát thiết bị trên các hệ điều hành khác nhau với vô số chức năng, từ BlackBerrys và điện thoại di động, tới servers, routers và switches. Những hệ thống này có thể giúp bạn xác định các hoạt động cụ thể và số liệu hiệu xuất, đưa ra kết quả cho phép doanh nghiệp giải quyết các yêu cầu khác nhau, đưa ra các mối đe dọa an ninh nội bộ và cung cấp nhiều hiển thị hoạt động hơn.

Việc quyết định dùng cái gì để giám sát mạng thì rất quan trọng. Bạn phải chắc rằng cấu trúc sơ đồ mạng của công ty bạn thì luôn cập nhật. Đó là bản đồ chính xác để đưa ra các loại mạng khác nhau nhằm đáp ứng việc giám sát, server đang chạy trên hệ điều hành nào, có bao nhiêu máy tính để bàn và có bao nhiêu thiết bị từ xa có thể truy cập cho mỗi mạng. Trả lời cho các câu hỏi trên sẽ làm cho việc lựa chọn công cụ giám sát trở nên đơn giản hơn.

**3.2. Giám sát mạng quan trọng như thế nào?**

Bạn có thể nghĩ rằng nếu mạng đưa ra và chạy, không có lý do để gây rối với nó. Tại sao bạn lại quan tâm về việc thêm một dự án cho các nhà quản lý mạng của bạn. Lý do để khẳng định việc giám sát mạng là nhằm duy trì sức khỏe của mạng lưới, đảm bảo sẵn sàng và cải thiện hiệu suất. NMS cũng có thể giúp bạn xây dựng cơ sở dữ liệu thông tin quan trọng mà bạn có thể dùng để lên kế hoạch trong sự phát triển trong tương lai.

Giám sát mạng giống như sự viếng thăm của chuyên gia tim mạch. Nếu bác sĩ của bạn đang theo dõi dấu hiệu nguy hiểm như chảy máu qua các mạch, van và buồng của tim, thì hệ thống giám sát mạng của bạn đang theo dõi dữ liệu chuyển qua dây cáp thông qua server, switches, các kết nối và routers.

Dĩ nhiên, giám sát mạng ở các công ty không giải quyết cho ảnh chụp nhanh hàng năm của hiệu năng hệ thống. Họ không chỉ theo dõi sau khi xuất hiện các triệu chứng đáng lo ngại. Họ giám sát mạng của họ 24 giờ một ngày và mỗi ngày.

**3.3 Giám sát mạng có thể giám sát gì?**

Người ta dùng hệ thống giám sát mạng thường để kiểm tra băng thông sử dụng, kiểm tra hiệu suất của ứng dụng và hiệu suất của máy chủ.

Giám sát lưu lượng là nhiệm vụ cơ bản, một trong những việc xây dựng hệ thống mạng và duy trì các nhiệm vụ cơ bản. Nó thường tập chung vào các vấn đề hỗ trợ người dùng nội bộ. Vì vậy hệ thống giám sát mạng tiến hóa để giám sát các loại thiết bị như:

* BlackBerrys
* Cell phones
* Servers and desktops
* Routers
* Switches

Một số hệ thống mạng đi kèm với việc phát hiện tự động, khả năng ghi lại thiết bị liên tục khi chúng được thêm vào, gỡ bỏ hoặc trải qua những thay đổi cấu hình. Những công cụ này tách riêng các thiết bị tự động:

* Ip address
* Service
* Type (switch, router, etc)
* Physical location

Ngoài những lợi thế hiển nhiên của việc biết chính xác và thực tế những gì bạn đã khai triển, hệ thống giám sát mạng còn có thể tự động phát hiện và phân loại công đoạn, giúp bạn có kế hoạch phát triển.

**3.4 Hệ thống giám sát mạng có thể giám sát những loại mạng nào?**

Một hệ thống giám sát (NMS) sẽ giúp định hướng trong môi trường phức tạp, đưa ra các báo cáo, người quản lý có thể sử dụng các báo cáo này để:

* Xác nhận việc tuân thủ quy định và chính sách
* Tiết kiệm chi phí tiềm lực bằng cách tìm nguồn dữ liệu dư thừa
* Giải quyết hiệu quả việc bị lấy cắp thông tin
* Trợ giúp xác định năng suất của nhân viên
* Spot quá tải thiết bị trước khi nó có thể mang xuống một mạng lưới
* Xác định liên kết mạng diện rộng yếu và thắt cổ chai
* Do độ trễ, hoặc do chuyển tải dữ liệu bị trễ
* Tìm vất thường trong mạng nội bộ có thể cho biết một mối đe dọa an ninh.

Nhưng một NMS không phải là hệ thống phát hiện (IDS) hoặc hệ thống phòng chống (IPS). Một NMS có thể phát hiện các hành động khó chịu, nhưng đó không phải là nhiệm vụ của nó.

**3.6 Giám sát mạng có thể trả lời những câu hỏi gì?**

Một báo cáo giám sát sẽ giúp bạn trả lời câu hỏi khó khăn:

* Giúp làm đơn giản hóa và đồng nhất hệ thống với chi phí thấp, giúp đưa ra quyết định thay thế các phân đoạn mạng với chi phí chấp nhận được?
* Hệ điều hành và ứng dụng nào chạy trên server, và chúng cần thiết?
* Người sử dụng đại diện cho ai và cái gì được họ gửi?
* Làm thế nào để gần với công suát của máy chủ?
* Thiết bị từ xa gì được sử dụng, và chúng được sử dụng gì?
* Làm thế nào và từ đâu thiết bị từ xa gia nhập vào hệ thống?
* Ai và những nguồn gì đang quản lý hệ thống?

Dĩ nhiên, bỏ qua thông tin này và báo cáo tình trạng tốt, như thế có thể kết luận rằng không có vấn đề gì, có nghĩa là không có lý do thể thay đổi mọi thứ. Đó thường là kết luận sai vì doanh nghiệp không tồn tại một trạng thái ổn định.

**3.7 Giám sát mạng có thể làm gì cho chúng ta?**

Giám sát mạng cẩn thận cho phép giám đốc điều hành tất cả thông tin họ cần để chứng minh việc nâng cấp mạng và mở rộng mạng là cần thiết để hỗ trợ doanh nghiệp thành công trong tương lai.

Service-level agreements(SLA) khó thực thi bên bộ phận khách hàng bởi vì nó đưa ra những điều khoản rất là khắt khe.

Hệ thống giám sát mạng làm việc hiệu quả sẻ thông cho nhà quản lý biết thiết bị, dịch vụ hoặc ứng dụng được phép hoạt động ở mức độ nào.

**3.8 Hệ thống giám sát mạng có những công cụ gì?**

Bản thân những hệ thống giám sát mạng có thể là phần mềm hoặc firmware, đơn giản hay phức tạp.

Một trong những công cụ đơn giản nhất là gửi tín hiệu đến thiết bị và xem thời gian trả về là bao lâu (digital echolocation). Thích hợp hơn với hầu hết các nhà quản lý là các công cụ liên quan đến các kiểm tra thông tin thường và các kịch bản theo dõi và có thể đưa ra nhiều báo cáo đa dạng với các đồ hoạ, với điều kiện tổng kết từ thiết bị cụ thể trong mạng lưới rộng khắp.

Các công cụ mã nguồn mỡ có tính mở rộng cao, không tốn. Và chúng làm việc với hầu hết các công cụ và phù hợp với hầu hết các nền tảng.

Không có vấn đề gì đáng lo khi bạn chọn công cụ, mặc dù tích cực tìm hiểu xem chúng làm tốt như thế nào trong môi trường của bạn, đặc biệt với các hệ điều hành trên mạng của bạn.

Nếu như mạng của bạn trở nên quá phức tạp và bạn không thể kiểm soát được những gì đang xảy ra, bạn có thể theo dõi outsource. Outsourcers tạo ra các mức của dịch vụ và các gói chức năng để bao quát nhiều môi trường mạng và ngân sách.

Sản phẩm giám sát mạng có thể miễn phí hoàn toàn (như với ứng dụng mã nguồn mở) hoặc chúng cũng có thể vô cùng tốn kém.

**3.9 Những loại hệ thống giám sát mạng có giá trị?**

Công cụ mạng giám sát đến tất cả các khía cạnh và các mức phức tạp. Rất nhiều công cụ giao diện command (CLI) có giá trị. Một trong những cái có giá trị là *ping* một công cụ khá tin cậy trong hoạt động lý thuyết "KISS". Ping để kiểm tra một máy chủ cụ thể có thể truy cập mạng qua I, nó làm việc bằng cách gửi gói ICMP echo yêu cầu tới máy chủ mục tiêu chờ echo phản hồi. Ping ước lượng thời gian khứ hồi trong milli giây, hồ sơ bất kì gói tin mất mát và in ra một bảng tóm tắt khi hoàn tất.

Rõ ràng là rất tiện lợi cho những người không chuyên, hệ thống giám sát mạng với những biểu đồ các vấn đề quan hệ với công cụ CLI. Một sự phong phú của giải pháp giao diện web bao gồm chi tiết và các tính năng biểu đồ có sẵn. Những công cụ này có thể dễ dàng cài đặt và sử dụng. Nhiều người đến với cấu hình trước kịch bản. Plus, các bản đồ chúng đưa ra thì rất là quan trọng khi đặt cùng với bộ giám sát đại diện cho một nốt mạng quan trọng.

Công cụ mã nguồn mở luôn được ưa chuộng trong giới IT, có rất nhiều cho nhu cầu giám sát mạng. Chúng linh động và tốt hơn, tất cả hầu như là miễn phí hoặc rẻ. Ngoài ra, công cụ mã nguồn mở thì tương thích với hầu hết các công cụ hoặc nền tảng. Dữ liệu cho những công cụ mã nguồn mở hầu hết là XML.Ví dụ: một công cụ miễn phí theo GNU GPL bắt đầu như kịch bản khó diễn tả tới việc sử dụng đồ họa của một trường đại học kết nối với internet. Sau đó nó được sử dụng như là công cụ cho việc vẽ đồ họa cho các nguồn dữ liệu khác nhau như tốc độ, điện áp, nhiệt độ và số lượng bản in. Sau đó công dân mạng bắt đầu dùng phần mềm để thăm dò mạng, lấy lại MIB (Management Information Base) và SNMP (Simple Network Management Protocol), và dùng kịch bản Perl để đưa ra kết quả bằng đồ thị trên trang web. Công cụ nhanh chóng được sử dụng không chỉ công dân mạng mã nguồn mở giải pháp riêng của họ với nhau mà còn bởi các nhà cung cấp độc quyền lớn, những người vay mượn một số khả năng của công cụ để làm phong phú thêm các giải pháp riêng của họ.

Nếu bạn đang ở nơi buôn bán thiết bị mới, các hãng sản xuất thiết bị mạng đã cung cấp rất chi tiết thông tin cho thiết bị của họ, cộng thêm trị giá để mua. Việc của bạn là phải kiểm tra tính tương thích của công cụ, đặc biệt là với hệ điều hành trên mạng của bạn, xác định rõ độ hữu ích của công cụ cho kế hoạch tổng thể của bạn. Cuối cùng là giá cả. Ví dụ: bạn không muốn thấy bạn trong hoàn cảnh, nơi bạn mua server mới với công cụ giám sát cho một khu vực và công cụ giám sát không chạy tốt với sever của bạn, không hỗ trợ hệ điều hành.

Nếu bạn có nhiều thiết bị khác nhau, với khả năng làm việc không đồng đều và một đường cong học hỏi rộng lớn. Có những ứng dụng giám sát trên thị trường có thể kết hợp lại và làm đơn giản việc quản lý giám sát mạng lại. Họ làm được điều này bằng cách quản lý lưu lượng đến các công cụ riêng, cho dù chúng là thiết bị hay ứng dụng. Các thiết bị cung cấp ứng dụng cân bằng tải trên các mạng con khác nhau. Theo lý thuyết, quy trình này làm linh hoạt hơn và giảm bớt nghẽn tắc mạng gây ra bởi giám sát, làm chậm đường truyền kiểm tra nó. Đường cong học tập cũng giảm đi.

Mạng trở nên phức tạp, vì thế phải dùng hệ thống giám sát. Hội tụ, hoặc "triple play" mạng, kết hợp voice, video và truyền dữ liệu tốc độ cao qua một ống duy nhất. Những điều này cần quản lý và giám sát hiệu quả. Những loại mạng loại này cần hệ thống khảo sát rung động của mỗi gói, độ trễ và mất gói tin, và đó là dành cho người mới bắt đầu. Cách quản lý mạng truyền thống-sử dụng SNMP agents để thăm dò các thiết bị mỗi lần cách nhau 5 giây để xác định liệu mạng lưới có vấn đề. Có nhiều giải pháp có giá trị để giải quyết nhiều nhiệm vụ như hoạt động không an toàn trong khi mất nguồn, cung cấp hỗ trợ cho switch ports và VLANs, và chính xác giống như một màn hình LCD để khắc phục sự cố.

Nếu mạng của bạn trở lên quá phức tạp và bạn không thể kiểm soát những gì đang xảy ra, Những người khác có thể làm cho bạn. Có những công ty mà bạn có thể thuê để giám sát, quản lý, phân tích. Ví dụ, một dịch vụ cung cấp ở châu âu cung cấp các module khác nhau tới khách hàng mạng và các công ty sử dụng cả ba mạng. Một module của dịch vụ bao gồm thông tin của khách hàng trong một khoảng thời gian xác định, và đưa ra báo cáo hiệu xuất giao thông và ứng dụng. Một module khác lấy các thông tin và đưa ra khuyến nghị để cải thiện mạng hiệu quả. Module thứ 3 theo dõi liên tục, báo cáo, và hiệu suất báo cáo.

## Chi phí cho chúng là gì?

Giả pháp giám sát mạng có thể hoàn toàn miễn phí hoặc rất tốn kém. Hầu hết các công cụ mã nguồn mở là miễn phí, như những công cụ có thể được mua kèm với cơ sở hạ tầng. ứng dụng, phần mềm-giải pháp và các dịch vụ chỉ giao động trong khoảng từ 50 đô la đến hàng ngàn đô la.

Với các nhà cung cấp dịch vụ, bạn có thể tùy chọn trong danh mục các dịch vụ giám sát; có thể tiết kiệm thông qua lấy các thiết bị phát sinh phụ thuộc vào mạng. Có những trao đổi khác nhau. Mua dịch vụ có thể cung cấp cho bạn tiếp cận với công nghệ giám sát mới nhất; tương phản, lấy được thiết bị cung cấp nhiều chức năng hơn.

Một trong những điều chắc chắn khi nói đến giám sát mạng là chi phí mà bạn phải bỏ ra nếu không sử dụng những công nghệ này có thể sẽ lớn hơn bạn nghĩ rất nhiều, nếu bạn không nhận được hiệu suất và tính sẵn sàng. Bạn buộc lòng phải chịu tốn kém để chắc rằng mạng của bạn khỏe mạnh và an toàn. Giá trị của nó là công việc của bạn.

**CHƯƠNG 4: TỔNG QUAN VỀ IDS/IPS**

**4.1 Giới thiệu về IDS/ IPS**

**4.1.1 Định nghĩa**

Hệ thống phát hiện xâm nhập (IDS) là hệ thống có nhiệm vụ theo dõi, phát hiện và (có thể) ngăn cản sự xâm nhập, cũng như các hành vi khai thác trái phép tài nguyên của hệ thống được bảo vệ mà có thẻ dẫn đến việc làm tổn hại đến tính bảo mật, toàn vẹn và tính sẵn sàng của hệ thống