

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



QUẢN LÝ MẠNG VIỄN THÔNG

cuu duong than cong . com

(Dùng cho sinh viên hệ đào tạo đại học từ xa)

Lưu hành nội bộ

cuu duong than cong . com

HÀ NỘI - 2007

QUẢN LÝ MẠNG VIỄN THÔNG

Biên soạn : THS. NGUYỄN VĂN ĐÁT
TS. NGUYỄN TIẾN BAN
THS. DƯƠNG THANH TÚ
THS. NGUYỄN THỊ THU HẰNG
KS. LÊ SỸ ĐẠT

cuu duong than cong . com

LỜI NÓI ĐẦU

Hiện nay, bài toán quản lý mạng viễn thông luôn là mối quan tâm hàng đầu và là một trong những vấn đề quan trọng nhất cần giải quyết của các nhà khai thác viễn thông. Với những khả năng mà hệ thống quản lý mạng viễn thông đem lại cùng với sự phát triển của mạng lưới, các nhà khai thác đều xây dựng cho mình các hệ thống quản lý mạng thích hợp để nâng cao hiệu quả vận hành và khai thác mạng.

Mục tiêu của tài liệu là cung cấp cho học viên những kiến thức cơ bản trong quản lý mạng viễn thông như mô hình tổng thể của hệ thống quản lý mạng, các yêu cầu và quan điểm tiếp cận trong quản lý mạng, nguyên lý và các kiến trúc của mạng quản lý viễn thông TMN, giao thức quản lý mạng đơn giản SNMP và các vấn đề về quản lý mạng trên nền IP.

Với mục tiêu đặt ra như vậy, nội dung của tài liệu được chia thành 3 chương.

Chương 1 giới thiệu một số mô hình hệ thống quản lý như hệ thống quản lý mở, quản lý phân tán, quản lý trong băng và ngoài băng, các yêu cầu trong quản lý mạng cũng như là các quan điểm và cách tiếp cận trong quản lý mạng.

Chương 2 trình bày các nội dung liên quan đến mạng quản lý viễn thông TMN, trong đó đi sâu vào xu hướng quản lý tập trung dựa trên các giao thức và các tiêu chuẩn đã được chuẩn hóa nhằm nâng cao năng lực của mạng.

Chương 3 cung cấp những khái niệm cơ bản nhất về giao thức quản lý mạng đơn giản SNMP: các thành phần, chức năng và phương thức hoạt động của giao thức, đồng thời giới thiệu các phiên bản ứng dụng của SNMP và so sánh những điểm khác biệt giữa chúng.

Quản lý mạng viễn thông là một nội dung rất quan trọng, cần được nghiên cứu kỹ lưỡng để nâng cao hiệu quả vận hành và khai thác mạng. Yêu cầu đối với học viên sau khi học xong môn học này là phải nắm bắt được các yêu cầu chung về quản lý mạng, các thực thể vật lý cũng như các thực thể chức năng trong mạng quản lý viễn thông, các giao diện và chức năng quản lý, cách thức quản lý và điều hành mạng thông qua các giao thức quản lý khác nhau.

Tài liệu được biên soạn trong khoảng thời gian tương đối ngắn nên không tránh khỏi còn nhiều thiếu sót. Nhóm tác giả rất mong nhận được các ý kiến đóng góp của độc giả và những người quan tâm.

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Km10 Đường Nguyễn Trãi, Hà Đông-Hà Tây
Tel: (04) 5541221; Fax: (04) 5540587

Website: <http://www.ctptit.edu.vn>; E-mail: dhkx@ptit.edu.vn

cuu duong than cong . com

CHƯƠNG TRÌNH **PTIT**
ĐẠO TẠO ĐẠI HỌC TỪ XA

cuu duong than cong . com

CHƯƠNG I

TỔNG QUAN VỀ QUẢN LÝ MẠNG VIỄN THÔNG

Nội dung của chương giới thiệu cho học viên những khái niệm cơ bản trong quản lý mạng viễn thông như mô hình tổng quan của hệ thống quản lý mạng, các yêu cầu trong quản lý mạng, các quan điểm và cách tiếp cận trong quản lý mạng cũng như giới thiệu một số mô hình hệ thống quản lý như hệ thống quản lý mở, hệ thống quản lý phân tán, hệ thống quản lý trong băng và ngoài băng.

1.1. KHÁI NIỆM VỀ QUẢN LÝ, KHAI THÁC VÀ BẢO DƯỠNG MẠNG

Vào những thập niên cuối cùng của thế kỷ trước, công nghệ và dịch vụ truyền thông đã có sự phát triển mạnh mẽ, đánh dấu một bước tiến quan trọng trong lịch sử phát triển của loài người. Truyền thông, có thể hiểu nôm na như là một cách thức để truyền tải và trao đổi thông tin. Trong đó, Internet chính là ví dụ tốt nhất để minh họa cho sự bùng nổ mạnh mẽ và có ảnh hưởng lớn mạnh đến khả năng chia sẻ thông tin của con người ở thời điểm hiện tại cũng như trong tương lai.

Giấc mơ của con người về khả năng truy nhập thông tin toàn cầu, về sự trao đổi thông tin nhanh, tin cậy và giàu nội dung ngày nay đã tiến gần đến hiện thực, nhanh hơn bất kỳ người nào đã tiên đoán trước đây. Truyền thông số liệu, truyền thông video, phương tiện truyền thông vô tuyến và hữu tuyến ... tất cả đều đóng góp vai trò quan trọng, làm tăng khả năng điều khiển xuyên suốt thông tin trong các hoạt động kinh doanh hay các tổ chức, doanh nghiệp rộng lớn và toàn cầu.

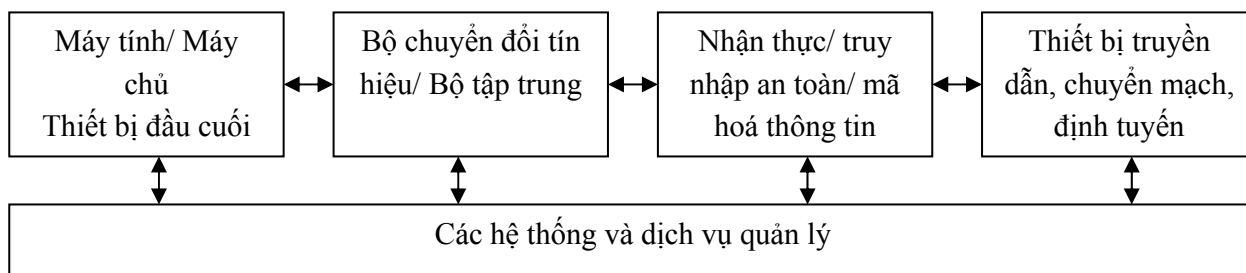
Hệ thống quản lý mạng là một hệ thống chuyên hoá nhằm mục đích giám sát và điều khiển một hệ thống rộng lớn bao gồm các tài nguyên mạng và các hệ thống máy tính, được sử dụng trong lĩnh vực truyền thông, trong sản xuất, kinh doanh, trong lĩnh vực tài chính, ngân hàng hay giáo dục cũng như trong lĩnh vực nghiên cứu và phát triển.

Sự ra đời của các hệ thống quản lý mạng cũng là một yêu cầu cấp thiết để ngăn ngừa, chẩn đoán, định cấu hình và giải quyết các vấn đề phát sinh do sự lớn mạnh, phức tạp và không đồng nhất của môi trường, đa nhà cung cấp, đa giao thức, đa công nghệ của hệ thống mạng và các máy tính.

Mặc dù các hệ thống quản lý mạng là thành phần giá trị gia tăng của công nghệ truyền thông nhưng nó lại đóng vai trò quan trọng trong việc quản lý, khai thác và bảo dưỡng các hệ thống truyền dẫn, chuyển mạch và điều hành, đảm bảo cho quá trình trao đổi thông tin được diễn ra bình thường.

1.2. MÔ HÌNH TỔNG QUÁT HỆ THỐNG MẠNG

Nhiệm vụ của quản lý mạng là theo dõi, giám sát và điều khiển tất cả các thành phần tham gia vào quá trình truyền thông từ điểm đầu đến điểm cuối hay từ nguồn đến đích. Các thành phần tham gia vào quá trình truyền thông này rất khác nhau. Đó có thể là các máy chủ, máy trạm đóng vai trò như là nguồn và đích thông tin, các thiết bị chuyển đổi dữ liệu/ tín hiệu như bộ chuyển đổi giao thức, bộ tập trung, bộ ghép kênh, các thiết bị điều khiển việc truy nhập vào mạng như nhận thực, bảo mật truy nhập, mã hoá và giải mã cũng như tất cả các thiết bị khác sử dụng trong quá trình truyền dẫn, chuyển mạch và định tuyến (hình 1.1).



Hình 1.1. Mô hình tổng quát hệ thống mạng

Nhiệm vụ của quản lý mạng rất rõ ràng nhưng thực hiện được điều này lại không đơn giản một chút nào. Hãy thử hình dung với mỗi một thiết bị lại có một danh sách đặc tả các chi tiết và có hàng tá các công nghệ khác nhau với hàng trăm các thiết bị được phát triển, thiết kế và sản xuất bởi hàng ngàn các nhà cung cấp. Tất cả điều là các thực thể của hệ thống quản lý mạng nhất là khi đi vào xem xét việc truyền tải thông tin từ đầu cuối đến đầu cuối với các chức năng giám sát, chẩn đoán, điều khiển và đưa ra báo cáo.

Máy tính cá nhân, máy trạm, server, máy vi tính cỡ nhỏ, máy vi tính cỡ lớn, các thiết bị đầu cuối, thiết bị đo kiểm, máy điện thoại, tổng đài điện thoại nội bộ, các thiết bị truyền hình, máy quay, modem, bộ ghép kênh, bộ chuyển đổi giao thức, CSU/DSU, bộ ghép kênh thống kê, bộ ghép và giải gói, thiết bị tương thích ISDN, card NIC, các bộ mã hoá và giải mã tín hiệu, thiết bị nén dữ liệu, các gateway, các bộ xử lý front-end, các trung kế đường dây, DSC/DAC, các bộ lặp, bộ tái tạo tín hiệu, các chuyển mạch ma trận, các bridge, router và switch, tất cả mới chỉ là phần đầu của danh sách các thiết bị sẽ phải được quản lý.

Toàn cảnh của bức tranh quản lý phải bao gồm quản lý các tài nguyên mạng cũng như các tài nguyên của các hệ thống máy tính như hàng ngàn các doanh nghiệp, người sử dụng, các ứng dụng hệ thống, các cơ sở dữ liệu khác nhau cũng như các hệ thống phức tạp, chuyên hoá và rộng lớn.

Tất cả các thông tin trên được thu thập, trao đổi và được kết hợp với các hoạt động quản lý mạng dưới dạng các số liệu quản lý bởi các kỹ thuật tương tự như các kỹ thuật sử dụng trong mạng truyền số liệu. Tuy nhiên sự khác nhau căn bản giữa truyền thông số liệu và trao đổi thông tin quản lý là việc trao đổi thông tin quản lý đòi hỏi các trường dữ liệu chuyên hoá, các giao thức truyền thông cũng như các mô hình thông tin chuyên hoá, các kỹ năng chuyên hoá để có thể thiết kế, vận hành hệ thống quản lý cũng như biên dịch các thông tin quản lý về báo lỗi, hiện trạng hệ thống, cấu hình và độ bảo mật.

1.3. CÁC YÊU CẦU QUẢN LÝ

Sự đa dạng của các tài nguyên được quản lý mà dễ nhận thấy nhất ở các trường truyền tin như thoại, số liệu, truyền thông video... đã tạo ra các quan điểm khác nhau về chức năng và yêu cầu quản lý trong các hệ thống quản lý.

1.3.1. Các chức năng quản lý lớp cao

Mặc dù có rất nhiều quan điểm khác nhau về mô hình quản lý nhưng chúng đều thống nhất bởi các chức năng quản lý nằm ở ba lớp trên cùng. Đó là giám sát, điều khiển và đưa ra báo cáo.

Chức năng giám sát có nhiệm vụ thu thập liên tục các thông tin về trạng thái của các tài nguyên được quản lý sau đó chuyển các thông tin này dưới dạng các sự kiện và đưa ra các cảnh báo khi các tham số của tài nguyên mạng được quản lý vượt quá ngưỡng cho phép.

Chức năng quản lý có nhiệm vụ thực hiện các yêu cầu của người quản lý hoặc các ứng dụng quản lý nhằm thay đổi trạng thái hay cấu hình của một tài nguyên được quản lý nào đó.

Chức năng đưa ra báo cáo có nhiệm vụ chuyển đổi và hiển thị các báo cáo dưới dạng mà người quản lý có thể đọc, xem xét toàn cảnh hoặc tìm kiếm, tra cứu thông tin được báo cáo.

Trong thực tế, tùy theo từng công việc cụ thể mà còn có một vài chức năng khác được kết hợp với các hệ thống quản lý và các ứng dụng quản lý được sử dụng như quản lý kế hoạch dự phòng thiết bị, dung lượng, triển khai dịch vụ, quản lý tóm tắt tài nguyên, quản lý việc phân phối tài nguyên mạng/ các hệ thống, quản lý việc sao lưu và khôi phục tình trạng hệ thống, vận hành quản lý tự động. Phần lớn các chức năng phức tạp kể trên đều nằm trong hoặc được xây dựng dựa trên nền tảng của ba chức năng quản lý lớp cao là giám sát, điều khiển và đưa ra báo cáo.

1.3.2. Các yêu cầu quản lý của người sử dụng

Các yêu cầu quản lý của người sử dụng được đưa ra dưới đây dựa trên quan điểm của người sử dụng về quản lý. Bao gồm:

- Khả năng giám sát và điều khiển mạng cũng như các thành phần của hệ thống máy tính từ đầu cuối đến đầu cuối.
- Có thể truy nhập và cấu hình lại từ xa các tài nguyên được quản lý.
- Dễ dàng trong việc cài đặt, vận hành và bảo dưỡng hệ thống quản lý cũng như các ứng dụng của nó.
- Bảo mật hoạt động quản lý và truy nhập của người sử dụng, bảo mật truyền thông các thông tin quản lý.
- Có khả năng đưa ra các báo cáo đầy đủ và rõ nghĩa về các thông tin quản lý.
- Quản lý theo thời gian thực và hoạt động quản lý hàng ngày được thực hiện một cách tự động.
- Mềm dẻo trong việc nâng cấp hệ thống và có khả năng tương thích với nhiều công nghệ khác nhau.
- Có khả năng lưu trữ và khôi phục các thông tin quản lý.

1.3.3. Các động lực thúc đẩy công nghệ quản lý mạng

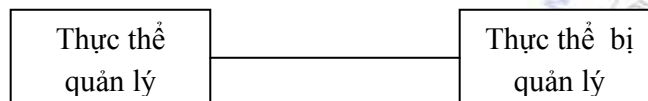
Mặc dù thuật ngữ “quản lý mạng” mới được chấp nhận vào giữa những năm 80 của thế kỷ trước nhờ sự ra đời bộ công cụ quản lý của IBM (IBM NetView) nhưng cho đến nay quản lý mạng đã cố gắng phát triển ngang bằng với sự phát triển của các hệ thống viễn thông, truyền thông số liệu và mạng các hệ thống máy tính. Đối với hệ thống viễn thông và truyền thông số liệu, công nghệ quản lý tập trung vào quản lý các thiết bị truyền dẫn và chuyển mạch (bao gồm các thiết bị phần cứng, các kết nối, các kênh luồng) cùng với các thiết bị chuyển đổi và điều khiển truy nhập. Còn đối với các hệ thống máy tính, công nghệ quản lý lại tập trung vào quản lý các tài nguyên hệ thống máy rộng lớn (như phần cứng, các giao diện, bộ nhớ, các thiết bị lưu trữ số liệu, ...) và các ứng dụng/các cơ sở dữ liệu.

Tuy nhiên, với sự hội tụ của hệ thống viễn thông và hệ thống máy tính mà điển hình là sự tích hợp của hệ thống điện thoại trên máy tính (thoại trên Internet), quan điểm chung hiện nay cho rằng trong tương lai khái niệm mạng sẽ là mạng của sự kết nối của tất cả các hệ thống trên và quản lý mạng sẽ là quản lý mạng truyền thông số liệu rộng khắp.

1.4. CÁC QUAN ĐIỂM VÀ CÁCH TIẾP CẬN TRONG QUẢN LÝ MẠNG

1.4.1. Các thực thể của hệ thống quản lý mạng

Ban đầu, hệ thống quản lý mạng được xây dựng dựa trên mô hình khá đơn giản. Trong mô hình này, quản lý được định nghĩa là sự tương tác qua lại giữa hai thực thể: thực thể quản lý và thực thể bị quản lý. Thực thể quản lý đặc trưng bởi hệ thống quản lý, nền tảng quản lý (platform) và/hoặc ứng dụng quản lý. Thực thể bị quản lý đặc trưng bởi các tài nguyên bị quản lý. Hình 1.2 chỉ ra mô hình đơn giản của hệ thống quản lý, nó cũng tương tự như mô hình nền tảng của truyền thông.



Hình 1.2. Mô hình nền tảng của quản lý

Để truyền thông với các tài nguyên bị quản lý mà chưa có bất kỳ cơ cấu tự nhiên nào để truyền thông tin quản lý, người ta cần phải tạo ra một thành phần trung gian, đó là agent. Agent cũng có thể là agent quản lý hoặc agent bị quản lý. Manager chính là thực thể quản lý trong khi đó agent là thực thể ẩn dưới sự tương tác giữa manager và các nguồn tài nguyên bị quản lý thực sự (hình 1.3).

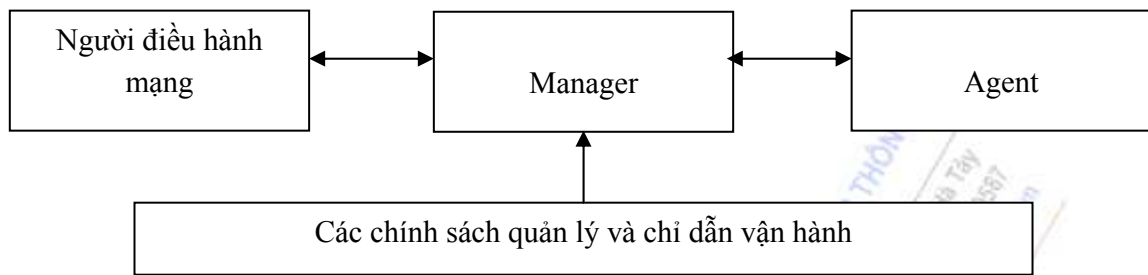


Hình 1.3. Mô hình Manager-Agent

Mô hình Manager-Agent rất thông dụng, được sử dụng để miêu tả sự tương tác giữa thực thể quản lý và thực thể bị quản lý ở các lớp cao. Đây cũng chính là lý do mà các mô hình được tạo ra tự nhiên cho mục đích quản lý đều gần với mô hình Manager-Agent. Tuy nhiên, trong thực tế thì mô hình Manager-Agent phức tạp hơn thế nhiều (hình 1.4)

Chúng ta có thể hiểu rõ sự phức tạp này hơn khi xem xét sự tương tác giữa manager hay các ứng dụng quản lý với người vận hành mạng. Ngoài ra còn có các thành phần khác, tuy không rõ ràng bằng nhưng lại chiếm vị trí khá quan trọng trong sự tương tác giữa các manager với các agent, đó là các chính sách quản lý và chỉ dẫn vận hành, được đưa tới manager để chuyển tới người điều hành mạng.

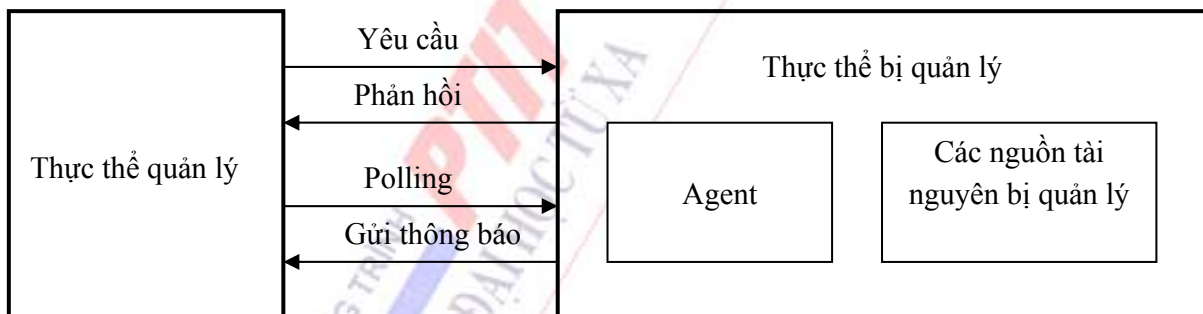
Còn có một vài mô hình khác cũng được sử dụng cho việc trao đổi thông tin quản lý như mô hình client-server hay mô hình application-object server. Những mô hình này, về bản chất, được dùng để xây dựng các ứng dụng phân bố hoặc các môi trường đối tượng phân bố.



Hình 1.4. Mô hình Manager-Agent thực tế

1.4.2. Quan điểm quản lý Manager-Agent

Các quan điểm về quản lý đều cho rằng chức năng quan trọng nhất trong quản lý chính là sự truyền thông giữa thực thể quản lý và thực thể bị quản lý. Và điều này được thực hiện dựa trên mô hình yêu cầu-phản hồi. Manager sẽ yêu cầu từ agent các thông tin quản lý đặc trưng và thực thể bị quản lý, thông qua agent, sẽ phản hồi lại bằng một bản tin chứa đầy đủ thông tin được yêu cầu. Nếu truyền thông yêu cầu-phản hồi được sử dụng liên tục để tìm kiếm mỗi agent và các đối tượng bị quản lý tương ứng thì cơ chế này được gọi là polling và lần đầu tiên được ứng dụng để quản lý trong môi trường internet dựa trên giao thức quản lý mạng đơn giản SNMP (Simple Network Management Protocol) (hình 1.5)



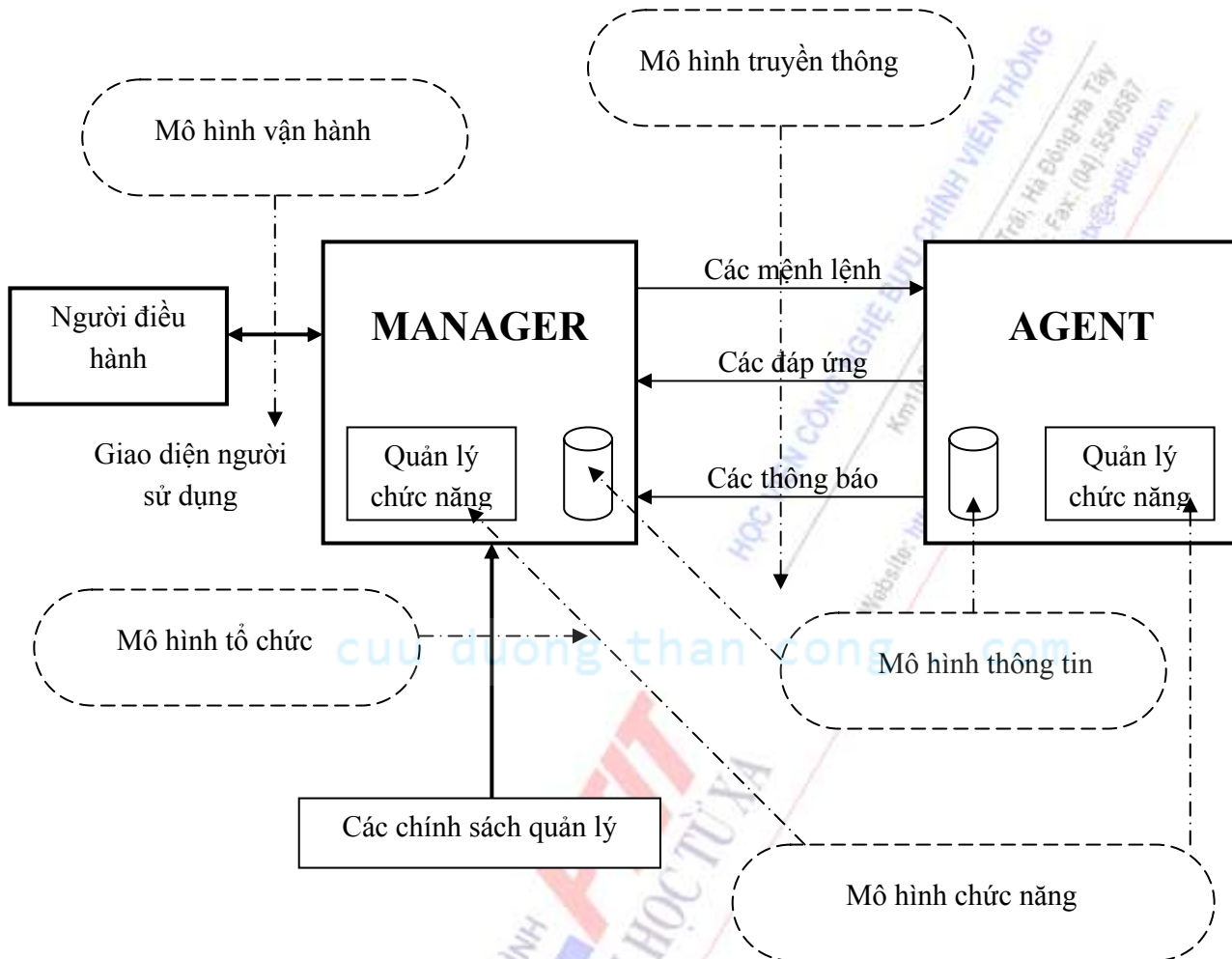
Hình 1.5. Mô hình truyền thông Manager-agent

Cơ chế yêu cầu - phản hồi được coi là một cơ chế truyền thông đồng bộ. Điều này có nghĩa là, manager sẽ chờ sự phản hồi từ agent trong một khung thời gian giới hạn nào đó trước khi nó tiến hành bất kỳ một sự kiện nào tiếp theo. Nếu quá thời gian cho phép mà không nhận được phản hồi, manager sẽ tiến hành phát lại yêu cầu.

Bên cạnh cơ chế yêu cầu- phản hồi còn có một cơ chế nữa cho sự truyền thông giữa manager và agent, đó là cơ chế thông báo. Cơ chế thông báo là một cơ chế không đồng bộ. Trong cơ chế này, agent sẽ gửi thông báo đến manager những thay đổi quan trọng về trạng thái của các tài nguyên bị quản lý và yêu cầu manager lưu ý đến hay can thiệp vào.

1.4.3. Mô hình quan hệ Manager-agent

Khi xây dựng các hệ thống quản lý, có rất nhiều khía cạnh, vấn đề cần phải quan tâm. Bên cạnh mô hình truyền thông Manager-Agent còn có rất nhiều mô hình khác được sử dụng kết hợp cùng với mối quan hệ giữa manager và các agent. Đó là mô hình kiến trúc, mô hình tổ chức, mô hình chức năng và mô hình thông tin (hình 1.6).



Hình 1.6. Mô hình quan hệ Manager-Agent.

Mô hình kiến trúc sử dụng để thiết kế, cấu trúc các thành phần tham gia vào tiến trình quản lý. Điều này có nghĩa là manager hay các manager và các agent cung cấp các thông tin quản lý thông qua kiến trúc mạng. Manager có thể được thiết kế như là một cơ sở quản lý bao gồm một cơ cấu quản lý và một bộ các ứng dụng quản lý cung cấp các chức năng quản lý thực sự như quản lý cấu hình, quản lý lỗi và quản lý hiệu năng.

Mô hình vận hành định ra giao diện của người sử dụng với hệ thống quản lý trong đó chỉ rõ trạng thái cũng như kiểu định dạng của các tương tác tới người sử dụng như điều khiển các đối tượng được quản lý, hiển thị và tìm kiếm các sự kiện, các bản tin hay báo động với người điều hành trong trường hợp cảnh báo nghiêm trọng. Phần lớn các đặc điểm của hoạt động điều hành quản lý này đều có trong các chỉ tiêu kỹ thuật của hệ thống in trong các tài liệu hướng dẫn sử dụng.

Mô hình chức năng định ra cấu trúc của các chức năng quản lý giúp cho hệ thống quản lý thực hiện các ứng dụng quản lý. Mô hình chức năng có cấu trúc phân lớp. Các chức năng cơ bản trong mô hình này là quản lý cấu hình, quản lý hiệu năng, quản lý lỗi, độ bảo mật và thống kê. Ngoài ra trong các chức năng cơ bản này còn tích hợp một vài chức năng khác như chức năng tạo phiếu báo lỗi, trợ giúp trực tuyến, hoạt động giúp đỡ/ dự phòng, lập kế hoạch lưu lượng... Ở các lớp bậc cao trong mô hình chức năng đều là các ứng dụng thực hiện các chức năng phức hợp như tương quan các sự kiện/ cảnh báo, các hệ thống chuyên gia và quản lý tự động.

Mô hình tổ chức liên quan chặt chẽ đến các chính sách quản lý và thủ tục vận hành. Mô hình này sẽ xác định các miền quản lý, sự phân chia quyền điều hành cũng như quyền truy nhập của người sử dụng vào hệ thống quản lý cũng như hệ thống quản lý mạng khách hàng. Mô hình này cũng cung cấp khả năng trao đổi vai trò giữa các manager và các agent cũng như sự hợp tác toàn cục giữa manager này với các manager khác hay với các ứng dụng quản lý.

Mô hình thông tin là mô hình được đề cập cuối cùng trong mô hình quan hệ Manager-Agent nhưng lại nắm vai trò quan trọng trong tất cả các vấn đề liên quan đến quản lý. Mô hình thông tin định ra bản tóm tắt các nguồn tài nguyên được quản lý dưới dạng thông dụng mà các manager và agent đều có thể hiểu được. Mô hình thông tin cũng xây dựng một cơ sở để định dạng, đặt tên và đăng nhập các nguồn tài nguyên được quản lý. Trong mô hình thông tin, thuật ngữ “đối tượng quản lý” được sử dụng nhằm trừu tượng hoá các nguồn tài nguyên vật lý và logic bị quản lý. Việc truy nhập đến các nguồn tài nguyên bị quản lý phải thông qua các đối tượng quản lý. Cơ sở dữ liệu chứa các thông tin quản lý được gọi là MIB (Management Information Base). Khi chúng ta tham khảo tới một MIB cá biệt nào đó có nghĩa là chúng ta đang tham khảo đến miền hay môi trường đặc tả chi tiết định dạng của các đối tượng quản lý. Định dạng của đối tượng quản lý đã được chuẩn hoá và dựa trên cơ sở chuẩn hoá này một manager tiến hành thực hiện giao thức chuyên hoá và truyền thông với các agent phân tán trên cùng một MIB.

1.4.4. Các miền quản lý

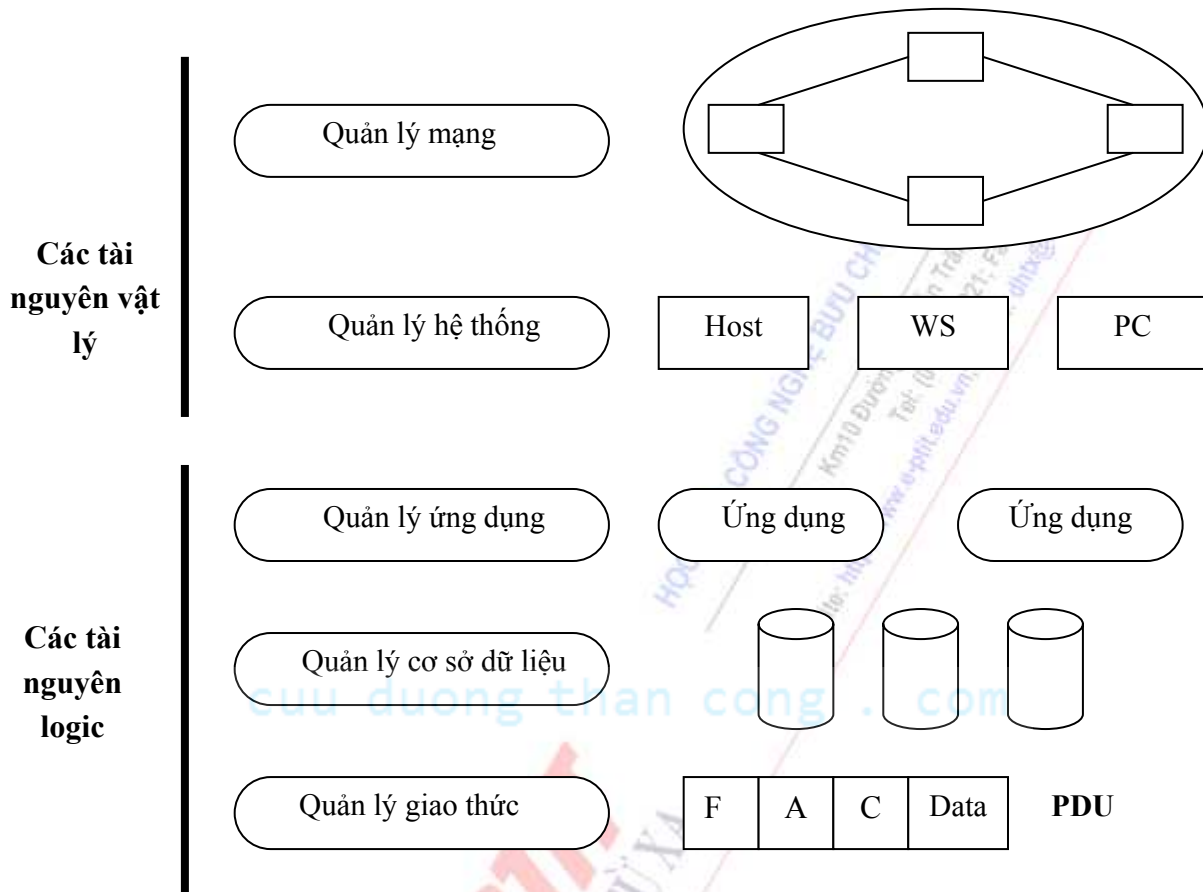
Như đã được đề cập trong phần trước của chương, quan điểm quản lý mạng lần đầu tiên được khởi phát bởi IBM. Các sản phẩm IBM NetView thực chất là sự kết hợp của quản lý hệ thống mainframe với quản lý mạng. Từ đó đến nay quan điểm về quản lý đã thay đổi rất nhiều. Đầu tiên, người ta phân tách khái niệm quản lý mạng với quản lý hệ thống máy tính. Sau này, với sự phát triển của các cơ sở nền tảng quản lý, sự khác nhau giữa quản lý mạng và quản lý hệ thống dần được xoá bỏ.

Ngày nay, khi xem xét bản chất của các tài nguyên bị quản lý, phần lớn các quan điểm đều cho rằng có hai miền quản lý chính: quản lý nguồn tài nguyên vật lý và quản lý nguồn tài nguyên logic. Các nguồn tài nguyên vật lý là các thành phần phần cứng tham gia vào quá trình trao đổi thông tin của hệ thống mạng viễn thông và mạng truyền số liệu. Miền quản lý này được gọi là quản lý mạng. Quản lý các tài nguyên vật lý của hệ thống máy tính như các bộ vi xử lý, bộ nhớ, thiết bị vào/ra, thiết bị lưu trữ ... được gọi là quản lý hệ thống.

Quản lý nguồn tài nguyên logic bao gồm quản lý các ứng dụng và quản lý các cơ sở dữ liệu. Cả hai phần này đều gắn với các hệ thống máy tính. Quản lý dịch vụ, quản lý người sử dụng, quản lý các dịch vụ giao dịch phân tán, quản lý luồng dữ liệu ... cũng được coi là quản lý nguồn tài nguyên logic (hình 1.7).

Ngoài ra còn có một miền độc lập khác được xếp vào các nguồn tài nguyên logic đặc biệt. Đó là các giao thức chuẩn trong truyền thông. Ví dụ như các giao thức phân lớp, các dịch vụ phân

lớp, các dịch vụ quản lý gắn kèm. Kiểu quản lý này được ứng dụng để quản lý các giao diện của các công nghệ đặc biệt như ATM, SONET và WDM dưới hình thức các kênh thông tin gắn kết hay các thực thể quản lý lớp LMEs (Layer Management Entities) đi cùng. Khái niệm về kiểu quản lý này đã được đưa ra trong mô hình tham chiếu cơ sở OSI, thiết lập nên kiến trúc và quản lý phân cấp chuẩn hoá.



Hình 1.7. Phân lớp miền quản lý

1.5. HỆ THỐNG QUẢN LÝ MỞ

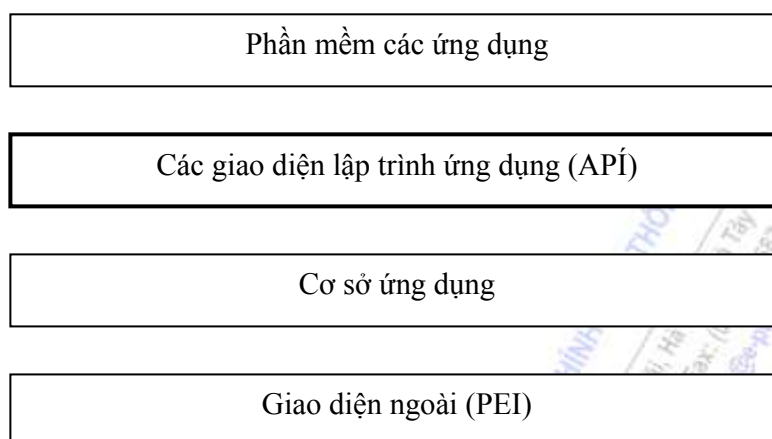
Để có thể đánh giá được các hệ thống quản lý cần phải có một mô hình tham chiếu. Đó chính là hệ thống mở và mô hình tương ứng của nó là mô hình hệ thống quản lý mở.

1.5.1. Mô hình hệ thống quản lý mở

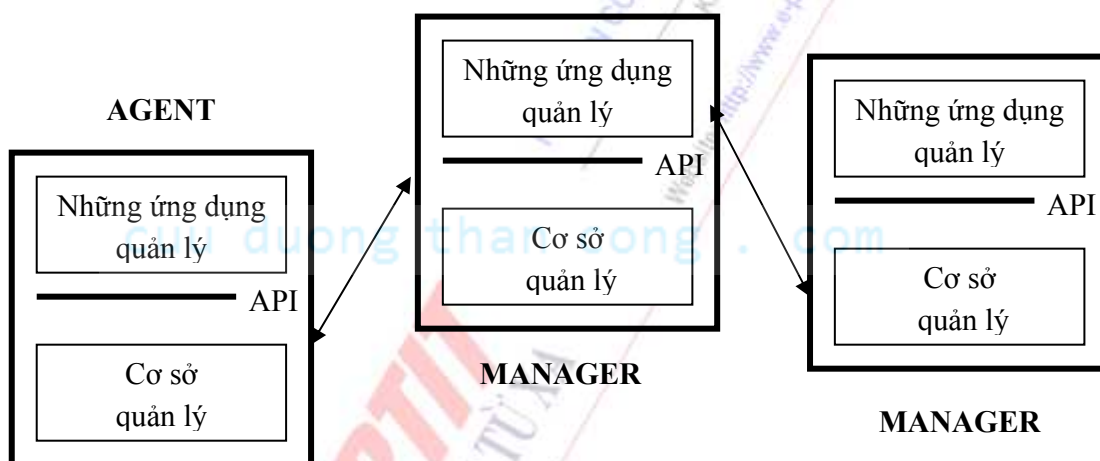
Mô hình hệ thống mở là mô hình được thiết kế dưới dạng 4 thực thể và các thực thể này phải có mối quan hệ ràng buộc lẫn nhau. Bốn thực thể đó là: Cơ sở ứng dụng, các ứng dụng, các giao diện lập trình ứng dụng APIs (Application Programming Interfaces) và giao diện ngoài PEI (Platform External Interface). (hình 1.8).

Mô hình hệ thống mở cũng được áp dụng cho các hệ thống quản lý hay nói cách khác là cho các manager và các agent. Trong trường hợp này các ứng dụng sẽ là các ứng dụng quản lý chuyên hoá cung cấp các chức năng quản lý lỗi, quản lý cấu hình, quản lý hiệu năng, bảo mật và thống kê. Cơ sở quản lý bao gồm cơ cấu tổ chức quản lý và cơ sở tính toán. Các dịch vụ quản lý chuyên hoá

bao gồm các dịch vụ quản lý sự kiện, các dịch vụ truyền thông, các dịch vụ cung cấp giao diện đồ hoạ cho người sử dụng và các dịch vụ về cơ sở dữ liệu. (hình 1.9).



Hình 1.8. Mô hình hệ thống mở



Hình 1.9. Hệ thống quản lý mở.

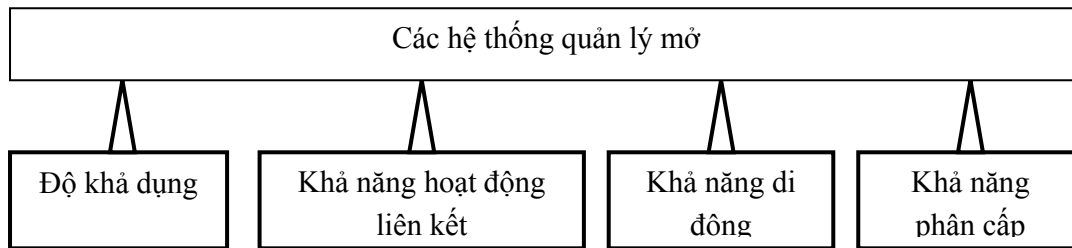
Như đã đề cập ở phía trên, thành phần mấu chốt của các hệ thống mở là các APIs. Ở đây, các APIs là các APIs chuyên hoá cho phép phát triển các ứng dụng quản lý bởi việc sử dụng các dịch vụ cơ sở quản lý chuyên hoá. Các cơ sở quản lý là các thực thể độc lập nhưng không tách biệt. Chúng truyền thông với các agent bị quản lý và với các hệ thống quản lý khác. Các giao diện ngoài trong trường hợp này là các giao diện chuẩn hoá xác định các hoạt động, các dịch vụ và các giao thức quản lý.

1.5.2. Các yêu cầu đối với hệ thống quản lý mở

Có bốn yêu cầu mô tả đặc điểm của các hệ thống mở cũng như các hệ thống quản lý mở. Đó là: độ khả dụng, khả năng hoạt động liên kết, khả năng di động và khả năng phân cấp (hình 1.10).

Độ khả dụng biểu thị khả năng dễ dàng cài đặt, vận hành và bảo dưỡng của một hệ thống quản lý. Nó cũng bao hàm cả độ ổn định và hiệu năng cao.

Khả năng hoạt động liên kết thể hiện khả năng trao đổi thông tin quản lý một cách trong suốt giữa cơ sở quản lý với các agent bị quản lý hay giữa các hệ thống quản lý ngang hàng.



Hình 1.10. Các yêu cầu đối với hệ thống quản lý mở.

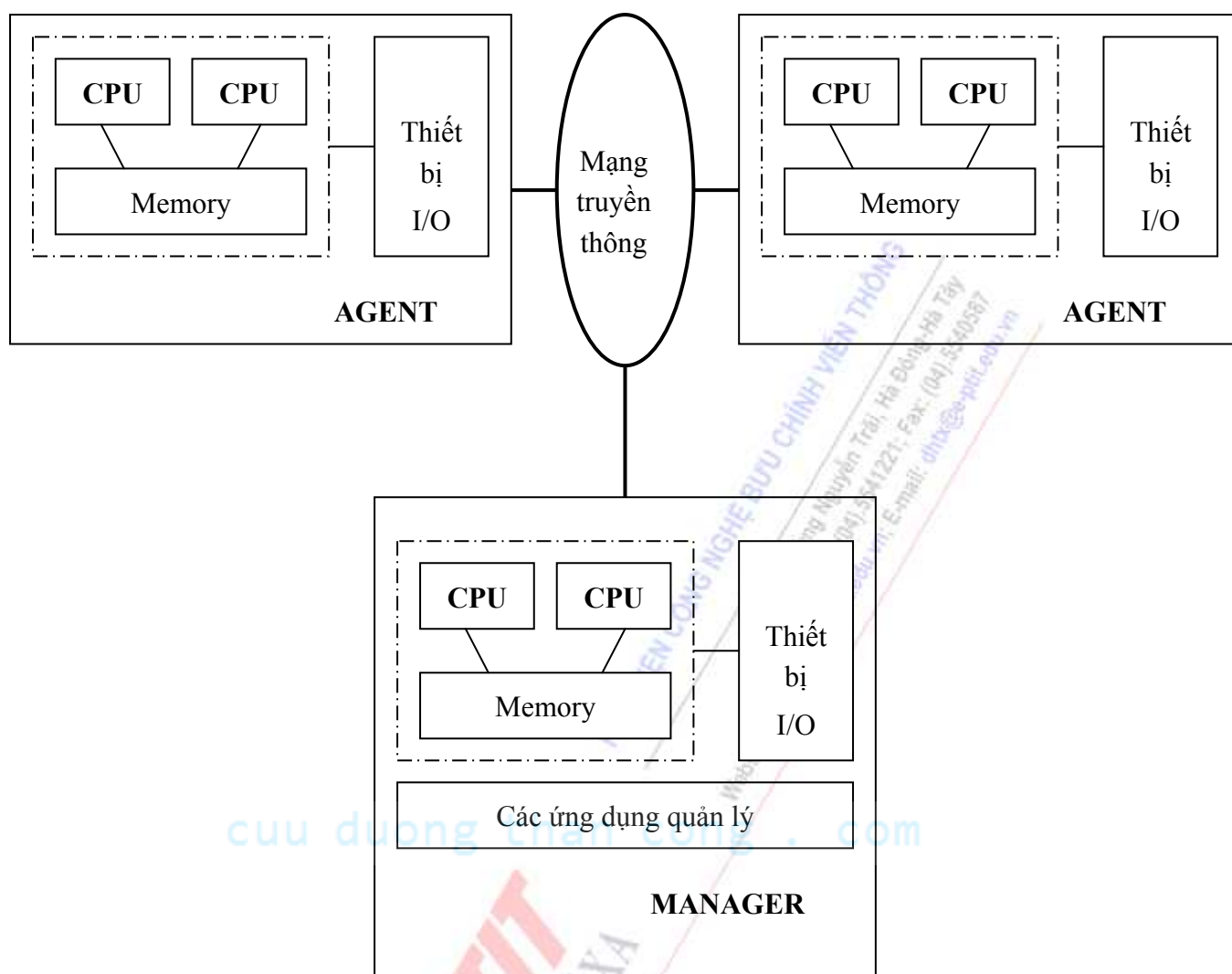
Khả năng di chuyển diễn tả sự ổn định của cơ sở quản lý hay các ứng dụng của các hệ thống quản lý khi bị thay đổi môi trường (cơ sở tính toán) hay nói cách khác, cơ sở quản lý hay các ứng dụng của các hệ thống quản lý không bị thay đổi hay sự thay đổi là tối thiểu.

Khả năng nâng cấp là khả năng hệ thống có thể nâng cấp, mở rộng phạm vi quản lý, phạm vi người sử dụng, các chức năng quản lý mà không làm thay đổi thiết kế ban đầu.

1.6. HỆ THỐNG QUẢN LÝ PHÂN TÁN

Một hệ thống (đơn xử lý hay đa xử lý) được coi là một hệ thống tự trị nếu các quá trình xử lý trong hệ thống cùng chia sẻ bộ nhớ. Trái ngược lại, hệ thống phân tán là hệ thống bao gồm các hệ thống tự trị được liên kết lại với nhau mà không có sự chia sẻ bộ nhớ.

Phần lớn các hệ thống máy tính, mạng viễn thông, mạng truyền số liệu là phân tán. Chúng liên kết lại với nhau trong một mạng truyền thông để truyền tải thông tin hay các bản tin phục vụ cho một mục đích truyền thông nào đó. Quản lý mạng có nghĩa là quản lý các tài nguyên mạng và hệ thống máy tính đa dạng mà phần lớn là tách biệt nhau về mặt vật lý. Chính vì vậy, bản chất của hệ thống quản lý mạng là phân tán.



Hình 1.11. Quản lý hệ thống phân tán

1.6.1. Kiến trúc hệ thống quản lý phân tán

Thực chất của hệ thống quản lý là tập trung hay phân tán không chỉ xác định bởi sự phân tán vật lý của phần tử (manager và agent) mà còn xác định bởi sự tập trung cũng như quá trình xử lý thông tin quản lý (hình 1.11).

Nếu một hệ thống được thiết kế để thu thập tất cả các thông tin quản lý từ tất cả các agent (thiết lập nên miền quản lý) về một điểm, người ta sẽ coi đó là hệ thống quản lý tập trung. Nếu sự thu thập thông tin quản lý phải tiến hành qua một vài quá trình xử lý liên kết với nhau và thông tin này được lưu trữ trong các cơ sở dữ liệu phân tán thì người ta coi đó là hệ thống quản lý phân tán.

Trong hệ thống quản lý phân tán đích thực, có rất nhiều người sử dụng hay nói cách khác là người điều hành mạng, tất cả đều được coi là các client quản lý, truy nhập vào các server quản lý thông qua các mạng cục bộ hay mạng diện rộng. Các manager sẽ điều khiển các ứng dụng quản lý, được nắm giữ bởi một MIB nào đó trong một miền quản lý riêng biệt. Mỗi một manager chỉ đảm nhiệm một số lượng agent cụ thể trong miền quản lý của nó.

Đối với kiến trúc quản lý phân tán thực sự, các server (hay manager) có thể trao đổi thông tin quản lý với nhau, giữ đồng bộ thông tin MIB được chia sẻ, tiếp tục miền quản lý của manager bị lỗi và các nhà điều hành hệ thống có thể tác động với nhiều manager. (hình 1.12).

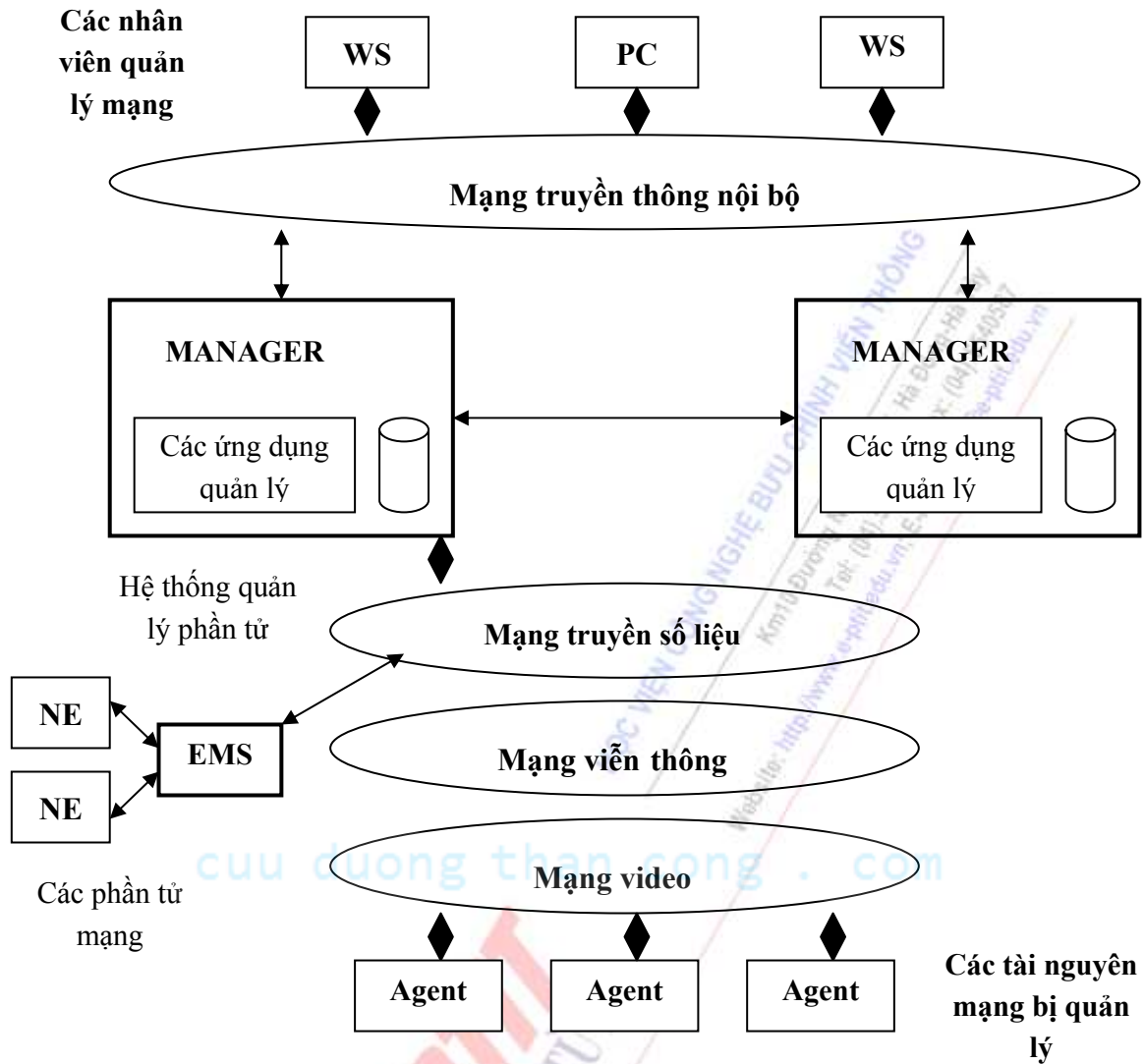
Tất nhiên với những hệ thống như kể trên đều sử dụng giả thiết manager là manager cấp cao có quyền truy nhập và cấu hình lại các agent từ xa và mỗi agent lại đóng vai trò như là một agent quản lý để thu thập thông tin về các đối tượng bị quản lý và các quá trình quản lý.

1.6.2. Hệ thống quản lý trong băng và ngoài băng

Như vậy, toàn bộ phần trên đây đã đưa ra các mô hình giới thiệu cho chúng ta biết các khái niệm về quản lý mạng, các trường quản lý, hoạt động của các liên mạng truyền tải thông tin quản lý. Nhưng tất cả đều chỉ là thiết kế hạ tầng thông tin quản lý. Phần lớn các hệ thống quản lý đều trao đổi thông tin quản lý dựa trên các mạng truyền thông, truyền tải các thông tin khác nhau như thoại, số liệu, video.

Cho mục đích quản lý, người ta cần phải tạo ra các giao thức chuyên hoá, sự vận hành và các thực thể ứng dụng chuyên hoá. Tuy nhiên các thông tin quản lý lại được truyền tải trên cùng cơ sở hạ tầng vật lý truyền thông các thông tin thương mại khác. Trong trường hợp này, người ta gọi đó là hệ thống quản lý trong băng. Đây là một giải pháp kinh tế rất hiệu quả. Tuy nhiên cũng có một vài hạn chế. Do chia sẻ cùng kênh dữ liệu nên thông tin quản lý có thể sẽ chiếm dụng một khoảng đáng kể băng tần và điều này có thể ảnh hưởng toàn diện đến hiệu năng trao đổi dữ liệu cũng như việc thu thập thông tin quản lý.

Chính vì những hạn chế kể trên mà một vài hệ thống quản lý đã sử dụng các kênh ngoài băng (out-of-band channels). Hệ thống quản lý ngoài băng đưa ra giải pháp sử dụng các dải băng tần nằm ngoài dải tần truyền thông dữ liệu. Ví dụ như sử dụng dải tần thấp của kênh thoại truyền thống (50 Hz - 200 Hz) để tạo ra các kênh số liệu truyền thông tin quản lý.



Hình 1.12. Kiến trúc quản lý mạng phân tán.

Giải pháp trên đây được sử dụng để quản lý các modem băng tần thoại. Một giải pháp khác là sử dụng các bit dự trữ trong luồng bit truyền tải (ví dụ các bit trong ghép kênh luồng T1) để tạo ra các kênh dữ liệu dùng cho mục đích quản lý hoặc sử dụng các trường ấn định trong các khung hoặc tế bào phát của công nghệ SONET và ATM.

CÂU HỎI ÔN TẬP CHƯƠNG 1

1. Các chức năng quản lý lớp cao của hệ thống quản lý mạng là:
 - a. Giám sát, điều khiển và đưa ra báo cáo.
 - b. Phát hiện lỗi, giám sát và điều khiển.
 - c. Định cấu hình, giám sát và đưa ra báo cáo.
 - d. Điều khiển, bảo mật truy nhập và định cấu hình.
2. Thuật ngữ “quản lý mạng” được chấp nhận vào giữa những năm 80 của thế kỷ trước nhờ sự ra đời bộ công cụ quản lý của

- a. IBM.
 - b. Compact.
 - c. HP.
 - d. Alcatel.
3. Manager chính là:
- a. Thực thể quản lý.
 - b. Thực thể bị quản lý.
 - c. Agent.
 - d. Các nguồn tài nguyên bị quản lý.
4. Agent chính là:
- a. Thực thể bị quản lý.
 - b. Thực thể quản lý.
 - c. Các nguồn tài nguyên bị quản lý.
 - d. đối tượng trung gian thể hiện sự tương tác giữa manager và các nguồn tài nguyên bị quản lý.
5. Mô hình thông dụng cho việc mô tả sự tương tác giữa thực thể quản lý và thực thể bị quản lý là:
- a. Manager -Agent.
 - b. Client - Server.
 - c. Application -Object server.
6. Cơ chế yêu cầu - phản hồi là cơ chế
- a. Đồng bộ.
 - b. Cận đồng bộ.
 - c. Không đồng bộ.
7. Cơ chế gửi thông báo là cơ chế
- a. Đồng bộ.
 - b. Cận đồng bộ.
 - c. Không đồng bộ.
8. MIB là từ viết tắt của:
- a. Management Information Base.
 - b. Mathematics Information Base.
 - c. Management Information Basic.
 - d. Management Informatic Base.
9. Phần lớn các quan điểm hiện tại đều cho rằng, có miền quản lý chính.
- a. 1.
 - b. 2.
 - c. 3.
 - d. 4.

10. Hệ thống quản lý phân tán là hệ thống:

- a. Đơn xử lý.
- b. Đa xử lý.
- c. Chia sẻ bộ nhớ.
- d. Bao gồm các hệ thống tự trị và không chia sẻ bộ nhớ.

11. Hệ thống quản lý ngoài băng là hệ thống

- a. Sử dụng các dải băng tần nằm ngoài dải tần truyền thông dữ liệu.
- b. Sử dụng các bit dự trữ trong luồng bit truyền tải.
- c. Sử dụng các trường ấn định trong các khung hoặc tế bào phát của công nghệ SONET hoặc ATM.
- d. Cả ba đặc điểm trên.

12. Quản lý các giao thức chuẩn trong truyền thông được xếp vào miền quản lý nào?

- a. Nguồn tài nguyên vật lý.
- b. Nguồn tài nguyên logic.
- c. Miền quản lý đặc biệt không trực thuộc hai miền kể trên.

HỌC VIỆN CÔNG NGHỆ LƯU CHỈNH KIẾN THỨC
Số 10 Đường Nguyễn Trãi, Hà Nội - Việt Nam
Tel: (04) 35405587
Web: <http://www.viettel.com.vn>; Email: dhk@vnet.vn

cuu duong than cong . com

CHƯƠNG TRÌNH PTIT
ĐÀO TẠO ĐẠI HỌC TỪ XA
cuu duong than cong . com

CHƯƠNG 2

MẠNG QUẢN LÝ VIỄN THÔNG TMN

Mục đích của chương 2 là cung cấp cho người học các nội dung liên quan đến mạng quản lý viễn thông TMN. Với xu hướng của việc quản lý tập trung dựa trên các giao thức và các tiêu chuẩn được chuẩn hóa và mong muốn nâng cao năng lực của mạng, TMN ra đời đáp ứng những yêu cầu đó.

Hiện nay, vấn đề quản lý mạng luôn là mối quan tâm hàng đầu và là một trong những vấn đề quan trọng nhất trong mạng viễn thông của các nhà khai thác viễn thông. Với những khả năng mà hệ thống quản lý mạng viễn thông đem lại, cùng với sự phát triển của mạng lưới các nhà khai thác đều xây dựng cho mình các hệ thống quản lý mạng để áp dụng quản lý cho các mạng riêng. Nhằm đạt được thống nhất giữa các hệ thống quản lý mạng, khả năng liên kết cũng như nâng cao năng lực và hiệu quả sử dụng của các hệ thống Liên minh viễn thông quốc tế (ITU-T) đã đưa ra các khuyến nghị và các mô hình mạng quản lý viễn thông (TMN). Trong chương này trình bày các nội dung về nguyên lý của TMN, các chuẩn liên quan đến TMN cũng như các nội dung về các mô hình chức năng, mô hình vật lý, các giao diện quản lý...

Học viên cần nắm bắt được các yêu cầu chung về quản lý viễn thông, các thực thể vật lý cũng như các thực thể chức năng trong mạng quản lý viễn thông TMN và đặc biệt là các giao diện quản lý và các chức năng quản lý trong TMN.

2.1 NGUYÊN LÝ CHUNG VÀ CÁC KHUYẾN NGHỊ TMN

2.1.1 Khái niệm và nguyên lý của TMN

TMN (Telecommunication Management Network) là mạng quản lý viễn thông cung cấp các hoạt động quản lý liên quan tới mạng viễn thông. ITU-T đã công bố từ năm 1988 một số khuyến nghị về các hệ thống quản lý điều hành mạng viễn thông. Các khuyến nghị này tập hợp thành họ khuyến nghị M.30. Các khuyến nghị này thường xuyên được bổ sung, sửa đổi nhằm đưa đến những tiêu chuẩn thống nhất về hệ thống điều hành, quản lý mạng viễn thông đối với toàn cầu.

Trước hết, như định nghĩa trong khuyến nghị của ITU-T M.3100 (1995) do nhóm nghiên cứu IV: ***“TMN là một mạng riêng liên kết các mạng viễn thông tại những điểm khác nhau để gửi/nhận thông tin đi/dến mạng và để điều khiển các hoạt động của mạng”***. Nói một cách khác, TMN sử dụng một mạng quản lý độc lập để quản lý mạng viễn thông bằng các đường thông tin riêng và các giao diện đã được chuẩn hoá.

TMN chứa nhiều hệ điều hành, một mạng thông tin dữ liệu và những phần tử quản lý. TMN chỉ ra trạng thái thực hiện chức năng quản lý của phần tử mạng thuộc phạm vi của TMN (như hệ thống chuyên mạch, hệ thống truyền dẫn .v.v.). Ở dưới là mạng dữ liệu mà TMN dùng để truyền tải thông tin quản lý có thể giống như một mạng mà TMN quản lý hoặc được thiết kế như mạng truyền dẫn. TMN phải cung cấp các chức năng và thông tin quản lý giữa các hệ điều hành với nhau, giữa các hệ điều hành với các thành phần mạng và các thông tin liên quan tới các hệ điều hành khác.

Mạng quản lý viễn thông cung cấp các chức năng quản lý và truyền thông cho việc khai thác, quản lý, bảo dưỡng mạng và các dịch vụ viễn thông trong môi trường đa nhà cung cấp thiết

bị. Mạng quản lý viễn thông thống nhất việc điều hành quản lý các mạng khác nhau trong đó các thông tin quản lý được trao đổi qua các giao diện và giao thức đã chuẩn hoá.

TMN không chỉ quản lý sự đa dạng của mạng viễn thông mà còn quản lý một phạm vi lớn về thiết bị, phần mềm và những dịch vụ trên mỗi mạng. Sau đây là một số ví dụ về các mạng, các dịch vụ viễn thông và một số thiết bị chính có thể được quản lý bởi TMN:

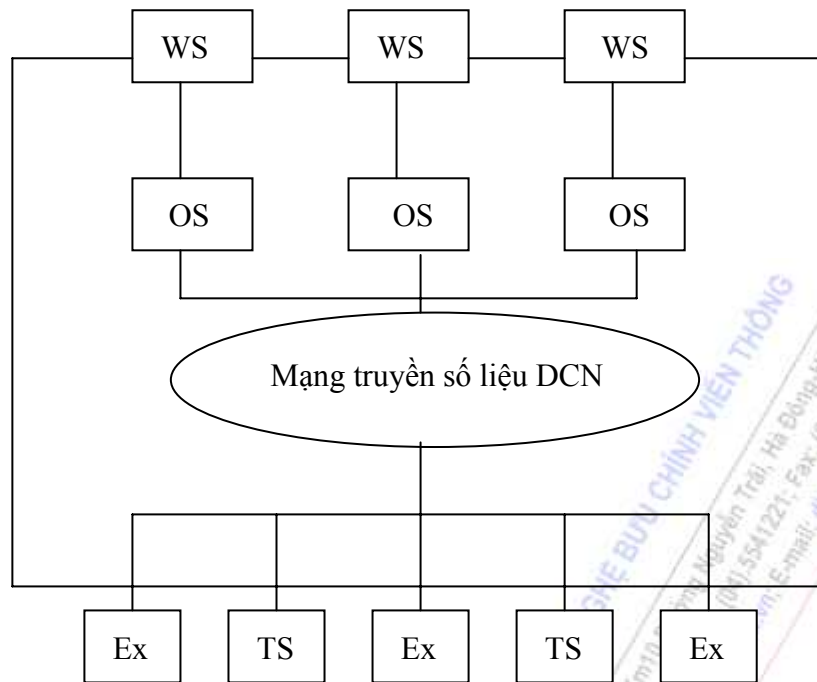
- Các mạng công cộng và mạng riêng bao gồm cả mạng dịch vụ ISDN (Intergrated Services Digital Network) băng rộng và băng hẹp (bao gồm cả ATM), các mạng thông tin di động, các mạng thoại riêng, các mạng riêng ảo và các mạng thông minh.
- Bản thân TMN.
- Các thiết bị truyền dẫn (bộ ghép kênh, bộ phối luồng, thiết bị chuyển kênh SDH...).
- Các hệ thống truyền dẫn số và tương tự (cáp, cáp sợi quang, vô tuyến, vệ tinh...).
- Các tổng đài số và tương tự.
- Các mạng WAN, LAN, MAN.
- Các mạng chuyển mạch gói và chuyển mạch kênh.
- Các dịch vụ viễn thông, các dịch vụ kèm theo và đầu cuối người sử dụng.

2.1.2 Quan hệ giữa TMN và mạng viễn thông

Nhiệm vụ của mạng quản lý viễn thông là quản lý để khai thác các dịch vụ trên mạng viễn thông có hiệu quả, đồng thời nó hỗ trợ các dịch vụ viễn thông tạo ra nguồn doanh thu mới và giảm chi phí quản lý, khai thác và bảo dưỡng mạng. Vì vậy nó phải đảm bảo tính linh hoạt, có khả năng mở rộng và nâng cấp, tiết kiệm tài nguyên mạng. Mạng quản lý viễn thông có thể quản lý tập trung hoặc phân tán phù hợp với quy mô mạng quản lý, nó có thể là một mạng rất đơn giản kết nối một hệ thống khai thác (OS) với một thành phần mạng (NE), nó có thể là một mạng rất phức tạp kết nối nhiều OS, NE và máy trạm (WS).

Mạng quản lý viễn thông không chỉ cung cấp chức năng quản lý và truyền thông giữa các OS, giữa OS và các phần tử mạng viễn thông, nó còn có thể cung cấp các chức năng quản lý và truyền thông cho các mạng quản lý khác để hỗ trợ quản lý cho các mạng viễn thông quốc gia và quốc tế.

Mạng viễn thông gồm rất nhiều thiết bị viễn thông (số hoặc tương tự) như các hệ thống truyền dẫn, hệ thống chuyển mạch, các thiết bị ghép kênh, các bộ xử lý điều khiển, các thiết bị đầu cuối... trong mạng quản lý viễn thông chúng được gọi là các phần tử mạng (NE). Lưu ý rằng về mặt chức năng, TMN là một mạng riêng để quản lý mạng viễn thông, nó đáp ứng nhu cầu trao đổi thông tin quản lý, nó kết nối với mạng viễn thông và các mạng khác qua các điểm tham chiếu khác nhau, hay nói cách khác một số phần của mạng TMN có thể là một mạng logic gắn kết trong mạng viễn thông. Hình 2.1 mô tả mối quan hệ giữa TMN và mạng viễn thông.



Hình 2.1: Mối quan hệ giữa TMN và mạng viễn thông

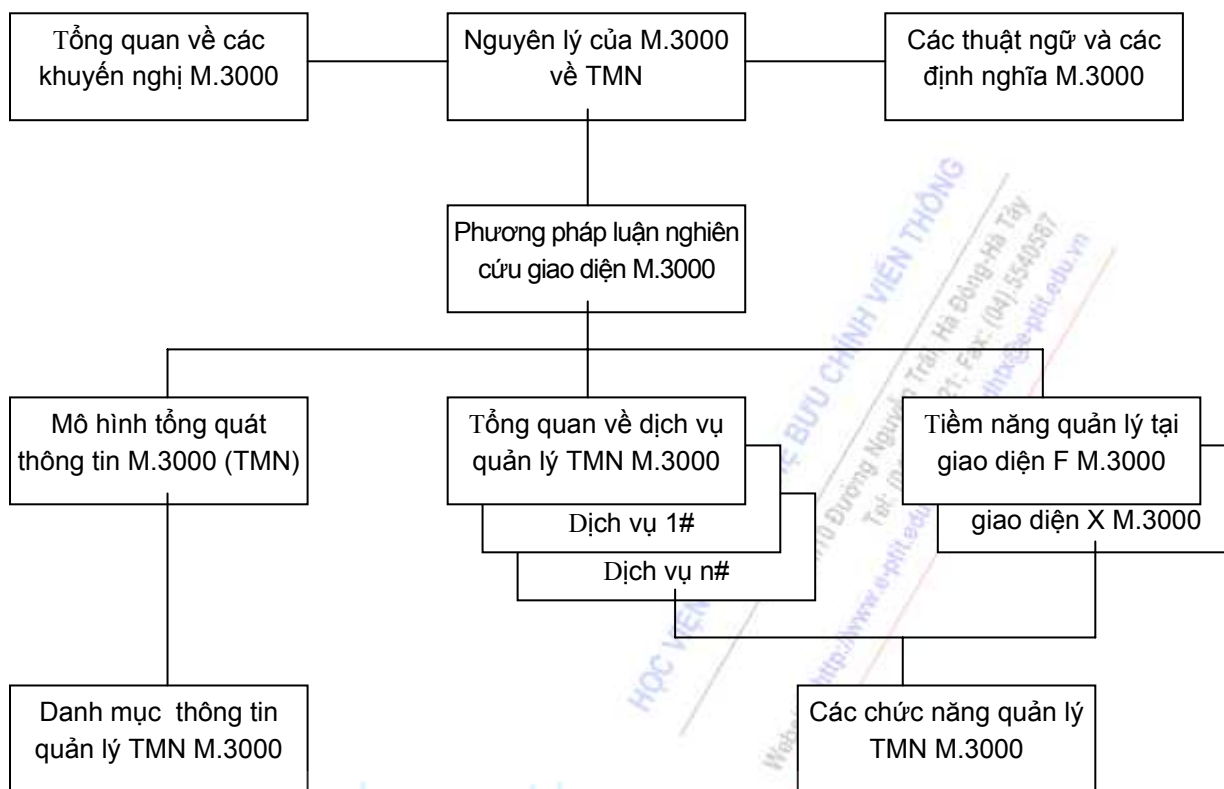
2.1.3 Các khuyến nghị của TMN

TMN được Ban dịch vụ của Liên minh Viễn thông Quốc tế (ITU-T - International Telecommunications Union - Telecommunications Services Sector) xác định trong chuỗi các khuyến nghị M.30. Bảng 2.1 dưới đây cho ta thấy các khuyến nghị của TMN và ngày ban hành, sửa đổi bổ sung mới nhất.

Bảng 2.1: Các khuyến nghị của TMN

Tiêu đề của khuyến nghị	Ký hiệu	Ngày
Tổng quan về các khuyến nghị TMN	M.3000	10/94
Các nguyên tắc cho TMN	M.3010	05/96
Thông số kỹ thuật giao diện TMN	M.3020	07/95
Mô hình thông tin mạng quản lý	M.3100	07/95
Báo cáo sự thích ứng đối tượng quản lý cho Mô hình giao diện mạng	M.3101	07/95
Tập hợp các thông tin quản lý TMN	M.3180	10/92
Các dịch vụ quản lý TMN: tổng quan	M.3200	10/92
Các dịch vụ quản lý TMN: bảo dưỡng của quản lý B-ISDN	M.3207.1	05/96
Các dịch vụ quản lý TMN: Lỗi và thực hiện quản lý cho truy nhập ISDN	M.3211.1	05/96
Khả năng quản lý TMN tại giao diện F	M.3300	10/92
Khung yêu cầu quản lý cho giao diện X của TMN	M.3320	04/97
Các chức năng quản lý của TMN	M.3400	04/97

Khi các mạng viễn thông mang có TMN chúng trở thành dễ dàng phối hợp về mạng và thiết bị giữa các nhà cung cấp dịch vụ với nhau. Tóm lại khả năng phối hợp có thể đạt được giữa các mạng được điều hành.



Hình 2.2: Mối liên hệ giữa các khuyến nghị TMN

TMN sử dụng các nguyên tắc hướng đối tượng điều hành và các giao diện chuẩn xác định truyền thông giữa các thực thể điều hành trên mạng. Chuẩn giao diện điều hành dành cho TMN được gọi là giao diện Q3. Kiến trúc TMN và các giao diện được định nghĩa trong các khuyến nghị M.3000, được xây dựng trên cơ sở các chuẩn kết nối các hệ thống mở (OSI - Open System Interconnection) hiện hành. Những chuẩn này bao gồm nhưng không giới hạn đến :

- Thủ tục thông tin điều hành chung (CMIP - Common Management Information Protocol) - xác định các dịch vụ trao đổi giữa các thực thể là như nhau.
- Gợi ý để xác định các đối tượng điều hành (GDMO - Guideline For Definition of Managed Objects) - cung cấp tạm thời cho việc phân loại và mô tả các nguồn lực được điều hành.
- Một chú ý syntax rút gọn (ASN.1 - Abstract Syntax Notation One) - cung cấp luật syntax cho các kiểu dữ liệu.
- Mô hình quy chiếu kết nối hệ thống mở (Open Systems Interconnect Reference Model) - xác định 7 lớp của mô hình quy chiếu OSI.

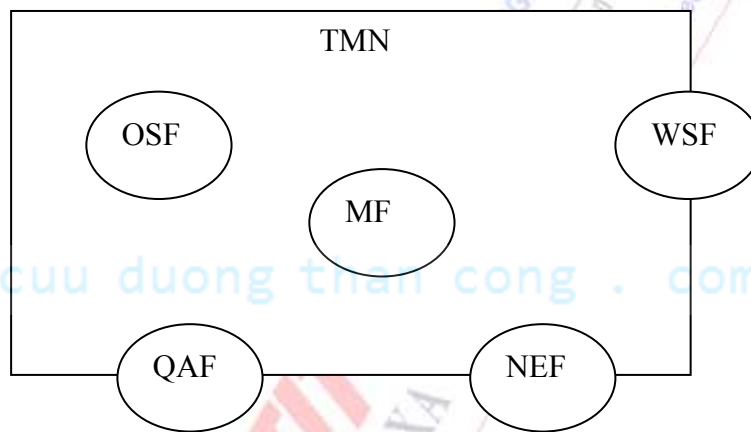
Từ khi ban hành, các chuẩn TMN đã được bám sát và theo nó là hàng loạt các tổ chức xây dựng tiêu chuẩn như Diễn đàn điều hành mạng (Network Management Forum - NMF), hãng Bellcore, Viện tiêu chuẩn Viễn thông Châu Âu (ETSI - European Telecommunications Standards Institute). Tổng thể NMF và Bellcore đã tạo nên các yêu cầu chi tiết; tại cùng thời điểm đó các

diễn đàn công nghệ trung tâm như: Diễn đàn phối hợp khai thác Mạng cáp quang đồng bộ SIF (SONET - Synchronous Optical Network Interoperability Forum) và diễn đàn Phương thức truyền dẫn không đồng bộ ATMF (Asynchronous Transfer Mode Forum) cùng đưa ra các giao diện phù hợp yêu cầu điều hành của TMN.

2.2 KIẾN TRÚC CHỨC NĂNG

TMN có ý nghĩa đối với truyền tải và quá trình thông tin liên quan tới việc quản lý các mạng thông tin. Cấu trúc chức năng của TMN bao gồm một tập các khối chức năng, một tập các điểm tham chiếu và một tập các chức năng. Khối chức năng là thực thể logic trình diễn chức năng quản lý quy định. Các điểm tham chiếu hay còn gọi là điểm tiêu chuẩn phân chia giữa hai khối chức năng và hai khối chức năng thông tin với nhau thông qua điểm tham chiếu. Một hoặc nhiều hơn các chức năng thành phần tạo ra một khối chức năng, việc truyền thông tin giữa các khối là chức năng thông tin số liệu.

Các khối chức năng được minh họa trong hình vẽ:



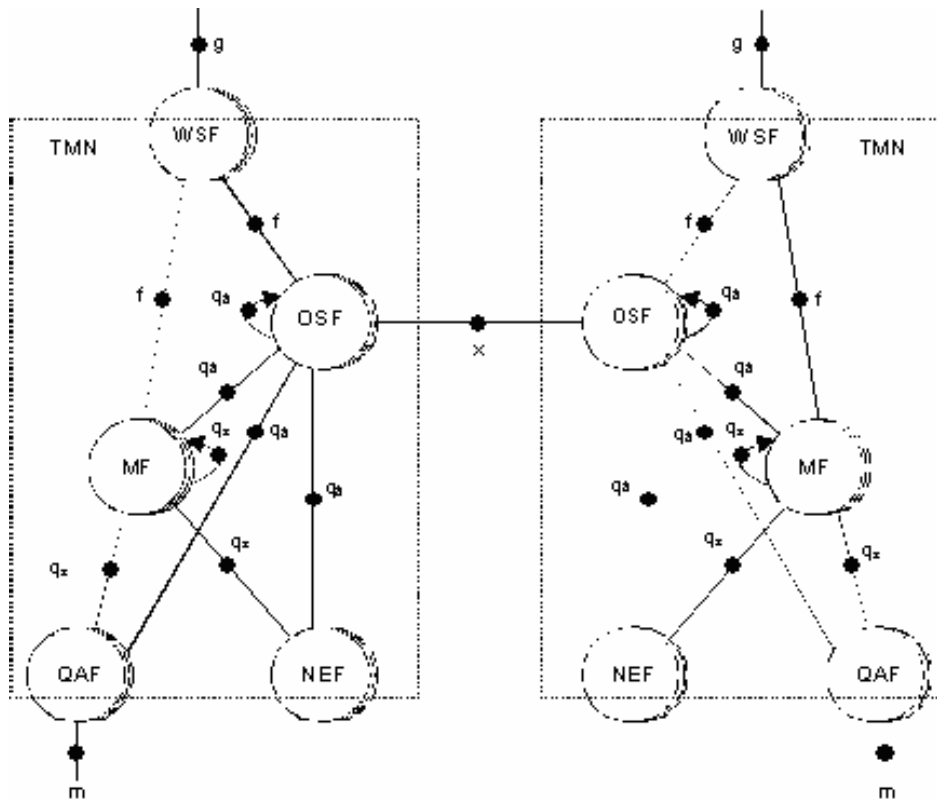
Hình 2.3: Các khối chức năng của TMN

Chức năng của TMN bao gồm:

- Chức năng phân tử mạng NEF.
- Chức năng hệ thống điều hành OSF.
- Chức năng trạm làm việc WSF.
- Chức năng thích ứng QAF
- Chức năng trung gian MF.

Chức năng của TMN là cung cấp các phương tiện để truyền tải và xử lý các thông tin có liên quan đến vấn đề quản lý mạng viễn thông và dịch vụ. Ta xem xét các thành phần dưới đây:

- Một tập các chức năng quản lý để giám sát, điều khiển và kết hợp mạng.
- Một tập các phân tử mạng được quản lý.
- Khả năng cho người sử dụng TMN truy nhập hoạt động quản lý và nhận được sự trình bày về kết quả của hoạt động.



Hình 2.4: Các khối chức năng và các điểm tham chiếu

Các điểm tham chiếu và giao diện trong TMN sẽ được trình bày trong mục 2.3 về kiến trúc vật lý TMN.

2.2.1. Chức năng phần tử mạng NEF

NEF (Network Element Function) là một khối chức năng thông tin của TMN nhằm mục đích giám sát hoặc điều khiển. NEF cung cấp các chức năng viễn thông và hỗ trợ trong mạng viễn thông cần được quản lý. NEF bao gồm các chức năng viễn thông - đó là chủ đề của việc quản lý. Các chức năng này không phải là thành phần của TMN nhưng được thể hiện đối với TMN thông qua NEF.

2.2.2. Chức năng hệ điều hành OSF.

OSF (Operation System Function) cung cấp các chức năng quản lý. OSF xử lý các thông tin quản lý nhằm mục đích giám sát phối hợp và điều khiển mạng viễn thông.

Chức năng này bao gồm:

- Hỗ trợ ứng dụng các vấn đề về cấu hình, lỗi, hoạt động, tính toán, và quản lý bảo mật.
- Chức năng tạo cơ sở dữ liệu để hỗ trợ: cấu hình, topology, tình hình điều khiển, trạng thái và tài nguyên mạng.
- Hỗ trợ cho khả năng giao tiếp giữa người và máy thông qua thiết bị đầu cuối của người sử dụng.
- Các chương trình phân tích cung cấp khả năng phân tích lỗi và phân tích hoạt động.

- Khuôn dạng dữ liệu và bản tin hỗ trợ thông tin giữa hai thực thể chức năng TMN hoặc giữa hai khối chức năng TMN của các thực thể bên ngoài (người sử dụng hoặc một TMN khác).
- Phân tích và quyết định, tạo khả năng cho đáp ứng quản lý. Có hai khía cạnh: hỗ trợ cho phần tử được quản lý bởi OSF, cung cấp các chức năng viễn thông là các đối tượng quản lý cho mạng viễn thông cần được quản lý. Sự quản lý này được thể hiện đối với TMN thông qua các chức năng hỗ trợ lưu lượng. Các chức năng cấu trúc không phải là một phần của TMN, tuy nhiên các chức năng hỗ trợ lại là một phần bản thân TMN.

2.2.3. Chức năng trạm làm việc WSF.

WSF (Work Station Function) cung cấp chức năng cho hoạt động liên kết giữa người sử dụng với OSF. WSF có thể được xem như chức năng trung gian giữa người sử dụng và OSF. Nó chuyển đổi thông tin ra khỏi OSF thành khuôn dạng có khả năng thể hiện được với người sử dụng. Vị trí của WSF như một cổng giao tiếp nằm trên ranh giới của TMN.

2.2.4. Chức năng thích ứng Q

QAF (Q Adapter Function) cung cấp sự chuyển đổi để kết nối NEF hoặc OSF tới TMN, hoặc những phần tử mạng không thuộc TMN với TMN một cách độc lập.

Chức năng thích ứng Q được sử dụng để liên kết tới các phần tử TMN mà chúng không hỗ trợ các điểm tham chiếu TMN chuẩn. Một ví dụ được minh họa ở hình vẽ dưới. Trong ví dụ này một thực thể chức năng điều hành phi TMN (non-TMN OSF) và một thực thể phần tử mạng phi TMN (non-TMN NEF) được kết nối tới TMN. Nhiệm vụ của cả hai QAF là biên dịch giữa điểm tham chiếu q và điểm tham chiếu m. Vì q là các điểm tham chiếu TMN còn m là các điểm tham chiếu phi TMN, hình vẽ chỉ ra QAF tại biên của TMN.



Hình 2.5: Chức năng thích ứng Q

2.2.5. Chức năng trung gian MF

MF (Mediation Function) hoạt động để truyền thông tin giữa OSF và NEF, cung cấp chức năng lưu trữ, lọc, biến đổi... trên các dữ liệu nhận được từ NEF. Chức năng trung gian hoạt động trên thông tin truyền qua giữa các chức năng quản lý và các đối tượng quản lý. MF cung cấp một tập các chức năng cổng nối (Gateway) hay chuyển tiếp (Relay), nó làm nhiệm vụ cất giữ (lưu), biến đổi phù hợp, lọc phân định và tập trung thông tin. Vì MF cũng bao gồm các chức năng xử lý và truyền tải thông tin, do đó không có sự phân biệt lớn giữa MF và OSF.

Các chức năng của MF:

Các chức năng truyền tải thông tin ITF (Information Transfer Function).

- Biến đổi giao thức.

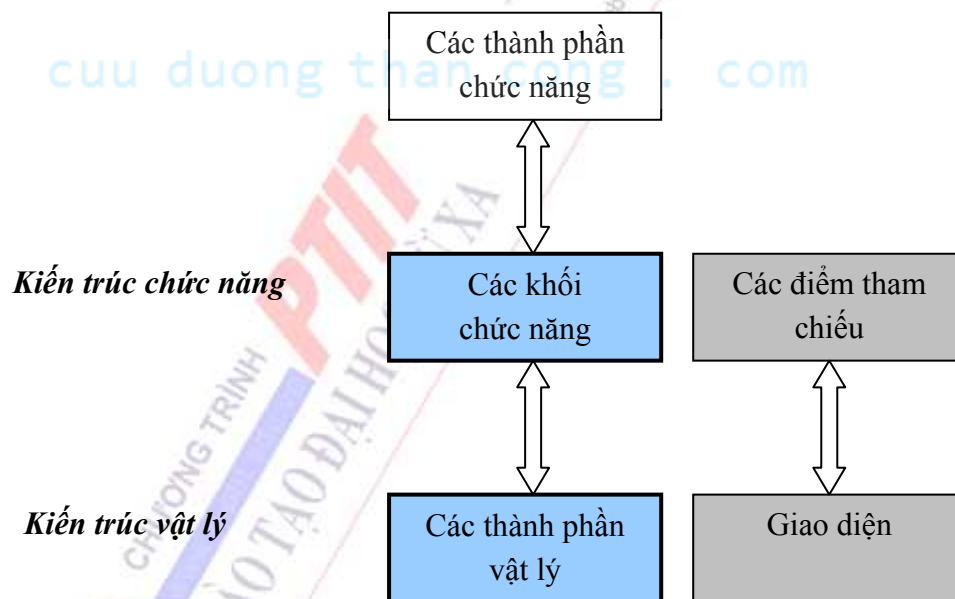
- Biến đổi bản tin.
- Biến đổi tín hiệu.
- Dịch/ ánh xạ địa chỉ.
- Định tuyến.
- Tập trung.

Các chức năng xử lý thông tin:

- Thực hiện.
- Hiển thị.
- Lưu giữ.
- Lọc.

2.3 KIẾN TRÚC VẬT LÝ

Tiếp theo mô hình chức năng, kiến trúc vật lý TMN chỉ rõ giới hạn của các nút mạng và các giao diện thông tin giữa các nút. Các nút (như OS và các phần tử mạng) và các sự liên kết giữa các nút có thể được ánh xạ tới cả những thực thể phần cứng và phần mềm. TMN bao gồm năm loại nút khác nhau và 4 loại liên kết. Mỗi nút được ký hiệu bởi chức năng cung cấp bởi nút đó. Mỗi đường liên kết được ký hiệu bởi giao diện giữa hai nút.



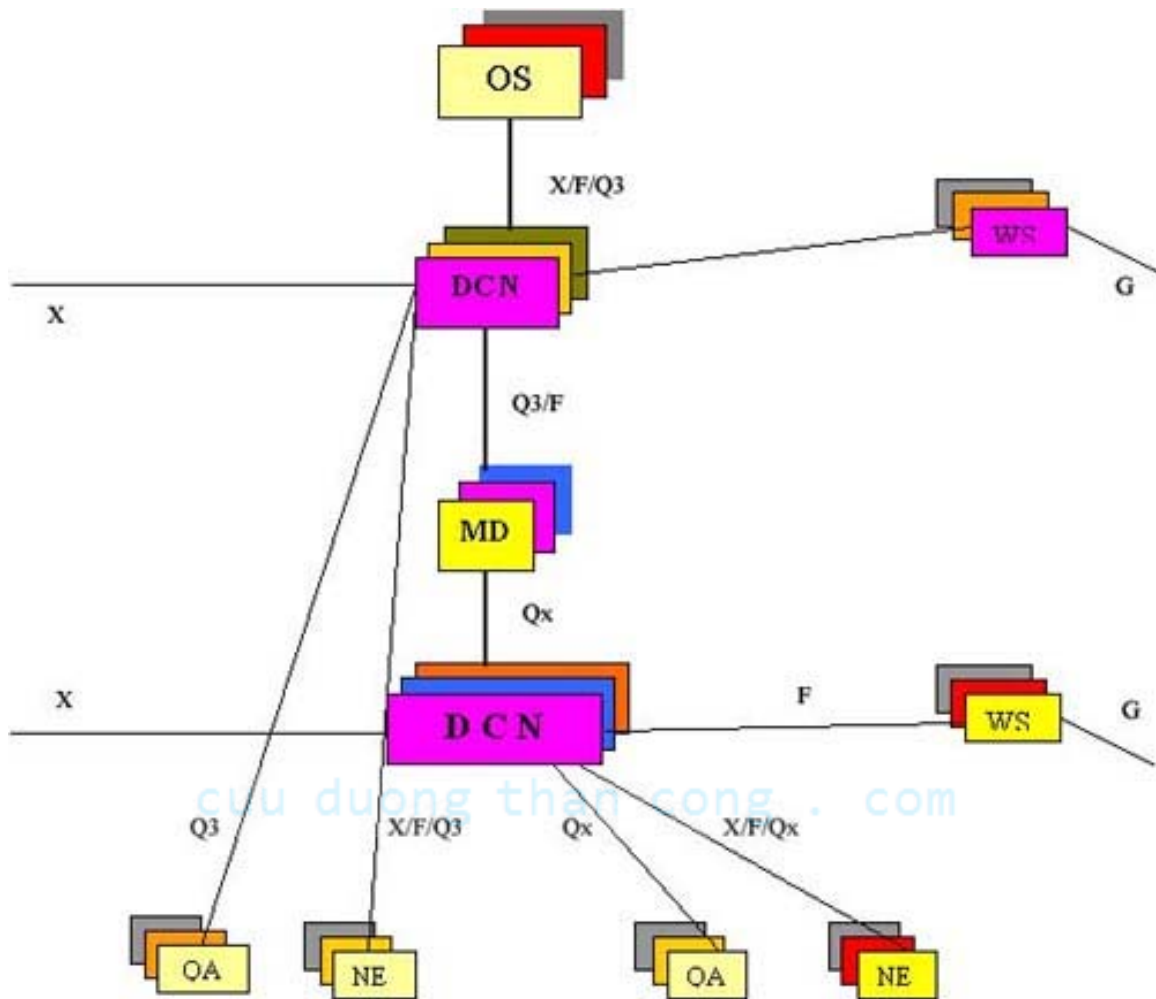
Hình 2.6: Quan hệ giữa mô hình chức năng và kiến trúc vật lý

TMN là một mạng, nó có nút, đường liên kết và các giao diện. Nút trong TMN có thể là một hệ thống phần cứng, một hệ ứng dụng phần mềm hoặc kết hợp cả hai.

2.3.1. Các khối vật lý

Các chức năng quản lý có thể được thực hiện trong sự khác nhau của các cấu hình vật lý. Mỗi quan hệ của các khối chức năng tới thiết bị vật lý được trình bày ở bảng 2.2. Nó định rõ các khối vật lý quản lý theo tập các khối chức năng mà mỗi khối này được cho phép để chứa đựng.

Đối với mỗi khối vật lý, có một khối chức năng mà là đặc điểm của nó và có tính chất bắt buộc để chứa đựng. Nơi đó còn tồn tại các chức năng khác tùy chọn cho các khối vật lý để bao hàm.



Hình 2.7: Kiến trúc vật lý TMN

2.3.1.1 Hệ điều hành OS:

OS là hệ thống mà thực hiện các chức năng hệ điều hành OSF như đã miêu tả trong kiến trúc chức năng TMN. OS có thể cung cấp tùy chọn và QAF và các WSF. Trong thực tế nó xử lý thông tin có liên quan tới quản lý viễn thông nhằm mục đích theo dõi điều khiển và giám sát mạng viễn thông. OS cung cấp khả năng chủ yếu của hệ thống quản lý TMN, OS cung cấp khả năng giám sát hoặc khả năng điều khiển cho đáp ứng quản lý. Một OS có thể được kết nối với OS khác, với cả một TMN giống nó hoặc một TMN khác.

Cấu hình chức năng của OS:

Cấu hình của OS phụ thuộc cấu hình của OSF. Một OSF dịch vụ có liên quan tới các khía cạnh dịch vụ mạng và thực hiện hầu hết các quy tắc của giao diện khách hàng. Một OSF là một mạng cơ sở ứng dụng TMN, chịu trách nhiệm cung cấp mức thông tin mạng cho OSF dịch vụ. Nó liên lạc với NEF hoặc MF để mang theo các chức năng quản lý trên phần tử mạng.

Cấu hình vật lý của một OS:

Cấu trúc vật lý của OS có khả năng thực hiện các việc phân phối hoặc tập hợp. Một OS tập hợp bộ chức năng OS hoàn chỉnh trong một hệ thống đơn. Một OS phân phối có thể có chức năng phân phối dọc theo số lượng của các OS:

- Yêu cầu thời gian thực cho lựa chọn giao thức TMN, đây là một nhân tố rất quan trọng trong kiến trúc vật lý của OS. Sự lựa chọn phần cứng phụ thuộc rất nhiều vào việc có hay không một OS cung cấp dịch vụ thời gian thực, gần thời gian thực hay không phải thời gian thực.
- Truyền tải thông tin quản lý. Cho một OS phân phối, phần tử mạng phải liên lạc và quản lý rất nhiều OS.
- Yêu cầu dung sai lỗi. Một OS phân phối ít khi xảy ra sự cố nghiêm trọng do nguyên nhân là sự kết nối không thành công của kênh lẻ.
- Nghiên cứu quản lý và tổ chức.

2.3.1.2 Phân tử mạng NE:

Phân tử mạng NE bao gồm thiết bị viễn thông (hoặc các nhóm/các phần của thiết bị viễn thông) và thiết bị trợ giúp hoặc bất kỳ mục hoặc các nhóm, các mục tính toán liên quan tới môi trường viễn thông mà thực hiện các NEF.

Phân tử mạng NE có thể bao gồm bất kỳ tùy chọn của các khối chức năng quản lý theo các yêu cầu thực hiện của nó. NE có một hoặc nhiều hơn các giao diện loại Q tiêu chuẩn và có thể có tùy chọn các giao diện F và B2B/C2B.

NE tồn tại như thiết bị mà không có một giao diện tiêu chuẩn sẽ giành được sự truy cập tới cơ sở hạ tầng quản lý thông qua một chức năng tương thích Q. Chức năng tương thích Q này sẽ cung cấp chức năng cần thiết để biến đổi giữa giao diện quản lý tiêu chuẩn và không tiêu chuẩn.

Bảng 2.2: Môi quan hệ của khối vật lý và khối chức năng quản lý

	NEF	MDF	QAF	OSF	WSF
NE	M*	O	O	O	O
MD		M	O	O	O
QA			M		
OS		O	O	M	O
WS					M
M: Bắt buộc O: Tùy chọn					

2.3.1.3 Thiết bị trung gian MD

Một MD thực hiện chức năng trung gian như đã định nghĩa trong kiến trúc chức năng TMN. Nhiệm vụ của chức năng trung gian là xử lý thông tin truyền giữa OS và phân tử mạng đảm bảo làm cho thông tin phù hợp. Chức năng tại những điểm này có thể là lưu trữ, chuyển đổi, lọc, sắp xếp và phân loại thông tin.

Quá trình trung gian:

Sau đây là danh sách nhận dạng năm quá trình trung gian phù hợp với khối chức năng trung gian như đã miêu tả trong kiến trúc chức năng TMN:

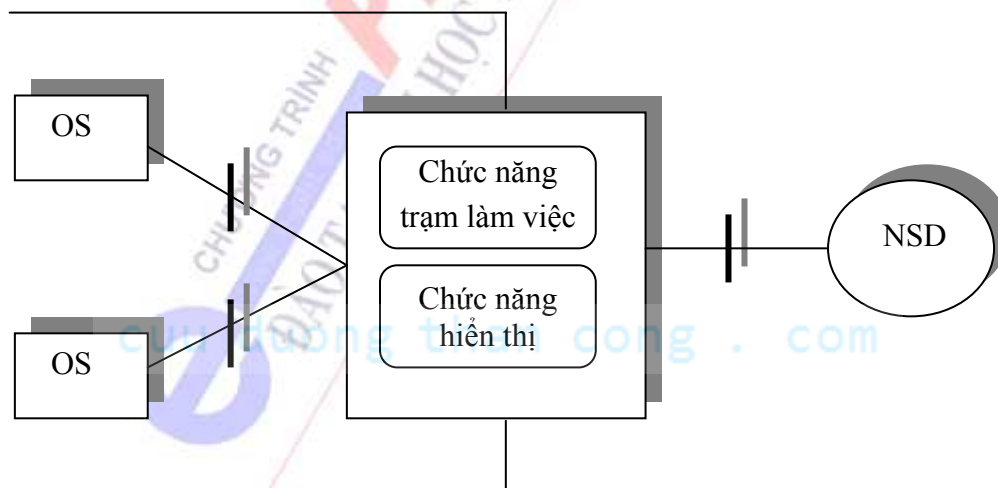
- Chuyển đổi thông tin. Chuyển đổi giữa các mô hình thông tin là một loại xử lý, quá trình chuyển đổi thông tin sẽ chuyển đổi rất nhiều mô hình thông tin thành mô hình thông tin đồng nhất, biến đổi thông tin từ MIP nội hạt tuân theo mô hình thông tin đồng nhất.
- Liên kết làm việc. Quá trình này cung cấp giao thức để thiết lập và dàn xếp kết nối bằng cách duy trì phạm vi thông tin.
- Xử lý dữ liệu. Quá trình này cung cấp tập trung, lựa chọn dữ liệu, đặt khuôn dạng cho dữ liệu và biên dịch dữ liệu.
- Ra quyết định. Quá trình này bao gồm truy nhập trạm làm việc, sắp xếp, lưu trữ dữ liệu, định tuyến dữ liệu, truy nhập kiểm tra.
- Lưu trữ dữ liệu. Quá trình này bao gồm lưu trữ cơ sở dữ liệu, cấu hình mạng, phân loại thiết bị, dự trữ bộ nhớ.

Cấu hình của thiết bị trung gian

Chức năng trung gian có thể thực hiện như một thiết bị trung gian. Trong trường hợp đứng một mình, những giao diện trước của NE, QA, và OS là giao diện cơ bản của Qx và Q3. Khi trung gian là một phần của NE, chỉ những giao diện cụ thể trước OS sẽ là giao diện chuẩn. Chức năng trung gian có thể cũng được thực hiện như một vai trò thay thế cho thiết bị trung gian, thiết bị trung gian được xem như thành phần không rõ ràng nhất của TMN. Trong thực tế một đáp ứng Q thường được đề cập tới như là thiết bị trung gian.

2.3.1.4 Trạm làm việc WS

WS là hệ thống mà thực hiện các WSF. Các chức năng trạm làm việc dịch thông tin ở điểm tham chiếu f tới một khuôn dạng có thể hiển thị ở điểm tham chiếu giao diện người máy và ngược lại.



Hình 2.9: Trạm làm việc WS

Một trạm làm việc TMN có thể trở thành đầu cuối kết nối thông tin số liệu tới một OS hay một MD. Thiết bị kết nối đầu cuối này có khả năng biên dịch thông tin ở điểm tham chiếu f đã được mô tả trong mô hình thông tin TMN thành khung hiển thị cho người sử dụng ở điểm

tham chiếu g hay ngược lại. Thiết bị đầu cuối sẽ có lưu giữ dữ liệu, xử lý dữ liệu và hỗ trợ giao diện.

Như trong hình vẽ trên, ta thấy một phần của trạm làm việc nằm trong ranh giới TMN và một phần ở bên ngoài TMN. Một trạm làm việc thực hiện hai loại chức năng: chức năng hiển thị và chức năng WSF.

Chức năng hiển thị cung cấp cho người sử dụng đầu vào, đầu ra vật lý và những phương tiện diễn giải để xâm nhập, hiển thị và sửa đổi những chi tiết của thông tin bên trong của một TMN. Chức năng này cũng cung cấp sự hỗ trợ cho giao diện người-máy, được gọi là điểm tham chiếu g. Giao diện người-máy có thể là một hàng lệnh, đường dẫn hay cửa sổ cơ sở.

Một WSF cung cấp cho người sử dụng những chức năng chung tại thiết bị đầu cuối để xử lý đầu vào, đầu ra của dữ liệu đến hay đi từ thiết bị đầu cuối của người sử dụng. Những chức năng này bao gồm an toàn truy cập tới thiết bị đầu cuối, phân tách và xác nhận tính hợp lệ đầu vào; đặt khuôn dạng và xác nhận tính hợp lệ của đầu ra; duy trì cơ sở dữ liệu, hỗ trợ danh mục, màn hình, cửa sổ và thanh cuộn.

Một trạm làm việc phải có một giao diện F và không gồm bất kỳ OSF nào. Nếu OSF và WSF được kết hợp làm một thì sẽ được xem như một OS. Lưu ý rằng một trạm làm việc như là một nút của TMN nó không truyền đạt cùng ý nghĩa như "trạm làm việc" trong thế giới máy tính.

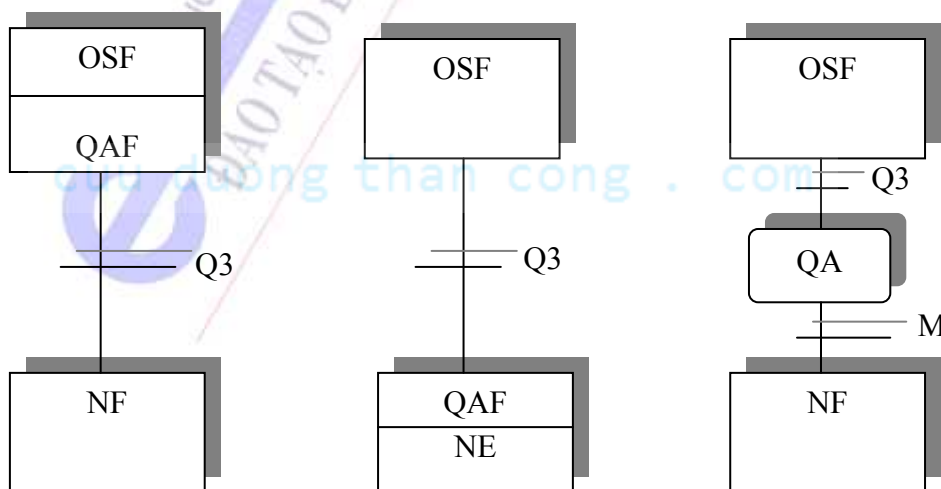
2.3.1.5 Thành phần Đáp ứng QA

Một đáp ứng Q có thể là một phần cứng, phần mềm hoặc là sự kết hợp cả hai. Đáp ứng Q thực hiện chức năng đáp ứng Q (QAF) nơi chuyển đổi một giao diện phi TMN thành một giao diện TMN. Một QAF biến đổi giao diện cho giao diện lớp Q3 và Qx. Một đáp ứng Q có thể gồm một hay nhiều QAF.

Đáp ứng Q phản ánh sự ảnh hưởng lẫn nhau của TMN và những hệ thống đã tồn tại. Đó là điều luôn khó được chứng minh để xây dựng đáp ứng Q dokhó khăn trong việc sắp xếp giữa giao diện TMN và những giao diện khác.

Gần đây trong nền công nghiệp, rất nhiều người sử dụng thuật ngữ thiết bị trung gian thay cho nghĩa đáp ứng Q. Trên thực tế sự sử dụng đó rất thông dụng, thuật ngữ thiết bị trung gian bao hàm ý nghĩa của đáp ứng Q.

Cấu hình đáp ứng Q:



Hình 2.10: Các cấu hình khác nhau của đáp ứng Q

Đáp ứng Q có thể là trường hợp như mô tả trong hình vẽ dưới. Sự vận dụng vật lý của một đáp ứng Q có thể thay đổi từ một hệ thống này tới một hệ thống khác.

Xử lý đáp ứng Q:

Một QAF thực hiện hai chức năng cơ bản: chuyển đổi thông tin và chuyển đổi giao thức.

Chuyển đổi thông tin:

QAF đưa ra mô hình thông tin TMN trong một mô hình phi TMN và ngược lại. Điều này đòi hỏi QAF hiểu cú pháp, ý nghĩa và cấu trúc MBI của cả hai mô hình thông tin liên quan. Đáp ứng Q làm biến đổi loại của những mô hình thông tin phi TMN thành những mô hình thông tin TMN. Những mô hình thông tin TMN được định nghĩa cho giao diện Q3 giữa những phần tử mạng và EML OS bao gồm:

- Mô hình thông tin quản lý khách hàng (Q.824.0 đến Q.824.4,1995 ITU-T) và mô hình thông tin quản lý chuyển tải (Q.823,1996 ITU-T).
- Mô hình thông tin phần bản tin được truyền tải của mạng SS7(Q.751.1 ITU-T).

2.3.1.6 Mạng thông tin dữ liệu (DCN)

Thực hiện đầy đủ chức năng thông tin dữ liệu (DCF) của kiến trúc chức năng TMN và cung cấp sự kết nối giữa các nút TMN. Đặc biệt một DCN liên kết những phần tử mạng, đáp ứng Q, thiết bị trung gian tới OS qua giao diện Q3 và liên kết các thiết bị trung gian tới những phần tử mạng và những đáp ứng Q qua giao diện Qx. Còn có một số hạn chế trong thành phần mạng để tạo nên một DCN. Chúng có thể gồm những mạng dữ liệu chuyển mạch gói, những mạng chuyển mạch công cộng hay những mạng khu vực. Một yêu cầu duy nhất đó là cung cấp khả năng trung chuyển giữa các điểm nút TMN. Mặc dù DCN có thể là một mạng tách rời, nhưng trong thực tế DCN thường là một hệ thống được quản lý bởi TMN.

2.3.2. Các giao tiếp

Điểm tham chiếu là điểm mang tính khái niệm để trao đổi thông tin giữa các chức năng không chồng lấn lên nhau (được mô tả trên Hình 2.11). Điểm tham chiếu có thể trở thành một giao diện khi: Các khối chức năng kết nối với nó là các thiết bị riêng biệt về mặt vật lý. Các điểm tham chiếu bao gồm: q; f; x; g và m.

Các điểm tham chiếu xác định ranh giới dịch vụ giữa hai khối chức năng quản lý. Mỗi điểm tham chiếu yêu cầu về các đặc tính giao thức truyền tin khác nhau, nó được định nghĩa để khái quát thủ tục trao đổi thông tin giữa các khối chức năng khác nhau. Điểm tham chiếu có khả năng trở thành giao diện khi có một kết nối vật lý giữa hai thiết bị riêng rẽ.

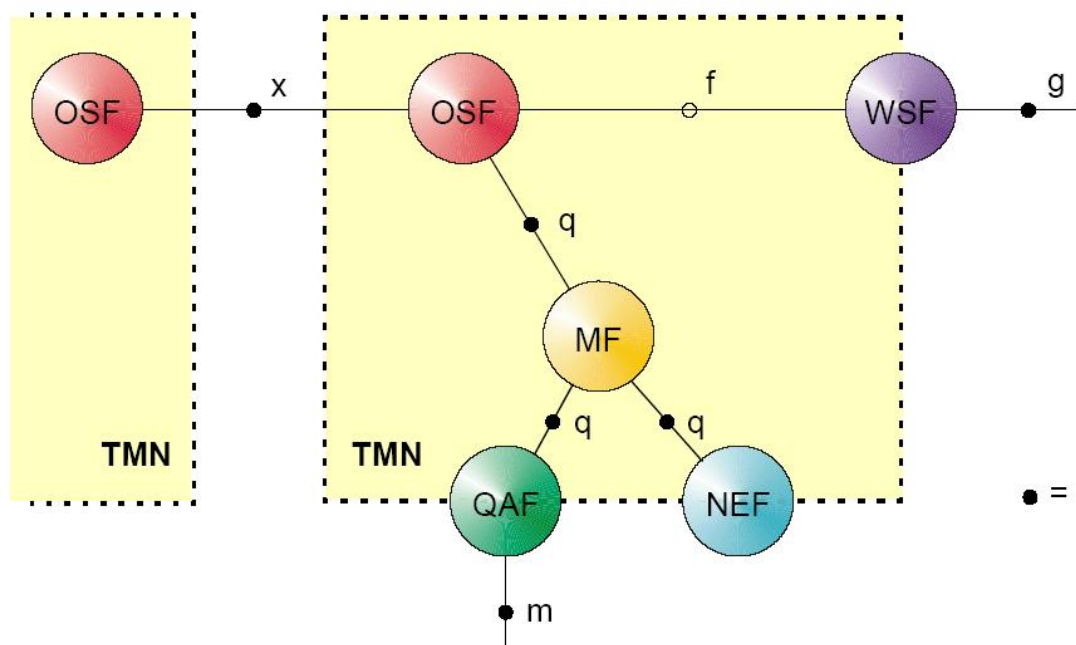
Trong 5 loại điểm tham chiếu trên, TMN có 3 loại điểm tham chiếu được định nghĩa như sau:

- q Giữa OSF, QAF, MF và NEF
- f Giữa OSF hoặc MF với WSF
- x Giữa OSF của hai TMN

Ngoài ra hai điểm tham chiếu phi TMN (non-TMN) được định nghĩa là :

- g Giữa WSF và người sử dụng (users)
- m Giữa QAF và thực thể non-TMN bị quản lý

Hình 2.11 mô tả sự liên kết các khối chức năng qua các điểm tham chiếu



Hình 2.11: Các điểm tham chiếu

Điểm tham chiếu q kết nối các chức năng TMN như: OSF; MF; NEF; QAF trực tiếp với nhau hoặc qua DCF; trong nhóm q thì q3 kết nối: NEF - OSF; MF - OSF; QAF - OSF; OSF - OSF; qx kết nối MF - MF; MF - NEF; MF - QAF.

Điểm tham chiếu f kết nối OSF và MF với WSF;

Điểm tham chiếu x kết nối các chức năng OSF thuộc các TMN khác nhau, hoặc kết nối giữa một OSF trong môi trường TMN với một chức năng trong môi trường không phải TMN.

Điểm tham chiếu g không được coi như một phần TMN kể cả khi nó mang thông tin về TMN; điểm tham chiếu g không phải TMN đặt bên ngoài TMN (giữa người dùng và WSF).

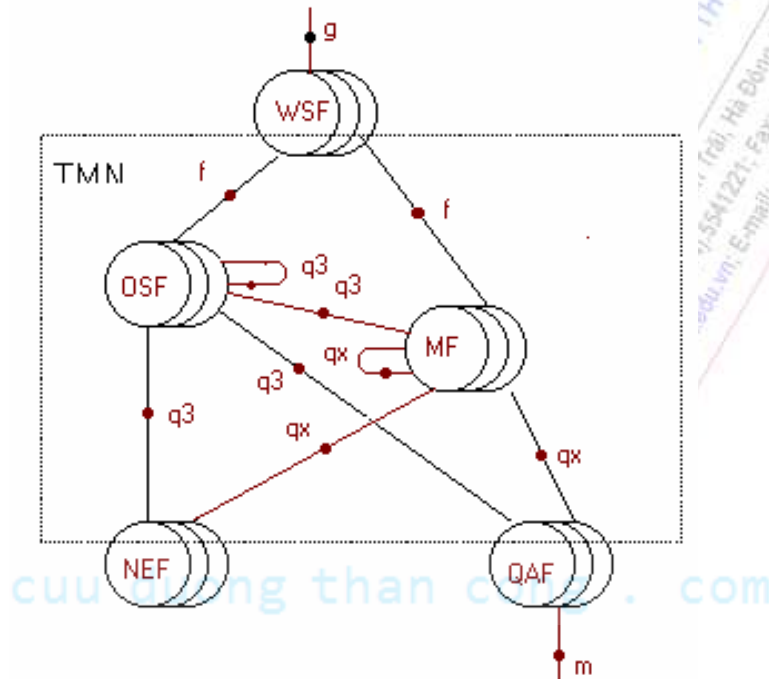
Điểm tham chiếu m cũng nằm ngoài TMN, giữa QAF và các thực thể bị điều hành phi TMN hoặc các thực thể bị điều hành nhưng không theo các khuyến nghị TMN (cho phép quản lý các NE phi TMN qua môi trường TMN).

Các chức năng NE, OS, WS, QA, MD được kết nối với nhau qua các giao diện chuẩn của DCN. Các giao diện DCN đảm bảo khả năng tương tác của các hệ thống được kết nối với nhau để thực hiện chức năng điều hành/ lập kế hoạch TMN. Giao diện Qx hỗ trợ một tập hợp nhỏ chức năng bằng các giao thức đơn giản phù hợp với NE, không yêu cầu nhiều chức năng khai thác bảo trì OAM (Operation And Maintenance); Qx có thể truyền đưa thông tin hai chiều liên quan đến các sự kiện: thay đổi trạng thái cảnh báo, khởi tạo lại cảnh báo, điều khiển mạch vòng; đối với ứng dụng này có thể lựa chọn một số giao thức hỗ trợ dịch vụ ít nhất là từ các lớp 1 và 2 của mô hình tham chiếu OSI; Các giao diện Qx với tập hợp giao thức phức tạp là bắt buộc để hỗ trợ một tập hợp chức năng khai thác bảo trì OAM lớn hơn và đòi hỏi phải có thêm các dịch vụ giao thức bổ sung từ lớp 3 đến lớp 7. Giao diện Qx với một tập hợp các giao thức phức tạp thường được sử dụng cho NE và MD phức tạp.

2.3.3 Các giao diện

Khi hai khối chức năng của các thiết bị riêng biệt có kết nối vật lý qua một điểm tham chiếu thì điểm tham chiếu trở thành giao diện.

Giao diện TMN đảm bảo khả năng tương tác của các hệ thống được kết nối với nhau nhằm thực hiện chức năng quản lý/lập kế hoạch TMN. Giao diện TMN định nghĩa bản tin tương thích chung cho tất cả các chức năng quản lý, lập kế hoạch TMN mà không phụ thuộc vào loại thiết bị hoặc nhà cung cấp thiết bị.



Hình 2.12: Các điểm tham chiếu TMN

Điểm tham chiếu:	q_x	q_3	x	f	$(g$	$m)$
	↓	↓	↓	↓		
Giao diện:	Q_x	Q_3	X	F		

Hình 2.13: Quan hệ giữa điểm tham chiếu và giao diện

2.3.3.1 Giao diện Q

Giao diện Q được áp dụng tại điểm tham chiếu q , để cung cấp tính linh hoạt trong hỗ trợ giao thức truyền thông. Giao diện Q được chia thành:

- Giao diện Q_3 được áp dụng tại điểm tham chiếu q_3
- Giao diện Q_x được áp dụng tại điểm tham chiếu q_x

Giao diện Q_3 là giao diện của hệ thống khai thác bất cứ thực thể TMN nào kết nối trực tiếp tới OS đều sử dụng giao diện Q_3 . Giao diện Q_3 hỗ trợ một tổ hợp chức năng rất phức tạp, và vì vậy nó đòi hỏi rất nhiều dịch vụ giao thức để đảm đương nhiệm vụ này

Giao diện Qx được áp dụng tại điểm tham chiếu qx, Qx là phần giao tiếp giữa NE và MD, MD và QA. Giao diện Qx hỗ trợ một tập hợp nhỏ chức năng bằng cách sử dụng giao thức đơn giản nhưng phù hợp với các thành phần mạng không đòi hỏi nhiều chức năng và được sử dụng với số lượng lớn như thay đổi trong trạng thái cảnh báo, khởi tạo lại cảnh báo...

Hai nhóm giao diện Q3 và Qx được xếp thứ tự theo số dịch vụ truyền thông mà nó cung cấp và độ phong phú cũng như độ phức tạp của các ứng dụng TMN mà chúng hỗ trợ. Thông thường giao diện Q3 cung cấp các dịch vụ và giao thức phức tạp hơn, thực hiện nhiều chức năng hơn cho mỗi thành phần mạng (NE). Khi một thành phần mạng chỉ có giao diện Qx muốn kết nối tới OS thì phải qua thiết bị trung gian (MD)

2.3.4 Giao diện X

Giao diện X áp dụng tại điểm tham chiếu x, dùng để liên kết hai TMN với nhau hoặc giữa TMN với một loại mạng quản lý khác. Các bản tin và giao thức được định nghĩa cho giao diện X cũng có thể thích hợp cho giao diện Q3 sử dụng giữa các OS.

Mô hình thông tin tại giao diện X giới hạn khả năng truy nhập từ bên ngoài mạng quản lý viễn thông, và có thể yêu cầu thêm các giao thức để đảm bảo an toàn

2.3.5 Giao diện F

Giao diện F áp dụng cho điểm tham chiếu f, cần thiết cho sự kết nối giữa trạm làm việc WS với các khối cơ bản của TMN thông qua mạng truyền số liệu (DCN)

2.4 KIẾN TRÚC PHÂN LỚP LÔGIC

Kiến trúc phân lớp logic hay phân tầng logic (LLA) là một khái niệm về cấu trúc của chức năng quản lý mà tổ chức và các nhóm nghiên cứu gọi là “các tầng logic” và khái niệm này mô tả mối quan hệ giữa các tầng. Một tầng logic là một khái niệm riêng biệt phản ánh các nội dung quản lý riêng biệt được sắp xếp bởi các mức khái niệm trừu tượng khác nhau (chẳng hạn tầng quản lý kinh doanh, tầng quản lý dịch vụ, tầng quản lý mạng, tầng quản lý phần tử).

Những tác động qua lại chức năng giữa các khối chức năng OSF trong vòng các tầng logic khác nhau được mô tả bởi điểm tham chiếu. Qua điểm tham chiếu tương tự, các khối chức năng quản lý truyền thông tin quản lý phù hợp để được thực hiện chức năng quản lý theo lý thuyết.

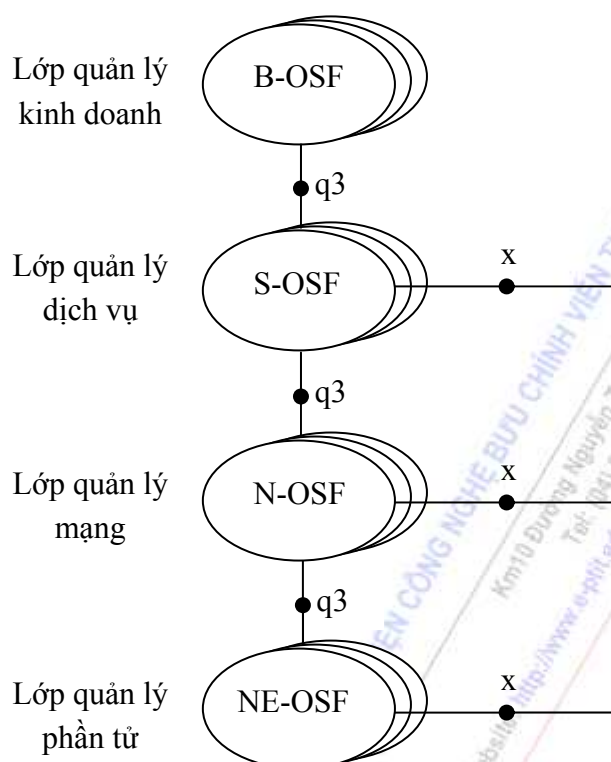
Mối quan hệ của kiến trúc phân tầng logic và kiến trúc thông tin quản lý có thể được mô tả bởi kiến trúc thông tin quản lý đưa ra qua một loạt quan niệm. Mỗi quan niệm thực hiện các phần tử thông tin từ các mô hình thông tin mà có thể được trưng bày hoặc chuyển đổi ở các điểm tham chiếu giữa các khối chức năng trong các tầng của LLA.

Mạng quản lý viễn thông là một hệ thống vừa có khả năng quản lý các thực thể vật lý như các thành phần mạng NE, thiết bị nguồn, thiết bị điều hoà nhiệt độ... vừa có khả năng quản lý các thực thể logic như lập kế hoạch dịch vụ, lịch làm việc, kế toán, an toàn, an ninh, ký kết hợp đồng...

Để đơn giản hoá quá trình thiết kế mạng quản lý viễn thông TMN, người ta chia các chức năng TMN ra thành bốn lớp quản lý chức năng. Mỗi lớp vừa có nhiệm vụ quản lý các thực thể trong lớp vừa có nhiệm vụ cung cấp các thông tin quản lý cho lớp bên trên

- Lớp quản lý phần tử mạng (NEML- Network Element Management Layer)
- Lớp quản lý mạng (NML- Network Management Layer)

- Lớp quản lý dịch vụ (SML- Service Management Layer)
- Lớp quản lý kinh doanh (BML- Business Management Layer)



Hình 2.14: Các lớp quản lý của TMN

2.4.1. Lớp quản lý phần tử NEML

Lớp quản lý phần tử mạng chịu trách nhiệm quản lý các NE. Các thông tin quản lý TMN do các NE cung cấp. NEML chịu trách nhiệm giao tiếp giữa thông tin quản lý và cấu trúc hạ tầng mạng quản lý viễn thông

Hay nói cách khác lớp quản lý phần tử mạng có nhiệm vụ quản lý từng phần tử mạng hoặc một nhóm các phần tử mạng (mạng con). Các chức năng mạng quản lý viễn thông do khối điều khiển mạng con (SNC) cung cấp. Lớp quản lý phần tử mạng có ba vai trò cơ bản sau:

- Kiểm soát và phối hợp một tập con các phần tử mạng trên cơ sở chức năng phần tử mạng riêng
- Kiểm soát và phối hợp một tập con các phần tử mạng trên cơ sở chức năng tập hợp chung
- Thu thập và quản lý các số liệu thống kê, trạng thái và số liệu về hoạt động của các phần tử mạng trong phạm vi điều khiển của mình

Lớp quản lý phần tử mạng có một hoặc nhiều hơn một phần tử OSF (có vai trò riêng biệt) trên một cơ sở chuyển giao từ lớp quản lý tài nguyên cho vài tập con của các chức năng phần tử mạng. Như một mục tiêu, một quan điểm độc lập nhà cung cấp thiết bị sẽ được cung cấp tới lớp quản lý tài nguyên.

2.4.2. Lớp quản lý mạng NML

Lớp quản lý mạng thực hiện quản lý bao quát toàn mạng dựa trên thông tin NE do các OS của NEMML cung cấp. Lớp này cung cấp các chức năng về cấu hình mạng, phân tích hiệu năng và thống kê mạng. NML kết hợp hoạt động với hỗ trợ các yêu cầu của lớp quản lý dịch vụ. OS trong NML giao tiếp với OS trong các lớp khác qua giao diện tiêu chuẩn

Lớp quản lý mạng có bốn vai trò cơ bản sau:

- Điều khiển và phối hợp trên toàn mạng, bao gồm tất cả các phần tử mạng trong phạm vi hoặc trong vùng của nó
- Cung cấp, đình chỉ hoặc thay đổi tính năng mạng để hỗ trợ việc cung cấp dịch vụ
- Bảo dưỡng, duy trì các tính năng cơ bản của mạng
- Thu thập, lưu trữ và thống kê các số liệu về mạng và giao tiếp với lớp quản lý dịch vụ về hiệu năng, mức độ sử dụng mạng

2.4.3. Lớp quản lý dịch vụ SML

Lớp quản lý dịch vụ sử dụng thông tin nhận từ lớp quản lý mạng để quản lý các dịch vụ cung cấp cho khách hàng. Lớp quản lý dịch vụ có trách nhiệm đối với các vấn đề về hợp đồng dịch vụ đang cung cấp cho khách hàng hoặc sẵn sàng cung cấp cho khách hàng mới. Nó làm đầu mối để liên hệ với khách hàng về toàn bộ giao dịch dịch vụ như lắp đặt, cung cấp dịch vụ, chất lượng dịch vụ. Lớp quản lý dịch vụ có bốn vai trò cơ bản sau:

- Gặp gỡ khách hàng và giao tiếp với các nhà quản trị khác.
- Giao tiếp với nhà cung cấp dịch vụ.
- Bảo dưỡng số liệu trạng thái.
- Duy trì mối tương tác giữa các dịch vụ.

Lớp quản lý dịch vụ chịu trách nhiệm đàm phán, thoả thuận giữa khách hàng và nhà cung cấp dịch vụ.

Tầng quản lý dịch vụ (SML) hỗ trợ các chức năng để quản lý phân phối và đảm bảo các dịch vụ tới người dùng theo những sự mong đợi khách hàng. Nó thực hiện các chức năng để:

- Quản lý các tiểu sử vấn tắt dịch vụ, mỗi tiểu sử vấn tắt dịch vụ biểu diễn các yêu cầu các tài nguyên dịch vụ và mạng cần kích hoạt dịch vụ. Các miền quản lý tài nguyên dịch vụ (SRM) và quản lý tài nguyên truyền dẫn (NRM) bên dưới sắp xếp các yêu cầu này vào các thông số mạng của các phần tử mạng nằm dưới.
- Quản lý kết hợp các thuê bao thông thường tới tập các lý lịch vấn tắt tương ứng hợp đồng các thuê bao này.
- Quản lý dịch vụ và các tài nguyên mạng yêu cầu cho phép kích hoạt các dịch vụ theo hợp đồng người sử dụng, bao gồm yêu cầu kết nối và các đặc tính kết hợp của nó: băng thông, QoS, mức SLA.
- Giám sát các dịch vụ kích hoạt để bảo đảm hội tụ SLA bằng hợp đồng và sự ảnh hưởng của chi tiết không cụ thể ở các chức năng (phân phối thông tin tới người khai thác, giảm bớt các chỉ số tới hệ thống tính cước trong trường hợp QoS quá thấp, vv...)

2.4.4. Lớp quản lý kinh doanh BML

Lớp quản lý kinh doanh chịu trách nhiệm về toàn bộ hoạt động của hệ thống và giao tiếp với các hệ thống quản lý khác. Trong khi những chức năng chính của lớp quản lý dịch vụ và lớp quản lý mạng là sử dụng tối ưu các nguồn tài nguyên thì các chức năng của lớp quản lý kinh doanh là quyết định đầu tư và đưa vào sử dụng các tài nguyên mới. Nó thực hiện lập kế hoạch ở mức vĩ mô, dự toán kinh phí, đặt mục tiêu, quyết định hành chính, thoả thuận thương mại...

Lớp quản lý kinh doanh có vai trò cơ bản sau:

- - Hỗ trợ tiến trình ra quyết định đầu tư và sử dụng hiệu quả các nguồn tài nguyên mới.
- - Hỗ trợ quản lý OA & M liên quan tới ngân sách.
- - Hỗ trợ việc cung cấp và yêu cầu OA & M liên quan tới nguồn nhân lực.
- - Bảo dưỡng số liệu toàn bộ hệ thống.

2.5 CÁC CHỨC NĂNG QUẢN LÝ TRONG TMN

Phần này giới thiệu năm chức năng của TMN. Những lý thuyết kiến trúc này đã được chấp nhận rộng rãi trong lĩnh vực quản lý mạng viễn thông.

Các mạng viễn thông ngày nay được đặc trưng bởi sự kết hợp chặt chẽ giữa các dịch vụ và tài nguyên mạng, được triển khai theo một chuỗi các đa lớp: các mạng OAM&P và các hệ thống điều hành cho mỗi một cặp dịch vụ và tài nguyên tương ứng. Tổ chức thành các nhóm riêng biệt thực hiện các chức năng tương tự. Sự lặp lại của các cấu trúc lớp này liên quan đến các hoạt động vận hành của công nghệ cũ. Hơn nữa, các phần tử được quản lý có các thuộc tính riêng biệt đối với các chức năng OAM&P. Do đó mạng quản lý cũng phải tạo ra các vùng quản lý riêng biệt cho các phần tử này và các vùng này ít liên quan với nhau. Tổ chức riêng biệt này làm cho môi trường quản lý trở nên phức tạp, kém hiệu quả và không kinh tế.

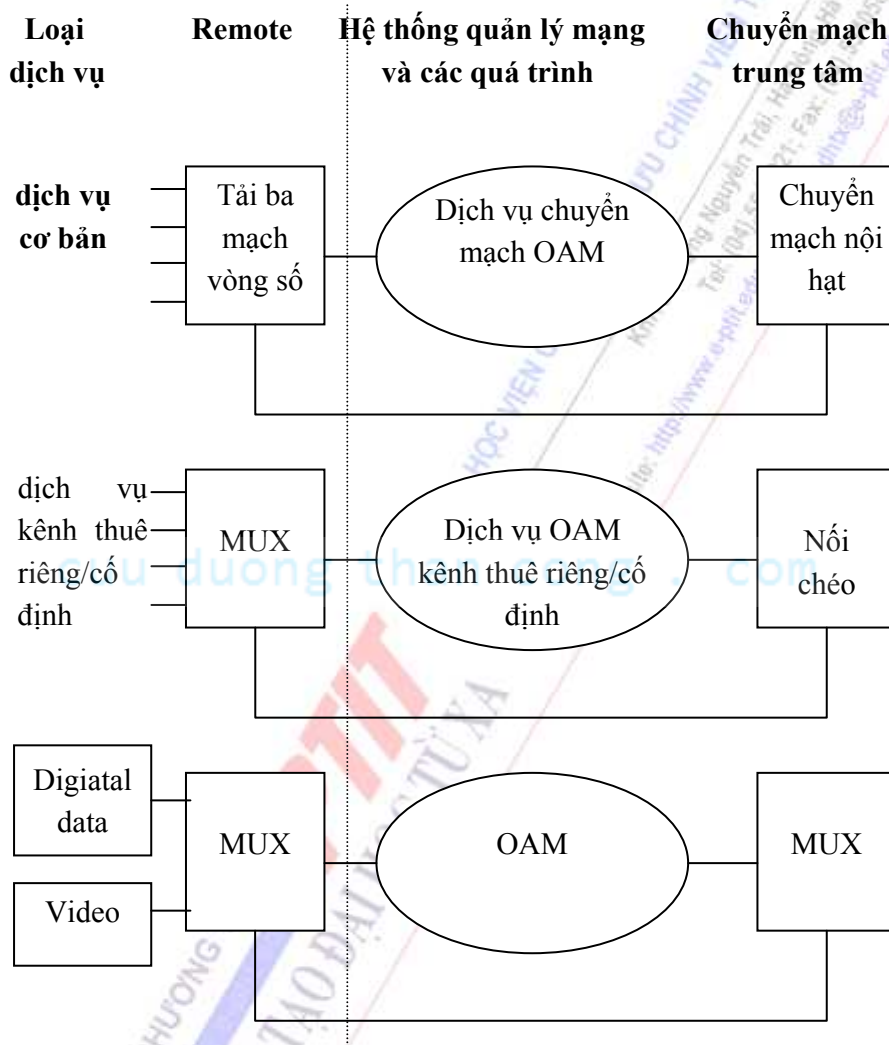
Quản lý mạng cổ điển sử dụng các thủ tục, các quá trình xử lý và các công cụ để lập cấu hình, tách lỗi, hiển thị đặc tính, an toàn, tính toán và các chức năng quản lý khác. Về cơ bản được xây dựng dựa vào quan hệ chủ tớ (master-slave) giữa quản lý hay hệ thống vận hành (OS) và các phần tử mạng (NE). Phần tử mạng chỉ có chức năng vận hành cơ bản với khả năng điều khiển hạn chế các hoạt động hoặc ra quyết định trong phạm vi xử lý cuộc gọi và truyền tải thông tin. Các hệ thống vận hành thực hiện toàn bộ công việc OAM&P: xử lý dữ liệu do các phần tử mạng cung cấp, ra quyết định, chỉ dẫn các phần tử mạng thực hiện các thao tác thích hợp.

Quan hệ chủ tớ này làm giảm hiệu quả hoạt động. Ví dụ, các tài nguyên logic, như dữ liệu ít được sử dụng chung do các phần tử mạng và hệ thống vận hành được thiết kế độc lập. Hơn nữa, các thiết bị có các giao diện quản lý cấu hình và lỗi đặc trưng riêng cũng như các hoạt động riêng. Các hệ thống quản lý mạng bắt buộc phải xác định các hoạt động của từng phần tử mạng và các giao diện. Do đó mất nhiều thời gian và phức tạp trong việc tạo ra một công nghệ hay dịch vụ mới.

Các yếu tố khác đã được tính đến trong sự phức tạp này. Ví dụ, các hệ thống quản lý mạng được xây dựng một cách tổng quát để tối ưu công việc của các nhà cung cấp dịch vụ hoặc các nhóm công tác tại một thời điểm cụ thể đối với một hệ công nghệ. Kiểu phát triển này được thực hiện một cách độc lập giữa các đơn vị tổ chức và rất ít quan tâm đến sự hoạt động tương hỗ ở cấp hệ thống. Nhiều bản sao dữ liệu, mỗi cái gắn liền với một cấp hệ thống hoặc chức năng nhất định và gắn với những thế hệ thiết bị cũ hoặc những thiết bị bổ sung mới, được tổ hợp lại qua mạng,

tạo nên cả một vấn đề về đồng bộ dữ liệu. Kết quả là tạo khó khăn cho nhà cung cấp dịch vụ mạng, và tạo khó khăn cho việc phát triển các dịch vụ, các công nghệ mạng, quá trình quản lý mạng với sự thay đổi mạnh của công nghiệp viễn thông.

Kiến trúc và hệ thống điều khiển là chìa khoá cho cải tiến các hệ thống quản lý mạng cũ có nhiều hạn chế để đáp ứng các yêu cầu của mạng tương lai. Bằng việc phân bố và xây dựng lại cơ sở dữ liệu mạng để có được các ưu điểm của các phần tử mạng thông minh, thực hiện các giao thức và bản tin tiêu chuẩn, chia sẻ các chức năng OAM&P giữa các hệ thống điều hành và phần tử mạng thông minh sẽ cho phép phát triển các dịch vụ mới và các yêu cầu đã nêu ở trên.



Hình 2.15: Quan hệ dịch vụ và hệ thống quản lý mạng

Quan điểm mạng thông minh sẽ được áp dụng trong mạng quản lý viễn thông (TMN), nguyên tắc thông tin quản lý định nghĩa mối quan hệ cơ bản giữa các khối chức năng mạng cơ bản (hệ thống điều hành, mạng thông tin số liệu, phần tử mạng) bằng các giao diện chuẩn. TMN còn giới thiệu nguyên tắc điều khiển phân mạng trong đó phân mạng đóng vai trò quan trọng trong việc phát triển mạng quản lý đáp ứng các yêu cầu tương lai. Phân mạng là tập hợp các phần tử mạng có các tính chất chung (công nghệ, chức năng) và được các ứng dụng quản lý mạng xem như là một thực thể đơn lẻ.

Từ quan điểm quản lý mạng, quản lý mạng được chia thành năm nhóm chức năng, mỗi nhóm biểu diễn một tập các hoạt động do người quản lý hay khách hàng thực hiện. Trong nhiều

trường hợp, cả hệ thống quản lý mạng và các phần tử mạng thông minh cùng tham gia thực hiện. Việc vận hành quản lý được phân tách dựa trên cơ sở định nghĩa tổng quát OSI về các chức năng OAM&P và theo một cách chung nhất đối với các loại hình dịch vụ và công nghệ, các chức năng quản lý bao gồm:

- Quản lý hiệu năng;
- Quản lý sự cố;
- Quản lý cấu hình;
- Quản lý tài khoản;
- Quản lý bảo mật.

2.5.1 Quản lý hiệu năng

Cung cấp hoạt động với khả năng kiểm soát và tiêu chuẩn để đánh giá sự liên tục của tài nguyên mạng để phân tích sự đánh giá đó và tạo ra sự điều chỉnh để cải thiện hoạt động mạng. Quản lý hiệu năng bao gồm 4 nhóm chức năng cơ bản: giám sát, điều khiển quản lý, phân tích và đảm bảo chất lượng đặc tính.

Thu thập các loại dữ liệu về: lưu lượng mạng (thời gian, số cuộc gọi thực hiện thành công, tỷ lệ thành công và không thành công các cuộc gọi qua từng nút mạng); dữ liệu đo chất lượng truyền dẫn; các dữ liệu quản lý phần mềm nút chuyển mạch bao gồm các số liệu về cập nhật phần mềm, sự cố phần mềm, hệ thống tự khởi động lại; dữ liệu về các mã chọn cuối của các nút chuyển mạch; dữ liệu khiếu nại khách hàng; dữ liệu từ phía đối tác, . . .

Từ các loại số liệu thu thập nói trên tiến hành chọn lọc dữ liệu, đánh giá mức độ phản ánh nhiều ít đến hiệu quả khai thác mạng trên cả hai mặt kỹ thuật và kinh tế.

Từ các số liệu thống kê hàng ngày, hàng tháng, hàng năm phân tích đưa ra xu thế hoạt động của mạng trên các tiêu chí: lưu lượng, lỗi và sự cố, chất lượng độ tin cậy thiết bị, khả năng đáp ứng của người khai thác và hàng loạt số liệu khác, đưa ra xu thế của mạng trong tương lai gần và xa để có kế hoạch bổ sung cần thiết.

2.5.1.1 Giám sát hoạt động

Được chia ra thành giám sát trạng thái lưu lượng, giám sát hoạt động lưu lượng, cung cấp trạng thái hiện tại của mạng, đó là các phần tử mạng và các dịch vụ được cung cấp bởi mạng. Các bản tin chức năng giá trị dịch vụ của NE như trạng thái bận hoặc rỗi của nhóm mạch, trạng thái tắc nghẽn của tổng đài, sự nhận tín hiệu điều khiển tắc nghẽn và trạng thái tắc nghẽn của mạng báo hiệu. Chức năng giám sát hoạt động lưu lượng đánh giá hoạt động của mạng và lưu lượng được tải trên mạng.

Chức năng thông báo dữ liệu nhóm mạch và thông số trên cơ sở liệt kê, đánh giá tải chuyển mạch, tắc nghẽn chuyển mạch và đánh giá tải của mạng báo hiệu.

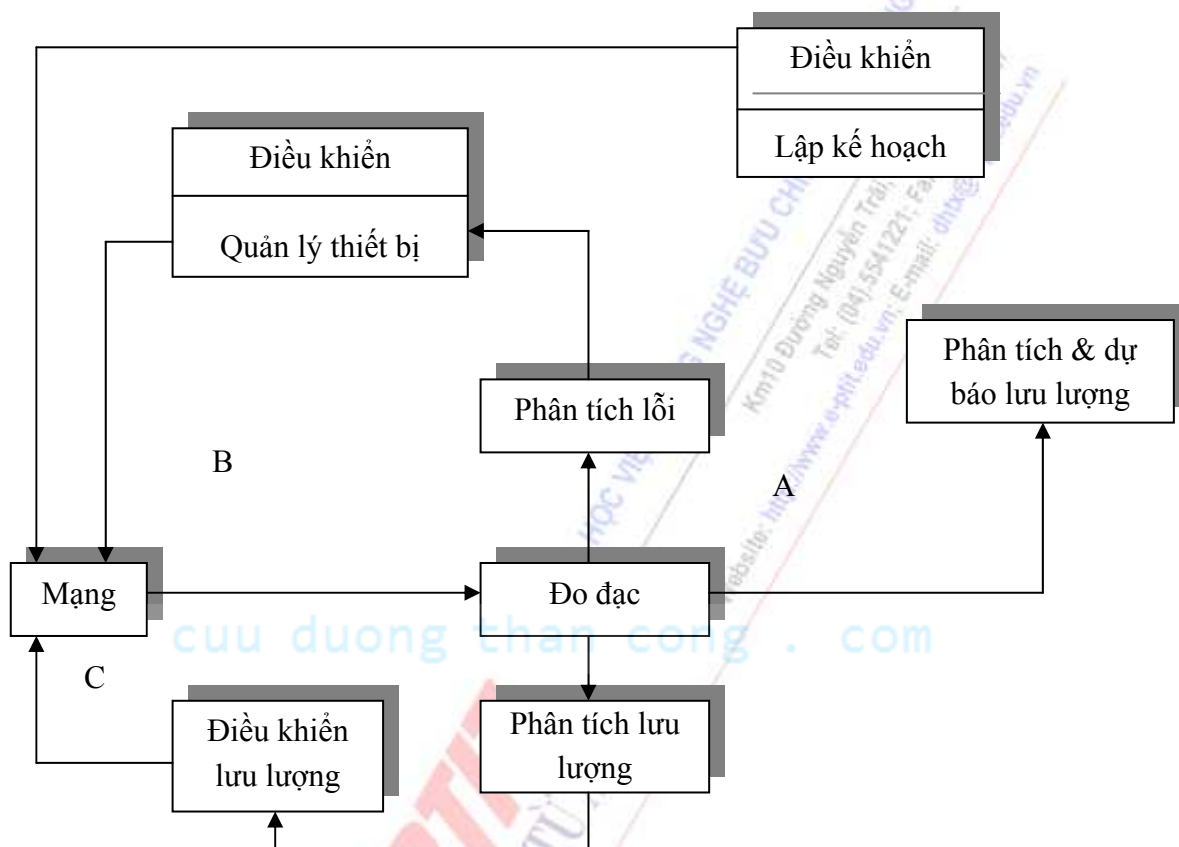
2.5.1.2 Điều khiển quản lý hoạt động

Được chia thành điều khiển lưu lượng và chức năng quản lý lưu lượng. Chức năng điều khiển lưu lượng quan tâm tới sự thiết lập di chuyển thủ công hay tự động trên lưu lượng mạng. Chức năng quản lý lưu lượng chú ý đến các hoạt động như thiết lập, chuyển đổi, di chuyển, đánh giá liệt kê, mức (ngưỡng) hoạt động, lập kế hoạch, quản lý cơ sở dữ liệu mạng.

2.5.1.3 Phân tích hoạt động

Chú ý tới sự phân tích và dữ liệu hoạt động dịch vụ được thu thập bởi chức năng giám sát hoạt động. Dữ liệu hoạt động có thể yêu cầu xử lý thêm và phân tích để đánh giá mức hoạt động của toàn bộ mạng.

Hình vẽ chỉ ra mẫu đơn giản của quản lý mạng và điều khiển mô tả giống như ba chu trình hoặc ba vòng. Mỗi vòng bao gồm giám sát mạng, xử lý dữ liệu và các lỗi ra hoặc các hoạt động điều khiển của một số kiểu. Yếu tố quan trọng của các vòng này là thời gian dành cho mỗi vòng.



Hình 2.16: Các vòng quản lý mạng.

- Vòng A là vòng dự phòng mạng. Vòng này sử dụng các phép đo mạng như là một giá trị đầu vào để dự báo lưu lượng và quá trình định ra kích cỡ mạng cụ thể. Kết quả là một sự nhận biết về nhu cầu dung lượng qua mạng trong tương lai có thể dùng trong việc thiết lập kế hoạch chương trình xây dựng mạng. Thời gian cho quá trình này là vài năm kể từ khi đo đạc đến khi xây dựng hoàn chỉnh mạng mới.
- Vòng B là vòng phân tích hoạt động của mạng. Hoạt động của mạng được giám sát và phân tích kết quả để chỉ rõ các xu hướng lỗi. Các chương trình quản lý có thể được sử dụng để sửa lại bất kỳ các vấn đề lỗi nào. Giám sát và phân tích có thể vượt quá chu kỳ ngày, tuần hoặc một số tháng. Các kết quả cũng sử dụng như mục đích để lập kế hoạch cho các chức năng này.
- Vòng C là vòng quản lý lưu lượng mạng. Hoạt động của mạng được giám sát trong thời gian thực và các chiến lược điều khiển thực hiện để vượt qua sự đổ vỡ của mạng một cách nhanh nhất khi nó xảy ra. Thời gian cho quá trình này là từ vài phút đến vài giờ.

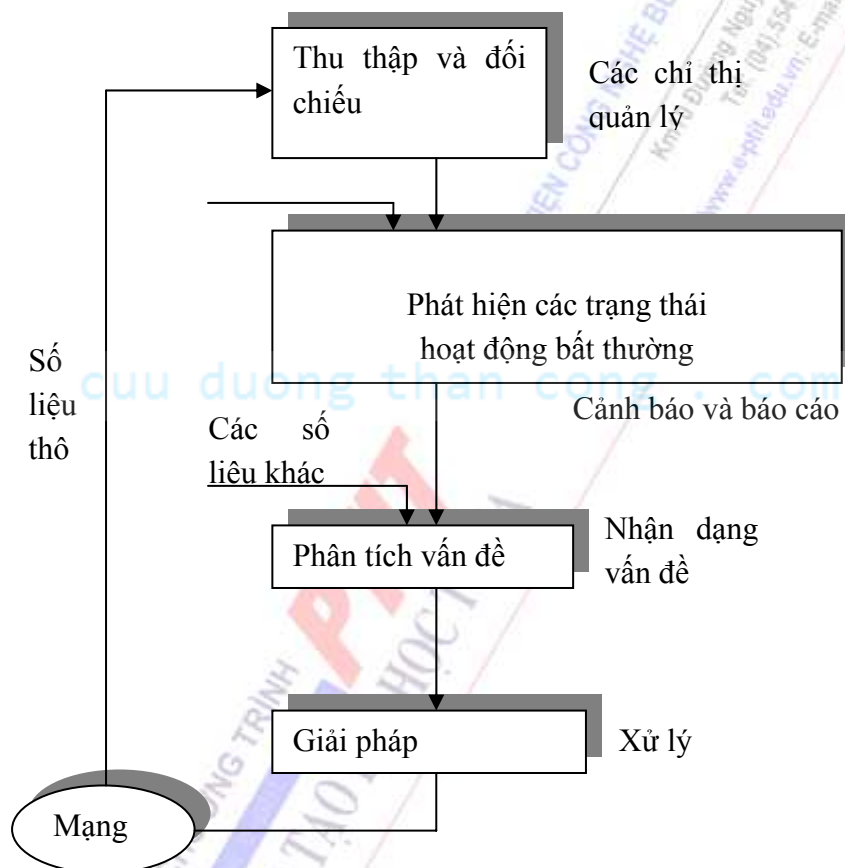
Một tình huống là dưới sự nghiên cứu điều khiển, các nguyên nhân cơ bản có thể đưa ra để hỗ trợ cho người sử dụng trong tương lai hoặc sửa lỗi thiết bị hay lỗi thiết kế.

2.5.1.4 Đảm bảo chất lượng hoạt động

Chú ý tới các hoạt động để đảm bảo chất lượng của dịch vụ và thông báo kết quả phân tích. Các hoạt động này bao gồm giám sát và đảm bảo chất lượng kết nối, tình trạng nguyên vẹn của bản tin, cộng tác với quản lý lỗi để thiết lập nguyên nhân của lỗi tài nguyên và kết hợp với quản lý cấu hình để thay đổi định tuyến và tham số điều khiển tải.

2.5.2 Quản lý sự cố

Quản lý sự cố là tập hợp các chức năng cho phép phát hiện, cô lập và sửa các sự cố những hoạt động không bình thường của mạng viễn thông và môi trường của mạng. Bao gồm 3 chức năng chính: giám sát cảnh báo, cô lập sự cố, sửa chữa và kiểm tra lỗi.



Hình 2.17: Lưu đồ giám sát mạng

- Giám sát cảnh báo bao gồm: phân tích số liệu thu được từ các cảnh báo khác nhau, chọn lọc số liệu cảnh báo để so sánh tìm ra mối tương quan giữa các thành phần mạng và tương quan theo thời gian. Chức năng này cung cấp khả năng giám sát trạng thái của NE trong thời gian gần với thời gian thực. Khi có lỗi xuất hiện, NE sẽ thông báo lỗi lên hệ thống điều hành, dựa vào đó TMN quyết định tính chất và mức độ của lỗi.
- Cô lập sự cố: Từ các thông tin về lỗi và sự cố xảy ra trên mạng, phân tích và cần thiết thì dùng các phương tiện đo kiểm tra mạng để xác định nguyên nhân gây ra lỗi, vị trí xảy ra lỗi và sự cố trên mạng. Việc kiểm tra lỗi có thể thực hiện bằng một trong hai cách sau

đây: TMN chỉ thị cho NE thực hiện việc phân tích mạch hoặc các hoạt động thiết bị, việc xử lý được thực hiện hoàn toàn bên trong NE và kết quả được tự động đưa tới TMN. Cách thứ hai là việc phân tích được thực hiện bên trong TMN, trong trường hợp này TMN chỉ yêu cầu NE cung cấp truy nhập tới mạch hoặc thiết bị quan tâm và không có các tin báo nào khác trao đổi với NE.

- Sửa chữa và kiểm tra lỗi: Kiểm tra thực trạng và mức độ nguy hiểm của lỗi, phạm vi ảnh hưởng của lỗi và xử lý lỗi bằng các phương tiện như hiệu chỉnh các chỉ tiêu, khôi phục hoặc khởi tạo lại cấu hình hệ thống. Khi thông tin sự cố ban đầu không đủ để xác định lỗi thì thông tin bổ sung do các thủ tục xác định vị trí lỗi cung cấp, các thủ tục này có thể sử dụng các hệ thống kiểm tra bên trong và bên ngoài và có thể đặt dưới sự điều khiển của hệ thống quản lý mạng viễn thông.

2.5.3. Quản lý cấu hình

Quản lý cấu hình thực hiện việc lập kế hoạch và cài đặt NE, liên kết NE với mạng và hình thành những dịch vụ khách hàng sử dụng mạng. Theo khuyến nghị M3400 (1992) của ITU-T việc quản lý cấu hình được chia làm 3 nội dung chính: cung cấp; trạng thái và điều khiển NE; và cài đặt NE.

- Cung cấp cấu hình mạng từ khi mới lắp đặt và sự thay đổi cấu hình đến hiện tại.
- Quản lý Trạng thái cấu hình đang làm việc.
- Quản lý việc lắp đặt phần cứng theo cấu hình đã được thiết kế.
- Quản lý việc khởi tạo hệ thống theo cấu hình đã định.
- Quản lý số lượng thiết bị, phụ tùng để thay thế và đã được thay thế để có được cấu hình hiện tại.
- Quản lý việc sao lưu cấu hình được thay đổi theo quá trình khai thác và bảo dưỡng mạng lưới trên cả phần cứng và phần mềm, chất lượng khi thay đổi cấu hình trên thực tế, khôi phục lại cấu hình

2.5.3.1 Cung cấp

Là một bộ thủ tục mang những thiết bị đã được cài đặt vào dịch vụ và được chia thành những nhóm chức năng khác nhau. Một là cấu hình NE cung cấp một bộ những chức năng quản lý cấu hình của một NE. Bao gồm những nhiệm vụ như báo cáo cấu hình thông tin tới một hệ thống bên ngoài và thay đổi cấu hình để phù hợp với sự thêm vào, xoá đi hay sự sửa đổi cấu hình của NE. Một chức năng khác là quản lý NE liên quan tới hệ thống quản lý. Những nhiệm vụ gồm đặt đồng hồ, lưu trữ, khởi tạo xử lý và tắt máy. Nhóm chức năng còn lại quản lý cơ sở dữ liệu NE nhằm cung cấp khả năng để sắp xếp, lưu giữ và cập nhật cơ sở dữ liệu.

2.5.3.2 Trạng thái và điều khiển NE

Cung cấp một bộ chức năng để thực hiện báo cáo trạng thái, liệt kê các bản tin trạng thái và chấp nhận yêu cầu của bản tin trạng thái. Nó có thể là bản tin trạng thái mạng, trạng thái mạng vòng thuê bao, trạng thái mạng truyền dẫn hoặc kết hợp các mạng trên.

2.5.3.3 Cài đặt NE.

Cung cấp sự cài đặt cho thiết bị và những phần mềm tạo nên mạng viễn thông. Công việc bao gồm sự xác định một bộ hoạt động cài đặt, cùng với sự liên tục và liệt kê hoạt động để đạt được hiệu suất cao nhất và trở ngại tối thiểu với hoạt động đang diễn ra.

2.5.4 Quản lý tài khoản.

Cung cấp việc thiết lập các chức năng cho phép việc sử dụng dịch vụ mạng được đo đạc và giá thành cho việc sử dụng được xác định. Nó cung cấp các khả năng:

- Thu thập số liệu liên quan tới tính cước.
- Thiết lập các tham số phục vụ cho việc lập hóa đơn.
- Thu thập số liệu cuộc gọi khách hàng, kênh thuê riêng theo tốc độ và dung lượng khách hàng thuê và chất lượng dịch vụ từ các hệ thống thống kê tự động và nhân công trên mạng để tính cước khách hàng theo các quy định hiện hành hợp pháp hợp lệ, cung cấp hoá đơn chi tiết hoặc tổng hợp cho khách hàng tùy theo quy định hợp pháp.
- Khi thu thập được những số liệu sai dẫn đến sự vô lý làm thiệt hại đến khách hàng thì phải sửa cho phù hợp thực tế khách quan và đáng tin cậy để khách hàng khỏi bị thiệt thòi. Giải quyết các khiếu nại khách hàng là công việc rất đa dạng, phức tạp trong đó nhiều khi vượt khỏi khả năng các phương tiện kỹ thuật

2.5.5 Quản lý bảo mật.

Đây là chức năng cung cấp và đảm bảo khả năng truy cập an toàn tới các chức năng và năng lực của các thành phần cấu thành mạng lưới (Network Element – NE). Đây là chức năng cung cấp khả năng truy cập an toàn tới các thành phần thuộc hệ thống mạng điều hành mạng viễn thông (TMN) như: các hệ thống khai thác (OS – Operation System), các bộ điều khiển mạng cấp dưới (SNC – Subnetwork Control) và các thiết bị trung gian (MD – Mediation Device).

Nhằm quản lý và điều khiển quyền truy nhập tới các tài nguyên trên mạng, quản lý bảo mật bao gồm các chức năng sau:

- Xác định quyền truy nhập.
- Điều khiển truy nhập.
- Mã hóa và kiểm soát khóa mã hóa.
- Ủy quyền truy nhập.
- Đăng ký bảo mật.

Ngoài các chức năng trên còn có một số các chức năng quản lý mạng quan trọng khác chưa được chuẩn hóa, mặc dù đó là một phần của cơ cấu quản lý mạng tổng thể:

- Lập kế hoạch: Cài đặt các tài nguyên, phát triển và sử dụng các dịch vụ...
- Quản lý lực lượng lao động: Lập kế hoạch và điều khiển các hoạt động của nhóm cán bộ điều hành...
- Quản lý vật tư: Lưu giữ các thiết bị sử dụng để cài đặt, sửa chữa mạng...

2.6 KIẾN TRÚC THÔNG TIN

Kiến trúc thông tin sử dụng cách tiếp cận TMN dựa trên mô hình tham chiếu các hệ thống mở OSI. TMN sử dụng cùng một khái niệm quản lý-tác nhân (manager-agent) như trong mô hình OSI. Kiến trúc thông tin TMN là một bản sao của kiến trúc thông tin OSI, vì vậy chúng ta sẽ không đề cập nhiều về kiến trúc thông tin TMN. Các thông tin quản lý TMN được xem xét từ hai khía cạnh sau đây:

Mô hình thông tin quản lý:

Mô hình thông tin quản lý thể hiện một cách tổng quát các xu hướng quản lý tài nguyên mạng và các hoạt động quản lý hỗ trợ có liên quan. Mô hình thông tin xác định có thể trao đổi thông tin theo các tiêu chuẩn xác định. Hoạt động này nhằm hỗ trợ mô hình thông tin tại mức ứng dụng và bao hàm cả các chức năng ứng dụng quản lý như lưu trữ, tái hiện và xử lý thông tin. Các chức năng được bao hàm tại mức này được xem như là “Các khối chức năng TMN”.

Trao đổi thông tin quản lý:

Trao đổi thông tin quản lý bao gồm các DCF được kết hợp như một mạng thông tin và cùng với MCF cho phép các thành phần vật lý xác định liên kết tới một mạng viễn thông qua một giao diện nào đó. Mức hoạt động này chỉ bao gồm các cơ cấu thông tin như các giao thức ngăn xếp.

Đối tượng trao đổi thông tin trong các hệ thống quản lý được mô hình hoá dưới dạng các đối tượng quản lý, đối tượng quản lý được định nghĩa bởi:

- Các thuộc tính rõ ràng tại ranh giới của nó;
- Các hoạt động quản lý có thể được sử dụng đối với nó;
- Các tác động mà đối tượng thực hiện nhằm đáp ứng các hoạt động quản lý hoặc các hoạt động thuộc loại kích hoạt. Nó có thể là cục bộ hoặc mở rộng;
- Các nút mà đối tượng đưa ra.

Ngoài ra, một số vấn đề cần quan tâm thêm khi xem xét mô hình kiến trúc thông tin của TMN đó là:

- Không cần sắp xếp tương ứng một một giữa các đối tượng quản lý và các tài nguyên thực (có thể là vật lý hoặc logic).
- Một tài nguyên có thể được thể hiện bởi một hoặc nhiều đối tượng. Khi một tài nguyên được thể hiện bởi nhiều đối tượng quản lý thì mỗi đối tượng sẽ cung cấp một cách nhìn khác nhau đối với tài nguyên. lưu ý rằng các đối tượng này có thể được ghép cặp trong các tác động của chúng thông qua các quan hệ vật lý hoặc logic.
- Các đối tượng quản lý tồn tại và nó thể hiện là các tài nguyên logic của TMN hơn là tài nguyên của mạng viễn thông.
- Nếu một tài nguyên không được thể hiện bởi một đối tượng quản lý, nó không thể được quản lý thông qua giao diện quản lý. Nói cách khác là nó không được hệ thống quản lý nhìn thấy.
- Một đối tượng quản lý có thể cung cấp một cách nhìn tổng quát đối với các tài nguyên được thể hiện bởi các đối tượng quản lý.

Các đối tượng quản lý có thể được gắn liền, nghĩa là đối tượng quản lý có thể thể hiện các tài nguyên lớn bao hàm các tài nguyên đã được mô hình hóa như một thành phần của đối tượng lớn.

2.6.1. Mô hình đối tượng trên cơ sở OSI

Để cho phép định nghĩa các nguồn tài nguyên bị quản lý một cách hiệu quả, kiến trúc thông tin TMN sử dụng các nguyên lý quản lý OSI và được dựa trên mô hình hướng đối tượng.

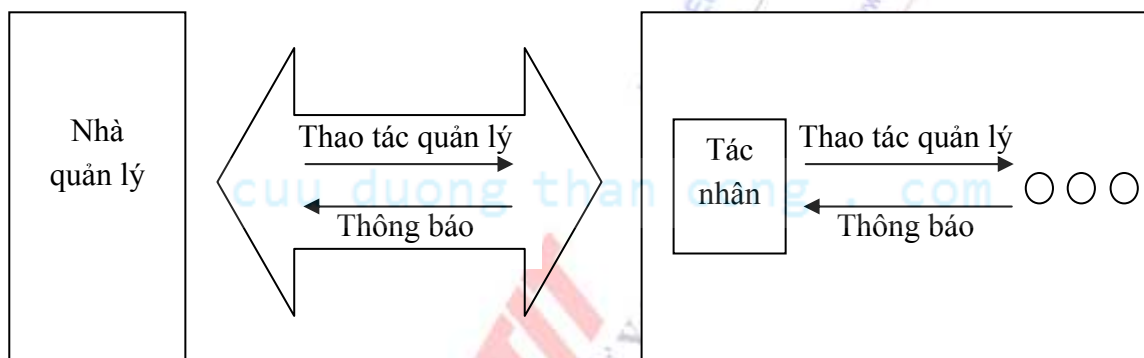
Các hệ thống quản lý trao đổi thông tin được mô hình hoá dưới dạng các đối tượng quản lý, đó là cách nhìn trừu tượng đối với các nguồn tài nguyên đang được quản lý, nghĩa là các

hệ thống quản lý xác nhận các hoạt động quản lý tại các giao diện mà các hệ thống truyền thông quản lý tương tác với nhau. Nó không hạn chế việc triển khai thực hiện bên trong của các hệ thống quản lý viễn thông. Đối tượng quản lý được định nghĩa bởi:

- Các thuộc tính có thể nhìn thấy được tại ranh giới của nó
- Các hoạt động quản lý có thể được áp dụng cho nó
- Hoạt động của đối tượng quản lý để đáp lại các hoạt động quản lý hoặc để phản ứng với các kích thích liên quan tới các loại quản lý khác (bên trong: vượt quá ngưỡng, hoặc bên ngoài: tương tác với các đối tượng khác)
- Các thông báo do đối tượng phát ra

2.6.2. Mô hình đối tượng phân tán

Quản lý môi trường viễn thông là một ứng dụng xử lý thông tin. Do môi trường bị quản lý bị phân tán, quản lý mạng cũng là một ứng dụng phân tán bao gồm việc trao đổi các thông tin quản lý giữa các tiến trình quản lý nhằm mục tiêu giám sát, điều khiển các nguồn tài nguyên vật lý cũng như logic của mạng (truyền dẫn, chuyển mạch).



Hình 2.18: Mối quan hệ nhà quản lý/ tác nhân/ đối tượng

Đối với một tương tác quản lý nhất định, tiến trình quản lý có thể đóng một trong hai vai trò sau:

- Vai trò nhà quản lý: đưa ra các chỉ thị, yêu cầu thao tác quản lý và nhận thông báo hoạt động quản lý
- Vai trò tác nhân: quản lý các đối tượng bị quản lý liên quan và trả lời các lệnh do nhà quản lý của tác nhân phát ra. Nó cũng phản ánh số liệu của các đối tượng này cho nhà quản lý, đồng thời thông báo cho nhà quản lý về ứng xử của những đối tượng này.

Mọi sự trao đổi quản lý giữa nhà quản lý và tác nhân được thực hiện trong một tập hợp nhất quán các hoạt động quản lý (khởi tạo thông qua vai trò nhà quản lý và các thông báo do các tác nhân phát ra). Phương thức các tác nhân tương tác với các nguồn tài nguyên mà chúng chịu trách nhiệm quản lý phụ thuộc vào các nhà chế tạo.

CÂU HỎI ÔN TẬP CHƯƠNG 2

- Theo mô hình tham chiếu OSI, một hệ thống TMN có bao nhiêu lớp
 - A. 3
 - B. 4
 - C. 5
 - D. 7
- Trong mô hình chức năng TMN, các khối chức năng chính của TMN có thể thực hiện cả chức năng quản lý (manager) và tác nhân (agent)
 - A. true
 - B. false
- Giao diện Q3 là giao diện duy nhất mà QA, MD hoặc NE có thể sử dụng để giao tiếp trực tiếp với OS.
 - A. true
 - B. false
- Có bao nhiêu khối chức năng trong mô hình chức năng TMN
 - A. 3
 - B. 4
 - C. 5
 - D. 6
- Khối chức năng nào trong TMN cung cấp chức năng cho hoạt động liên kết giữa người sử dụng với OSF
 - A. NEF
 - B. WSF
 - C. QAF
 - D. MF
- Khối chức năng nào cung cấp sự chuyển đổi để kết nối NEF hoặc OSF tới TMN, hoặc những phần tử mạng không thuộc TMN với TMN một cách độc lập
 - A. NEF
 - B. OSF
 - C. QAF
 - D. MF
- Khối chức năng nào có hai nhiệm vụ chính là truyền tải thông tin và xử lý thông tin
 - A. NEF
 - B. OSF
 - C. QAF
 - D. MF
- Kiến trúc phân lớp logic chia mô hình quản lý của TMN thành bao nhiêu lớp
 - A. 3
 - B. 4
 - C. 5
 - D. 6
- Kết nối giữa các lớp quản lý trong mô hình LLA của TMN thông qua điểm tham chiếu
 - A. q
 - B. f
 - C. x
 - D. m
- Trong mô hình LLA của TMN, lớp _____ vừa có nhiệm vụ quản lý các thực thể trong lớp vừa có nhiệm vụ cung cấp các thông tin quản lý cho lớp NML.

- A. Lớp quản lý phần tử mạng (NEML- Network Element Manager Layer)
- B. Lớp quản lý mạng (NML- Network Manager Layer)
- C. Lớp quản lý dịch vụ (SML- Service Manager Layer)
- D. Lớp quản lý kinh doanh (BML- Business Manager Layer)

11. Có bao nhiêu chức năng quản lý trong mô hình TMN
- A. 3
 - B. 4
 - C. 5
 - D. 6
12. Trong TMN, định nghĩa bao nhiêu điểm tham chiếu TMN
- A. 2
 - B. 3
 - C. 4
 - D. 5
13. Trong TMN, định nghĩa bao nhiêu điểm tham chiếu phi TMN (non-TMN)
- A. 2
 - B. 3
 - C. 4
 - D. 5
14. Giữa trạm làm việc WSF và người dùng là điểm tham chiếu
- A. q
 - B. x
 - C. f
 - D. g
15. Điểm tham chiếu giữa QAF và thực thể phi TMN bị quản lý là _____
- A. q
 - B. x
 - C. m
 - D. g
16. Khi nói đến TMN, điểm tham chiếu nào sau đây là điểm tham chiếu TMN
- A. q
 - B. x
 - C. f
 - D. g
 - E. m
17. Khi nói đến TMN, điểm tham chiếu nào sau đây là điểm tham chiếu phi TMN (non-TMN)
- A. q
 - B. x
 - C. f
 - D. g
 - E. m
18. Điểm tham chiếu _____ nằm giữa OSF của hai hệ thống TMN
- A. q
 - B. x
 - C. f
 - D. g
 - E. m
19. Khái niệm mạng quản lý viễn thông TMN được ITU-T công bố lần đầu tiên vào năm nào?
- A. 1985
 - B. 1990
 - C. 1988
 - D. 1995
20. TMN chỉ sử dụng duy nhất một hệ điều hành OS để thực hiện chức năng quản lý?

A. Đúng B. Sai

21. Hai chức năng hệ điều hành OSF của hai TMN được kết nối thông qua điểm tham chiếu:
- A. q C. f
B. m D. x
22. Trong một TMN, chức năng trung gian MF được kết nối với chức năng WSF thông qua điểm tham chiếu _____
- A. q C. f
B. g D. x
23. Kết nối trực tiếp hai QAF trong TMN thông qua điểm tham chiếu _____
- A. q C. f
B. g D. x
24. Giao tiếp giữa NE và MD sử dụng giao diện _____
- A. Q3 C. F
B. Qx D. X
25. Để kết nối hai hệ thống TMN với nhau, giao diện _____ được sử dụng
- A. Q3 C. F
B. Qx D. X
26. Tất cả các thực thể được kết nối trực tiếp với OS thông qua giao diện _____
- A. Q3 C. F
B. Qx D. X
27. Trong kiến trúc phân lớp logic TMN, _____ là lớp quản lý mạng
- A. NEML C. SML
B. NML D. BML
28. Trong kiến trúc phân lớp logic TMN, _____ là lớp quản lý kinh doanh
- A. NEML C. SML
B. NML D. BML
29. Điểm tham chiếu _____ phân chia hai lớp quản lý SML và NML
- A. q3 C. f
B. qx D. x
30. Quản lý hiệu năng bao gồm 4 nhóm chức năng cơ bản nào?
- A. Giám sát, phát hiện lỗi, cảnh báo và khắc phục lỗi
B. Giám sát, điều khiển quản lý, phân tích và đảm bảo chất lượng đặc tính.
C. Giám sát, phát hiện lỗi, phân tích và khắc phục lỗi
D. Giám sát, điều khiển quản lý, phân tích và khắc phục lỗi

31. Trong các chức năng quản lý của TMN, _____ là tập hợp các chức năng cho phép phát hiện, cô lập và sửa các sự cố những hoạt động không bình thường của mạng viễn thông và môi trường của mạng.
- A. Quản lý hiệu năng
 - B. Quản lý sự cố
 - C. Quản lý cấu hình
 - D. Quản lý tài khoản
 - E. Quản lý bảo mật
32. Theo khuyến nghị M3400 (1992) của ITU-T việc quản lý cấu hình được chia làm 3 nội dung chính:
- A. Lập cấu hình; quản lý trạng thái và cài đặt
 - B. Quản lý trạng thái NE; cài đặt NE và cảnh báo
 - C. Cung cấp; trạng thái và điều khiển NE; và cài đặt NE
 - D. Cung cấp, quản lý cấu hình và cảnh báo
33. Trong các chức năng quản lý, _____ cung cấp và đảm bảo khả năng truy cập an toàn tới các chức năng và năng lực của các thành phần cấu thành mạng lưới
- A. Quản lý hiệu năng
 - B. Quản lý sự cố
 - C. Quản lý cấu hình
 - D. Quản lý tài khoản
 - E. Quản lý bảo mật
34. Có thể nói kiến trúc thông tin TMN là một bản sao của OSI?
- A. Đúng
 - B. Sai

CHƯƠNG 3

GIAO THỨC QUẢN LÝ MẠNG ĐƠN GIẢN SNMP

Mục đích của chương 3 là cung cấp cho người đọc những khái niệm cơ bản nhất về giao thức quản lý mạng đơn giản SNMP: các thành phần, chức năng và phương thức hoạt động của giao thức, đồng thời giới thiệu các phiên bản ứng dụng mới nhất của SNMP.

Phần đầu chương giới thiệu tổng quan về SNMP, cấu trúc và đặc điểm cũng như hoạt động của giao thức này. Sau đó giới thiệu các phiên bản sau của SNMP và phân tích được những khác biệt của các phiên bản sau với phiên bản SNMP đầu tiên.

Quản lý mạng viễn thông là một nội dung rất quan trọng trong việc nghiên cứu, vận hành viễn thông nói chung và đặc biệt là mạng viễn thông trên nền IP nói riêng. Vì vậy cần tìm hiểu chi tiết về các thành phần SNMP và hoạt động của giao thức thông qua nhiều lệnh khác nhau do các chuẩn phiên bản SNMP cung cấp.

Học viên cần phải nắm được các khái niệm cơ bản về quản lý viễn thông, từ mô hình mạng trên nền IP đến những mô hình mạng quản lý viễn thông hiện đại và cách thức hoạt động, điều hành mạng viễn thông qua các giao thức quản lý mạng đơn giản.

3.1 GIỚI THIỆU CHUNG VỀ SNMP

Trong lĩnh vực Internet, việc quản lý mạng, thiết bị và các trạm được gọi là hoạt động quản lý mạng, đối chiếu với thuật ngữ sử dụng trong TMN. Bất kỳ cuốn sách nào khi đề cập đến quản lý mạng TCP/IP đều không thể không thảo luận chi tiết về vai trò của giao thức quản lý mạng đơn giản SNMP và giám sát từ xa (RMON) cho phép thực hiện giám sát trạng thái của các mạng từ xa qua những công cụ giám sát mạng điện rộng có tốc độ khá thấp.

Sự phát triển rất nhanh của SNMP song song với sự tiến triển của chồng giao thức TCP/IP. Với mong muốn giám sát được hiện năng của các cổng giao thức kết nối các mạng độc lập vào mạng Internet đã dẫn tới việc phát triển giao thức giám sát cổng đơn giản (SGMP-Simple Gateway Monitoring Protocol), được coi là tổ tiên của giao thức SNMP. Sự cần thiết có những chuyển đổi và cải thiện cho SGMP đã dẫn đến việc thành lập IAB – Hội đồng hoạt động Internet (Internet Activities Board), trong năm 1992 đã đổi tên thành Hội đồng kiến trúc Internet (Internet Architecture Board) khuyến nghị sự phát triển của chuẩn quản lý mạng Internet mở rộng trong RFC. Với sự ủng hộ của IAB, Tổ chức hỗ trợ kỹ thuật Internet (IETF) chịu trách nhiệm cho việc thiết kế, thử nghiệm và triển khai chuẩn quản lý mạng Internet mới này. Kết quả của những nỗ lực trên là nhóm các nhà nghiên cứu và kỹ sư IETF đã xuất bản ba RFC vào tháng 8 năm 1988, tạo cơ sở cho giao thức SNMP (Bảng 3.1).

Trong bảng 3.1, để ý là RFC không phải là những tài liệu có nội dung cố định, chúng sẽ được xem xét nhiều lần và hiệu chỉnh trước khi chính thức chấp nhận là một chuẩn trong cộng đồng Internet. Một khi đã được chuẩn hóa, theo thời gian nếu thay đổi thì nó thường được thay thế bằng một RFC khác.

Bảng 3.1 : Những RFC ban đầu định nghĩa SNMP

RFC 1065	Kiến trúc và nhận dạng thông tin quản lí cho các liên mạng dựa trên nền giao thức TCP/IP.
RFC 1066	Cơ sở thông tin quản lí cho việc Quản lí mạng của các liên mạng dựa trên nền giao thức TCP/IP.
RFC 1067	Giao thức quản lí mạng đơn giản

Sau khi ra đời SNMP đã nhanh chóng trở thành một giao thức quản lí mạng thông dụng cho các mạng máy tính dựa trên cơ sở TCP/IP. SNMP làm cho việc trao đổi thông tin quản lí giữa các thiết bị mạng hoạt động tại tầng ứng dụng của ISO/OSI trở nên thuận tiện hơn song bên cạnh đó nó cũng có những hạn chế (xem phân tích đặc tính của SNMP trong bảng 3.2).

Bảng 3.2: Đặc tính của SNMP

<i>Ưu điểm</i>	<i>Khuyết điểm</i>
<ul style="list-style-type: none"> - Có thể giảm được chi phí cho việc triển khai phương thức đại lý dùng giao thức SNMP. - Việc cài đặt SNMP vào thiết bị trong cấu hình mạng đơn giản. - Có thể bổ sung thêm một cách không hạn chế thiết bị và các nhà cung cấp cũng như là những đối tượng quản lí. - SNMP là một giải pháp có hiệu quả cho việc quản lí thiết bị nhiều nhà cung cấp. 	<ul style="list-style-type: none"> - SNMP làm tăng lưu lượng đáng kể. - SNMP không cho phép phân bổ tác động trực tiếp cho các đại lý. - Không có sự điều khiển tổng hợp của nhiều nơi quản lí.

IETF tạo ra SNMP nhằm cho phép quản lí từ xa các thiết bị dựa trên nền tảng IP. Nó hỗ trợ một cách rộng rãi các thiết bị như máy chủ, máy in, bộ nối, bộ định tuyến, hub... Giao thức này được trình bày một cách chi tiết trong tài liệu RFC 1157 của IETF.

Năm 1993, SNMP Version 2 (SNMPv2) được IETF đưa ra với mục đích giải quyết vấn đề tồn tại trong SNMPv1 là cơ chế đảm bảo bảo mật. SNMPv2 có nhiều thay đổi so với SNMPv1 như hỗ trợ các mạng trung tâm cấp cao, mạng phân tán, cơ chế bảo mật, làm việc với khối dữ liệu lớn... Tuy nhiên SNMPv2 không được chấp nhận hoàn toàn bởi vì SNMPv2 chưa thỏa mãn vấn đề bảo mật và quản trị bởi vậy năm 1996 những phần bảo mật trong SNMPv2 bị bỏ qua và SNMPv2 được gọi là “SNMPv2 trên cơ sở truyền thông” hay SNMPv2c.

Năm 1998, IETF bắt đầu đưa ra SNMPv3 được định nghĩa trong RFCs 2571-2575. Về bản chất, SNMPv3 mở rộng để đạt được cả hai mục đích là bảo mật và quản trị. SNMPv3 hỗ trợ kiến trúc theo kiểu module để có thể dễ dàng mở rộng. Như thế nếu các giao thức bảo mật được mở rộng chúng có thể được hỗ trợ bởi SNMPv3 bằng cách định nghĩa như là các module riêng.

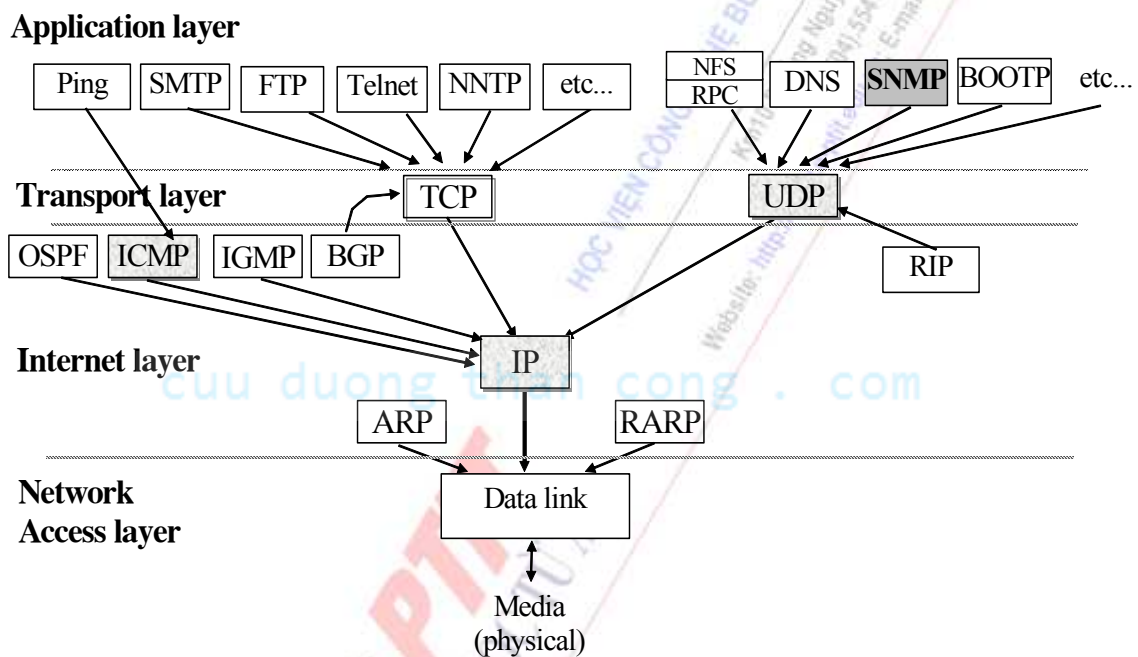
Bên cạnh đó một phần quan trọng của quản trị mạng là kiểm soát từ xa. Tính năng kiểm soát từ xa (Remote Monitoring - RMON) định nghĩa thêm vào SNMP MIB nhằm hỗ trợ việc quản trị liên mạng. RMON tạo cho người quản trị mạng khả năng kiểm soát toàn bộ mạng con hơn là các thiết bị đơn lẻ trong mạng con.

3.2. QUẢN LÝ TRUYỀN THÔNG TRONG SNMP

SNMP hoạt động dựa trên mô hình Manager/Agent. Manager được gọi là trạm quản lý mạng (QLM). Thông tin được trao đổi giữa Agent và Manager. Các phần tử mạng sẽ tiếp nhận các yêu cầu truy nhập từ hệ thống quản lý mạng vào cơ sở dữ liệu.

Giao thức SNMP sử dụng kiểu kết nối không định hướng để trao đổi thông tin giữa các phần tử và hệ thống quản lý mạng (trường hợp này là sử dụng UDP). UDP truyền các gói tin theo các khối riêng biệt. Tuy vậy có thể tùy ý sử dụng các giao thức khác để truyền các gói tin SNMP. Các gói tin sau khi truyền qua mạng, các phần tử mạng hay hệ thống quản lý mạng vẫn giữ nguyên định dạng của SNMP.

Hình 3.1 cho thấy vị trí giao thức SNMP trong mô hình chồng giao thức TCP/IP. Ta thấy, SNMP sử dụng giao thức dữ liệu đồ người sử dụng (UDP) làm giao thức lớp vận chuyển trên mạng IP.



Hình 3.1: SNMP trong TCP/IP

3.2.1 Quản lý liên lạc giữa nhà quản lý với các tác nhân

Nhìn trên phương diện truyền thông, nhà quản lý (manager) và các tác nhân (agent) cũng là những người sử dụng, sử dụng một giao thức ứng dụng. Giao thức quản lý yêu cầu cơ chế vận tải để hỗ trợ tương tác giữa các tác nhân và nhà quản lý.

Nhà quản lý trước hết phải xác định được các tác nhân mà nó muốn liên lạc. Có thể xác định được ứng dụng tác nhân bằng địa chỉ IP của nó và cổng UDP được gán cho nó. Cổng UDP 161 được dành riêng cho các tác nhân SNMP. Chương trình nhà quản lý gói lệnh SNMP vào một phong bì UDP/IP. Phong bì này chứa cổng nguồn, địa chỉ IP đích và cổng 161. Một thực thể IP tại chỗ sẽ chuyển giao khung UDP tới hệ thống bị quản lý. Tiếp đó, một thực thể UDP tại chỗ sẽ chuyển phát nó tới các tác nhân. Tương tự như vậy, lệnh TRAP cũng cần xác định những nhà quản lý mà nó cần liên hệ. Chúng sử dụng địa chỉ IP cũng như cổng UDP dành cho nhà quản lý SNMP, đó là cổng 162.

3.2.2 Cơ chế vận chuyển thông tin giữa nhà quản lý và tác nhân

Việc lựa chọn cơ chế vận chuyển có tính trực giao với giao thức truyền thông đó. SNMP chỉ đòi hỏi cơ chế truyền tải không tin cậy dữ liệu đồ (datagram) để truyền đưa các PDU (đơn vị dữ liệu giao thức) giữa nhà quản lý và các tác nhân. Điều này cho phép sự ánh xạ của SNMP tới nhiều nhóm giao thức. Mô hình vận chuyển datagram giảm được độ phức tạp của ánh xạ tầng vận chuyển. Tuy nhiên, vẫn phải nhận thức thấy sự tham gia của một số lựa chọn tầng vận chuyển. Các tầng vận chuyển khác nhau có thể sử dụng nhiều kỹ thuật đánh địa chỉ khác nhau. Các tầng vận chuyển khác nhau có thể đưa ra những hạn chế quy mô của PDU. Ánh xạ tầng vận chuyển có trách nhiệm phải xử lý các vấn đề đánh địa chỉ, hạn chế quy mô PDU và một số tham số tầng vận chuyển khác.

Trong phiên bản thứ hai của SNMP, người ta sử dụng kinh nghiệm để làm sắc nét và đơn giản hóa quá trình ánh xạ tới các chuẩn vận chuyển khác nhau. Giao thức quản lý được tách khỏi môi trường vận chuyển một cách trực giao, điều này cũng được khuyến khích sử dụng cho bất cứ nhóm giao thức nào.

3.2.3 Bảo vệ truyền thông liên lạc giữa nhà quản lý và các tác nhân khỏi sự cố

Trong điều kiện mạng thiếu ổn định và thiếu độ tin cậy thì sự liên lạc quản lý càng trở nên quan trọng. Làm thế nào để các nhà quản lý liên lạc với các tác nhân một cách tin cậy? Việc SNMP sử dụng cơ chế UDP để liên lạc đã có nghĩa là thiếu đi độ tin cậy rồi. SNMP hoàn toàn để lại cho chương trình nhà quản lý chịu trách nhiệm và xử lý việc mất thông tin. Các lệnh GET, GET-NEXT, và SET đều được phúc đáp bằng một lệnh GET-RESPONSE. Hệ thống có thể dễ dàng phát hiện ra việc bị mất một lệnh khi không nhận được lệnh trả lời. Nó có thể lặp lại yêu cầu đó một lần nữa hoặc có những hành động khác. Tuy nhiên, các bản tin TRAP do tác nhân tạo ra và không được phúc đáp khẳng định. Khi lệnh TRAP bị thất lạc, các chương trình tác nhân sẽ không biết về điều đó (tất nhiên là nhà quản lý cũng không hay biết về điều này). Thông thường các bản tin TRAP mang những thông tin hết sức quan trọng cho nhà quản lý, do vậy nhà quản lý cần chú ý và cần bảo đảm việc chuyển phát chúng một cách tin cậy.

Một câu hỏi đặt ra là làm thế nào để chuyển phát các bản tin TRAP tránh mất mát, thất lạc? Ta có thể thiết kế cho các tác nhân lặp lại bản tin TRAP. Biến số MIB có thể đọc số lần lặp lại theo yêu cầu. Lệnh SET của nhà quản lý có thể đặt cấu hình cho biến số này. Có một cách khác là tác nhân có thể lặp lại lệnh TRAP cho đến khi nhà quản lý đặt biến số MIB để chấm dứt sự cố. Hãy ghi nhớ rằng, cả hai phương pháp trên đều chỉ cho ta những giải pháp từng phần. Trong trường hợp thứ nhất, số lần lặp lại có thể không đủ để đảm bảo liên lạc một cách tin cậy. Trong trường hợp thứ hai, một sự cố mạng có thể dẫn đến việc hàng loạt bản tin TRAP bị mất tùy thuộc vào tốc độ mà các tác nhân tạo ra chúng. Điều này làm cho sự cố mạng trở nên trầm trọng hơn. Trong cả hai trường hợp, nếu ta cần chuyển phát những bản tin TRAP tới nhiều nhà quản lý, thì có thể xảy ra tình trạng không nhất quán giữa các nhà quản lý hoặc xảy ra hiện tượng thất lạc thông tin rất phức tạp. Nếu các tác nhân phải chịu trách nhiệm về thiết kế cho việc phục hồi những bản tin TRAP thì càng làm tăng thêm độ phức tạp trong việc quản lý các tác nhân trong môi trường đa nhà chế tạo.

Người ta cũng đã theo đuổi cải tiến cơ chế xử lý bản tin sự cố cho phiên bản thứ hai của SNMP. Thứ nhất là đơn nguyên TRAP được bỏ đi và thay thế nó bằng một lệnh GET/RESPONSE không yêu cầu. Lệnh này do tác nhân tạo ra và chuyển đến cho “nhà quản lý bẫy” tại cổng UDP-162. Điều này phản ánh một quan điểm là nhà quản lý sự cố có thể thống nhất

các bản tin sự cố rồi trả lời cho các yêu cầu ảo. Bằng cách bỏ đi một đơn thể, giao thức được đơn giản hóa. Người ta cũng bổ sung thêm một cơ sở thông tin quản lý đặc biệt TRAP MIB để thống nhất việc xử lý sự cố, các nhà quản lý nhận bản tin về các sự cố này và việc lặp lại để cải thiện độ tin cậy trong chuyển phát thông tin.

3.2.4 Ảnh hưởng của tầng vận chuyển tới khả năng quản lý mạng

Việc sử dụng mạng bị quản lý để hỗ trợ các nhu cầu thông tin liên lạc quản lý (quản lý trong băng) đã gây ra nhiều vấn đề thú vị. Việc quản lý trong băng và ngoài băng là hoàn toàn trực giao với việc lựa chọn giao thức quản lý. Quản lý trong băng có thể dẫn đến tình trạng mất liên lạc với một tác nhân đúng lúc tác nhân đó cần sự chú ý về quản lý (tùy thuộc vào nguồn của sự cố). Người ta có thể làm giảm nhẹ được vấn đề này nếu chính các thực thể mà tác nhân quản lý lại bảo vệ đường truy nhập tới các tác nhân này.

Có một ảnh hưởng nhỏ về khả năng quản lý xuất hiện trong bối cảnh đánh địa chỉ tầng vận chuyển. Ví dụ: có thể xác định được tác nhân SNMP một cách duy nhất bằng địa chỉ IP và số cổng UDP. Điều này có nghĩa là với một địa chỉ IP cho trước thì ta chỉ có thể tiếp cận được một tác nhân duy nhất. Hơn thế nữa, tác nhân này lại chỉ duy trì một cơ sở thông tin quản lý MIB duy nhất. Do vậy, với một địa chỉ IP duy nhất chỉ tồn tại một MIB. Việc gắn kết MIB với địa chỉ IP có thể hạn chế được độ phức tạp của biến số liệu mà tác nhân cung cấp. Xem xét trong cùng một hoàn cảnh trong đó hệ thống yêu cầu nhiều MIB để quản lý các thành phần khác nhau của nó. Cần phải thống nhất các MIB khác nhau này dưới một cây MIB tĩnh duy nhất để có thể truy nhập chúng thông qua một tác nhân duy nhất. Trong một số hoàn cảnh nhất định, việc thống nhất đó không thể thực hiện được. Trong những trường hợp như vậy, mỗi MIB đòi hỏi phải có riêng một nhóm giao thức SNMP/UDP/IP. Điều này dẫn tới sự phức tạp cao trong việc tổ chức quản lý (các thông tin tương quan từ nhiều MIB thuộc một hệ thống cho trước) cũng như việc truy nhập nó (thông qua nhiều địa chỉ IP).

Có một cách khác là một tác nhân duy nhất trong một hệ thống có thể giữ vai trò như một proxy mở rộng cho các tác nhân phụ đóng gói những MIB khác nhau cùng liên quan tới một phân hệ cho trước. Các phiên bản mở rộng SNMPv2 hỗ trợ phương pháp này để xử lý nhu cầu truyền thông của nhà quản lý. Các phiên bản mở rộng này cho phép tác nhân đóng vai trò như một nhà quản lý của các tác nhân con tại chỗ, do vậy cho phép tiếp cận hàng loạt các tác nhân con.

3.3 CẤU TRÚC VÀ ĐẶC ĐIỂM CỦA THÔNG TIN QUẢN LÝ

SMI định nghĩa một cơ cấu tổ chức chung cho thông tin quản lý. SMI nhận dạng các kiểu dữ liệu trong MIB và chỉ rõ cách thức miêu tả và đặt tên các tài nguyên trong MIB. SMI duy trì tính đơn giản và khả năng mở rộng trong MIB. Vì thế MIB chỉ lưu những loại dữ liệu đơn giản: các đối tượng vô hướng và các mảng hai chiều của các đối tượng vô hướng. SNMP chỉ có thể truy lục các vô hướng, gồm các thực thể trong bảng. SMI không cung cấp cách tạo hoặc truy xuất các cấu trúc dữ liệu phức tạp. Các MIB sẽ chứa các loại dữ liệu do nhà cung cấp tạo ra.

Để cung cấp phương pháp tiêu chuẩn biểu diễn thông tin quản trị, SMI cần làm những công việc sau:

- Cung cấp kỹ thuật tiêu chuẩn để định nghĩa cấu trúc của MIB đặc biệt.
- Cung cấp kỹ thuật tiêu chuẩn để định nghĩa các đối tượng đơn lẻ, bao gồm cú pháp và giá trị của mỗi đối tượng.
- Cung cấp kỹ thuật tiêu chuẩn để mã hoá các giá trị đối tượng.

Sự mô tả các đối tượng bị quản lý được SMI thực hiện thông qua ngôn ngữ mô tả ASN.1. Việc định nghĩa loại đối tượng gồm 5 trường:

- **Object:** Tên của đối tượng, còn được coi như là phần mô tả đối tượng cho mỗi loại đối tượng cùng với phần nhận dạng đối tượng tương ứng của đối tượng.
- **Syntax:** Cú pháp cho loại đối tượng. Đó có thể là một trong các loại cú pháp đơn giản như: Integer, Octet String, Object Identifier, Null hay một cú pháp ứng dụng như: Địa chỉ mạng, bộ đếm, kiểu Gauss, Time Ticks, dạng dữ liệu không trong suốt, hay các loại dữ liệu ứng dụng mở rộng (có thể xem thêm trong RFC 1155 để biết thêm chi tiết).
- **Definition:** Các định nghĩa mô tả ngữ nghĩa của loại đối tượng.
- **Truy nhập (Access):** Phương pháp truy nhập có thể là: chỉ đọc, đọc-ghi hay không thể truy nhập.
- **Trạng thái (Status):** Có thể là cưỡng chế, tùy chọn hay không còn hiệu lực.

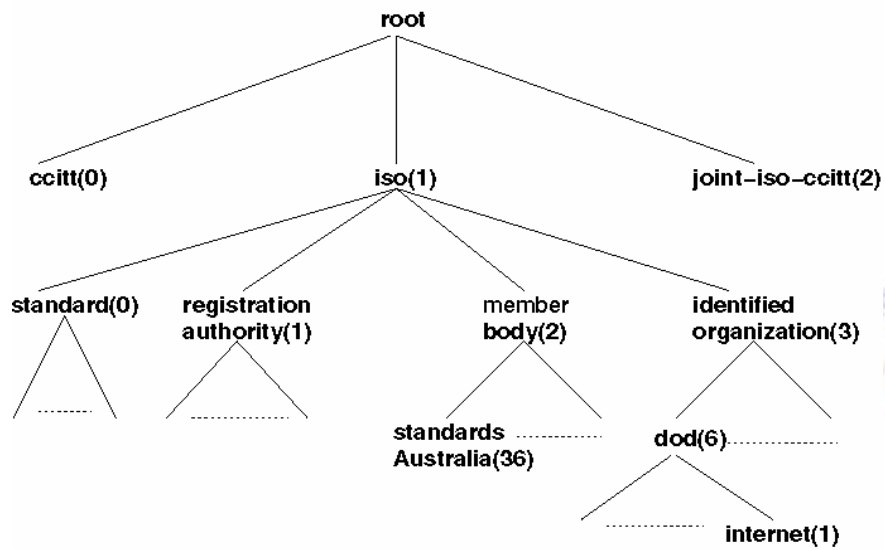
3.4 CƠ SỞ THÔNG TIN QUẢN LÝ (MIB)

3.4.1 Cấu trúc của MIB

Các đối tượng quản lý trong môi trường SNMP được sắp xếp theo cấu trúc hình cây có thứ bậc. Các đối tượng lá của cây là đối tượng quản lý thực, mỗi thành phần trong đó biểu thị cho tài nguyên, sự hoạt động hoặc các thông tin liên quan được quản lý. SNMP tận dụng cây đăng ký của OSI như là một thư mục thông tin bị quản lý. Các cây con được sử dụng để biểu thị nội dung logic, còn các biên số bị quản lý được lưu trữ tại các lá cây. Người ta sử dụng các biên số này để biểu diễn các thời điểm của thực thể tương ứng. Cấu trúc cây cơ sở dữ liệu này được các nhà thiết kế MIB định ra theo kiểu tĩnh. Chỉ có sự thay đổi mở rộng trong các giá trị của cơ sở dữ liệu và trong việc tạo ra hay xóa đi các hàng của bảng. Như minh họa tại Hình 3.2, người ta sử dụng cây đăng ký để đánh dấu các định nghĩa của các tiêu chuẩn khác nhau. Mỗi nút thuộc cây được đánh dấu bằng một tên (đặc điểm nhận dạng chung) và một con số (đặc điểm nhận dạng tương đối). Một nút được xác định duy nhất bằng cách nối các số từ gốc đến nút đó. Ví dụ: một cây con có nhãn Internet được xác định bằng đường 1.3.6.1. Cây con này được đặt trong tổ chức Internet để ghi lại các tiêu chuẩn của nó. Cây Internet có ba cây con liên quan đến quản lý, đó là quản lý (management), thực nghiệm (experimental) và cá nhân (private). Các cây con này được sử dụng để ghi lại các MIB khác nhau theo tiêu chuẩn Internet (MIB-II).

Mỗi dạng đối tượng liên kết trong một MIB là một nhận diện của kiểu ASN.1 OBJECT IDENTIFIER. Việc nhận dạng phục vụ cho việc đặt tên của đối tượng và cũng phục vụ cho việc nhận diện cấu trúc của các dạng đối tượng. Nhận diện đối tượng là một nhận diện duy nhất đối với một loạt đối tượng cụ thể. Giá trị của nó bao gồm một dãy các số nguyên. Tập các đối tượng đã định nghĩa có cấu trúc hình cây với gốc của cây là đối tượng dựa vào chuẩn ASN.1. Hiện tại, hai phiên bản của MIB đã được phát triển là MIB-I và MIB-II. Trong đó MIB-II là sự mở rộng của MIB-I.

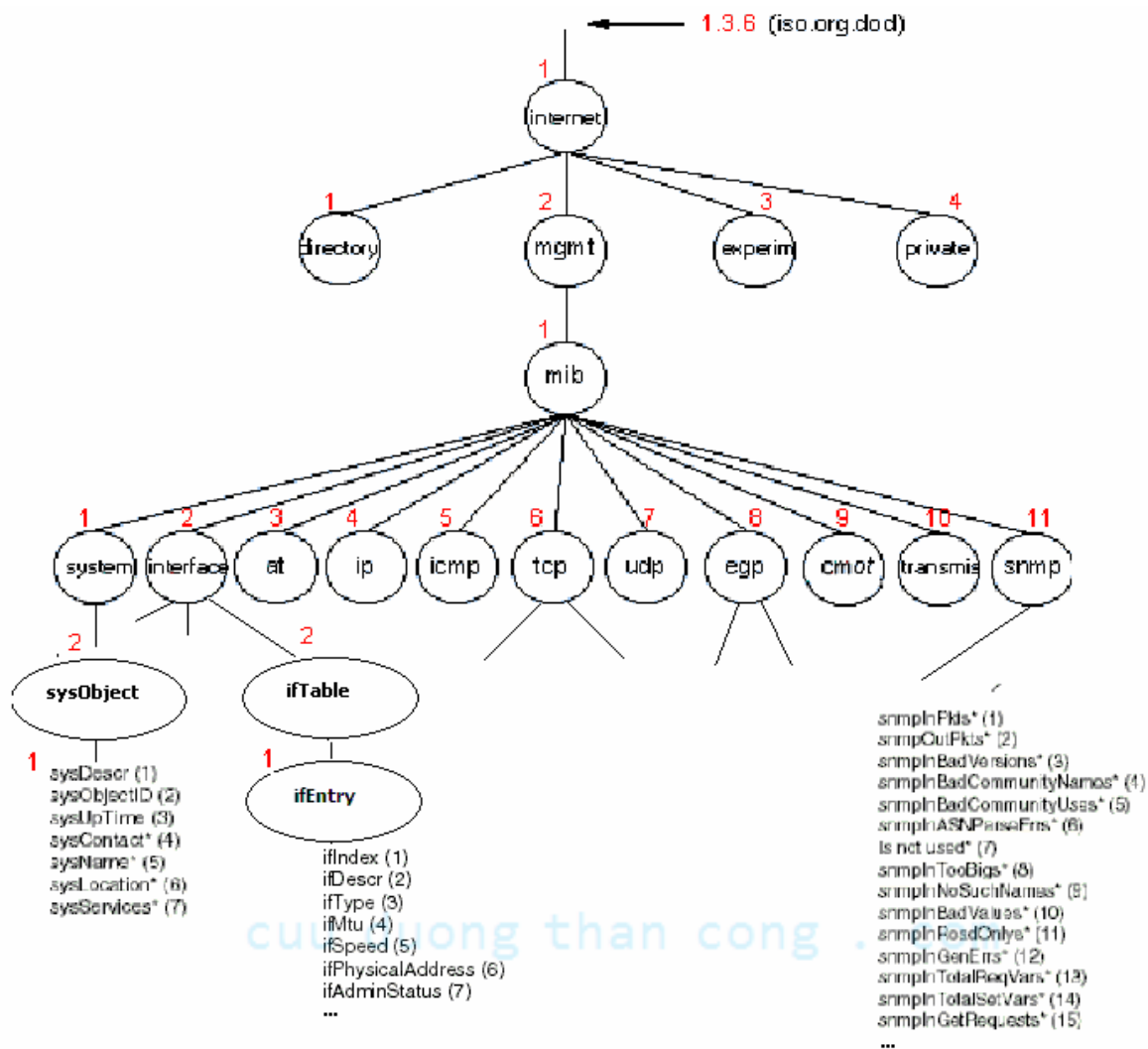
- Năm 1990, MIB-I được công bố theo RFC 1156, MIB-I phân tách đối tượng quản trị thành tám nhóm là: System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, và EGP.
- Năm 1991, MIB-II được đưa ra theo RFC 1213, MIB-II là siêu tập của MIB-I, được bổ sung một vài đối tượng và nhóm. MIB-II phân tách đối tượng quản trị thành 10 nhóm.



Hình 3.2: Cây đăng ký của OSI

Hình 3.3 minh họa tổ chức của cây MIB-II Internet. Mục tiêu của MIB này là cung cấp các biến số bị quản lý để xử lý nhóm giao thức Internet (IP, UDP, TCP, ICMP). Người ta chia MIB-II thành 11 cây chức năng con. Mỗi cây con đại diện cho một nhóm biến số liên quan trực tiếp đến thực thể bị quản lý (thực thể giao thức IP hoặc TCP). Các cây này lại tiếp tục được chia ra thành các cây con dưới nữa. Tại đáy của cây là lá, lá được sử dụng để đánh dấu các biến số bị quản lý thuộc một loại nhất định. Một số lá (như sysDesc mô tả hệ thống) chỉ đánh dấu một thời điểm duy nhất của biến số bị quản lý và chỉ đòi hỏi một tế bào lưu trữ duy nhất. Những lá khác (như tcpConnState mô tả trạng thái một đường kết nối TCP) có thể chỉ dẫn nhiều thời điểm khác nhau. Các thời điểm khác nhau này được tổ chức thành các cột của tế bào. Các cột này tạo thành một bảng mà các hàng của bảng này biểu diễn những thời điểm khác nhau của một thực thể (như một đường kết nối TCP hoặc một giao diện).





Hình 3.3: Cây MIB-II Internet

Việc đánh chỉ dẫn truy nhập đối với các thời điểm là một vấn đề đơn giản. Tế bào liên quan tới lá như vậy được coi là con của lá và được đánh nhãn là O. Ví dụ, biến số bị quản lý chứa số nhận dạng vật thể của hệ thống (tế bào ở bên dưới sysObject) được xác định bởi 1.3.6.2.1.1.2.0. Điều này có nghĩa là đường tới sysObject liên kết với O. Tuy nhiên các số liệu được xếp thành bảng lại đòi hỏi một cơ chế chỉ dẫn phức tạp hơn, bởi vì ta cần phải xác định mỗi hàng trong bảng một cách duy nhất (một thời điểm của thực thể).

3.4.2 Truy nhập MIB

Có thể nhìn nhận MIB như một ngôn ngữ đòi hỏi với cây MIB. Chương trình quản lý sử dụng các đơn nguyên GET, GET-NEXT để truy xuất dữ liệu từ MIB. Đá lại hai đơn nguyên này là GET-RESPONSE trả lại dữ liệu dưới dạng đôi biến số. Ta có thể sử dụng cả hai đơn nguyên để truy xuất nhiều biến số bị quản lý.

Lệnh GET trực tiếp chỉ ra tập hợp các biến số bị quản lý thông qua đặc điểm nhận dạng đường dẫn của chúng. Điều này rất hữu ích cho việc truy xuất dữ liệu dạng thông thường (không theo dạng bảng) bởi vì đường truy nhập là tĩnh và biết trước.

GET-NEXT được sử dụng để đi lại trên cây và áp dụng cho số liệu dạng bảng. Ta có thể tự truy xuất số liệu bằng cách đi lại trên cây MIB. Theo quy định của thứ tự này thì hệ thống truy xuất số liệu tại nút mẹ trước rồi mới đến nút con từ trái qua phải. Trong bảng, các cột được đánh

thứ tự từ trái qua phải và các hàng có thứ tự từ trên xuống dưới. Thứ tự này được gọi là thứ tự tiền tố (preorder).

GET và GET-NEXT cho ta phương tiện để truy xuất dữ liệu MIB. Bằng đơn nguyên SET ta có thể điều khiển được ứng xử của thiết bị. SET thường được sử dụng để khởi tạo hành động của tác nhân làm hiệu ứng bổ sung đối với những thay đổi của MIB. Ví dụ: ta có thể khởi động một thủ tục kiểm tra chuẩn đoán bằng cách đặt trạng thái hành chính của thiết bị (thông qua SET) là thử nghiệm. Điều này có nghĩa là các tác nhân phải chủ động giám sát những thay đổi của MIB và khởi tạo các hành động cần thiết. Điều này không giống với các hệ thống cơ sở dữ liệu thụ động mà ở đó sự cập nhật số liệu chỉ đơn thuần là việc ghi lại số liệu. Có một nhược điểm của việc truy xuất số liệu bằng lệnh GET-NEXT trong SNMP, đó là hệ thống cần phải truy nhập một hàng tại một thời điểm. Điều này có thể làm chậm quá trình đi lại trên cây, đặc biệt trong trường hợp bảng có kích thước lớn. Thường thì hệ thống phải quét và truy cập toàn bộ bảng. Để khắc phục nhược điểm này, trong phiên bản thứ hai SNMPv2 người ta đã thay lệnh GET-NEXT bằng lệnh GET-BULK. Lệnh GET-BULK đã truy cập một số hàng liên tục vừa vào một khung UDP. Ta có thể nhìn nhận việc này như là việc tổng quan hóa lệnh GET-NEXT để cải thiện thời gian truy cập đối với dữ liệu dạng bảng.

3.4.3 Nội dung của MIB

Cấu trúc thông tin quản lý (SMI) cho ta một mô hình đơn giản về số liệu bị quản lý. Mô hình này được định nghĩa bằng ngôn ngữ mô phỏng cú pháp dữ liệu ASN.1. SMI mô phỏng sáu loại dữ liệu, đó là bộ đếm, kiểu (gauge), tích tắc thời gian, địa chỉ mạng, địa chỉ IP và số liệu đếm không trong suốt (opaque). Bộ đếm được sử dụng để diễn đạt sự lấy mẫu tích tụ của chuỗi thời gian. Kiểu (gauge) diễn đạt các mẫu của chuỗi thời gian, tích tắc thời gian được sử dụng để đo thời gian tương đối, còn loại số liệu không trong suốt thì được sử dụng để mô tả một chuỗi bit bất kỳ. Người ta cũng sử dụng các loại dữ liệu cơ sở chung như số nguyên chuỗi octet, đặc điểm nhận dạng vật thể xác định số liệu bị quản lý. Việc giới hạn các loại dữ liệu trong SMI và hạn chế quy mô của các hạng mục số liệu trong MIB đã làm giảm nhiều độ phức tạp của việc tổ chức lưu trữ, mã hóa, giải mã số liệu. Trong môi trường tác nhân có nguồn tài nguyên hạn chế thì sự đơn giản hóa và việc điều khiển nguồn tài nguyên hạn chế giữ một vai trò trung tâm trong việc thiết kế SNMP.

SMI cũng bao gồm một MACRO mở rộng đặc biệt của ASN.1 là OBJECT-TYPE. Macro này phục vụ như một công cụ chính để xác định các vật thể bị quản lý tại lá của cây MIB. Macro OBJECT-TYPE cho ta phương tiện để định nghĩa biến số bị quản lý và gán cho nó một loại dữ liệu, một phương pháp truy nhập (đọc, viết, đọc/viết), một trạng thái (bắt buộc, tùy ý) và một vị trí cây MIB tĩnh (đặc điểm nhận dạng đường). Định nghĩa của Macro OBJECT-TYPE và của các biến số bị quản lý được trình bày trong bảng với phần thứ nhất của định nghĩa MIB cho ta các đặc tính nhận dạng đường này đối với các mode bên trong của cây MIB và được gán vào nhiều loại dữ liệu nhận dạng vật thể. Ta có thể xác định đặc điểm nhận dạng của một nút bằng cách buộc một con số với đặc điểm nhận dạng nút mẹ của nó. Khi các nút bên trong đã được xác định, bằng Macro OBJECT-TYPE hệ thống có thể tạo ra các nút tại lá cây. Các nút tại lá cây này xác định loại dữ liệu (cú pháp) của các biến số bị quản lý mà chúng lưu trữ. Các nút lá cây cũng điều khiển việc truy nhập, xác định trạng thái và đường đặc điểm nhận dạng vật thể để truy nhập biến số bị quản lý.

Dưới đây là một số điểm hữu ích cần lưu ý về các định nghĩa này và cách sử dụng chúng:

1. Các đặc điểm nhận dạng vật thể xác định vị trí của các nút bên trong (như “system”,

“interface”) hoặc lá trên cây MIB (sysDescr, ifInError). Ta có thể tạo ra đặc điểm nhận dạng đường bằng cách ghép đường mẹ với nhánh của nút (ví dụ sysDescr={system 1}).

2. Các bảng được tạo nên dưới dạng chuỗi của các hàng. Các hàng xác định ra các cột của bảng. Ví dụ: bảng tạo giao diện được thiết lập từ các cột được dành riêng cho các tham số giao diện khác nhau (ifSpeed, ifInError). Các tham số cột khác nhau này được đăng ký như lá dưới cây con ifEntry mô tả trong bảng.
3. Các định nghĩa cấu trúc MIB chỉ đơn giản cho ta một cấu trúc về cú pháp. Tiếng Anh được sử dụng để giải nghĩa cho các biến số khác nhau này. Hai phiên bản triển khai thực hiện MIB khác nhau có thể diễn giải nghĩa của một số biến khác nhau. Đôi khi ta không thể đảm bảo việc tuân thủ các ngữ nghĩa.
4. Hệ thống có thể sử dụng các định nghĩa chính thức của MIB để tạo ra MIB và cấu trúc truy nhập chúng. Bộ biên dịch sử dụng các định nghĩa này để tạo ra cấu trúc cơ sở dữ liệu cho việc lưu trữ MIB. Điều này làm đơn giản hóa quá trình phát triển MIB.
5. Việc triển khai thực hiện MIB là rõ ràng. Ta có thể lưu trữ các số liệu không phải dạng bảng trong cấu trúc dữ liệu tuyến tính cố định. Hệ thống cần tạo khả năng cho số liệu dạng bảng thu nhỏ hoặc mở rộng khi các hàng của bảng bị xóa đi hay được bổ sung. Ta có thể dùng cấu trúc của một danh sách liên kết hoặc cây để biểu diễn các số liệu động như vậy (các bản ghi của bảng được lưu trữ tại lá cây).

Chúng ta cần nhìn nhận cấu trúc MIB theo các hệ thống cơ sở dữ liệu truyền thống. Người ta có thể sử dụng ngôn ngữ xử lý dữ liệu (DML) để tạo ra hệ thống cơ sở dữ liệu và mô tả cấu trúc của cơ sở dữ liệu. Ta có thể coi mô hình SMI hoặc các phiên bản mở rộng của ASN.1 như là ngôn ngữ DML để xây dựng MIB. Bộ biên dịch MIB cũng tương tự như bộ biên dịch DL, được sử dụng để tạo ra cấu trúc cơ sở dữ liệu từ một chương trình trừu tượng. Ta cũng có thể coi các đơn nguyên truy nhập giao thức như ngôn ngữ xử lý dữ liệu DML. Nhìn trên quan điểm hệ thống cơ sở dữ liệu truyền thống thì ta có thể coi SNMP như là một hệ thống cơ sở dữ liệu thứ bậc đơn giản mà bản chất của nó do các ngôn ngữ DL (SMI) và DML xác định (các đơn nguyên giao thức).

3.4.4 Các đối tượng của MIB-II

Như đã giới thiệu trong Phần 3.4.1, MIB-II được đưa ra theo RFC 1213. MIB-II phân tách đối tượng quản trị thành 10 nhóm (trong 11 nhóm đưa ra trong bảng 3.3, nhóm số 9 mang tính chất lịch sử).

Bảng 3.3: Các nhóm đối tượng trong MIB-II

Nhóm	Đường đi	Vai trò
System Group	{1.3.6.1.2.1.1}	Nhóm hệ thống mô tả tổng quan về hệ thống bị quản lý dưới dạng văn bản ký tự ASCII. Bao gồm OID, độ dài thời gian từ thời điểm tái khởi động thực thể quản lý mạng và những chi tiết quản trị khác.
Interface Group	{1.3.6.1.2.1.2}	Nhóm giao diện: Dữ liệu giao diện phần cứng trên thiết bị chịu sự quản lý khi khai thác động và tĩnh. Thông tin này

		được trình bày dưới dạng bảng. Đối tượng đầu tiên (ifNumber) chỉ số giao diện trên thiết bị. Mỗi giao diện sẽ có một dòng tương ứng trong bảng với 22 cột/dòng. Các cột mang thông tin về giao diện như: tốc độ giao diện, địa chỉ (phần cứng) vật lý, trạng thái vận hành hiện thời và thống kê về gói.
Address Translation Group	{1.3.6.1.2.1.3}	Nhóm phiên dịch địa chỉ gồm bản đồ địa chỉ IP và địa chỉ thuần vật lý (có trong MIB-I nhưng bị phản đối trong MIB-II). “Phản đối” nghĩa là MIB-II vẫn có nhóm này để tương thích với MIB-I, song có lẽ sẽ bị loại trừ trong những phiên bản sau. Nhóm phiên dịch địa chỉ cung cấp một bảng để phiên dịch giữa địa chỉ IP và địa chỉ (phần cứng) vật lý. Trong MIB-II và những phiên bản sau, mỗi nhóm giao thức sẽ chứa bảng phiên dịch riêng của nó. Nó chứa một bảng với mỗi dòng gồm 3 cột.
IP Group	{1.3.6.1.2.1.4}	Nhóm giao thức Internet này là bắt buộc với tất cả các nút và cung cấp thông tin trên các máy trạm và router sử dụng IP. Nhóm này chứa một con số của các đối tượng vô hướng cung cấp số liệu thống kê dữ liệu đồ liên quan tới IP và ba bảng sau: bảng địa chỉ (ipAddrTable), bảng phiên dịch địa chỉ IP sang địa chỉ vật lý (ipNetToMediaTable) và bảng hướng đi IP (ipForwardTable). RFC 1354 đã định nghĩa ipForwardTable, thay thế ipRoutingTable trong MIB-II.
ICMP Group	{1.3.6.1.2.1.5}	Nhóm giao thức bản tin điều khiển Internet là thành phần bắt buộc của IP và được định nghĩa trong RFC 792. Nhóm ICMP cung cấp các bản tin điều khiển nội mạng và thực hiện nhiều vận hành ICMP trong thực thể bị quản lí. Nhóm ICMP gồm 26 đối tượng vô hướng duy trì số liệu thống kê cho nhiều loại bản tin ICMP như số lượng các bản tin ICMP Echo Request nhận được hay số lượng bản tin ICMP Redirect đã gửi đi.
TCP Group	{1.3.6.1.2.1.6}	Nhóm giao thức điều khiển truyền tải là bắt buộc và cung cấp thông tin liên quan tới vận hành và kết nối TCP. Nhóm này có 14 đối tượng vô hướng và một bảng. Những đối tượng vô hướng này ghi lại các tham số TCP và số liệu thống kê, như số lượng kết nối TCP mà thiết bị hỗ trợ, hoặc tổng số lượng phân đoạn (segment) TCP đã truyền. Bảng tcpConnTable chứa thông tin liên quan tới kết nối TCP cụ thể.
UDP Group	{1.3.6.1.2.1.7}	Nhóm giao thức dữ liệu đồ người sử dụng là bắt buộc và cung cấp thông tin liên quan tới hoạt động UDP. Vì UDP là kết nối vô hướng nên nhóm này nhỏ hơn nhiều so với nhóm TCP có hướng. Nó không phải biên dịch thông tin của những nỗ lực kết nối, thiết lập, tái lập ... Nhóm UDP chứa bốn đối tượng vô hướng và một bảng. Những đối tượng vô hướng này duy

		trì thông kê dữ liệu đồ liên quan tới UDP, ví dụ: số lượng dữ liệu đồ gửi từ thực thể này. Bảng udpTable chứa thông tin địa chỉ và cổng.
EGP Group	{1.3.6.1.2.1.8}	Nhóm giao thức cổng ngoài là bắt buộc với mọi hệ thống có triển khai EGP. EGP truyền đạt thông tin giữa các hệ thống tự trị (autonomous systems), và được mô tả chi tiết trong RFC 904. Nhóm EGP gồm 5 đối tượng vô hướng và một bảng. Những đối tượng vô hướng này duy trì những thông kê bản tin liên quan tới EGP. Bảng egpNeighTable chứa thông tin EGP lân cận.
CMOT (OIM) Group	{1.3.6.1.2.1.9}	Trong quá trình phát triển của Khung công việc quản lý mạng Internet (Internet Network Management Framework), có lúc đã cố gắng sử dụng SNMP làm một bước chuyển tiếp trong hoàn cảnh thúc bách có chuẩn quản lý mạng, và để tạo Giao thức thông tin quản lý chung (CMIP) trên nền TCP/IP (CMOT) giải pháp dài hạn OSIcompliant. Kết quả là, nhóm CMOT được đặt trong MIB-II. Tuy nhiên, kinh nghiệm cho thấy là SNMP không phải là giải pháp chuyển tiếp, và giao thức quản lý mạng liên quan tới OSI chỉ yêu cầu các MIB. Vì vậy, không chắc chắn là bạn sẽ gặp nhóm OIM trong bất kỳ thiết bị quản lý hoặc agent SNMP thương mại nào trên thị trường. Tuy nhiên, nhóm CMOT đã được giữ chỗ {1.3.6.1.2.1.9} trong MIB-II. RFC 1214 chi tiết hóa cây con này, đặc tả OSI Internet Management (OIM) MIB. Hiện tại, RFC 1214 được xếp loại là giao thức “lịch sử”.
Transmission Group	{1.3.6.1.2.1.10}	Nhóm truyền dẫn chứa các đối tượng liên quan đến việc truyền dẫn dữ liệu. RFC 1213 không định nghĩa những đối tượng này rõ ràng. Tuy nhiên, tài liệu này cho biết là những đối tượng truyền dẫn này sẽ nằm trong cây con thực nghiệm {1.3.6.1.3} cho tới khi chúng được “chứng minh”.
SNMP Group	{1.3.6.1.2.1.11}	Nhóm SNMP cung cấp thông tin về các đối tượng SNMP. Có tổng cộng 30 đối tượng vô hướng trong nhóm này, bao gồm những thông kê bản tin SNMP, số lượng đối tượng MIB khôi phục (retrieved) và số lượng bẫy SNMP đã gửi.

Mỗi nhóm mô tả một cách tổng quan về thuộc tính đối tượng. Bảng 3.4 cho ta nội dung chi tiết về nhóm hệ thống.

Bảng 3.4: Nhóm hệ thống trong MIB-II

Cây con nhóm hệ thống 1.2.1.1.2	Nội dung	
sysDescr	(1)	Mô tả văn bản của một hệ thống bị quản lý
sysObjectID	(2)	Nhận dạng nhà chế tạo của hệ thống dưới dạng cây con MIB thuê riêng

sysUpTime	(3)	Thời gian theo thang 1/100 giây tính từ khi bắt đầu quản lý mạng của hệ thống
sysContact	(4)	Thông tin về tên và truy nhập của người chịu trách nhiệm
sysName	(5)	Tên hệ thống
sysLocation	(6)	Vị trí hệ thống
sysServices	(7)	Các dịch vụ hệ thống

3.5 ĐIỀU HÀNH SNMP

3.5.1 Các thành phần của SNMP

Hệ thống quản lý mạng dựa trên SNMP gồm ba thành phần: bộ phận quản lý (manager), đại lý (agent) và cơ sở dữ liệu gọi là Cơ sở thông tin quản lý (MIB). Mặc dù SNMP là một giao thức quản lý việc chuyển giao thông tin giữa ba thực thể trên, song nó cũng định nghĩa mối quan hệ client-server (chủ tớ). Ở đây, những chương trình client là bộ phận quản lý, trong khi client thực hiện ở các thiết bị từ xa có thể được coi là server. Khi đó, cơ sở dữ liệu do agent SNMP quản lý là đại diện cho MIB của SNMP. Hình 3.4 minh họa mối quan hệ giữa ba thành phần SNMP này.

3.5.1.1 Bộ phận quản lý (manager)

Bộ phận quản lý là một chương trình vận hành trên một hoặc nhiều máy tính trạm. Tùy thuộc vào cấu hình, mỗi bộ phận quản lý có thể được dùng để quản lý một mạng con, hoặc nhiều bộ phận quản lý có thể được dùng để quản lý cùng một mạng con hay một mạng chung. Tương tác thực sự giữa một người sử dụng cuối (end-user) và bộ phận quản lý được duy trì qua việc sử dụng một hoặc nhiều chương trình ứng dụng mà, cùng với bộ phận quản lý, biến mặt bằng phần cứng thành Trạm quản lý mạng (NMS). Ngày nay, trong thời kỳ các chương trình giao diện người sử dụng đồ họa (GUI), hầu hết những chương trình ứng dụng cung cấp môi trường cửa sổ chỉ và click chuột, thực hiện liên vận hành với bộ phận quản lý để tạo ra những bản đồ họa và biểu đồ cung cấp những tổng kết hoạt động của mạng dưới dạng thấy được.

Qua bộ phận quản lý, những yêu cầu được chuyển tới một hoặc nhiều thiết bị chịu sự quản lý. Ban đầu SNMP được phát triển để sử dụng trên mạng TCP/IP và những mạng này tiếp tục làm mạng vận chuyển cho phần lớn các sản phẩm quản lý mạng dựa trên SNMP. Tuy nhiên SNMP cũng có thể được chuyển qua NetWare IPX và những cơ cấu vận chuyển khác.

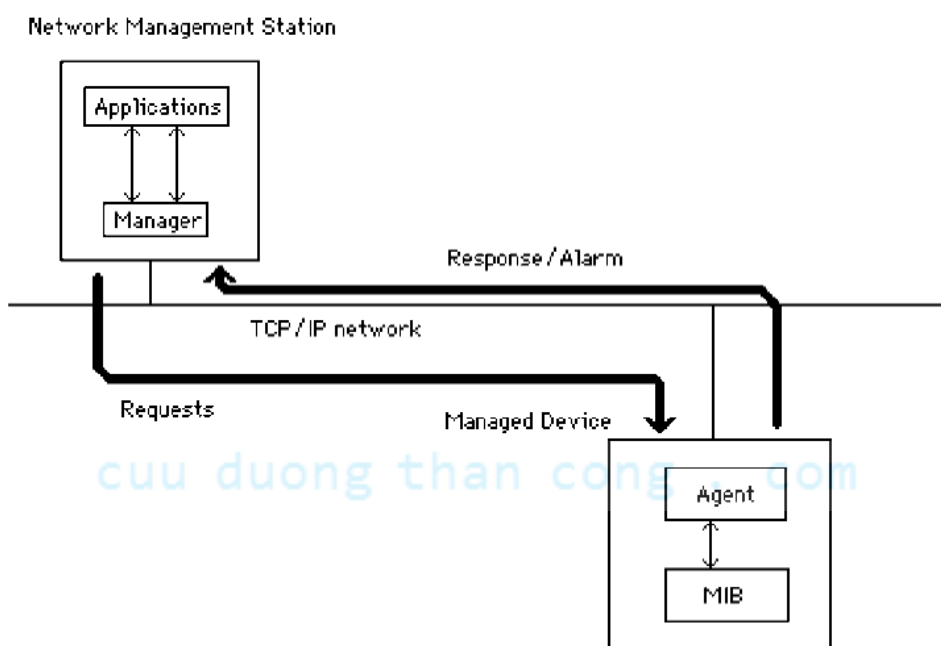
3.5.1.2 Agent

Thiết bị chịu sự quản lý (Managed device): Là một nút mạng hỗ trợ giao thức SNMP và thuộc về mạng bị quản lý. Thiết bị có nhiệm vụ thu thập thông tin quản lý và lưu trữ để phục vụ cho hệ thống quản lý mạng. Những thiết bị chịu sự quản lý, đôi khi được gọi những phần tử mạng, có thể là những bộ định tuyến và máy chủ truy nhập-Access Server, những switch và những bridge, những hub, máy tính hay là những máy in trong mạng.

Mỗi thiết bị chịu sự quản lý bao gồm phần mềm hoặc phần sụn (firmware) dưới dạng mã phiên dịch những yêu cầu SNMP và đáp ứng của những yêu cầu đó. Phần mềm hoặc phần sụn này được coi là một agent. Mặc dù mỗi thiết bị bắt buộc bao gồm một agent chịu quản lý trực tiếp,

những thiết bị tương thích không theo SNMP cũng có thể quản lý được nếu như chúng hỗ trợ một giao thức quản lý độc quyền. Để thực hiện được điều này, bạn phải giành được một agent ủy nhiệm (proxy agent). Proxy agent này có thể được xét như một bộ chuyển đổi giao thức vì nó phiên dịch những yêu cầu SNMP thành giao thức quản lý độc quyền của thiết bị không hoạt động theo giao thức SNMP.

Mặc dù SNMP chủ yếu là giao thức đáp ứng thăm dò (poll-respond) với những yêu cầu do bộ phận quản lý tạo ra dẫn đến những đáp ứng trong agent, agent cũng có khả năng đề xướng ra một “đáp ứng tự nguyện”. Đáp ứng tự nguyện này là điều kiện cảnh báo từ việc giám sát agent với hoạt động đã được định nghĩa trước và chỉ ra rằng đã tới ngưỡng định trước. Dưới sự điều khiển SNMP, việc truyền cảnh báo này được coi là cái bẫy (trap).



Hình 3.4: Mối quan hệ giữa các thành phần SNMP.

3.5.1.3 Cơ sở thông tin quản lý - MIB

Mỗi thiết bị chịu sự quản lý có thể có cấu hình, trạng thái và thông tin thống kê rất đa dạng, định nghĩa chức năng và khả năng vận hành của thiết bị. Thông tin này có thể bao gồm việc thiết lập chuyển mạch phần cứng, những giá trị khác nhau lưu trữ trong các bảng ghi nhớ dữ liệu, bộ hồ sơ hoặc các trường thông tin trong hồ sơ lưu trữ ở các file và những biến hoặc thành phần dữ liệu tương tự. Nhìn chung, những thành phần dữ liệu này được coi là Cơ sở thông tin quản lý của thiết bị chịu sự quản lý. Xét riêng, mỗi thành phần dữ liệu biến đổi được coi là một đối tượng bị quản lý và bao gồm tên, một hoặc nhiều thuộc tính, và một tập các hoạt động (operation) thực hiện trên đối tượng đó. Vì vậy MIB định nghĩa loại thông tin có thể khôi phục từ một thiết bị chịu sự quản lý và những bố trí (settings) thiết bị mà bạn có thể điều khiển từ hệ thống quản lý.

3.5.2 Các lệnh cơ bản trong SNMP

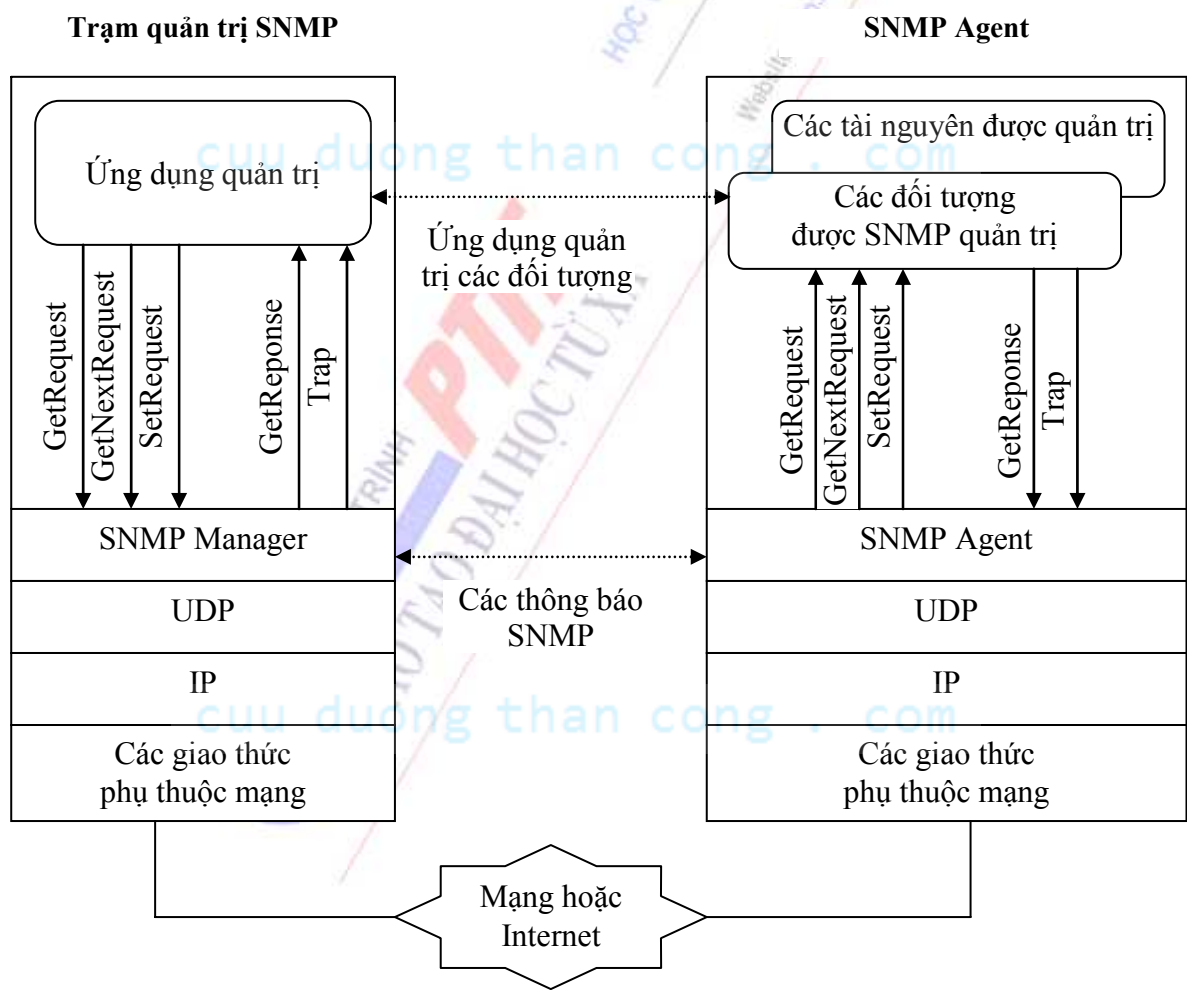
SNMP sử dụng các dịch vụ chuyển tải dữ liệu được cung cấp bởi các giao thức UDP/IP. Một ứng dụng của Manager phải nhận dạng được Agent cần thông tin với nó. Một ứng dụng của Agent được nhận dạng bởi địa chỉ IP của nó và một cổng UDP. Một ứng dụng Manager đóng gói yêu cầu SNMP trong một UDP/IP, UDP/IP chứa mã nhận dạng cổng nguồn, địa chỉ IP đích và mã 62

nhận dạng cổng UDP của nó. Khung UDP sẽ được gửi đi thông qua thực thể IP tới hệ thống được quản lý, tại đó khung UDP sẽ được phân phối bởi thực thể UDP tới Agent. Tương tự các bản tin TRAP phải được nhận dạng bởi các Manager. Các bản tin sử dụng địa chỉ IP và mã nhận dạng cổng UDP của Manager SNMP.

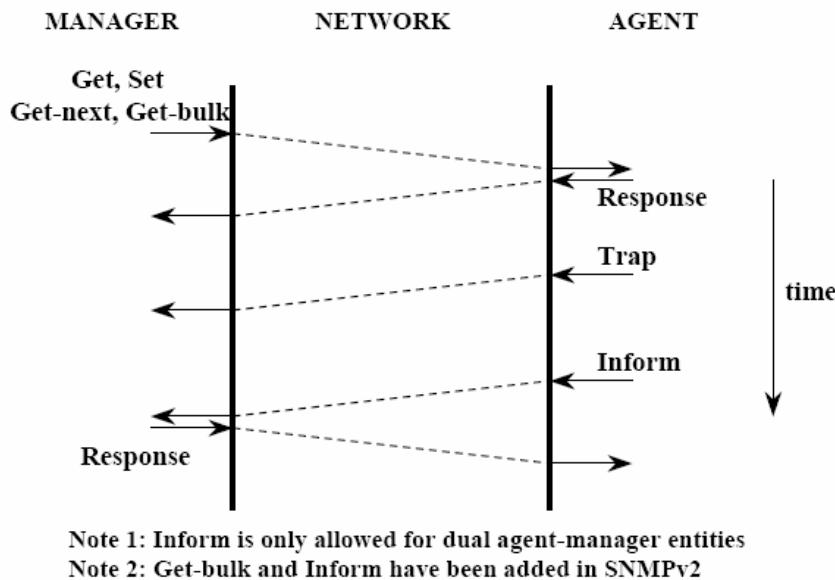
SNMP sử dụng 3 lệnh cơ bản là Read, Write, Trap và một số lệnh tùy biến để quản lý thiết bị.

- *Lệnh Read:* Được SNMP dùng để đọc thông tin từ thiết bị. Các thông tin này được cung cấp qua các biến SNMP lưu trữ trên thiết bị và được cập nhật bởi thiết bị.
- *Lệnh Write:* Được SNMP dùng để ghi các thông tin điều khiển lên thiết bị bằng cách thay đổi giá trị các biến SNMP.
- *Lệnh Trap:* Dùng để nhận các sự kiện gửi từ thiết bị đến SNMP. Mỗi khi có một sự kiện xảy ra trên thiết bị một lệnh Trap sẽ được gửi tới NMS.

SNMP điều khiển, theo dõi thiết bị bằng cách thay đổi hoặc thu thập thông tin qua các biến giá trị lưu trên thiết bị. Các Agent cài đặt trên thiết bị tương tác với những chip điều khiển hỗ trợ SNMP để lấy nội dung hoặc viết lại nội dung (hình 3.5).



Hình 3. 5: Mô hình giao thức hoạt động SNMP



Hình 3.6: Hoạt động giao thức SNMP

3.6 SNMPv2

3.6.1 Các thực thể của SNMPv2

Trong SNMPv2 đã có một số thay đổi sau so với SNMPv1 đó là :

- Thay đổi trong cấu trúc thông tin quản lý SMI
- Những giao thức cho phép hoạt động và tương thích với SNMPv2.
- Trao đổi thông tin cấp quản lý

Do vậy về cơ bản những thực thể trong SNMPv2 cũng tương tự như trong phiên bản một, tuy nhiên để phục vụ cho thông tin cấp quản lý những thực thể cấp quản lý cần được thêm vào MIB.

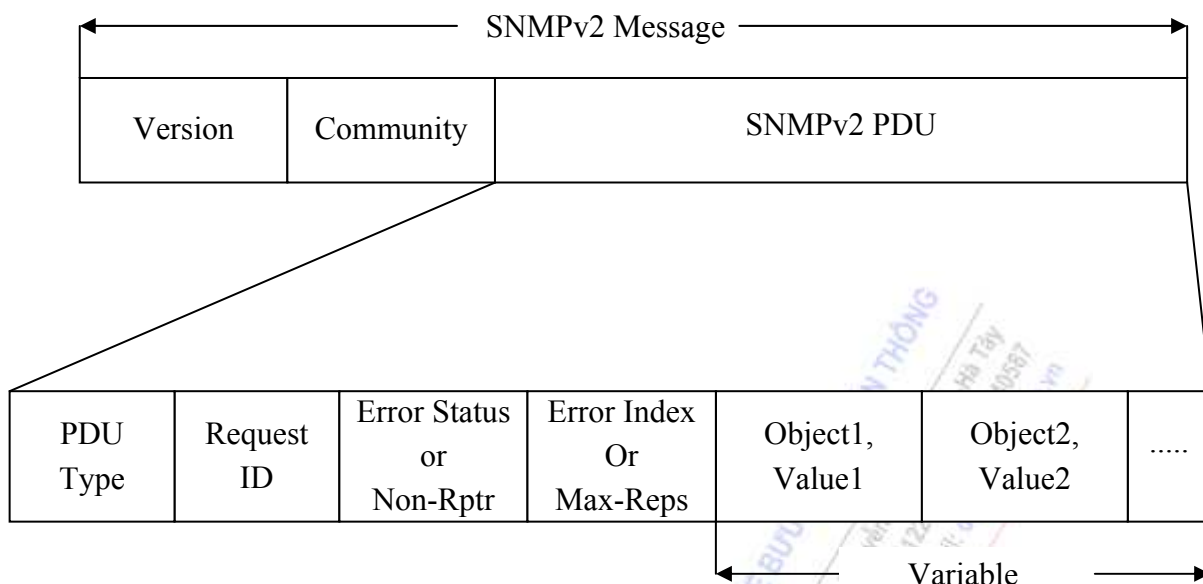
3.6.2 Cấu trúc lệnh và bản tin trong SNMPv2

Trong SNMPv2 việc trao đổi thông tin giữa trạm quản lý và các đối tượng quản lý nhằm lấy thông tin và thiết lập các tham số được thực hiện thông qua 5 lệnh cơ bản (phiên bản 1) cộng thêm 2 lệnh (trong phiên bản 2), thông tin trao đổi sử dụng dạng bản tin.

3.6.2.1 Cấu trúc bản tin

Thông tin trao đổi sử dụng dạng bản tin SNMPv2 chứa các đơn vị dữ liệu giao thức (PDU). Trong SNMPv2 có tám kiểu bản tin PDU. Cấu trúc các bản tin này gồm các trường như hình vẽ 3.1.

Trong đó: Trường Version: có giá trị là 1 thể hiện đây là SNMPv2. Các trường khác tương tự như trong SNMPv1. điều này chỉ ra, hiện nay, bất kỳ một bảo mật nào cũng được cung cấp cho SNMPv2 phải dựa vào khái niệm truyền thông SNMPv1. Nếu có một thoả thuận trong tương lai về cấu trúc bảo mật mới, nó phải được thực hiện dưới dạng một kiểu bản tin mới.



Hình 3.7: Cấu trúc dạng bản tin SNMPv2

- GetRequest, GetNextRequest, SetRequest và SNMPv2-Trap PDU có cùng dạng với Response và InformRequest PDU với các trường error-status và error-index luôn là 0.
- Trường request-id: giá trị của trường này trong một đáp ứng PDU đáp ứng phải bằng giá trị trong trường tương ứng của PDU yêu cầu. Người quản trị có thể gán một số duy nhất cho mỗi yêu cầu còn lại đến cùng một Agent để có thể phân biệt các đáp ứng cho các yêu cầu kép.
- Trong trường PDU Type, các giá trị thể hiện như sau:

Kiểu PDU	Giá trị
GetRequest	0
GetNextRequest	1
Response	2
SetRequest	3
GetBulkRequest	4
InformRequest	5
SNMPv2-Trap	6
Report	7

Trường error-status được sử dụng trong các dạng bản tin như trong bảng 3. sau:

Bảng 3.5: Sử dụng trường trạng thái lỗi trong các bản tin bản tin

SNMPv2 Error	Get	GetNext	GetBulk	Set	Inform
noError	x	x	x	x	x
tooBig	x	x		x	x
noSuchName ¹					
badValue ¹					

readOnly ¹						
genErr	X	X	X		X	
noAccess					X	
wrongType					X	
wrongLength					X	
wrongEncoding					X	
wrongValue					X	
noCreation					X	
inconsistentValue					X	
resourceUnavailable					X	
commitFailed					X	
undoFailed					X	
authorizationError	x ²	x ²	x ²		x ²	x ²
notWritable					X	
inconsistentName					X	

Với 1: Không được sử dụng bởi đối tượng SNMPv2 (chỉ có năng lực uỷ quyền). Dùng để tương thích với SNMPv1.

Với 2: Không sử dụng đến trong SNMPv2 chỉ để tương thích với SNMPv1

Trường error-index: Khi trường error-status khác 0, giá trị error-index thể hiện biến (đối tượng) trong danh sách liên kết biến gây ra lỗi. Biến đầu tiên trong danh sách có chỉ mục là 1. Biến thứ hai là 2...

Trường các biến liên kết: Trường này cho phép một toán tử đơn được áp dụng trong một nhóm phiên bản đối tượng. Nó bao gồm một chuỗi các cặp, phần tử đầu tiên là nhận dạng đối tượng và thành phần thứ hai là một trong số sau:

- value: giá trị liên quan với mỗi phiên bản đối tượng; được mô tả trong một PDU yêu cầu.
- unspecified: giá trị NULL khi sử dụng trong yêu cầu lấy thông tin.
- noSuchObject: thể hiện một Agent không thể thực hiện với đối tượng được tham chiếu bởi nhận dạng đối tượng đó.
- noSuchInstance: phiên bản đối tượng không tồn tại cho toán tử này.
- endOfMibView: thể hiện một cố gắng tham chiếu đến một nhận dạng đối tượng bên ngoài phần cuối của MIB tại Agent.

3.6.2.2 Truyền một bản tin SNMPv2

Qui tắc gửi và nhận bản tin của Manager và Agent được thể hiện trong bảng 3.6.

Bảng 3.6 : Quy tắc gửi và nhận một bản tin

SNMPv2 PDU	Agent Generate	Agent Receive	Manager Generate	Manager Receive
GetRequest		X	X	
GetNextRequest		X	X	
Response	X		X	X
SetRequest		X	X	
GetBulkRequest		X	X	
InformRequest			X	X
SNMPv2-Trap	X			X

Một phần tử SNMPv2 thực hiện các hành động sau để truyền một PDU cho một phần tử SNMPv2 khác:

- Sử dụng ASN.1 để mô tả một PDU.
- PDU này được chuyển sang dịch vụ xác nhận cùng với các địa chỉ nguồn và đích của truyền thông và một tên truyền thông. Dịch vụ xác nhận sau đó thực hiện những biến đổi bất kỳ theo yêu cầu cho sự trao đổi này như mã hoá hoặc thêm mã xác nhận và trả lại kết quả.
- Phần tử giao thức sau đó lập nên bản tin, gồm trường số hiệu phiên bản, tên truyền thông vào kết quả của bước trên.
- Đối tượng ASN. 1 mới này sau đó được mã hoá sử dụng BER và gửi đến dịch vụ giao vận.

3.6.2.3 Nhận một bản tin SNMPv2

Một phần tử SNMPv2 thực hiện các hành động sau để nhận một bản tin SNMPv2:

- Kiểm tra cú pháp cơ bản của bản tin và loại bỏ bản tin nếu cú pháp sai.
- Kiểm tra số hiệu phiên bản và loại bỏ bản tin nếu không tương hợp.
- Phần tử giao thức sau đó chuyển trên người sử dụng, phần PDU của bản tin và các địa chỉ nguồn và đích của bản tin tới dịch vụ xác nhận. Nếu xác nhận bị sai, dịch vụ xác nhận bản tin cho phần tử giao thức SNMPv2 nơi tạo ra Trap và loại bỏ bản tin. Nếu xác nhận hoàn thành dịch vụ xác nhận trả lại một PDU theo dạng của một đối tượng ASN.1.
- Phần tử giao thức thực hiện kiểm tra cú pháp cơ bản của bản tin và loại bỏ bản tin nếu cú pháp sai. Ngược lại dùng truyền thông theo tên, chính sách truy cập SNMPv2 tương ứng sẽ được chọn và PDU được xử lý tiếp theo.

3.6.3 MIB cho SNMPv2

3.6.3.1 Cơ sở thông tin quản trị (MIB) trong SNMPv2.

MIB trong SNMPv2 định nghĩa các đối tượng mô tả tác động của một phần tử SNMPv2. MIB này gồm 3 nhóm:

- Nhóm hệ thống (System group): là một mở rộng của nhóm system trong MIB-II gốc, bao gồm một nhóm các đối tượng cho phép một Agent SNMPv2 mô tả các đối tượng tài nguyên của nó.
- Nhóm SNMP (SNMP group): một cải tiến của nhóm snmp trong MIB-II gốc, bao gồm các đối tượng cung cấp các công cụ cơ bản cho hoạt động giao thức.
- Nhóm các đối tượng MIB (MIB objects group): một tập hợp các đối tượng liên quan đến các SNMPV2-Trap PDU và cho phép một vài phần tử SNMP 2 cùng hoạt động, thực hiện như trạm quản trị, phối hợp việc sử dụng của chúng trong toán tử Set của SNMPv2.

Nhóm hệ thống: Nhóm system định nghĩa trong SNMPv2 giống trong MIB-II và bổ sung một vài đối tượng mới. Các đối tượng mới này có tên bắt đầu bằng sysOR, chúng liên quan đến tài nguyên hệ thống và được sử dụng bởi một Agent SNMPv2 để mô tả các đối tượng tài nguyên mà việc điều khiển chúng tùy thuộc vào cấu hình động bởi một quản trị.

Nhóm SNMP: Nhóm này gần giống như nhóm SNMP được định nghĩa trong MIB-II nhưng có thêm một số đối tượng mới và loại bỏ một số đối tượng ban đầu. Nhóm snmp chứa một vài thông tin lưu lượng cơ bản liên quan đến toán tử SNMPv2 và chỉ có một trong các đối tượng là bộ đếm chỉ đọc 32-bit.

Nhóm các đối tượng MIB: Nhóm các đối tượng MIB chứa các đối tượng thích hợp thêm vào việc điều khiển các đối tượng MIB. Phần đầu của nhóm này là một nhóm con, snmpTrap, bao gồm hai đối tượng liên quan đến Trap:

- snmpTrapOID: là nhận dạng đối tượng của Trap hoặc thông báo được gửi hiện thời. Giá trị của đối tượng này xuất hiện như một varbind thứ hai trong mọi SNMPv2-Trap PDU và InformRequest PDU.
- snmpTrapEnterprise: là nhận dạng đối tượng của tổ chức liên quan đến Trap được gửi hiện thời. Khi một Agent ủy quyền SNMPv2 ánh xạ một Trap PDU sang một SNMPv2-Trap PDU, biến này xuất hiện như một varbind cuối cùng.

Phần thứ hai của nhóm này là một nhóm con, snmpSet, bao gồm một đối tượng đơn snmpSerialNo. Đối tượng này được sử dụng để giải quyết hai vấn đề có thể xuất hiện khi sử dụng toán tử Set: Thứ nhất là một quản trị có thể sử dụng nhiều toán tử Set trên cùng một đối tượng MIB. Các toán tử này cần thực hiện theo một trật tự được đưa ra thậm chí khi chúng được truyền không theo thứ tự. Thứ hai là việc sử dụng đồng thời các toán tử Set trên cùng một đối tượng MIB bởi nhiều quản trị có thể gây ra một sự mâu thuẫn hoặc cơ sở dữ liệu sai.

Đối tượng snmpSet được sử dụng theo cách sau: Khi một quản trị muốn đặt một hay nhiều giá trị đối tượng trong một Agent, đầu tiên nó nhận giá trị của đối tượng snmpSet. Sau đó nó gửi SetRequest PDU có danh sách biến liên kết bao gồm cả đối tượng snmpSet với giá trị đã nhận được của nó. Nếu nhiều quản trị gửi các setRequestPDU sử dụng cùng một giá trị của snmpSet, cái đến Agent trước sẽ được thực hiện (giả sử không có lỗi) kết quả làm tăng snmpSet; các toán tử set còn lại sẽ bị lỗi vì không phù hợp với giá trị snmpSet. Hơn nữa, nếu một quản trị muốn gửi một

chuỗi các toán tử set và đảm bảo rằng chúng được thực hiện theo một trật tự nhất định thì đối tượng snmpSet phải được gộp vào trong mỗi toán tử.

3.6.3.2 Các trạng thái thích ứng cho SNMPv2

Mục đích của các trạng thái thích ứng là để định nghĩa một thông báo dùng để chỉ rõ mức giới hạn thấp nhất có thể chấp nhận khi thực hiện ở mức thông thường. Có 4 macro được định nghĩa:

Macro OBJECT-GROUP: Macro này dùng để chỉ rõ một nhóm các đối tượng được quản trị có liên quan và là đơn vị cơ bản của tính thích ứng. Nó cung cấp một phương thức cho một nhà sản xuất mô tả tính thích ứng và cấp độ của nó bằng cách chỉ ra những nhóm nào được bổ sung. Macro OBJECT-GROUP gồm các mệnh đề chính sau:

- Mệnh đề OBJECTS: liệt kê các đối tượng trong nhóm có giá trị mệnh đề MAX-ACCESS là accessible-for-Notify, read-Only, read-write hoặc read-create.
- Mệnh đề STATUS: chỉ ra định nghĩa này là hiện thời hay đã qua.
- Mệnh đề DESCRIPTION: chứa một định nghĩa nguyên bản của nhóm cùng với một mô tả của bất kỳ quan hệ nào với nhóm khác.
- Mệnh đề REFERENCE: dùng để gộp một tham chiếu qui lại vào một nhóm được định nghĩa trong một vài khối thông tin khác.

Macro NOTIFICATION-GROUP: Được dùng để định nghĩa một tập hợp các thông báo cho các mục đích thích ứng, gồm các mệnh đề chính sau:

- Mệnh đề NOTIFICATIONS: Liệt kê mỗi thông báo chứa trong nhóm thích ứng.
- Mệnh đề STATUS: chỉ ra khi nào định nghĩa này là hiện thời hay đã qua.
- Mệnh đề DESCRIPTION: chứa một định nghĩa nguyên bản của nhóm cùng với một mô tả của bất kỳ quan hệ nào với nhóm khác.
- Mệnh đề REFERENCE: có thể được sử dụng để gộp một tham chiếu qua lại vào một nhóm được định nghĩa trong một vài khối thông tin khác.

Macro MODULE-COMPLIANCE: Chỉ ra một tập nhỏ nhất của các yêu cầu liên quan đến việc thêm một hay nhiều khối MIB. Các mệnh đề STATUS, DESCRIPTION, và REFERENCE có ý nghĩa tương tự như trong các macro OBJECTS-GROUP và NOTIFICATION-GROUP.

Macro AGENT-CAPABILITIES: Dùng để cung cấp thông tin về các khả năng có trong một phần tử giao thức Agent SNMPv2. Nó được sử dụng để mô tả mức độ hỗ trợ đặc biệt, mà một Agent yêu cầu, liên quan đến một nhóm MIB. Về bản chất, các tính khả năng thể hiện các cải tiến hoặc biến đổi nhất định liên quan đến các macro OBJECT-TYPE trong các khối MIB.

3.6.3.3 Sự phát triển của nhóm interfaces trong MIB - II

Nhóm interfaces của MIB-II định nghĩa một tập các đối tượng quản trị để bất kỳ giao tiếp mạng nào cũng có thể được quản lý độc lập với dạng nhất định của giao tiếp.

Nhóm interfaces: Bao gồm đối tượng ifNumber và bảng ifTable. Đối tượng ifNumber phản ánh số lượng giao tiếp và do vậy là số lượng hàng trong bảng ifTable. Tuy nhiên không cần

giới hạn số lượng sơ đồ các giao tiếp trong dải 1 đến giá trị của ifNumber. Điều này cho phép thêm/bớt động các giao tiếp.

Bảng mở rộng giao tiếp: Bảng mở rộng giao tiếp ifXTable cung cấp thông tin thêm cho bảng ifTable. Bảng ifXTable mở rộng bảng ifTable đã được sửa đổi, do vậy nó được sắp xếp bằng ifIndex từ bảng ifTable.

Bảng giao tiếp khối: Bảng ifstackTable đưa ra các quan hệ giữa các hàng trong ifTable mà được hỗ trợ bởi cùng giao tiếp vật lý với mức trung bình. Nó thể hiện các lớp con nào đang chạy trên các lớp con khác. Mỗi mục trong ifStackTable định nghĩa một quan hệ giữa hai mục trong ifTable.

Bảng giao tiếp kiểm tra: Bảng ifTestTable định nghĩa các đối tượng cho phép một quản trị hướng dẫn một Agent kiểm tra một giao tiếp với nhiều lỗi. Bảng chứa một mục cho một giao tiếp.

Bảng nhận địa chỉ chung: Bảng này chứa một mục cho mỗi địa chỉ mà từ đó hệ thống sẽ nhận các gói tin trên một giao tiếp cụ thể, ngoại trừ khi hoạt động trong chế độ ngẫu nhiên. Tức là bảng này liệt kê các địa chỉ mà hệ thống này chấp nhận và để từ đó hệ thống này sẽ giữ lại các gói chứa một trong các địa chỉ này như là địa chỉ đích.

3.7 SNMPv3

Như đã trình bày trong chương trước, bản thân SNMPv2 đã có phần bảo đảm bảo mật được thêm vào, tuy nhiên phần này chưa tạo được sự đồng thuận của người sử dụng do tính tiện lợi và bảo mật của nó. Để sửa chữa những thiếu hụt đó SNMPv3 được giới thiệu như một chuẩn đề nghị cho lĩnh vực quản trị mạng và được trình bày chi tiết lần đầu tiên vào năm 1998 với các tài liệu RFC2271 - RFC2275. Chuẩn này đưa ra nhằm hoàn thiện hơn vấn đề quản trị và bảo mật.

Tháng 4 năm 1999 và tháng 12 năm 2002, những cải tiến, bổ sung nhằm làm hoàn thiện hơn SNMPv3 được trình bày trong các tài liệu RFC2570-RFC2576 (năm 1999) và RFC3410-RFC3418 (năm 2002). Các tài liệu từ RFC3410 đến RFC3418 trình bày một cách chi tiết và đầy đủ nhất về SNMPv3, cơ sở thông tin quản trị SNMPv3, cấu trúc thông tin quản trị SNMPv3, sự tương thích giữa SNMPv1, SNMPv2, SNMPv2c và SNMPv3...

Mục đích chính của SNMPv3 là hỗ trợ kiến trúc theo kiểu module để có thể dễ dàng mở rộng. Theo cách này, nếu các giao thức bảo mật mới được mở rộng chúng có thể được hỗ trợ bởi SNMPv3 bằng các định nghĩa như là các module riêng. Cơ sở thông tin quản trị và các dạng bản tin sử dụng trong SNMPv3 cũng hoàn toàn tương tự trong SNMPv2.

3.7.1 Các đặc điểm mới của SNMPv3

SNMPv3 dựa trên việc thực hiện giao thức, loại dữ liệu và uỷ quyền như SNMPv2 và cải tiến phần an toàn. SNMPv3 cung cấp an toàn truy cập các thiết bị bằng cách kết hợp sự xác nhận và mã hoá các gói tin trên mạng. Những đặc điểm bảo mật cung cấp trong SNMPv3 là:

- Tính toàn vẹn thông báo : Đảm bảo các gói tin không bị sửa trong khi truyền.
- Sự xác nhận: Xác nhận nguồn của thông báo gửi đến.
- Mã hoá: Đảo nội dung của gói tin ngăn cản việc gửi thông báo từ nguồn không được xác nhận.

SNMPv3 cung cấp cả mô hình an toàn và các mức an toàn. Mô hình an toàn là thực hiện việc xác nhận được thiết lập cho người sử dụng và nhóm các người sử dụng hiện có. Mức an toàn là mức bảo đảm an toàn trong mô hình an toàn. Sự kết hợp của mô hình an toàn và mức an toàn sẽ xác định cơ chế an toàn khi gửi một gói tin.

Tuy nhiên việc sử dụng SNMPv3 rất phức tạp và cồng kềnh. Tuy đây là sự lựa chọn tốt nhất cho vấn đề bảo mật của mạng. Nhưng việc sử dụng sẽ tốn rất nhiều tài nguyên do trong mỗi bản tin truyền đi sẽ có phần mã hóa BER. Nó sẽ chiếm một phần băng thông đường truyền do đó làm tăng phí tổn mạng.

Mặc dù được coi là phiên bản đề nghị cuối cùng và được coi là đầy đủ nhất nhưng SNMPv3 vẫn chỉ là tiêu chuẩn dự thảo và vẫn đang được nghiên cứu hoàn thiện.

3.7.2 Những thay đổi hỗ trợ bảo mật và nhận thực trong SNMPv3

3.7.2.1 Các thành phần và nguyên tắc trao đổi thông tin

Cấu trúc phân tử SNMP

Tất cả các Agent SNMP và trạm quản trị SNMP trước đây nay được gọi là các phân tử SNMP. Một phân tử SNMP được tạo ra từ hai phần: một công cụ SNMP (SNMP engine) và các phần mềm ứng dụng SNMP (application(s)).

SNMP engine

Công cụ SNMP cung cấp các dịch vụ cho quá trình gửi và nhận các bản tin, chứng thực và mã hoá các bản tin, điều khiển truy cập tới các đối tượng quản lý. Có một sự kết hợp 1-1 giữa công cụ SNMP và phân tử SNMP chứa nó.

Công cụ SNMP chứa bốn thành phần là:

- Dispatcher: Bộ điều vận.
- Message Processing Subsystem: Phân hệ xử lý bản tin.
- Security Subsystem: Phân hệ bảo mật.
- Access Control Subsystem: Phân hệ điều khiển truy cập.

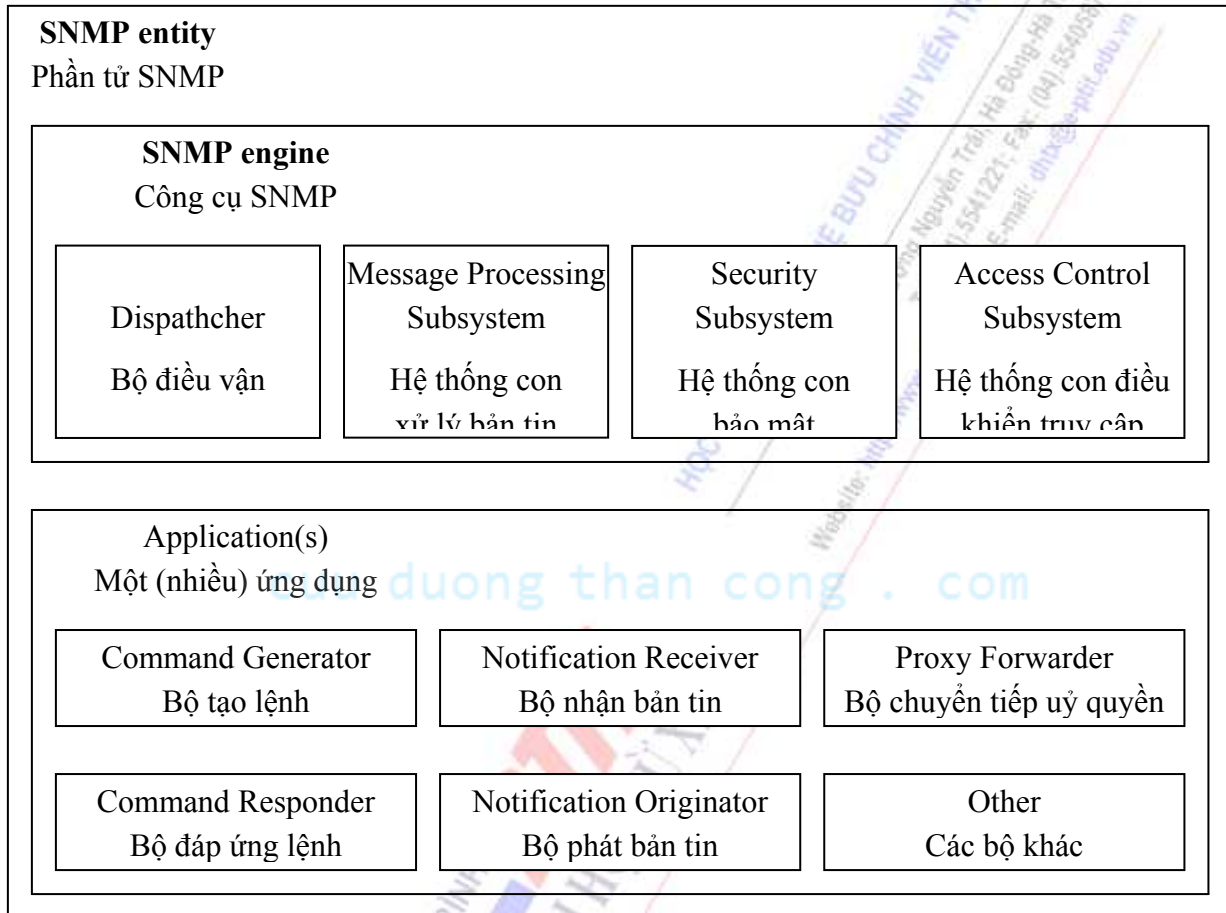
Bộ điều vận: Trong mỗi phân tử SNMP chỉ có một bộ điều vận duy nhất. Nó cho phép sự hỗ trợ tồn tại nhiều phiên bản khác nhau của bản tin SNMP. Bộ điều vận có trách nhiệm:

- Gửi và nhận các bản tin SNMP.
- Xác định các phiên bản của bản tin và tương tác tương ứng với các mô hình xử lý bản tin. Khi nhận được một bản tin, bộ điều vận xác định số hiệu phiên bản của bản tin và sau đó chuyển bản tin đến khối xử lý bản tin tương ứng. Nếu bản tin không thể phân tích để xác định phiên bản thì bộ đếm snmpInASNParseErrs tăng lên và bản tin bị loại bỏ. Nếu phiên bản không được hỗ trợ bởi phân hệ xử lý bản tin thì bộ đếm snmpInBadVersions tăng lên và bản tin bị loại bỏ.
- Cung cấp một giao diện trừu tượng tới ứng dụng SNMP cho sự gửi và nhận của PDU tới ứng dụng.
- Cung cấp một giao diện trừu tượng tới các ứng dụng SNMP mà nó cho phép chúng gửi một PDU tới một phân tử SNMP ở xa.

Phân hệ xử lý bản tin: Phân hệ xử lý bản tin có trách nhiệm: chuẩn bị các bản tin để gửi đi và trích dữ liệu từ các bản tin nhận được.

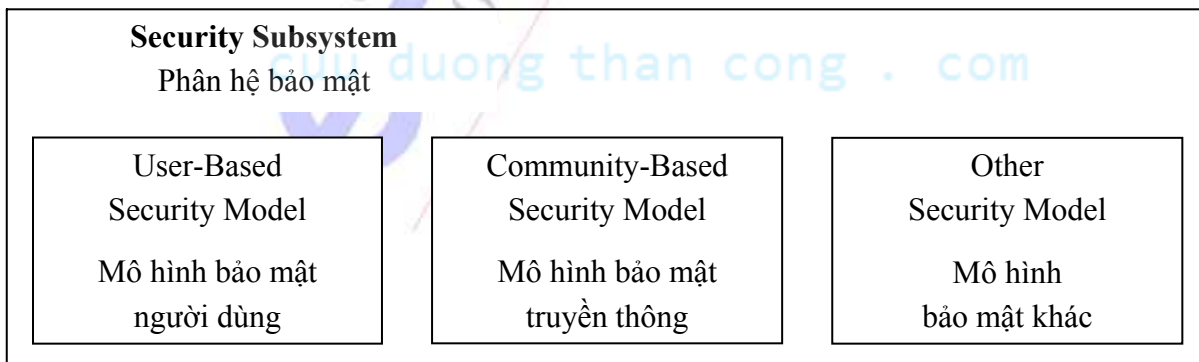
Phân hệ xử lý bản tin được tạo thành từ một hoặc nhiều khối xử lý bản tin. Sơ đồ sau đưa ra một phân hệ xử lý bản tin hỗ trợ các mô hình SNMPv3, SNMPv1, SNMPv2 và một vài mô hình khác.

Phân hệ bảo mật: Các phân hệ bảo mật cung cấp các dịch vụ bảo mật như: xác nhận bản tin, mã hoá và giải mã các bản tin để đảm bảo bí mật.



Hình 3.8 Cấu trúc phần tử SNMP

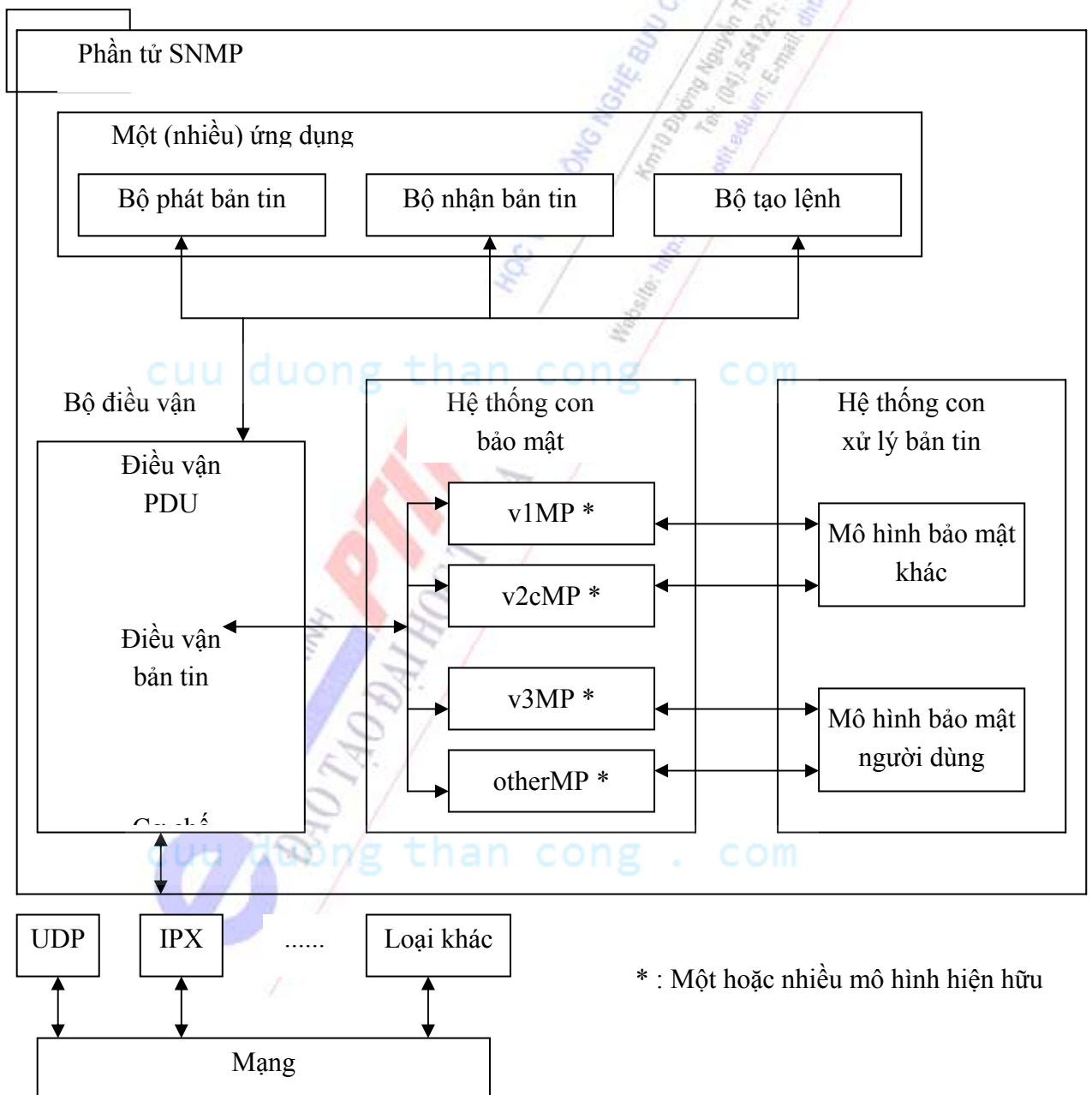
Sơ đồ sau đưa ra phân hệ bảo mật hỗ trợ các mô hình cho SNMPv3, mô hình trên cơ sở truyền thông và vài mô hình khác. Mô hình trên cơ sở truyền thông hỗ trợ SNMPv1 và SNMPv2c.



Hình 3.9 Phân hệ bảo mật

Mô hình bảo mật trên cơ sở người dùng sẽ bảo vệ các bản tin SNMPv3 từ các mối nguy hiểm:

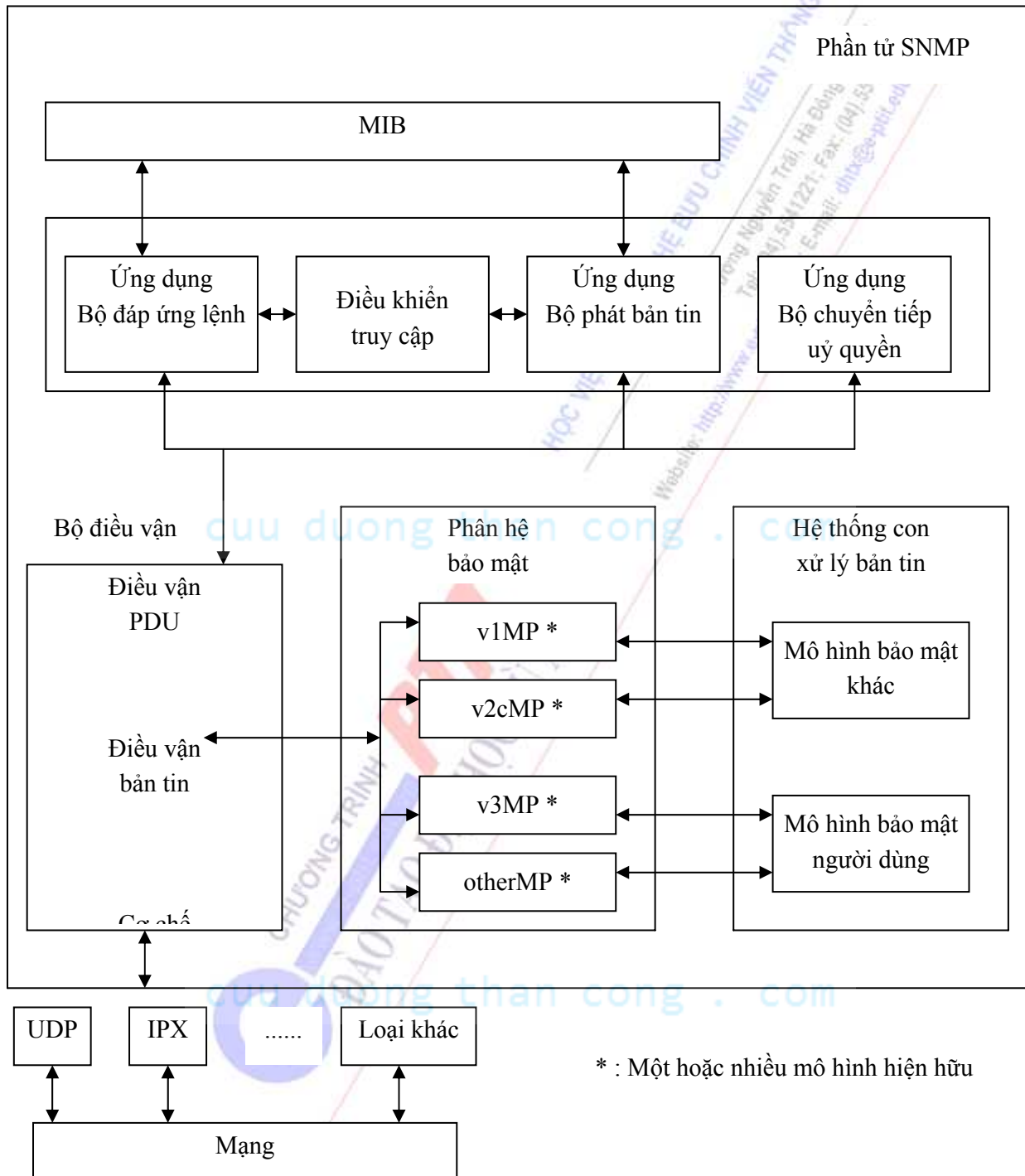
- Một người được phép gửi một bản tin mà có thể bị sửa trong khi truyền bởi một phần tử SNMP không được phép.
- Người dùng không được phép cố gắng giả trang như người dùng được phép.
- Sửa chuỗi bản tin SNMP dựa trên cơ sở UDP là dịch vụ vận chuyển không liên kết. Các bản tin có khả năng bị bắt giữ và sắp xếp lại, làm chậm và có thể chuyển lại sau đó.
- Nghe trộm, do các bản tin cho phép được mã hoá, một ai đó nghe trộm trên đường dây sẽ không thể phán đoán rằng họ nhận được gì.



Hình 3.10: Các thành phần của một SNMP Manager.

Phân hệ điều khiển truy cập : Trách nhiệm của phân hệ điều khiển truy cập là: xác định khi nào việc truy cập vào một đối tượng quản trị là được phép. Hiện nay mới định nghĩa một mô hình: mô hình điều khiển truy cập trên cơ sở thẩm tra (View-base Access Control Model-VACM). Cấu trúc SNMPv3 cho phép các mô hình điều khiển truy cập bổ sung được định nghĩa trong tương lai.

Phần mềm ứng dụng SNMPv3



Hình 3.11 Các thành phần của một SNMP Agent.

Đối với SNMPv3 khi nói đến các ứng dụng, ta cần xem đây là các ứng dụng nội bộ bên trong phần tử SNMP. Các ứng dụng nội bộ này thực hiện công việc như tạo ra các bản tin SNMP,

đáp ứng lại các bản tin nhận được, nhận các bản tin và chuyển tiếp các bản tin giữa các phần tử. Hiện có năm loại ứng dụng đã được định nghĩa:

Các bộ tạo lệnh (Command Generator): Tạo ra các lệnh SNMP để thu thập hoặc thiết lập các dữ liệu quản lý.

- Các bộ đáp ứng lệnh (Command Responder): Cung cấp việc truy cập tới dữ liệu quản lý. Ví dụ các lệnh Get, GetNext, Get-Bulk và Set PDUs được thực hiện bởi các bộ đáp ứng lệnh.
- Các bộ tạo bản tin (Notification Originator): Khởi tạo Trap hoặc Inform.
- Các bộ nhận bản tin (Notification Receiver) Nhận và xử lý các bản tin Trap hoặc Inform.
- Các bộ chuyển tiếp uỷ nhiệm (Proxy Forwarder): Chuyển tiếp các thông báo giữa các phần tử SNMP.

SNMP Manager: Một phần tử SNMP bao gồm một hoặc nhiều các bộ tạo lệnh và/hoặc các bộ nhận bản tin giữa các phần tử SNMP. Một SNMP Manager được giới thiệu ở dưới:

SNMP Agent: Một phần tử SNMP bao gồm một hoặc nhiều các bộ đáp ứng lệnh và/hoặc các bộ tạo bản tin (cùng với công cụ SNMP kết hợp chúng) được gọi là một SNMP Agent. Một SNMP Agent được giới thiệu ở hình 3.11

Gửi một bản tin hoặc một yêu cầu

Quá trình gửi một bản tin hoặc một yêu cầu gồm các bước sau:

- Yêu cầu ứng dụng được tạo ra như sau
- Nếu giá trị messageProcessingModel không miêu tả một mô hình xử lý bản tin được biết tới từ bộ điều vận thì giá trị errorIndication được trả lại cho ứng dụng gọi tới và không có hành động nào được xử lý nữa.
- Bộ điều vận tạo ra sendPduHandle cho quá trình xử lý tiếp theo.
- Bộ điều vận bản tin gửi yêu cầu tới module xử lý bản tin phiên bản đặc trưng và được xác định bởi messageProcessingModel
- Nếu statusInformation biểu thị lỗi, thì giá trị errorIndication được trả lại cho ứng dụng gọi tới và không có hành động nào được xử lý nữa.
- Nếu statusInformation biểu thị sự chấp thuận, thì sendPduHandle được trả về ứng dụng và outgoingMessage được gửi đi. Truyền thông được sử dụng để gửi outgoingMessage được trả về qua destTransportDomain và địa chỉ mà nó gửi được trả về qua destTransportAddress.
- Quá trình xử lý một bản tin gửi đi hoàn tất.

Gửi một đáp ứng tới mạng

Quá trình gửi một đáp ứng một bản tin diễn ra như sau:

- Tạo ra một ứng dụng chứa yêu cầu sử dụng

- Bộ điều vận bản tin sẽ gửi yêu cầu tới mô hình xử lý bản tin thích hợp được nhận biết qua giá trị messageProcessingModel. Khi đó một đáp ứng chuẩn bị được gửi đi
- Nếu result là errorIndication thì errorIndication sẽ trả lại ứng dụng gọi tới và không có hành động nào được xử lý nữa.
- Nếu result được chấp nhận thì outgoingMessage được gửi đi. Truyền thông được sử dụng để gửi outgoingMessage được trả về qua destTransportDomain và địa chỉ mà nó gửi được trả về qua destTransportAddress.

Quá trình điều phối bản tin của bản tin SNMP nhận được

- Giá trị snmpInPkts được tăng lên.
- Nếu gói tin không phân tách được đầy đủ phiên bản của bản tin SNMP hoặc nếu phiên bản không được hỗ trợ thì giá trị snmpInASNParseErrs được tăng lên và bản tin nhận được bị loại bỏ và không xử lý nữa.
- Nguồn gốc của transportDomain và transportAddress được xác định.
- Bản tin chuyển qua mô hình xử lý bản tin và thành phần dữ liệu trừu tượng được trả về bởi bộ điều vận:
- Nếu result là errorIndication không thích hợp thì bản tin bị huỷ bỏ và quá trình xử lý kết thúc.
- Tiếp theo, tùy vào giá trị của sendPduHandle là rỗng hay không rỗng ta có hai hướng xử lý tiếp.

Điều phối PDU của bản tin SNMP nhận được

Nếu sendPduHandle là rỗng thì bản tin nhận được là một yêu cầu hoặc một bản tin. Quá trình xử lý như sau:

- Giá trị của contextEngineID và pduType được phối hợp để quyết định xem ứng dụng đã đăng ký cho một bản tin hay một yêu cầu.
- Nếu không có ứng dụng nào được đăng ký:
 - ✓ snmpUnknownPDUHandlers được tăng lên.
 - ✓ Một đáp ứng được chuẩn bị tạo ra
 - ✓ Nếu result là thành công thì bản tin chuẩn bị được gửi đi. Quá trình xử lý kết thúc.
- Trường hợp còn lại: Pdu được xử lý

Bản tin đến là một đáp ứng:

- Giá trị sendpduHandle được xác định. Ứng dụng đang đợi đáp ứng này được xác định thông qua sendpduHandle.
- Nếu không có ứng dụng nào đợi, bản tin bị huỷ bỏ và quá trình xử lý kết thúc. stateReference được giải phóng. nmpUnknownPDUHandlers được tăng lên. Quá trình xử lý kết thúc.

- Nếu xuất hiện ứng dụng đang đợi thì đáp ứng được trả về:

3.7.2.2 Mô hình bảo mật dựa trên người dùng

Các giao diện dịch vụ trừu tượng

Các giao diện dịch vụ trừu tượng được định nghĩa để mô tả các giao diện khái niệm giữa các phân hệ khác nhau bên trong một phần tử SNMP. Một cách tương tự, một tập các giao diện dịch vụ trừu tượng đã được định nghĩa bên trong mô hình bảo mật dựa trên người dùng (USM: User-base Security Model) để mô tả các giao diện khái niệm giữa các dịch vụ USM chung và các dịch vụ riêng và xác thực độc lập.

Những giao diện dịch vụ trừu tượng này được định nghĩa bởi một tập các giao diện nguyên thủy mà xác định các dịch vụ cung cấp và các phần tử dữ liệu trừu tượng mà phải được truyền đi khi các dịch vụ được gọi. Phần này liệt kê các giao diện nguyên thủy mà đã được định nghĩa cho mô hình bảo mật dựa trên người dùng.

Các giao diện nguyên thủy xác thực mô hình bảo mật dựa trên người dùng

Mô hình bảo mật dựa trên người dùng cung cấp các giao diện nguyên thủy bên trong để truyền dữ liệu đi và đến giữa bản thân mô hình bảo mật và dịch vụ xác thực

Các giao diện nguyên thủy bảo mật của mô hình bảo mật dựa trên người dùng

Mô hình bảo mật dựa trên người dùng cung cấp các giao diện nguyên thủy để truyền dữ liệu đi và về giữa bản thân mô hình bảo mật và dịch vụ bảo mật (privacy service)

Người dùng của mô hình bảo mật dựa trên người dùng

Các hoạt động quản lý sử dụng mô hình bảo mật này phải sử dụng một tập định nghĩa trước các ID người dùng. Đối với bất cứ người dùng nào mà với tư cách của họ, các hoạt động quản lý được xác thực tại một phần tử SNMP nào đó, mà phần tử SNMP đó phải có thông tin về người dùng đó. Một phần tử SNMP mà muốn giao tiếp với một phần tử SNMP khác cũng phải có thông tin về một người dùng được biết bởi máy đó, bao gồm thông tin về các thuộc tính có thể dùng được của người dùng đó.

Một người dùng và các thuộc tính của họ được xác định như sau:

- UserName: Một chuỗi thể hiện tên của người dùng.
- securityName: Một chuỗi có thể đọc được thể hiện người dùng theo một khuôn dạng, đó là tính độc lập của mô hình bảo mật. Có một mối quan hệ một-một giữa userName và securityName.
- authProtocol: Một dấu hiệu cho biết các bản tin đã gửi với vai trò của người dùng này có được xác thực hay không, và nếu có, kiểu giao thức xác thực đã được sử dụng là gì. Có hai giao thức như vậy được định nghĩa trong ghi chú này:
 - ✓ Giao thức xác thực HMAC-MD5-96.
 - ✓ Giao thức xác thực HMAC-SHA-96.
- authKey: Nếu các bản tin được gửi với vai trò người dùng này được xác thực, khoá xác thực (bảo mật) đối với việc sử dụng cùng giao thức xác thực. Chú ý rằng khoá xác thực của người dùng thông thường sẽ khác nhau đối với các phần tử

SNMP xác thực khác nhau. authKey không thể truy nhập thông qua SNMP. Các yêu cầu chiều dài của authKey được định nghĩa bởi authProtocol được sử dụng.

- authKeyChange và authOwnKeyChange: Các duy nhận để cập nhật từ xa khoá nhận thức. Làm như vậy theo một cách bảo mật, vì thế việc cập nhật có thể được hoàn thành mà không cần sử dụng bảo vệ riêng (privacy protection).
- privProtocol: Một dấu hiệu cho biết các bản tin đã gửi với vai trò người dùng này có được bảo vệ khỏi bại lộ không, và nếu như vậy, kiểu giao thức bảo mật nào được sử dụng. Một giao thức như vậy được định nghĩa trong ghi chú này: giao thức mã hoá đối xứng CBC-DES.
- privKey: Nếu các bản tin đã gửi với vai trò người dùng này có thể được mã hoá/giải mã, khoá bảo mật đối với việc sử dụng giao thức bảo mật là gì. Chú ý rằng khoá bảo mật của người dùng thông thường sẽ khác nhau đối với các phần tử SNMP xác thực khác nhau. privKey không thể truy cập thông qua SNMP. Các yêu cầu độ dài của privKey được định nghĩa bởi privProtocol được sử dụng.
- privKeyChange and privOwnKeyChange: Cách duy nhất để cập nhật từ xa khoá mã hoá. Làm như vậy là một cách bảo mật, do đó việc cập nhật có thể được hoàn thành mà không cần tới bảo vệ riêng.

Các bản tin SNMP sử dụng mô hình bảo mật

Cú pháp của một bản tin SNMP sử dụng mô hình bảo mật này giữ vững khuôn dạng bản tin đã định nghĩa trong tài liệu Mô hình xử lý bản tin các phiên bản trước (ví dụ như RFC3412).

Trường msgSecurityParameters trong các bản tin SNMPv3 có kiểu dữ liệu OCTET STRING. Các giá trị của nó là chuỗi BER theo thứ tự ASN. 1

Các dịch vụ được cung cấp bởi mô hình bảo mật dựa trên người dùng

Phần này mô tả các dịch vụ được cung cấp bởi mô hình bảo mật dựa trên người dùng với các đầu vào và đầu ra của chúng.

Các dịch vụ cho việc sinh ra một bản tin SNMP gửi đi: Khi một phân hệ xử lý bản tin (MP) gọi module bảo mật dựa trên người dùng để bảo vệ một bản tin SNMP gửi đi, nó phải sử dụng dịch vụ thích hợp được cung cấp bởi module bảo mật. Có hai dịch vụ được cung cấp:

- Một dịch vụ sinh ra một bản tin yêu cầu
- Một dịch vụ để sinh ra một bản tin trả lời

Cho đến khi tiến trình hoàn thành, module bảo mật dựa trên người dùng trả lại statusInformation. Nếu tiến trình thành công, bản tin đã hoàn thành với việc bảo mật và xác thực được áp dụng nếu nó được yêu cầu như vậy thì securityLevel cụ thể được trả lại. Nếu tiến trình không thành công, thì một errorIndication được trả lại.

Các dịch vụ cho việc xử lý bản tin SNMP đến: Khi phân hệ xử lý bản tin (MP) gọi module bảo mật dựa trên người dùng để kiểm tra độ bảo mật đúng đắn của bản tin đến, nó phải sử dụng dịch vụ được cung cấp cho một bản tin đến. Cho đến khi hoàn thành tiến trình, module bảo mật dựa trên người dùng trả lại statusInformation, và nếu tiến trình thành công, các phần tử dữ liệu thêm vào cho việc xử lý sâu hơn bản tin. Nếu tiến trình không thành công,

thì một errorIndication, có thể với một OID và cặp giá trị của một bộ đếm lỗi mà đã được tăng lên.

Tạo ra một bản tin SNMP gửi đi

Phần này mô tả thủ tục được sinh ra bởi một phân tử SNMP khi nó sinh ra một bản tin chứa một hoạt động quản lý (như một yêu cầu, một phản hồi, một bản tin, một báo cáo) với vai trò của một người dùng, với một securityLevel cụ thể.

- Nếu một securityStateReference được truyền đi (bản tin phản hồi hoặc báo cáo), thông tin liên quan đến người dùng được trích ra từ cachedSecurityData. cachedSecurityData bây giờ có thể bị loại bỏ. securityEngineID được thiết lập về snmpEngineID cục bộ. securityLevel được thiết lập về một giá trị cụ thể được chỉ ra bởi module gọi.
- Dựa trên securityName, thông tin liên quan đến người dùng tại snmpEngineID đích, được chỉ ra bởi securityEngineID, được trích ra từ bộ lưu trữ dữ liệu cấu hình cục bộ (LCD, usmUserTable). Nếu thông tin về người dùng không có ở LCD, thì một dấu hiệu lỗi (unknownSecurityName) được trả lại cho module gọi.
- Nếu securityLevel chỉ ra rằng bản tin đã được xác thực, nhưng người dùng không hỗ trợ cả giao thức xác thực và bảo mật, thì bản tin không được gửi đi. Một dấu hiệu lỗi (unsupportedSecurityLevel) được trả lại cho module gọi.
- Nếu securityLevel chỉ ra rằng bản tin được xác thực, nhưng người dùng không hỗ trợ một giao thức xác thực, thì bản tin không được gửi đi. Một dấu hiệu lỗi (unsupportedSecurityLevel) được trả lại cho module gọi.
- Nếu securityLevel chỉ ra rằng bản tin được bảo vệ khỏi sự bại lộ, thì chuỗi octet thể hiện scopedPDU đã đưa ra được mã hoá theo giao thức bảo mật của người dùng. Để làm như vậy, một lời gọi được thực hiện cho module bảo mật mà thực thi giao thức bảo mật của người dùng theo giao diện nguyên thủy trừu tượng.
- Nếu module bảo mật trả lại thất bại, thì bản tin không thể được gửi đi và một dấu hiệu lỗi (encryptionError) được trả lại cho module gọi.
- Nếu module bảo mật trả lại thành công, thì privParameters trả về được đưa vào trường msgPrivacyParameters của securityParameters và encryptedPDU phục vụ như là trọng tải của bản tin đang được chuẩn bị.
- Ngược lại, nếu securityLevel chỉ ra rằng bản tin không được bảo vệ khỏi sự bại lộ, thì một OCTET STRING có chiều dài bằng không được mã hoá vào trường msgPrivacyParameters của securityParameters và scopedPDU thuần văn bản phục vụ như là trọng tải của bản tin đang được chuẩn bị.
- securityEngineID đã được mã hoá thành một OCTET STRING vào trường msgAuthoritativeEngineID của securityParameters. Chú ý rằng một securityEngineID rỗng (chiều dài bằng không) là chấp nhận được đối với bản

tin yêu cầu, bởi vì nó sẽ làm cho phần tử SNMP (xác thực) ở xa trả lại một báo cáo PDU với securityEngineID chính xác được đặt trong msgAuthoritativeEngineID trong securityParameters của phần tử đã trả lại báo cáo PDU.

- Nếu securityLevel chỉ ra rằng bản tin được xác thực, thì các giá trị hiện thời của snmpEngineBoots và snmpEngineTime đáp ứng cho securityEngineID từ LCD được sử dụng.
- Ngược lại, nếu đây là một bản tin báo cáo hoặc phản hồi, thì giá trị hiện thời của snmpEngineBoots và snmpEngineTime đáp ứng cho snmpEngineID cục bộ từ LCD được sử dụng.
- Ngược lại, nếu đây là một bản tin yêu cầu, thì giá trị zero được sử dụng cho cả snmpEngineBoots và snmpEngineTime. Giá trị zero này được sử dụng nếu snmpEngineID rỗng.
- Các giá trị được mã hoá thành INTEGER vào các trường msgAuthoritativeEngineBoots và msgAuthoritativeEngineTime của securityParameters.
- userName được mã hoá thành một OCTET STRING vào trường msgUserName của securityParameters.
- Nếu securityLevel chỉ ra rằng bản tin được xác thực, bản tin được xác thực theo giao thức xác thực của người dùng. Để làm như vậy một lời gọi được thực hiện đối với module xác thực mà thực thi giao thức xác thực của người dùng.
- Nếu module xác thực trả lại thất bại, thì bản tin không thể được gửi đi và một dấu hiệu lỗi (authenticationFailure) được trả lại cho module xác thực.
- Nếu module xác thực trả lại thành công, thì trường msgAuthenticationParameters được đặt vào securityParameters và authenticatedWholeMsg thể hiện sự phát hành của bản tin đã xác thực đang được chuẩn bị.
- Ngược lại, nếu securityLevel chỉ ra rằng bản tin không được xác thực thì một OCTET STRING chiều dài bằng không được mã hoá vào trường msgAuthenticationParameters của securityParameters. wholeMsg bây giờ được phát hành và sau đó thể hiện bản tin đã xác thực đang được chuẩn bị.
- Bản tin đã hoàn thành với chiều dài của nó được trả lại cho module gọi với statusInformation thiết lập về thành công.

Xử lý một bản tin SNMP đến

Phần này mô tả các thủ tục được sinh ra bởi một phần tử SNMP bất cứ khi nào nó nhận được một bản tin chứa một hoạt động quản lý với vai trò của một người dùng, với một securityLevel cụ thể. Để đơn giản hoá các thành phần của thủ tục, việc giải phóng thông tin trạng thái không phải luôn được chỉ ra một cách rõ ràng. Như một nguyên tắc chung, nếu

thông tin trạng thái là có sẵn khi một bản tin bị loại bỏ, thông tin trạng thái cũng được loại bỏ. Hơn nữa, một dấu hiệu lỗi có thể trả lại một OID và giá trị cho một bộ đếm tăng dần và một giá trị tùy chọn cho securityLevel, và các giá trị cho contextEngineID hoặc contextName cho bộ đếm. Thêm vào đó, dữ liệu securityStateReference được trả lại nếu bất cứ thông tin nào như vậy có sẵn tại điểm mà lỗi được phát hiện.

- Nếu securityParameters nhận được không phải là sự phát hành liên tục của một OCTET STRING được định dạng theo UsmSecurityParameters đã định nghĩa ở trên, thì bộ đếm snmpInASNParseErrs [RFC3418] được tăng lên, và một dấu hiệu lỗi (parseError) được trả lại cho module gọi. Chú ý rằng chúng ta trả lại mà không có OID và giá trị của bộ đếm được tăng lên, bởi vì trong trường hợp này không đủ thông tin để sinh ra báo cáo PDU.
- Các giá trị của các trường tham số bảo mật được trích từ securityParameters. securityEngineID được trả lại cho bên gọi là giá trị của trường msgAuthoritativeEngineID. cachedSecurityData được chuẩn bị và một securityStateReference được chuẩn bị để tham chiếu tới dữ liệu này. Các giá trị được lưu trữ là: msgUserName.
- Nếu giá trị của trường msgAuthoritativeEngineID trong securityParameters là không biết thì: Một phần tử SNMP không xác thực mà thực hiện khôi phục có thể tạo ra một mục mới một cách tùy chọn trong kho dữ liệu cấu hình cục bộ (LCD) của nó và tiếp tục xử lý, hoặc bộ đếm usmStatsUnknownEngine được tăng lên và một dấu hiệu lỗi (unknownEngineID) cùng với OID và giá trị của bộ đếm đã tăng lên được trả lại cho module gọi.
- Chú ý rằng sự kiện nhận được msgAuthoritativeEngineID có chiều dài bằng không, hoặc có kích cỡ không hợp lệ khác nên được chọn để làm cho việc khôi phục engineID trở nên thuận lợi. Mặt khác, việc lựa chọn giữa a và b là một vấn đề phát sinh trong cài đặt.
- Thông tin về giá trị của các trường msgUserName và msgAuthoritativeEngineID được trích ra từ kho dữ liệu cấu hình cục bộ(LCD, usmUserTable). Nếu không có thông tin nào có sẵn cho người dùng, thì bộ đếm usmStatsUnknownUserNames được tăng lên và một dấu hiệu lỗi (unknownSecurityName) cùng với OID và giá trị của bộ đếm đã tăng lên được trả lại cho module gọi.
- Nếu thông tin về người dùng chỉ ra rằng nó không hỗ trợ securityLevel được yêu cầu bởi bên gọi, thì bộ đếm usmStatsUnsupportedSecLevels được tăng lên và một dấu hiệu lỗi (unsupportedSecurityLevel) cùng với OID và giá trị của bộ đếm đã tăng lên được trả lại cho module gọi.
- Nếu securityLevel chỉ ra rằng bản tin được xác thực, thì bản tin được xác thực theo giao thức xác thực của người dùng. Để làm như vậy, phải thực hiện một lời gọi đến module xác thực mà thực thi giao thức xác thực của người dùng theo giao diện nguyên thủy của dịch vụ trù tượng.

- Nếu module xác thực trả lại thất bại, thì bản tin không thể trung thực được, vì thế bộ đếm usmStatsWrongDigests được tăng lên và một dấu hiệu lỗi (authenticationFailure) cùng với OID và giá trị của bộ đếm đã tăng lên được trả lại cho module gọi.
- Nếu module xác thực trả lại thành công, thì bản tin là xác thực và có thể tin cậy được, vì thế việc xử lý được tiếp tục.
- Nếu securityLevel chỉ ra một bản tin đã xác thực, thì các giá trị cục bộ của snmpEngineBoots, snmpEngineTime và latestReceivedEngineTime đáp ứng cho giá trị của trường msgAuthoritativeEngineID được trích từ kho dữ liệu cấu hình cục bộ.
- Nếu giá trị đã trích ra của msgAuthoritativeEngineID giống với giá trị của snmpEngineID của phần tử SNMP xử lý (nghĩa là đây là một phần tử SNMP xác thực), thì nếu bất cứ điều kiện nào sau đây là đúng, thì bản tin được xem là ngoài cửa sổ thời gian:
 - ✓ Giá trị cục bộ của snmpEngineBoots là 2147483647.
 - ✓ Giá trị của trường msgAuthoritativeEngineBoots khác với giá trị cục bộ của snmpEngineBoots; hoặc giá trị của trường msgAuthoritativeEngineTime khác với khái niệm cục bộ của snmpEngineTime nhiều hơn ± 150 giây.
- Nếu bản tin được xem là ngoài cửa sổ thời gian, thì bộ đếm usmStatsNotInTimeWindows được tăng lên và một dấu hiệu lỗi (notInTimeWindow) cùng với OID, giá trị của bộ đếm đã tăng lên, và một dấu hiệu rằng lỗi phải được báo cáo với một securityLevel của authNoPriv, được trả lại cho module gọi.
- Nếu giá trị trích ra được của msgAuthoritativeEngineID không giống với giá trị snmpEngineID của phần tử SNMP xử lý (nghĩa là không phải là phần tử SNMP xác thực) thì ít nhất một trong các điều kiện sau là đúng:
 - ✓ Giá trị trích ra được của trường msgAuthoritativeEngineBoots lớn hơn khái niệm cục bộ của giá trị snmpEngineBoots, và giá trị trích ra được của trường msgAuthoritativeEngineTime lớn hơn giá trị của latestReceivedEngineTime, thì mục LCD đáp ứng cho giá trị đã trích được của trường msgAuthoritativeEngineID đã được cập nhật, bằng cách thiết lập.
 - ✓ Khái niệm cục bộ của giá trị snmpEngineBoots bằng giá trị của trường msgAuthoritativeEngineBoots.
 - ✓ Khái niệm cục bộ của giá trị snmpEngineTime bằng giá trị của trường msgAuthoritativeEngineTime và latestReceivedEngineTime bằng giá trị của trường msgAuthoritativeEngineTime.

- Nếu bất cứ điều kiện nào sau đây đúng, thì bản tin được xem là ngoài cửa sổ thời gian:
 - ✓ Khái niệm cục bộ của giá trị snmpEngineBoots là 2147483647.
 - ✓ Giá trị của trường msgAuthoritativeEngineBoots là nhỏ hơn khái niệm cục bộ của giá trị snmpEngineBoots hoặc giá trị của trường msgAuthoritativeEngineBoots bằng với khái niệm cục bộ của giá trị snmpEngineBoots và giá trị của trường msgAuthoritativeEngineTime lớn hơn 150 giây nhỏ hơn khái niệm cục bộ của giá trị snmpEngineTime.
- Nếu bản tin được xem là ngoài cửa sổ thời gian thì một dấu hiệu lỗi (notInTimeWindow) được trả lại cho module gọi.
- Nếu securityLevel chỉ ra rằng bản tin được bảo vệ khỏi sự bại lộ, thì OCTET STRING thể hiện encryptedPDU đã được giải mã theo giao thức bảo mật của người dùng để đạt được giá trị scopedPDU đã phát hành không được mã hoá. Để làm như vậy, phải thực hiện một lời gọi đến module bảo mật mà thực thi giao thức bảo mật của người dùng theo giao diện nguyên thủy trừu tượng.
- Nếu module bảo mật trả lại thất bại, thì bản tin không thể xử lý được, do đó bộ đếm usmStatsDecryptionErrors được tăng lên và một dấu hiệu lỗi (decryptionError) cùng với OID và giá trị của bộ đếm đã tăng lên được trả lại cho module gọi.
- Nếu module bảo mật trả lại thành công, thì scopedPDU đã giải mã là trọng tải bản tin được trả lại cho module gọi.
- Ngược lại, thành phần scopedPDU được giả thiết là thuần văn bản và là trọng tải bản tin được trả lại cho module gọi.
- maxSizeResponseScopedPDU được tính toán. Đây là kích cỡ tối đa được cho phép cho một scopedPDU đối với một bản tin phản hồi. Sự cung cấp được thực hiện đối với một tiêu đề bản tin mà cho phép cùng securityLevel như trong yêu cầu nhận được.
- securityName cho người dùng được khôi phục từ usmUserTable.
- Dữ liệu bảo mật được lưu trữ là cachedSecurityData, vì thế một phản hồi có thể thực hiện được cho bản tin này có thể và sẽ sử dụng cùng xác thực và các bảo mật.
- statusInformation được thiết lập là thành công và một kết quả trả lại được thực hiện cho module gọi truyền về các tham số OUT như được chỉ ra trong giao diện nguyên thủy processIncomingMsg.

Trong chương này mới chỉ đề cập đến từng bước trong quá trình xử lý bản tin còn chi tiết hơn về câu lệnh sinh viên cần nghiên cứu thêm ở tài liệu tham khảo.

CÂU HỎI ÔN TẬP CHƯƠNG 3

- SNMP là
 - Giao thức quản lí mạng đơn giản
 - Giao thức quản lí Internet đơn giản
 - Giao thức quản lí mạng đồng bộ
 - Giao thức giám sát mạng đơn giản
- SNMPv3 bổ sung ... so với phiên bản SNMP đầu tiên
 - Nhận thực
 - Tính di động
 - Bảo mật
 - Tính chính xác
- Có các phiên bản SNMP
 - SNMPv1
 - SNMPv2
 - SNMPv3
 - SNMPv4
- Trong cấu trúc cây MIB-II có ... đối tượng :
 - 8
 - 10
 - 12
 - 14
- SNMP là giao thức ứng dụng sử dụng giao thức ... ở lớp vận chuyển:
 - UDP
 - TCP
 - FTP
- Phiên bản nào của giao thức SNMP hỗ trợ tính bảo mật và nhận thực
 - SNMPv1
 - SNMPv2
 - SNMPv3
- Trong mô hình TCP/IP, SNMP nằm ở lớp:
 - Vật lý
 - Mạng
 - Vận chuyển
 - Ứng dụng
- SNMP sử dụng lệnh cơ bản là Read để
 - Đọc thông tin từ thiết bị
 - Ghi các thông tin điều khiển lên thiết bị
 - Dùng để nhận các sự kiện gửi từ thiết bị
- SNMP sử dụng lệnh cơ bản là Write để

- A. Đọc thông tin từ thiết bị
 - B. Ghi các thông tin điều khiển lên thiết bị
 - C. Dùng để nhận các sự kiện gửi từ thiết bị
10. SNMP sử dụng lệnh cơ bản là Trap để
- A. Đọc thông tin từ thiết bị
 - B. Ghi các thông tin điều khiển lên thiết bị
 - C. Dùng để nhận các sự kiện gửi từ thiết bị
11. Có bao nhiêu cây con liên quan tới quản lý trong cây Internet?
- A. 2
 - B. 3
 - C. 4
12. Hệ thống quản lý mạng dựa trên SNMP có bao nhiêu thành phần?
- A. 2
 - B. 4
 - C. 4
13. SNMP sử dụng các lệnh để quản lý thiết bị, trong đó lệnh Read dùng để
- A. Nhận các sự kiện gửi từ thiết bị đến SNMP
 - B. Ghi các thông tin điều khiển lên thiết bị
 - C. Đọc thông tin từ thiết bị.
 - D. Đọc thông tin quản lý.
14. Phần tử Agent trong SNMP có nhiệm vụ:
- A. Thu thập thông tin quản lý
 - B. Lưu trữ thông tin quản lý để phục vụ cho hệ thống quản lý mạng.
 - C. Điều khiển và quản lý các phần tử trong SNMP
15. Cấu trúc thông tin quản lý (SMI) mô phỏng bao nhiêu loại dữ liệu?
- A. 3
 - B. 4
 - C. 5
 - D. 6
16. Trong SNMPv2 đã có một số thay đổi sau so với SNMPv1 đó là :
- A. Thay đổi trong cấu trúc thông tin quản lý SMI
 - B. Những giao thức cho phép hoạt động và tương thích với SNMPv2.
 - C. Trao đổi thông tin cấp quản lý
 - D. Cả ba ý trên
17. Cấu trúc bản tin SNMPv2 bao gồm có
- A. 3 phần là Version, Community và PDU

B 2 phần là Version và Community

C có PDU.

D.4 phần là Version, Community, PDU và CRC

18. Trong SNMPv2 có kiểu PDU

- A. 5
- B. 6
- C. 7
- D. 8

19. Bản tin GetRequest được gửi từ

- A. Phần tử quản lý đến phần tử bị quản lý
- B. Phần tử bị quản lý đến phần tử quản lý
- C. Giữa các phần tử quản lý
- D. Giữa các phần tử bị quản lý

20. Bản tin Response được gửi từ

- A. Các phần tử bị quản lý
- B. Các phần tử quản lý
- C. Cả hai phần tử trên
- D. Không từ phần tử nào cả

21. Những loại bản tin nào được gửi giữa hai phần tử quản lý

- A. GetRequest
- B. GetNextRequest
- C. Response
- D. Response và InformRequest

22. Những loại bản tin nào được gửi bởi phần tử bị quản lý

- A. SetRequest
- B. GetBulkRequest và InformRequest
- C. Response
- D. SNMPv2-Trap

23. MIB trong SNMPv2 định nghĩa các đối tượng mô tả tác động của một phần tử SNMPv2 gồm

- A. 2 nhóm
- B. 3 nhóm
- C. 4 nhóm
- D. 5 nhóm

24. Trong SNMPv2, nhóm.....: là một mở rộng của nhóm system trong MIB-II gốc, bao gồm một nhóm các đối tượng cho phép một Agent SNMPv2 mô tả các đối tượng tài nguyên của nó.

- A. Nhóm hệ thống (System group)

- B. Nhóm SNMP (SNMP group)
 - C. Nhóm các đối tượng MIB (MIB objects group)
 - D. Nhóm quản lý (managing group)
25. Những đặc điểm bảo mật cung cấp trong SNMPv3 là
- A. Tính toàn vẹn thông báo : Đảm bảo các gói tin không bị sửa trong khi truyền.
 - B. Sự xác nhận: Xác nhận nguồn của thông báo gửi đến.
 - C. Mã hoá: Đảo nội dung của gói tin ngăn cản việc gửi thông báo từ nguồn không được xác nhận.
 - D. Cả ba ý trên
26. Trong SNMPv3, một phần tử SNMP được tạo ra từ
- A. Hai phần: một công cụ SNMP (SNMP engine) và các phần mềm ứng dụng SNMP (application(s)).
 - B. Các công cụ SNMP (SNMP engine)
 - C. Các phần mềm ứng dụng SNMP (application(s)).
 - D. Một agent của SNMP
27. Trong SNMPv3, công cụ SNMP chứa
- A. Bốn thành phần là: Bộ điều vận, phân hệ xử lý bản tin, phân hệ bảo mật, phân hệ điều khiển truy cập.
 - B. Ba thành phần là: Bộ điều vận, phân hệ xử lý bản tin, phân hệ bảo mật.
 - C. Hai thành phần là: Bộ điều vận, phân hệ xử lý bản tin.
 - D. duy nhất bộ điều vận.
28. Mô hình bảo mật trên cơ sở người dùng sẽ bảo vệ các bản tin SNMPv3 từ các mối nguy hiểm:
- A. Một người được phép gửi một bản tin mà có thể bị sửa trong khi truyền bởi một phần tử SNMP không được phép.
 - B. Người dùng không được phép cố gắng giả trang như người dùng được phép.
 - C. Sửa chuỗi bản tin SNMP dựa trên cơ sở UDP là dịch vụ vận chuyển không liên kết. Các bản tin có khả năng bị bắt giữ và sắp xếp lại, làm chậm và có thể chuyển lại sau đó.
 - D. Nghe trộm, do các bản tin cho phép được mã hoá, một ai đó nghe trộm trên đường dây sẽ không thể phán đoán rằng họ nhận được gì.
 - E. Cả bốn mối nguy hiểm trên
29. Trong mô hình bảo mật dựa trên người dùng, một người dùng và các thuộc tính của họ được xác định nhờ
- A. 6 tham số
 - B. 7 tham số
 - C. 8 tham số
 - D. 9 tham số

30. Các dịch vụ được cung cấp bởi mô hình bảo mật dựa trên người dùng bao gồm

- A. 2 dịch vụ
- B. 3 dịch vụ
- C. 4 dịch vụ
- D. 5 dịch vụ

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Km10 Đường Nguyễn Trãi, Hà Đông-Hà Tây
Tel: (04).5541221; Fax: (04).5540587

Website: <http://www.coitptit.edu.vn>; E-mail: dhkx@ptit.edu.vn

cuu duong than cong . com

CHƯƠNG TRÌNH **PTIT**
ĐẠO TẠO ĐẠI HỌC TỪ XA

cuu duong than cong . com

THUẬT NGỮ VIẾT TẮT

DES	Data Encryption Standard	Tiêu chuẩn mật mã hoá dữ liệu
ICMP	Internet Control Message Protocol	Giao thức kiểm soát thông báo Internet
IETF	Internet Engineering Task Force	Tổ chức hỗ trợ kỹ thuật Internet
IP	Internet Protocol	Giao thức Internet
ISO	International Standard Organisation	Tổ chức tiêu chuẩn hoá quốc tế
MIB	Management Information Base	Cơ sở thông tin quản lí
OS	Operating System	Hệ điều hành
OSI	Open System Interconnection	Hệ thống liên kết mở
RFC	Requests For Comments	
RMON	Remote Network Monitoring	Kiểm soát mạng từ xa
SGMP	Simple Gateway Monitoring Protocol	Giao thức kiểm soát cổng đơn giản
SMI	Structure of Management Information	Cấu trúc thông tin quản lí
SNMP	Simple Network Management Protocol	Giao thức quản lí mạng đơn giản
TCP	Transmission Control Protocol	Giao thức điều khiển giao vận
UDP	User Datagram Protocol	Giao thức dữ liệu người dùng



TÀI LIỆU THAM KHẢO

- [1] Divakara K. Udupa: Telecommunications Management Network. McGraw-Hill, 1999.
- [2] Gilbert Held: Managing TCP/IP Networks. John Wiley & Sons, 2000.
- [3] Tarek N. S., Mostafa H. A.: Fundamentals of Telecommunications Networks. John Wiley and Sons, 1994.
- [4] Understanding Telecommunications. Studentliteratur Ericsson, 1997.
- [5] Salah Aidarous, Thomas Plevyak: Telecommunication Network Management into the 21st Century – Techniques, Standards, Technologies, and Applications. IEEE Press, 1994.
- [6] Quản lý mạng trong xu thế phát triển mạng viễn thông thế hệ sau. Nguyễn Quý Minh Hiền. NXB Bưu Điện, 2003.
- [7] Công nghệ quản lý mạng hiện đại. Biên dịch: Nguyễn Hải Yến, NXB Bưu Điện, 2001.
- [8] Essential SNMP, 2nd Edition, Douglas Mauro, Kevin Schmidt, O'Reilly, 2005.

cuu duong than cong . com



MỤC LỤC

LỜI NÓI ĐẦU.....	1
CHƯƠNG I : TỔNG QUAN VỀ QUẢN LÝ MẠNG VIỄN THÔNG.....	3
1.1. KHÁI NIỆM VỀ QUẢN LÝ, KHAI THÁC VÀ BẢO DƯỠNG MẠNG.....	3
1.2. MÔ HÌNH TỔNG QUÁT HỆ THỐNG MẠNG	3
1.3. CÁC YÊU CẦU QUẢN LÝ	4
1.3.1. Các chức năng quản lý lớp cao	4
1.3.2. Các yêu cầu quản lý của người sử dụng.....	5
1.3.3. Các động lực thúc đẩy công nghệ quản lý mạng	5
1.4. CÁC QUAN ĐIỂM VÀ CÁCH TIẾP CẬN TRONG QUẢN LÝ MẠNG.....	6
1.4.1. Các thực thể của hệ thống quản lý mạng	6
1.4.2. Quan điểm quản lý Manager-Agent.....	7
1.4.3. Mô hình quan hệ Manager-agent	8
1.4.4. Các miền quản lý.....	9
1.5. HỆ THỐNG QUẢN LÝ MỞ.....	10
1.5.1. Mô hình hệ thống quản lý mở	10
1.5.2. Các yêu cầu đối với hệ thống quản lý mở.....	11
1.6. HỆ THỐNG QUẢN LÝ PHÂN TÁN	12
1.6.1. Kiến trúc hệ thống quản lý phân tán	13
1.6.2. Hệ thống quản lý trong băng và ngoài băng	14
CÂU HỎI ÔN TẬP CHƯƠNG 1.....	15
CHƯƠNG 2: MẠNG QUẢN LÝ VIỄN THÔNG TMN	18
2.1 NGUYÊN LÝ CHUNG VÀ CÁC KHUYẾN NGHỊ TMN.....	18
2.1.1 Khái niệm và nguyên lý của TMN	18
2.1.2 Quan hệ giữa TMN và mạng viễn thông.....	19
2.1.3 Các khuyến nghị của TMN	20
2.2 KIẾN TRÚC CHỨC NĂNG	22
2.2.1. Chức năng phần tử mạng NEF	23
2.2.2. Chức năng hệ điều hành OSF.....	23
2.2.3. Chức năng trạm làm việc WSF.....	24
2.2.4. Chức năng thích ứng Q	24
2.2.5. Chức năng trung gian MF	24
2.3 KIẾN TRÚC VẬT LÝ	25
2.3.1. Các khối vật lý	25
2.3.2. Các giao tiếp.....	30
2.3.3 Các giao diện.....	32
2.3.4 Giao diện X	33
2.3.5 Giao diện F.....	33
2.4 KIẾN TRÚC PHÂN LỚP LÔGIC	33
2.4.1. Lớp quản lý phần tử NEML	34
2.4.2. Lớp quản lý mạng NML	35

2.4.3. Lớp quản lý dịch vụ SML.....	35
2.4.4. Lớp quản lý kinh doanh BML	36
2.5 CÁC CHỨC NĂNG QUẢN LÝ TRONG TMN	36
2.5.1 Quản lý hiệu năng.....	38
2.5.2 Quản lý sự cố.....	40
2.5.3. Quản lý cấu hình.....	41
2.5.4 Quản lý tài khoản.....	42
2.5.5 Quản lý bảo mật.....	42
2.6 KIẾN TRÚC THÔNG TIN	42
2.6.1. Mô hình đối tượng trên cơ sở OSI.....	43
2.6.2. Mô hình đối tượng phân tán	44
CÂU HỎI ÔN TẬP CHƯƠNG 2	45
CHƯƠNG 3 : GIAO THỨC QUẢN LÝ MẠNG ĐƠN GIẢN SNMP	49
3.1 GIỚI THIỆU CHUNG VỀ SNMP	49
3.2. QUẢN LÝ TRUYỀN THÔNG TRONG SNMP	51
3.2.1 Quản lý liên lạc giữa nhà quản lý với các tác nhân.....	51
3.2.2 Cơ chế vận chuyển thông tin giữa nhà quản lý và tác nhân	52
3.2.3 Bảo vệ truyền thông liên lạc giữa nhà quản lý và các tác nhân khỏi sự cố	52
3.2.4 Ảnh hưởng của tầng vận chuyển tới khả năng quản lý mạng.....	53
3.3 CẤU TRÚC VÀ ĐẶC ĐIỂM CỦA THÔNG TIN QUẢN LÝ.....	53
3.4 CƠ SỞ THÔNG TIN QUẢN LÝ (MIB).....	54
3.4.1 Cấu trúc của MIB	54
3.4.2 Truy nhập MIB	56
3.4.3 Nội dung của MIB	57
3.4.4 Các đối tượng của MIB-II	58
3.5 ĐIỀU HÀNH SNMP.....	61
3.5.1 Các thành phần của SNMP	61
3.5.2 Các lệnh cơ bản trong SNMP	62
3.6 SNMPv2.....	64
3.6.1 Các thực thể của SNMPv2.....	64
3.6.2 Cấu trúc lệnh và bản tin trong SNMPv2.....	64
3.6.3 MIB cho SNMPv2	67
3.7 SNMPv3.....	70
3.7.1 Các đặc điểm mới của SNMPv3.....	70
3.7.2 Những thay đổi hỗ trợ bảo mật và nhận thực trong SNMPv3	71
CÂU HỎI ÔN TẬP CHƯƠNG 3	84
THUẬT NGỮ VIẾT TẮT	89
TÀI LIỆU THAM KHẢO	90

QUẢN LÝ MẠNG VIỄN THÔNG

Mã số: 411QLM460

Chịu trách nhiệm bản thảo

TRUNG TÂM ĐÀO TẠO BƯU CHÍNH VIỄN THÔNG 1

CHƯƠNG TRÌNH
ĐÀO TẠO ĐẠI HỌC TỪ XA
PTTH
cuu duong than cong . com