TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Bài giảng

QUẢN LÍ MẠNG VIỄN THÔNG

(Lưu hành nội bộ)

HÀ NỘI - 2009

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Bài giảng

QUẢN LÝ MẠNG VIỄN THÔNG

Biên soạn: **TS. Nguyễn Tiến Ban (chủ biên)**
ThS. Hoàng Trọng Minh
ThS. Nguyễn Thị Thu Hằng
ThS. Dương Thị Thanh Tú
KS. Nguyễn Đình Long

HÀ NỘI - 2009

LỜI NÓI ĐẦU

Cùng với sự phát triển mạnh mẽ của các giải pháp công nghệ hạ tầng mạng truyền thông, hàng loạt các yêu cầu mới được đặt ra đối với các vấn đề khai thác và triển khai hệ thống trong môi trường mạng thực tiễn. 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. Tùy thuộc vào các giải pháp công nghệ và các ứng dụng triển khai mà các nhà khai thác lựa chọn và xây dựng các hệ thống quản lý mạng thích hợp để nâng cao hiệu quả vận hành và khai thác mạng. Vì vậy, các giải pháp quản lý mạng luôn là một bài toán mang tính động và sát với công nghệ mạng lưới. Nhằm cung cấp cho học viên những kiến thức cơ bản trong quản lý mạng viễn thông, bài giảng này cung cấp cho sinh viên những kiến thức cơ bản về quản lý mạng viễn thông để qua đó hiểu được các cơ chế, kỹ thuật cũng như giao thức quản lý và giám sát mạng viễn thông.

Với mục tiêu đặt ra như vậy, nội dung của tài liệu được chia thành 4 chương.

Chương 1 giới thiệu các vấn đề cơ bản nhất của quản lý mạng, bao gồm các khái niệm, yêu cầu và kiến trúc của các mô hình quản lý mạng.

Chương 2 cung cấp các đặc tính, ứng dụng và phương thức hoạt động của giao thức quản lý mạng đơn giản SNMP nhằm đưa tới người đọc các kiến thức nền tảng của giao thức quản lý mạng trong môi trường hội tụ trên nền IP.

Chương 3 trình bày các nguyên tắc giám sát mạng thông dụng với các nguyên lí giám sát và điều khiển mạng từ xa.

Chương 4 trình bày các giải pháp quản lý mạng thực tiễn đối với một số công nghệ điển hình đang được triển khai trên thế giới cũng như ở Việt nam, các nguyên tắc và phương pháp này sẽ giúp người đọc có được những kiến thức tiếp cận với thực tiễn quản lý mạng viễn thông hiện nay.

Quản lý mạng viễn thông là một nội dung rất quan trọng, cần được nghiên cứu kĩ 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 lí 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.

Những ý kiến đóng góp xin gửi về :

Bộ môn Mạng viễn thông- Khoa Viễn thông 1- Học viện Công nghệ Bưu chính viễn thông
ĐT: 84-4-33515484 Fax: 84-4-33511405

Hà Nội, tháng 12 năm 2009

MỤC LỤC

THUẬT NGỮ VIẾT TẮT

API	Application Programming Interface	Giao diện lập trình ứng dụng
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
ASN	Abstract Syntax Notation	Chú ý cú pháp rút gọn
ATM	Asynchronous Transfer Mode	Phương thức truyền dị bộ
ATMF	ATM Forum	Diễn đàn ATM
BDI	Backward Defect Indicator	Chỉ thị lỗi hướng về
BGP	Border Gateway Protocol	Giao thức cổng biên
B-ISDN	Broadband ISDN	ISDN băng rộng
BML	Business Management Layer	Lớp quản lý kinh doanh
CBC-DES	Cipher Block Chaining - Data Encryption Standard	Giao thức mã hoá ma trận
CCITT	Consultative Committee for International Telegraph and Telephone	Ủy ban tư vấn về điện thoại và điện báo quốc tế (Tiền thân của ITU)
CLI	Command Line Interface	Giao diện dòng lệnh
CMIP	Common Management Information Protocol	Giao thức thông tin điều hành chung
CMIS	Common Management Information Services	Giao thức dịch vụ thông tin quản lý chung
CORBA	Common Object Request Broken Architecture	Kiến trúc CORBA
DCN	Data Communication Network	Mạng thông tin dữ liệu
DES	Data Encryption Standard	Tiêu chuẩn mật mã hoá dữ liệu
DML	Data Management Language	Ngôn ngữ xử lý dữ liệu
DTL	Designated Transit List	Danh sách chuyển tiếp mong muốn
ERO	Explicit Route Object	Đối tượng định tuyến hiện
ETSI	European Telecommunications Standards Institute	Viện tiêu chuẩn viễn thông Châu Âu
FDI	Forward Defect Indicator	Chỉ thị lỗi hướng đi
FR	Frame Relay	Chuyển tiếp khung
FTP	File Transfer Protocol	Giao thức truyền file
GDMO	Guideline for Definition of Managed Objects	Gợi ý để xác định các đối tượng điều hành
GMPLS	General Multi Protocol Label	Công nghệ chuyển mạch nhãn đa giao

	Switching	thức tổng quát
GUI	Graphic User Interface	Giao diện người dùng đồ hoạ
HMMP	Hypermedia Management Protocol	Giao thức quản lý đa phương tiện
IAB	Internet Architecture Board	Tổ chức kiến trúc Internet
ICMP	Internet Control Message Protocol	Giao thức kiểm soát thông báo Internet
ID	Identification	Nhận dạng
IETF	Internet Engineering Task Force	Tổ chức hỗ trợ kỹ thuật Internet
INMF	Internet Network Management Framework	Khung công việc quản lý mạng Internet
IP	Internet Protocol	Giao thức Internet
ISDN	Integrated Service Digital Network	Mạng số đa dịch vụ
ISO	International Standard Organisation	Tổ chức tiêu chuẩn hoá quốc tế
ITF	Information Transfer Function	Chức năng truyền tải thông tin
ITU	International Telecommunications Union	Hiệp hội viễn thông quốc tế
ITU-T	ITU-Telecommunication Sector	Tiểu ban viễn thông – Hiệp hội viễn thông quốc tế
LAN	Local Area Network	Mạng nội hạt
LSP	Label Switch Path	Đường chuyển mạch nhãn
MAC	Media Access Control	Điều khiển truy nhập phương tiện
MD	Mediation Device	Thiết bị trung gian
MF	Mediation Function	Chức năng trung gian
MIB	Management Information Base	Cơ sở thông tin quản lý
MOM	Manage Of Manager	Quản lý của quản lý
MPLS	Multi Protocol Label Switching	Chuyển mạch nhãn đa giao thức
NE	Network Element	Phần tử mạng
NEF	Network Element Function	Chức năng phần tử mạng
NEML	Network Element Management Layer	Lớp quản lý phần tử mạng
NGN	Next Generation Network	Mạng thế hệ kế tiếp (sau)
NMF	Network Management Forum	Diễn đàn điều hành mạng
NML	Network Management Layer	Lớp quản lý mạng
NMS	Network Management System	Hệ thống quản lý mạng
	Network Management Station	Trạm quản lý mạng
OS	Operating System	Hệ điều hành
OSI	Open System Interconnection	Hệ thống liên kết mở
PDU	Protocol Data Unit	Đơn vị dữ liệu giao thức

QAF	Q Adapter Function	Chức năng thích ứng Q
QoS	Quality of Service	Chất lượng dịch vụ
RARP	Reverse Address Resolution Protocol	Giao thức phân giải địa chỉ ngược
RED	Random Early Detection	Kỹ thuật loại bỏ sớm ngẫu nhiên
RMON	Remote Network Monitoring	Kiểm soát mạng từ xa
RSVP	Resource ReServation Protocol	Giao thức giành trước tài nguyên
SAME	System Application Management Entity	Thực thể quản lý ứng dụng hệ thống
SGMP	Simple Gateway Monitoring Protocol	Giao thức kiểm soát cổng đơn giản
SLA	Service Level Agreement	Thoả thuận mức dịch vụ
SMI	Structure of Management Information	Cấu trúc thông tin quản lý
	System Management Information	Thông tin quản lý hệ thống
SML	Service Management Layer	Lớp quản lý dịch vụ
SNMP	Simple Network Management Protocol	Giao thức quản lý mạng đơn giản
SONET	Synchronous Optical Network	Mạng quang đồng bộ
SS7	Signalling System Number 7	Mạng báo hiệu số 7
TCP	Transmission Control Protocol	Giao thức điều khiển giao vận
TCP/IP	Transmission Control Protocol/Internet Protocol (Suite)	Chồng giao thức TCP/IP
TDM	Time Division Multiplexing	Ghép kênh phân chia theo thời gian
TMN	Telecommunication Management Network	Mạng quản lý viễn thông
UDP	User Datagram Protocol	Giao thức dữ liệu người dùng
UML	Unified Modeling Language	Mô hình hướng đối tượng sử dụng
VACM	View-based Access Control Model	Mô hình điều khiển kết nối dựa trên các View
VPN	Virtual Private Network	Mạng riêng ảo
WAN	Wide Area Network	Mạng diện rộng
WDM	Wave Division Multiplexing	Ghép kênh quang theo bước sóng
WS	Work Station	Máy trạm (trạm làm việc)
WSF	Work Station Funtion	Chức năng trạm làm việc

CHƯƠNG 1

TỔNG QUAN VỀ QUẢN LÝ MẠNG

1.1 GIỚI THIỆU CHUNG

Sự phát triển và hội tụ mạng tiến tới mạng thế hệ kế tiếp NGN (Next Generation Network) trong những năm gần đây đã tác động mạnh mẽ tới tất cả các khía cạnh của mạng lưới, thậm chí cả về những nhận thức nền tảng và phương pháp tiếp cận Quản lý mạng cũng là một trong những lĩnh vực đang có những sự thay đổi và hoàn thiện mạnh mẽ trong cả nỗ lực tiêu chuẩn hoá của các tổ chức tiêu chuẩn lớn trên thế giới và yêu cầu từ phía người sử dụng dịch vụ. Mặt khác các nhà khai thác mạng, nhà cung cấp thiết bị và người sử dụng thường áp dụng các phương pháp chiến lược khác nhau cho việc quản lý mạng và thiết bị của mình. Mỗi nhà cung cấp thiết bị thường đưa ra giải pháp quản lý mạng riêng cho sản phẩm của mình. Trong bối cảnh hội tụ mạng hiện nay, số lượng thiết bị và dịch vụ rất đa dạng và phức tạp đã tạo ra các thách thức lớn trong vấn đề quản lý mạng.

Nhiệm vụ của quản lý mạng rất rõ ràng về mặt nguyên tắc chung, nhưng các bài toán quản lý cụ thể lại có độ phức tạp rất lớn. Điều này xuất phát từ tính đa dạng của các hệ thống thiết bị và các đặc tính quản lý của các loại thiết bị, và xa hơn nữa là chiến lược quản lý phải phù hợp với kiến trúc mạng và đáp ứng yêu cầu của người sử dụng. Một loạt các thiết bị điển hình cần được quản lý gồm: 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 đường trung kế, DSC/DAC, các bộ lặp, bộ tái tạo tín hiệu, các thiết bị chuyển mạch, các bridge, router và switch, tất cả mới chỉ là một phần 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 dịch vụ, người sử dụng, các ứng dụng hệ thống, các cơ sở dữ liệu khác nhau trong các loại môi trường ứng dụng. Về mặt kỹ thuật , tất cả thông tin trên được thu thập, trao đổi và được kết hợp với 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 biệt, các giao thức truyền thông cũng như các mô hình thông tin chuyên biệt, các kỹ năng chuyên biệt 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.

Khi mạng hội tụ tiến tới hạ tầng mạng thế hệ kế tiếp NGN, một khung làm việc và các khái niệm chung được các tổ chức tiêu chuẩn hóa quốc tế đưa ra như Tổ chức viễn thông quốc tế ITU (International Telecommunication Union), Viện tiêu chuẩn viễn thông Châu Âu ETSI (European Telecommunications Standards Institute), Tổ chức đặc trách kỹ thuật internet IETF (Internet Engineering Task Force)... Trong đó, theo quan điểm của tiểu ban chuẩn hoá viễn thông trong ITU (ITU-T), chức năng quản lý mạng liên quan tới một tập chức năng điều hành và quản lý mạng cho phép trao đổi thông tin quản lý giữa mặt bằng quản lý và các nguồn tài nguyên, dịch vụ và các mặt bằng khác. Khuyến nghị ITU-T M.3060/Y.2401 (03/2006) định nghĩa về các yêu cầu chung của quản lý mạng NGN gồm có một số các đặc điểm cơ bản như sau:

- Cung cấp khả năng quản lý nguồn tài nguyên NGN trên cả mạng lõi, mạng truy nhập, các thành phần liên kết nối, mạng khách hàng và thiết bị đầu cuối.
- Cung cấp khả năng quản lý nguồn tài nguyên dịch vụ độc lập với tài nguyên truyền tải, cho phép hỗ trợ phân biệt các dịch vụ người sử dụng đầu cuối.
- Cho phép khả năng kiến tạo dịch vụ mới cho người sử dụng trên môi trường kiến tạo dịch vụ của NGN.
- Cung cấp khả năng quản lý mạng tới các dịch vụ riêng của người sử dụng (báo cáo lỗi, bản ghi cước trực tuyến).
- Đảm bảo truy nhập an toàn các thông tin quản lý .
- Hỗ trợ các mạng giá trị eBussiness dựa trên các luật kinh doanh (khách hàng, nhà cung cấp dịch vụ, các đối thủ cạnh tranh, nhà cung cấp).
- Cho phép những người dùng cá nhân hoặc các tổ chức đưa luật riêng vào trong môi trường mạng chung.
- Đưa ra nhìn nhận tổng thể về các nguồn tài nguyên nhằm che dấu độ phức tạp và sự đa dạng của các công nghệ.
- Hỗ trợ vấn đề thu thập dữ liệu cước cho người điều hành mạng trên cả hai phương thức online và offline.
- Cung cấp khả năng khôi phục mạng khi mạng lỗi, giám sát mạng khách hàng, cung cấp dịch vụ tích hợp từ đầu cuối tới đầu cuối và tự động chỉ định nguồn tài nguyên.
- Cung cấp khả năng điều hành mạng dựa trên chất lượng dịch vụ.
- Khả năng trao đổi các thông tin quản lý qua các vùng biên mạng: Giữa vùng dịch vụ và vùng truyền tải, giữa mặt bằng điều khiển và mặt bằng quản lý và giữa các vùng quản lý .
- Có các giao diện quản lý trên các phần tử mạng tiêu chuẩn, dễ phát triển cho cả nhà cung cấp dịch vụ và người sử dụng dịch vụ.

- Có khả năng điều khiển, phân tích và tìm kiếm các thông tin quản lý thích hợp.

Trong kiến trúc phân lớp cuả NGN, tầng dịch vụ NGN cung cấp các chức năng điều khiển và quản lý dịch vụ mạng tới từng ứng dụng và người sử dụng đầu cuối. Tầng truyền tải truyền các thông tin giữa các thực thể và vùng quản lý gồm các mặt bằng để quản lý thông tin, chức năng và khía cạnh vật lí của các thực thể NGN. Các chức năng của tầng truyền tải được mô tả chi tiết trong NGN-FG II và nằm ngoài phạm vi của tài liệu này. Các chức năng quản lý hệ thống là nền tảng điều hành của NGN, các chức năng cung cấp khả năng quản lý NGN để cung cấp các dịch vụ NGN với chất lượng, độ bảo mật và độ tin cậy mong muốn của người sử dụng dịch vụ NGN. Các công nghệ này được bố trí phân tán trong các thực thể chức năng FE (Function Entity) và chúng tương tác với các chức năng quản lý phần tử mạng NE (Network Element), quản lý mạng và quản lý dịch vụ. Các chức năng quản lý thực hiện điều hành trên tầng truyền tải và tầng dịch vụ. Trong các tầng này các chức năng cơ bản gồm 5 vùng cơ bản: Quản lý lỗi, quản lý cấu hình, quản lý tài khoản, quản lý hiệu năng và quản lý bảo mật.

1.2 CÁC YÊU CẦU QUẢN LÍ MẠNG

Các cơ chế quản lý mạng được nhìn nhận từ hai góc độ, góc độ mạng chỉ ra hệ thống quản lý nằm tại các mức cao của mô hình OSI và từ phía người điều hành quản lý hệ thống. Mặc dù có rất nhiều quan điểm khác nhau về mô hình quản lý nhưng chúng đều thống nhất bởi ba chức năng quản lý cơ bản gồm: giám sát, điều khiển và đưa ra báo cáo tới người điều hành.

- 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, đánh giá hoặc tìm kiếm, tra cứu thông tin được báo cáo.

Trong thực tế, tuỳ 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.

Dưới góc độ của người điều hành quản lý mạng, một số yêu cầu cơ bản thường được đặt ra gồm:

- Khả năng giám sát và điều khiển mạng cũng như các thành phần của hệ thống thiết bị 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 .

1.2.1 Các kịch bản quản lý mạng

Nhiệm vụ quản lý mạng luôn gắn liền với kiến trúc mạng thực tiễn, vì vậy rất nhiều kịch bản khác nhau đã được triển khai trên các nền mạng thực tiễn. Một số yêu cầu quản lý được chỉ ra sau đây gồm: mạng khách hàng, lưu trữ dữ liệu phân tán, hệ thống bản đồ số tập trung và các hệ thống tài liệu chia sẻ, và hệ thống trợ giúp điều hành.

A, Yêu cầu quản lý khách hàng

Một hệ thống cung cấp dịch vụ tới khách hàng của các nhà cung cấp thường được phân cấp theo hợp đồng và theo dịch vụ gắn với các kỹ thuật khác nhau. Thông tin quản lý từ một số nguồn tài nguyên mức thấp yêu cầu sử dụng dịch vụ, các bộ tạo báo cáo lỗi, giám sát hiệu năng và quản lý các dịch vụ được cung cấp tại mức cao nhất của mối quan hệ giữa khách hàng và nhà cung cấp.

Quản lý mạng khách hàng định nghĩa sự chuyển dịch từ vấn đề quản lý phần tử tới vấn đề quản lý liên quan tới dịch vụ. Một số yêu cầu cơ bản được chỉ ra dưới đây:

- Mỗi nhà cung cấp dịch vụ phải quản lý được mạng của họ và một phần tích hợp trong đó là quản lý thành phần, liên quan tới việc giám sát độ khả dụng, mức độ sử dụng dung lượng, bảo mật và xác định lỗi các phần tử. Thêm vào đó là các nhiệm vụ quản lý liên quan tới chức năng của toàn mạng như định tuyến, ghép kênh, giám sát các kênh.
- Tại điểm truy nhập tới mạng, các dịch vụ cung cấp thường được dựa trên thỏa thuận mức dịch vụ thể hiện chất lượng dịch vụ cung cấp. Tại đó, nhiệm vụ quản

lý được thực hiện dựa trên việc giám sát chất lượng dịch vụ. Các giao diện khách hàng-nhà cung cấp cũng bao gồm các thủ tục báo cáo lỗi, tương thích dịch vụ hoặc cung cấp dịch vụ.

Trong kịch bản này, các khách hàng có thể truy nhập các thông tin quản lý đặc thù, ví dụ như chất lượng dịch vụ, khả năng sử dụng dịch vụ để phát triển các dịch vụ gia tăng giá trị hoặc dịch vụ mới. Cơ sở thông tin quản lý MIB (Management Information Base) do khách hàng sử dụng phải phản ánh được các dịch vụ và thoả thuận mức dịch vụ.

B, Lưu trữ dữ liệu phân tán

Một kịch bản thường sử dụng cho lưu trữ dữ liệu của các hệ thống là lưu trữ dữ liệu phân tán tại các vị trí khác nhau. Các hệ thống lưu trữ dữ liệu như vậy là một phần của hệ thống dữ liệu phức tạp, có các hệ thống file và cho phép truy nhập dữ liệu. Nếu một mạng gồm các hệ thống có cấu trúc khác nhau hoặc được cung cấp bởi các nhà cung cấp dịch vụ khác nhau thì hệ thống sẽ được bổ sung thêm một số chi tiết như các tham số hệ thống khác nhau mà người điều hành mạng thiết lập qua quản lý . Đảm bảo tính riêng tư và tính tuần tự của dữ liệu cũng là các yêu cầu cần đặt ra trong kịch bản này. Khía cạnh bảo mật chịu trách nhiệm cho tính riêng tư của dữ liệu kể cả các dữ liệu dự phòng, cập nhật và lưu trữ. Các chính sách được ứng dụng trong các hệ thống di chuyển dữ liệu từ các vùng khác nhau tại các mức phân cấp dữ liệu khác nhau.

C, Bản đồ số tập trung

Một hệ thống tìm kiếm khác cung cấp chức năng quản lý mạng hoàn toàn khác biệt là hệ thống bản đồ số tập trung. Hệ thống cơ sở dữ liệu bản đồ số cần một số nhiệm vụ quản lý như sau:

- Thiết lập một cấu trúc thư mục thích hợp gồm các dịch vụ thư mục.
- Tạo các máy chủ lưu trữ tạm thời truy nhập nhanh tại trung tâm.
- Tích hợp các chiến lược cache và cho phép chúng thay đổi.
- Định nghĩa và điều hành các thủ tục truy nhập độc lập với hạ tầng.
- Đảm bảo tính bảo mật thông qua các thủ tục nhận thực, trao quyền và mã khóa.
- Bảo vệ các vùng mạng riêng thông qua tường lửa hoặc các phương pháp riêng thích hợp.

D, Hệ thống chia sẻ tài liệu

Hệ thống chia sẻ tài liệu gồm hệ thống lưu trữ và hệ thống tìm kiếm nhanh với độ khả dụng lớn tới 98% trong thời gian làm việc. Các nhiệm vụ quản lý trong kịch bản này gồm:

- Giám sát các tham số QoS phù hợp với các yêu cầu SLA.
- Quản lý ứng dụng (phân tán phần mềm, tham số cung cấp cho cập nhật hệ thống tìm kiếm, hoạt động điều hành các ứng dụng tìm kiếm phân tán)

- Quản lý hệ thống và mạng: bảo mật của hoạt động hạ tầng và cập nhật dữ liệu.
- Quản lý người sử dụng và báo cáo các thông tin liên quan tới QoS.

E, Hệ thống trợ giúp người điều hành

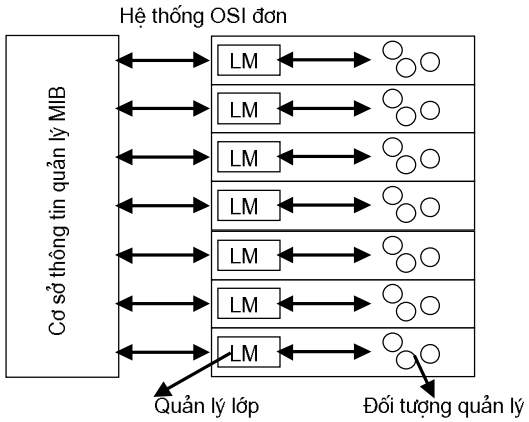
Giám sát lỗi là một tiến trình phức tạp và tiêu tốn thời gian do độ phức tạp của các hệ thống phân tán và các dịch vụ truyền thông. Các nhà cung cấp hạ tầng thường đưa ra các hệ thống trợ giúp, đường dây nóng, các máy chủ cuộc gọi để trợ giúp điều hành. Các bộ công cụ khác nhau thường được có sẵn trong hệ thống trợ giúp, công cụ tích cực sử dụng để giám sát hoặc điều khiển một hệ thống phân tán, công cụ thụ động hỗ trợ các trung tâm cuộc gọi gồm các hệ thống tài liệu và các báo cáo lỗi.

1.2.2 Các chức năng quản lý mạng

Các tổ chức tiêu chuẩn và các nhà cung cấp thiết bị đưa ra các hệ thống mạng khác nhau, vì vậy các chức năng quản lý mạng cũng rất đa dạng và biến đổi theo từng môi trường quản lý thực tế. Dưới góc độ tổng quan, các chức năng quản lý mạng thường được tham chiếu và triển khai theo mô hình kết nối hệ thống mở OSI (Open System Interconnection). Các chức năng quản lý hệ thống được phân lớp và được định nghĩa bởi các nhà quản lý mạng. Tập chức năng này phụ thuộc vào yêu cầu quản lý và gắn liền với các ứng dụng. Hệ thống quản lý mạng theo OSI là một tập các tiêu chuẩn quản lý mạng do tổ chức tiêu chuẩn quốc tế ISO (International Standard Organization) thực hiện. Một loạt các khuyến nghị được tổ chức này đưa ra bao hàm cả khung quản lý , giao thức và dịch vụ truyền thông quản lý , và cấu trúc của thông tin quản lý (serial X.7xx). Mô hình trao đổi thông tin quản lý được thực hiện trong 3 vùng phân cấp: quản lý hệ thống, quản lý lớp và điều hành lớp.

Nhiệm vụ quản lý hệ thống được thực hiện từ lớp ứng dụng và sử dụng khái niệm thực thể quản lý ứng dụng hệ thống SAME (System Application Management Entity) để quản trị hệ thống. Các giao thức lớp ứng dụng luôn là giao thức quan trọng nhất trong mô hình này, chúng có khả năng trao đổi các thông tin quản lý đáp ứng các yêu cầu quản lý và là cách tiếp cận nhanh nhất của người quản lý hệ thống với hệ thống. Nhiệm vụ quản lý lớp của mô hình OSI thực hiện quản lý các đối tượng thuộc lớp và trao đổi thông tin qua hệ thống giao thức tới các lớp kế cận.

Đối tượng bị quản lý nằm trong các lớp khác nhau thuộc mô hình OSI và thông tin quản lý nằm trong cơ sở dữ liệu thông tin quản lý MIB (Management Information Base). MIB được coi là một dạng cơ sở dữ liệu, nội dung của cơ sở dữ liệu này không chứa đối tượng bị quản lý mà chỉ chứa các thông tin liên kết với các đối tượng này. Hệ thống quản lý lớp thực hiện duy trì mối liên kết giữa đối tượng bị quản lý và thông tin trong cơ sở dữ liệu. Vì vậy, nếu xuất hiện lỗi tại lớp quản lý thì thông tin trong cơ sở dữ liệu không phản ánh đúng thực trạng quản lý của hệ thống.

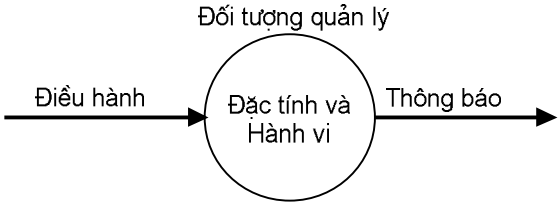


Hình 1.1: Mô hình hệ thống quản lý theo OSI

Các khía cạnh quản lý của mô hình OSI được chỉ ra gồm: thông tin, tổ chức, chức năng và truyền thông.

- Khía cạnh thông tin của mô hình quản lý hệ thống chỉ ra phương pháp trao đổi thông tin và phương pháp truy nhập tài nguyên quản lý của các lớp. Đối tượng bị quản lý được thể hiện qua các đặc tính nguyên thủy của đối tượng và hành vi của đối tượng.Các đối tượng bị quản lý được định nghĩa như là các thực thể lớp, các đấu nối, các thiết bị phần cứng. Hệ thống quản lý sẽ chỉ xem xét tới các đặc tính của đối tượng quản lý để thực hiện chức năng quản lý hệ thống.

- Mô hình quản lý theo OSI được tổ chức theo nguyên tắc tập trung, một khối quản lý có thể quản lý và điều hành một số đại diện quản lý (Agent). Môi trường quản lý OSI có thể phân vùng quản lý theo chức năng, vị trí địa lí hoặc công nghệ mạng. Vì vậy, các nhà quản trị mạng có thể hoàn toàn đưa ra các cấu hình khác nhau trong cách thức quản lý của họ.



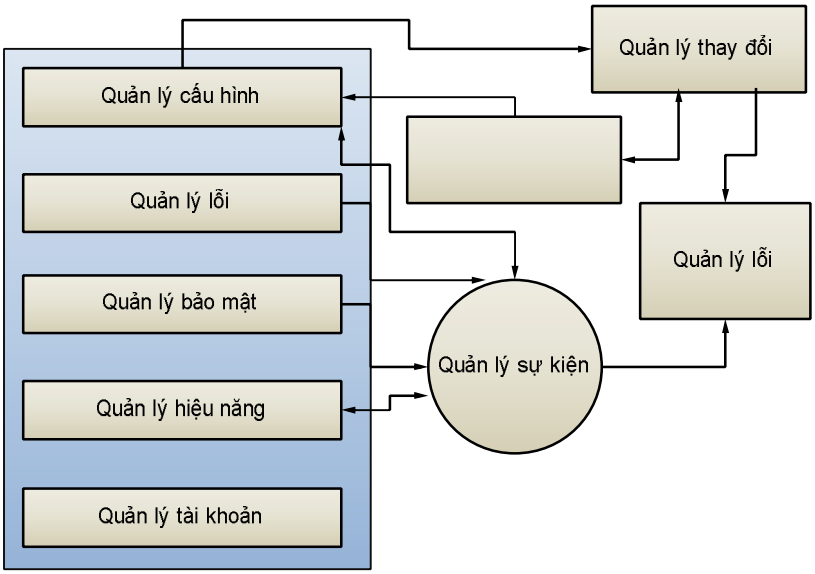
Hình 1.2: Quan hệ quản lý đối tượng

- Khía cạnh truyền thông trong mô hình quản lý OSI được định nghĩa trong chuẩn giao thức dịch vụ thông tin quản lý chung CMIS (Common Management Information Services). CMIS định nghĩa các dịch vụ cơ bản như: khôi phục thông tin quản lý , thay đổi đặc tính của đối tượng bị quản lý (thông qua agent), xoá bỏ và tạo ra các đối tượng quản lý mới, báo cáo các sự kiện trong quá trình quản lý .

  Các yêu cầu cơ bản trong khía cạnh truyền thông gồm: độ khả dụng, khả năng hoạt động liên kết, khả năng di chuyển và khả năng phân cấp.

- Độ khả dụng thể hiện 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.
- 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.
- 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 khi có sự thay đổi môi trường tính toán.
- Khả năng nâng cấp là khả năng đáp ứng khi hệ thống nâng cấp, mở rộng phạm vi quản lý , biến động của người sử dụng, các chức năng quản lý mà không thay đổi toàn bộ thiết kế ban đầu.

- Khía cạnh chức năng của mô hình quản lý được chia thành 5 vùng gồm có: Quản lý cấu hình, quản lý hiệu năng, quản lý lỗi, quản lý bảo mật và quản lý tài khoản. Kiến trúc quản lý theo ISO được thể hiện trên hình 1.3.



Hình 1.3: Các khối chức năng của kiến trúc quản lý theo ISO

- Quản lý cấu hình gồm các tiến trình xác định và xử lí các tham số thay đổi của các thiết bị và phương tiện truyền thông nhằm duy trì hoạt động chức năng của mạng. Các tham số có thể đặt, khởi tạo lại, hoặc đơn giản chỉ là hiển thị tham số cho người quản lý . Các hệ thống quản lý thông qua giao thức điều khiển quản lý để đưa ra các lệnh tới các thiết bị quản lý .
- Quản lý lỗi là một tiến trình phát hiện lỗi, xác định lỗi, cách ly lỗi và sửa lỗi. Bước quan trọng nhất trong quản lý lỗi là phát hiện các điều kiện bất bình thường của các thiết bị. Phát hiện lỗi có thể được thực hiện bằng nhiều phương

pháp gồm việc đặt ngưỡng cho các kiểu cảnh báo khác nhau hoặc từ các thông tin từ phía người sử dụng dịch vụ. Bước cuối cùng của quá trình quản lý lỗi có thể liên quan tới tiến trình thay đổi các tham số cho phù hợp trong quản lý cấu hình.

- Quản lý hiệu năng gồm một số tác vụ yêu cầu đánh giá mức sử dụng của các thiết bị mạng và phương tiện truyền dẫn và đặt các tham số phù hợp với yêu cầu thực tế. Quản lý hiệu năng sử dụng các thông tin giám sát thiết bị hoặc thông qua cơ sở dữ liệu trong quá trình thống kê. Quản lý hiệu năng liên quan mật thiết với quá trình quy hoạch mạng.
- Quản lý bảo mật mô tả một tập các tác vụ nhằm đảm bảo nhận thực người sử dụng và thiết bị, nén dữ liệu, phân bổ khoá bảo mật, duy trì và giám sát bản ghi bảo mật, phát hiện và ngăn chặn các xâm phạm không cho phép.
- Quản lý tài khoản liên quan tới quá trình tính cước và hoá đơn sử dụng dịch vụ, quản lý tài khoản cung cấp phương pháp tính phù hợp các yêu cầu của người sử dụng và hiện trạng mạng.

1.2.3 Khía cạnh tổ chức của quản lý mạng

Vấn đề quản lý các hạ tầng công nghệ truyền thông không chỉ xem xét từ các góc độ kỹ thuật mà còn là giải pháp tích hợp cho toàn bộ các đặc tính của mạng. Tiếp cận tích hợp gồm các giải pháp trong các lớp của mô hình quản lý , tương thích với cấu trúc của tổ chức quản lý như:

- Định nghĩa tiến trình quản lý hỗ trợ tiến trình kinh doanh với nhiều luật khác nhau.
- Định nghĩa các vùng có các chính sách quản lý và thủ tục quản lý riêng biệt.
- Xác định các giao diện giữa các vùng nhằm trao đổi thông tin quản lý và các hoạt động quản lý .
- Quy hoạch và thiết lập hạ tầng quản lý nhằm định ra các thủ tục cải thiện tiến trình quản lý và các công cụ quản lý cần thiết.
- Thiết lập một cấu trúc tổ chức và điều hành để thực hiện quản lý . Bao gồm các hệ thống điều hành, quản trị, lập kế hoạch, phân tích và trợ giúp điều hành.

Thuật ngữ điều hành được sử dụng để tham chiếu tới các điều kiện cụ thể của vấn đề quản lý kỹ thuật trong môi trường mạng. Khái niệm điều hành định nghĩa các ứng dụng quản lý phân tán cùng với các nhiệm vụ, công việc được chỉ định cho các đơn vị của tổ chức, các thủ tục và luồng thông tin.

Các hạ tầng thông tin có thể được cấu trúc thành các vùng (phân vùng logic) dựa trên:

- Sự khác biệt của các tổ chức hoặc công ty là các phần của môi trường quản lý . Ví dụ các nhà khai thác, nhà cung cấp dịch vụ internet, nhà cung cấp công cụ quản lý và các tổ chức người sử dụng.
- Cấu trúc có tổ chức của một công ty gồm các nhóm, khối và các vùng điều hành.
- Các điều kiện địa lý
- Các lĩnh vực kinh doanh
- Các khía cạnh xử lý dữ liệu
- Các kiểu tài nguyên, ví dụ như: phần cứng, hệ thống phần mềm, các phần mềm ứng dụng, dữ liệu, hạ tầng kỹ thuật .

Thiết lập các vùng cũng có nghĩa tạo ra các nhóm của đối tượng bị quản lý . Các nhóm này được gán các công việc khác nhau như lập kế hoạch, lựa chọn, thu thập thông tin, cung cấp và cải thiện, điều hành, bảo dưỡng và tương thích.

Khi một tổ chức quản lý được cung cấp, nó gồm các vấn đề liên quan tới trách nhiệm của các đơn vị trong tổ chức. Sự phân bổ các chức năng nhiệm vụ đóng vai trò quan trọng để xác định yếu tố truyền thông cần thiết cho quản lý cũng như là độ phức tạp của vấn đề bảo mật trong quản lý . Một vài mô hình thông dụng gồm quản lý tập trung, phân cấp và phân tán thường được ứng dụng trong các mô hình tổ chức quản lý .

1.2.4 Khía cạnh thời gian của quản lý mạng

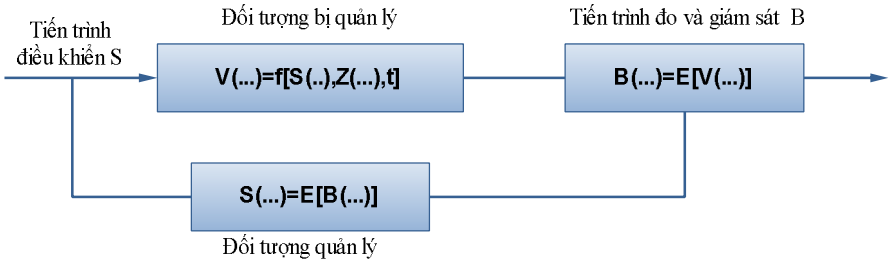
Khía cạnh thời gian là một vấn đề luôn được đặt ra và quan tâm trong các hoạt động quản lý mạng. Yếu tố thời gian tác động tới hàng loạt các vấn đề như lập kế hoạch, cung cấp, điều hành và thay đổi các nhiệm vụ quản lý mạng.

Trong giai đoạn xử lý lập kế hoạch, một loạt bước xử lý khác nhau thường được đặt ra như sau:

- Phân tích ứng dụng: Bước này xác định loại hình dịch vụ sẽ được cung cấp. Các dịch vụ được đặc trưng bởi các định nghĩa theo chức năng và chất lượng dịch vụ.
- Phân tích mức ưu tiên yêu cầu: Phân tích mức ưu tiên chỉ ra cách thức phân bổ tài nguyên hệ thống cho người sử dụng và liên quan tới cấu hình và các mối quan hệ lưu lượng.
- Phân tích kích thước yêu cầu: Bước xử lý này xác định khả năng phân bổ dữ liệu từ một mốc thời gian và mức tăng trưởng theo thời gian.
- Phân tích thành phần: Phân tích thành phần thiết lập kiểu và số lượng các thành phần được đưa vào hệ thống phân tán gồm các đặc tính giao diện và phần mềm.
- Phân tích các điều kiện khác: Một số các điều kiện khác có thể ảnh hưởng tới vấn đề lập kế hoạch và lựa chọn sản phẩm bao gồm: bảo vệ đầu tư, thời gian

khả dụng, các yêu cầu bảo vệ dữ liệu, khả năng mở rộng, giá thành, phát triển công nghệ, chiến lược thị trường và tiêu chuẩn hóa.

- Lập kế hoạch đưa hệ thống vào hoạt động: Đây là một tiến trình xử lý gồm rất nhiều vấn đề: kiểm ta các thủ tục điều hành, xác lập tính tương thích trong lưu đồ tổ chức, lập kế hoạch lắp đặt phần cứng và phần mềm, v.v. Giai đoạn kiểm tra tính tương thích tác động ngược tới các giai đoạn lập kế hoạch khác. Các thông số kiểm tra được phản hồi trong các mạch vòng hồi tiếp tới các giai đoạn khác của tiến trình lập kế hoạch. Khía cạnh thời gian của của các đối tượng bị quản lý có thể nhận thấy qua các mạch vòng hồi tiếp kết quả (hình 1.4).



B: Kết quả điều khiển
F: Các luật phân tích và đo cho giám sát
E: Bộ hỗ trợ quyết định điều hành
S: Tiến trình điều khiển
Z: Trạng thái của đối tượng bị quản lý
V: Hành vị đối tượng bị quản lý
t: Thời gian

Hình 1.4: Khía cạnh thời gian của đối tượng bị quản lý

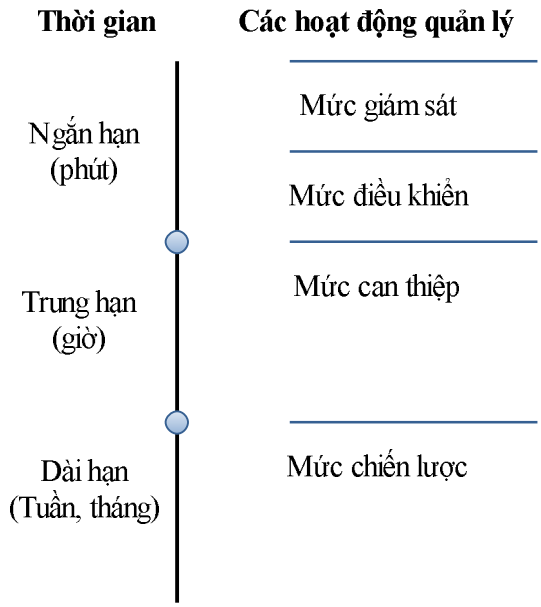
Các nguồn tài nguyên được điều khiển thông qua sự thay đổi các tham số nhận được trong quá trình quản lý . Kết quả đo được đánh giá bởi người quản lý hoặc hệ thống quản lý (bao gồm cả phân tích sự kiện và phân tích ngưỡng) có thể sử dụng để khởi tạo một quy trình quản lý mới.

Các hoạt động khác nhau được đặt trong các khoảng thời gian khác nhau trong giai đoạn điều hành hệ thống có thể gán vào trục thời gian như trên hình 1.5.

- Phạm vi ngắn hạn: Các nhiệm vụ ngắn hạn gồm các phép đo được thực hiện trong thời gian tính bằng giây hoặc phút. Các nhiệm vụ này gồm các nhiệm vụ giám sát trong thời gian ngắn để đảm bảo các mục tiêu điều hành như đảm bảo tính bảo mật hoặc độ khả dụng, hoặc xử lý bản tin lỗi và thay thế tài nguyên dự phòng.
- Phạm vi trung hạn: Các nhiệm vụ trung hạn được thực hiện theo chu kỳ tính bằng giờ. Trong khi các nhiệm vụ ngắn hạn thường được xử lý bởi các hệ thống quản lý tự động thì nhiệm vụ trung hạn thường do các chuyên gia quản lý đảm trách. Ví dụ các nhiệm vụ chẩn đoán lỗi, kiểm tra hệ thống, thay đổi cấu hình, kích hoạt và dừng hoạt động các module, thu thập và đánh giá dữ liệu đo ngắn hạn.

- Phạm vi dài hạn: Thời gian dài hạn được tính theo tuần hoặc tháng. Mục tiêu của các nhiệm vụ dài hạn là để sử dụng kinh nghiệm thu nhận được qua thời gian để cải thiện điều hành trong tương lai. Lập kế hoạch chính là khía cạnh then chốt trong phạm vi dài hạn này. Các nhiệm vụ dài hạn thường là nhiệm vụ bảo dưỡng, phân tích chiến lược và lập kế hoạch dung lượng.

Các dịch vụ tại mức giám sát có thể xác định các kiểu lỗi ngắn hạn, các dịch vụ tại mức can thiệp điều khiển sẽ nằm trong giai đoạn trung hạn. Mức điều khiển được đưa vào giữa mức giám sát và mức can thiệp đối với một số dịch vụ. Các dịch vụ dài hạn được coi là các mức chiến lược.



Hình 1.5: Khía cạnh thời gian và các hoạt động quản lý

Việc phân chia thời gian không chỉ nhận dạng các hoạt động quản lý mà còn đóng vai trò quan trọng cho các quá trình tạo công cụ và cơ sở dữ liệu. Vì vậy, đối với rất nhiều nhiệm vụ giám sát, các chu kỳ giám sát được quy định bởi khung thời gian. Khung thời gian này xác định những điểm cơ bản của các giải pháp với các tham số chuẩn và tính tuần tự tác động tới kích thước bộ đếm, kích thước bộ đệm, tần suất đo, độ chính xác của phép đo và các thủ tục phân tích. Nó cũng ảnh hưởng tới khía cạnh truyền thông và phân phối thông tin quản lý . Thời gian quản lý cũng ảnh hưởng tới các vấn đề quản lý số liệu lưu trữ.

1.3 CÁC CÁCH TIẾP CẬN TRONG QUẢN LÍ MẠNG

1.3.1 Các phương pháp tiếp cận quản lý mạng

Kiến trúc hệ thống quản lý mạng rất phức tạp và chủ yếu phụ thuộc vào kiến trúc hệ thống mạng, không có một luật hoặc một kỹ thuật cụ thể nào được coi là bắt buộc đối với các hệ thống mạng. Một số hướng tiếp cận được chỉ ra sau đây:

A, Quản lý hiện

Nếu hệ thống quản lý được con người khởi tạo và quản lý , phương pháp quản lý mạng này được gọi là quản lý hiện. Người quản lý sẽ khởi tạo quá trình và thực hiện quản lý trong suốt thời gian quản lý , có thể có một số chức năng tự động hỗ trợ cho công tác quản lý của người điều hành hệ thống nhưng vẫn được coi là phương pháp quản lý hiện. Một ưu điểm của phương pháp quản lý hiện là không cần thiết phải thiết kế chi tiết các chức năng quản lý trong giai đoạn thiết kế hệ thống, các vấn đề thực tế sẽ được người điều hành ra quyết định tuỳ thuộc vào các mục tiêu và điều kiện cụ thể trong quá trình khai thác. Như vậy, tiến trình thiết kế hệ thống sẽ giảm bớt độ phức tạp và thời gian. Quản lý hiện hữu dụng trong việc giải quyết các vấn đề không mong muốn xảy ra trong quá trình hoạt động thực tế của hệ thống, đồng thời yêu cầu các giải pháp tốt nhất được đưa ra từ phía người điều hành. Quản lý hiện rất phù hợp với chức năng quản lý lỗi. Nhược điểm của quản lý hiện là bị giới hạn khả năng xử lý và số lượng lỗi từ chính người điều hành hệ thống. Mặc dù giảm bớt được chi phí trong khâu thiết kế hệ thống nhưng lại làm tăng chi phí của giai đoạn điều hành hệ thống.

B, Quản lý ẩn

Khi hệ thống tự khởi tạo và điều hành, phương pháp quản lý này được gọi là quản lý ẩn, tất cả các chức năng quản lý được thực hiện bởi các module phần cứng và phần mềm một cách tự động. Sự khác biệt với phương pháp quản lý hiện là ở phương pháp thi hành. Về mặt nguyên tắc, hoàn toàn có thể thực hiện hai phương pháp quản lý trong cùng một hệ thống. Với các hệ thống thông minh và hệ thống chuyên gia hỗ trợ cho phương pháp quản lý ẩn, ranh giới giữa hai phương pháp quản lý được thu hẹp lại. Một số vấn đề lỗi cần phải được giải quyết bằng cả hai phương pháp đồng thời trong cả quá trình phát hiện và sửa lỗi.

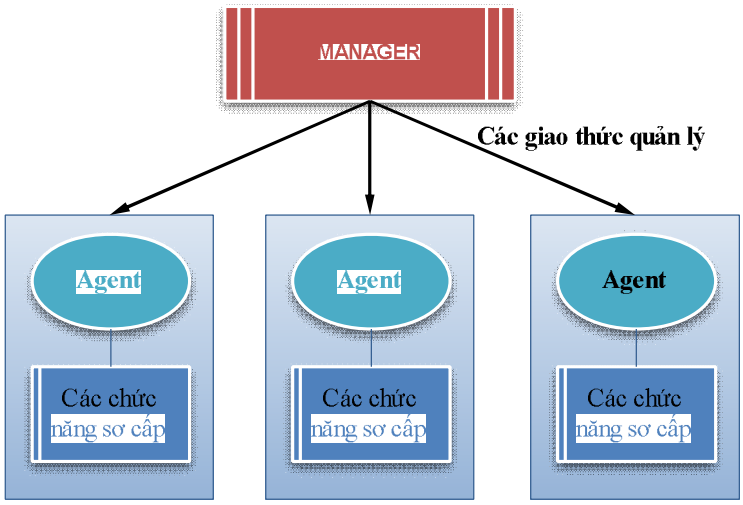
Trong giai đoạn thiết kế và điều khiển, các chức năng quản lý mạng được nhìn nhận dưới các gốc độ khác nhau. Khi giai đoạn vận hành hệ thống được bắt đầu, người sử dụng và nhà quản trị mạng phân biệt các chức năng nguyên thuỷ và các chức năng quản lý nhằm lựa chọn phương pháp quản lý theo thực tế.

C, Quản lý tập trung

Trong tiếp cận này chỉ có một thiết bị quản lý thu nhận các thông tin và điều khiển toàn bộ các thực thể mạng, ví dụ các thông tin liên quan tới các ứng dụng được lưu trữ tại một hệ thống quản lý đơn như chỉ ra trên hình 1.4. Các chức năng quản lý được thực hiện bởi manager (thiết bị quản lý), khả năng của hệ thống phụ thuộc rất lớn vào mức độ thông minh của manager. Kiến trúc này thường được sử dụng rất nhiều trong mạng hiện nay, nhất là với các mô hình doanh nghiệp có hạ tầng mạng riêng và có trung tâm quản trị mạng.

Để quản lý điều hành các chức năng sơ cấp, agent được đặt vào các hệ thống bị quản lý để thực hiện các chức năng sơ cấp nhằm hỗ trợ các chức năng khởi tạo, giám

sát và sửa đổi các hành vi của chức năng sơ cấp. So với các chức năng thuộc manager, chức năng Agent thường rất đơn giản, thông tin trao đổi từ manager tới các agent thông qua các giao thức thông tin quản lý như giao thức quản lý mạng đơn giản SNMP (Simple Network Management Protocol) và giao thức thông tin quản lý chung và dịch vụ thông tin quản lý chung CMIS/CMIP (Common Management Information Protocol), các giao thức này sẽ được thảo luận chi tiết trong chương 2. Hệ thống quản lý tập trung thường đặt trong một trạm làm việc, nếu manage lỗi hoặc hỏng thì toàn bộ hệ thống quản lý sẽ bị tê liệt, nếu lỗi chỉ xảy ra trong một phần mạng, thì một số phần tử mạng trong vùng mạng lỗi sẽ không được quản lý . Thêm vào đó, hệ thống quản lý tập trung rất khó mở rộng vì mức độ phức tạp của hệ thống tăng lên rất nhanh.



Hình 1.6: Mô hình quản lý tập trung

Một biến thể của hệ thống quản lý tập trung dựa trên tiếp cận nền gồm một mặt bằng quản lý 2 tầng: Nền tảng quản lý mạng và ứng dụng quản lý mạng. Nền quản lý mạng liên quan tới thủ tục thu thập thông tin và các tính toán đơn giản, trong khi đó ứng dụng quản lý việc sử dụng các dịch vụ cung cấp bởi nền quản lý để ra quyết định xử lý và hỗ trợ các chức năng lớp cao. Ưu điểm của tiếp cận này là các ứng dụng không phụ thuộc quá nhiều vào độ phức tạp của giao thức và sự phức tạp của thành phần mạng. Tuy nhiên, nhược điểm còn tồn tại trong mô hình này xuất phát từ khả năng mở rộng của việc quản lý tập trung. Một số đặc điểm cơ bản của mô hình này như sau:

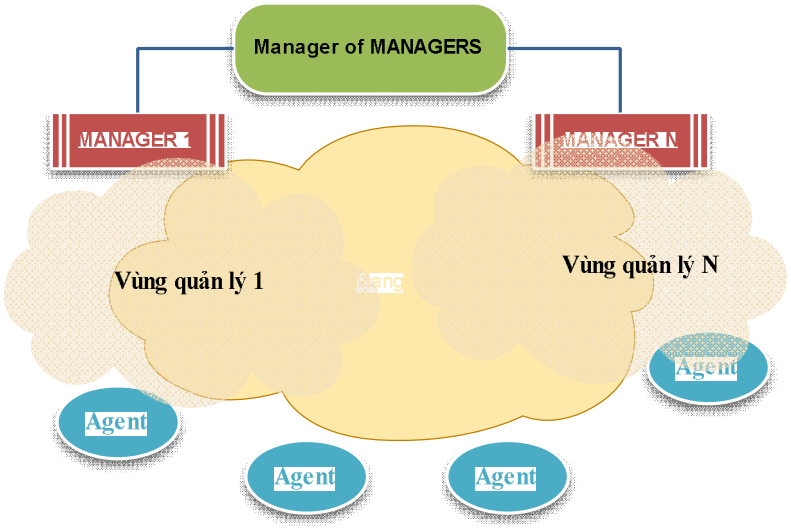
- Nền tảng quản lý mạng được đặt trên một hệ thống máy tính đơn.
- Để dự phòng hệ thống cần được lưu trữ bản sao tại một hệ thống khác.
- Hệ thống quản lý có thể truy nhập và chuyển các sự kiện tới bàn điều hành hoặc hệ thống khác.
- Thường được sử dụng cho cảnh báo và sự kiện lỗi trên mạng, các thông tin mạng và truy nhập tới các ứng dụng quản lý .

Ưu điểm:

- Quan sát cảnh báo và các sự kiện mạng từ một vị trí
- Bảo mật được khoanh vùng đơn giản

Nhược điểm:

- Lỗi hệ thống quản lý chính sẽ gây tác hại tới toàn bộ mạng.
- Tăng độ phức tạp khi có thêm các phần tử mới vào hệ thống.
- Tồn tại các hệ thống hàng đợi chờ xử lý khi có nhiều yêu cầu xử lý từ các thiết bị.



Hình 1.7: Mô hình quản lý phân cấp

D, Quản lý phân cấp

Trong tiếp cận này, hệ thống được chia thành các vùng tuỳ theo nhiệm vụ quản lý tạo ra một hệ thống phân cấp quản lý . Trung tâm xử lý đặt tại gốc của cây phân cấp, và các hệ thống phân tán được đặt tại các nhánh của cây. Hệ thống xử lý trung tâm truy nhập tới tất cả các hệ thống nhánh và chỉ ra các nhiệm vụ phân tán của nhánh. Kiến trúc phân cấp sử dụng khái niệm quản lý của quản lý và quản lý theo vùng. Mỗi một hệ thống quản lý vùng chịu trách nhiệm quản lý trong chính vùng đó và không liên quan tới các vùng khác.

Trong kiến trúc phân cấp, không có các thông tin trao đổi trực tiếp giữa các manager vùng. Kiến trúc này rất dễ mở rộng theo cả chiều rộng lẫn chiều sâu của cây phân cấp. Các đặc điểm cơ bản của hệ thống phân cấp như sau:

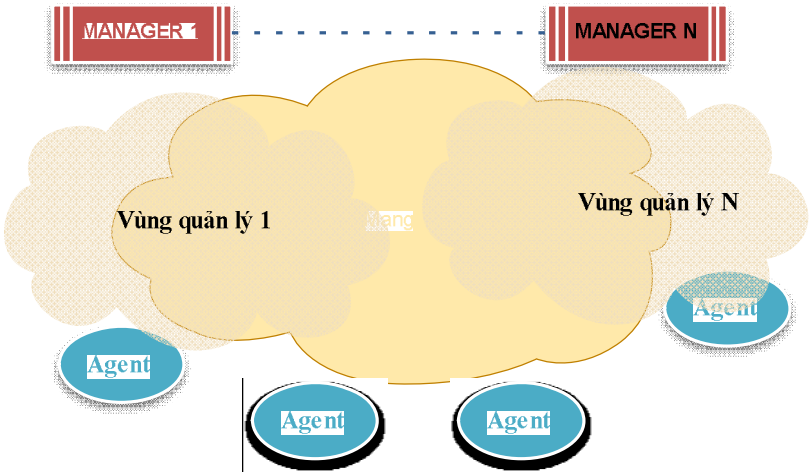
- Hệ thống quản lý vùng thường là hệ thống máy tính đa chức năng: truy nhập tới máy chủ trung tâm và đóng vai trò hoạt động như một client.
- Hệ thống quản lý không phụ thuộc vào một hệ thống đơn.
- Phân tán các chức năng quản lý mạng.
- Chức năng giám sát mạng được bố trí phân tán.
- Lưu trữ thông tin tập trung.

Ưu điểm:

- Có khả năng mở rộng hệ thống quản lý nhanh.

Nhược điểm:

- Thu thập thông tin phức tạp và tốn thời gian.
- Danh sách thiết bị quản lý bởi các client phải được xác định và cấu hình trước.



Hình 1.8: Mô hình quản lý phân tán

E, Quản lý phân tán

Hệ thống quản lý phân tán còn gọi là hệ thống quản lý ngang cấp và không có hệ thống trung tâm. Các khối quản lý đa chức năng chịu tránh nhiệm trên từng vùng mạng và trao đổi thông tin tới các hệ thống quản lý khác qua các giao thức ngang cấp. Các thiết bị quản lý sẵn sàng đưa ra các quyết định đối với các chức năng cơ sở. Bằng cách quản lý phân tán tới các trạm làm việc trên toàn mạng, công tác quản lý mạng tăng độ tin cậy và hiệu năng hệ thống trong khi giá truyền thông và tính toán giảm xuống. Tất cả các hệ thống quản lý đều thực hiện cùng một kiểu chức năng cơ sở và tương đương nhau.

Các đặc tính của hệ thống quản lý phân tán là tồn tại các hệ thống ngang cấp chạy đồng thời trên mạng số liệu. Trong giai đoạn khởi tạo mạng, mỗi một manager quản lý vùng quản lý một phần của hệ thống, vì vậy nếu số lượng hệ thống lớn, phương pháp điều khiển hiện không thể thực hiện được vì vậy quản lý phân cấp thường sử dụng hệ thống quản lý ẩn. Kiến trúc này là ý tưởng của các hệ thống tiêu chuẩn ISO và TMN.

Vấn đề xác định lỗi tổng thể và xử lý lỗi song song là các đặc tính mấu chốt của hệ thống quản lý phân tán. Một hệ thống quản lý phân tán sử dụng liên kết nối và các phần tử xử lý độc lập để tránh các điểm lỗi đơn. Với hệ thống quản lý phân tán, tỉ số hiệu năng / giá thành, độ mềm dẻo, khả năng mở rộng, tính khả dụng và độ tin cậy được nâng cao nhờ vào các chức năng đã được module hoá. Các dịch vụ phân tán có thể trong suốt với người sử dụng dịch vụ và họ không cần phân biệt đâu là dịch vụ tại

chỗ hoặc dịch vụ truy nhập từ xa. Điều này yêu cầu hệ thống quản lý phải đảm bảo tính chặt chẽ, độ an toàn cao, xác định lỗi tổng thể nhanh chóng và thời gian thực hiện nằm trong một giới hạn cho phép.

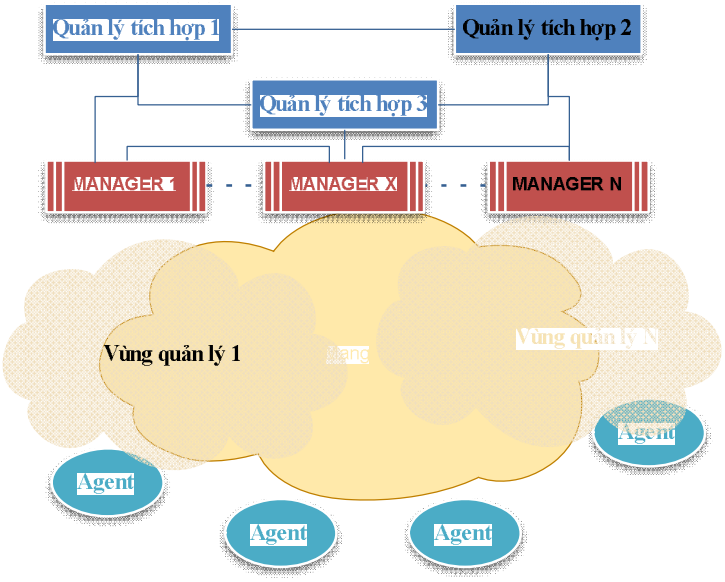
Một nhược điểm cơ bản của hệ thống quản lý phân tán xuất phát từ sự phức tạp trong vấn đề thay đổi chức năng quản lý sau khi giai đoạn điều hành được khởi tạo, vì việc thay đổi các chức năng liên quan tới quyết định quản lý , điều đó yêu cầu sửa đổi một số lượng lớn tài nguyên của các hệ thống mạng. Trong trường hợp thiếu các giải pháp quản lý chi tiết trong quá trình thiết kế, tiếp cận quản lý phân tán gặp rất nhiều khó khăn trong vấn đề đồng bộ hệ thống quản lý .

Tuy nhiên trong giai đoạn vận hành, đặc biệt là đối với một số kiểu lỗi mạng cần phải xác định thứ tự ưu tiên xử lý và không phụ thuộc vào một hệ thống cụ thể nào đó ra quyết định, phương pháp quản lý phân tán đem lại hiệu năng hơn rất nhiều so với phương pháp quản lý tập trung. Vì vậy, kiến trúc mạng thực tế thường có kiến trúc tích hợp và có các đặc điểm thường thấy như sau:

- Tổ hợp kiến trúc quản lý tập trung và kiến trúc phân tán.
- Sử dụng một số các hệ thống quản lý mạng ngang hàng trong đó mỗi nút ngang hàng có một cơ sở dữ liệu hoàn chỉnh, lưu trữ thông tin được đặt tại một vị trí và cho phép truy nhập cơ sở dữ liệu từ các vị trí.
- Phân tán các nhiệm vụ quản lý và nhiệm vụ giám sát toàn mạng.

F, Phương pháp quản lý lai ghép (hybrid)

Phương pháp quản lý lai ghép được xây dựng trên nguyên tắc tổ hợp của kiến trúc phân tán và kiến trúc phân cấp. Kiến trúc này rất thông dụng và thể hiện qua kiến trúc mạng. Mô hình phương pháp quản lý hybrid được chỉ ra trên hình 1.9.

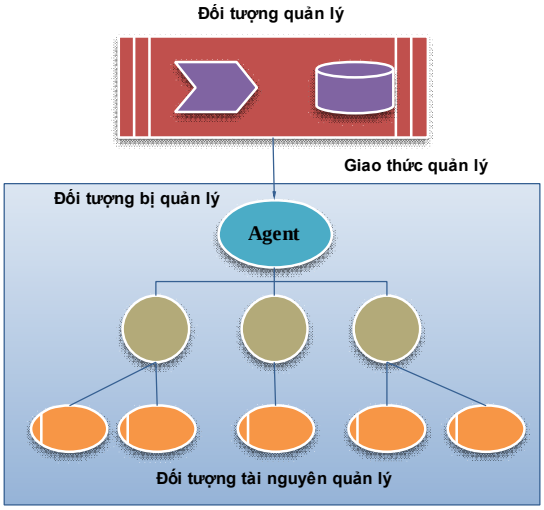


Hình 1.9: Mô hình quản lý lai ghép

Kiến trúc quản lý mạng hybrid sử dụng phương pháp quản lý gồm: các thành phần quản lý trên từng vùng và quản lý các quản lý MOM (Manage Of Manager). Trên nguyên tắc phân cấp và mối quan hệ giữa các thành phần quản lý vùng, thành phần quản lý vùng có thể thực hiện nhiệm vụ quản lý chéo giữa các vùng. Vì vậy, mô hình lai ghép rất thích hợp với môi trường có tính biến động lớn do đặc tính mềm dẻo của mô hình này.

G, Quản lý hướng đối tượng

- Quản lý hướng đối tượng được đề xuất bởi tổ chức tiêu chuẩn quốc tế ISO và tổ chức đặc trách kỹ thuật Internet IETF. Mục tiêu của quản lý hướng đối tượng tập trung vào giải quyết các vấn đề đặc biệt trong quản lý tài nguyên phân tán nhằm tạo ra một hệ thống quản lý mạng mở chung đối với các nguồn tài nguyên. Trong mô hình thông tin, thuật ngữ "đối tượng quản lý " được sử dụng nhằm trừu tượng hoá các nguồn tài nguyên vật lí và logic của thành phần quản lý và bị quản lý . Việc truy nhập đến các nguồn tài nguyên bị quản lý phải thông qua các đối tượng quản lý và đại diện quản lý .



Hình 1.10: Mô hình quản lý hướng đối tượng

Các tập đối tượng cơ bản gồm:

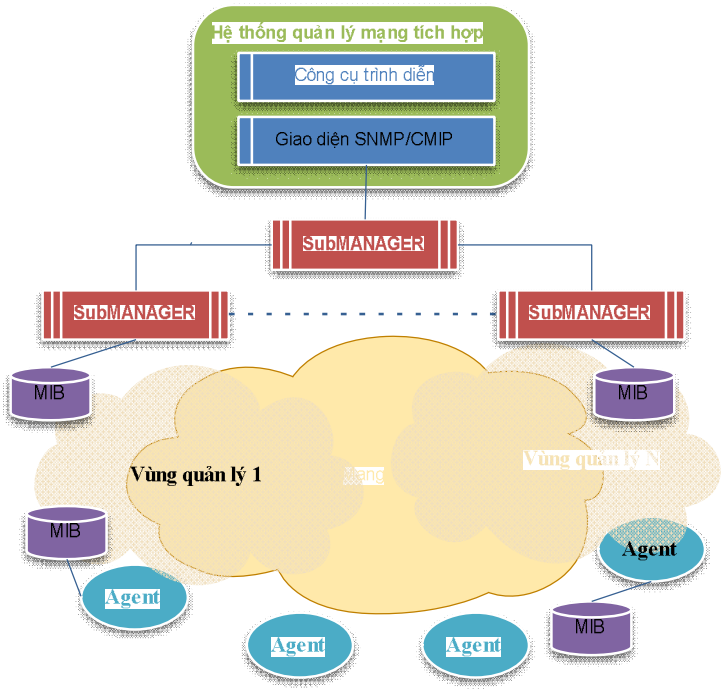
- *Đối tượng quản lý :* Đối tượng quản lý cung cấp điều khiển quản lý thông minh để thực thi các lệnh và điều khiển tài nguyên phân tán.
- *Đối tượng Agent:* Đối tượng đại diện cho thành phần bị quản lý trong ngữ cảnh quản lý , Agent cung cấp giao diện truyền thông tới đối tượng quản lý .
- *Đối tượng bị quản lý :* Các đối tượng bị quản lý cung cấp các thông tin tài nguyên mấu chốt tới đối tượng quản lý . Giao diện thuộc đối tượng bị quản lý được tiêu chuẩn hoá, gồm các luật chung để tạo và xoá các đặc tính của đối tượng bị quản lý . Đối tượng bị quản lý chịu trách nhiệm nhận các giá trị đặc tính và đặt các giá trị đặc tính cho các thực thể bị quản lý .

- *Các đối tượng tài nguyên bị quản lý :* Các đối tượng tài nguyên bị quản lý là các thực thể cụ thể trong mạng. ISO và IETF không định nghĩa cụ thể tới từng giao diện thực thể vì sự đa dạng và biến động của các thực thể.

H, Quản lý tích hợp

Tiếp cận quản lý tích hợp dựa trên tổ hợp của quản lý phân cấp, phân tán và quản lý hướng đối tượng bằng cách áp dụng kiến trúc CORBA (Common Object Request Broken Archictecture). Kiến trúc CORBA giả thiết các tập đối tượng phần mềm được phân tán trong các thực thể có khả năng tự điều khiển và kết hợp với nhau để giải quyết các lỗi trong hệ thống. Các đối tượng này được xử lý qua các ngôn ngữ hướng đối tượng (ví dụ như Smalltalk, C++ hoặc JAVA). Tập đối tượng phần mềm truyền thông với nhau thông qua các công nghệ phân tán như CORBA hoặc môi trường ngôn ngữ mở OLE (Open Language Environment).

Trong cách tiếp cận này, cấp quản lý trung gian được gọi là SubManager hoạt động như một phần tử trung gian giữa Manager và Agent hướng về phía Agent. SubManager có thể kiểm tra độc lập các giá trị quản lý của các cơ sở dữ liệu thông tin quản lý MIB (Management Information Base) bằng các giao thức quản lý . SubManager thu nhận các thông tin nguyên thuỷ từ các Agent và thực hiện tính toán, xử lý các giá trị cần thiết cho Manager. Phương pháp này giảm lưu lượng thông tin mức cao phải chuyển tới Manager.



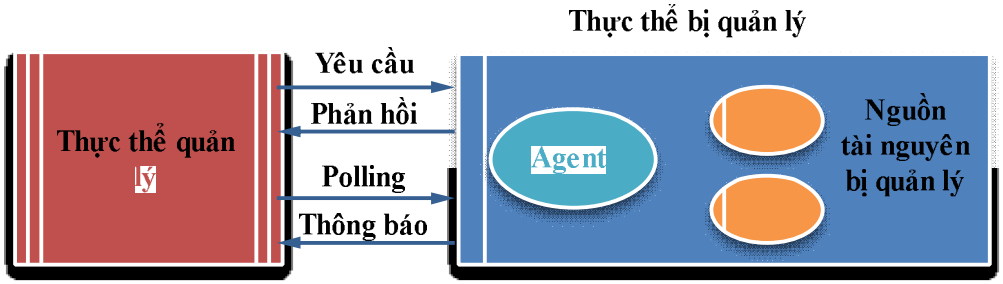
Hình 1.11: Mô hình quản lý tích hợp

Khi áp dụng kiến trúc CORBA vào tiếp cận quản lý tích hợp, nó cho phép trao đổi thông tin quản lý trực tiếp tới các Agent. CORBA coi toàn bộ các SubManager và Agent là đối tượng quản lý , trong từng trường hợp cụ thể mà các quyết định được đưa

ra qua SubManager hoặc không nhằm tránh các hiện tượng tắc nghẽn khi hệ thống trong điều kiện bất thường.

1.3.2 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. Khối quản lý sẽ yêu cầu đại diện quản lý (Agent) gửi 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. Cơ chế này 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 1.12: 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.

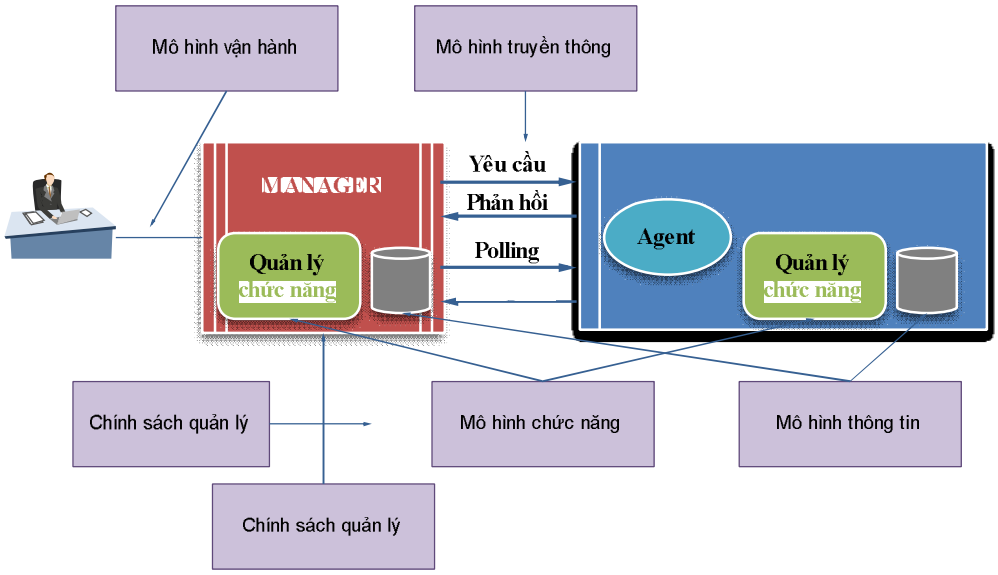
1.3.3. Mô hình quan hệ Manager-agent

Một hệ thống quản lý mạng xây dựng trên mô hình Manager-Agent được xây dựng không chỉ dựa trên mô hình truyền thông mà còn liên quan tới hàng loạt các mô hình khác như: mô hình kiến trúc, mô hình tổ chức, mô hình chức năng và mô hình thông tin (hình 1.13).

Mô hình kiến trúc sử dụng để thiết kế, cấu trúc các thành phần tham gia vào tiến trình quản lý . Trong mô hình kiến trúc, Manager đóng vai trò 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 cảnh báo tới người điều hành.

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 đảm nhiệm các chức năng cơ bản như quản lý cấu hình, hiệu năng, lỗi và các tác vụ hỗ trợ quản lý mức cao. 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.



Hình 1.13: Mô hình quan hệ Manager-Agent

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 chung cũng như hệ thống quản lý mạng khách hàng. Mô hình này thể hiện 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 cốt lõi của vấn đề quản lý . Mô hình thông tin đưa ra các tóm tắt về các nguồn tài nguyên được quản lý dưới dạng thông tin chung mà các manager và agent đều có thể hiểu được. Mô hình thông tin cũng xây dựng một cơ sở dữ liệu 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 lí 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. Khi tham khảo tới một MIB cá biệt nào

đó có nghĩa là thủ tục 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. Dựa trên cơ sở chuẩn hoá thông tin này, manger tiến hành thực hiện quản lý qua các giao thức chuyên biệt và truyền thông với các agent phân tán trên cùng một MIB.

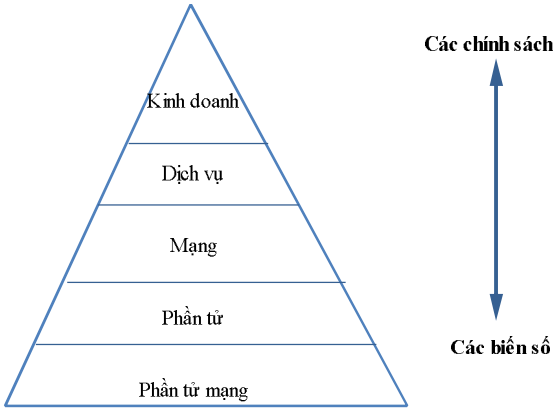
1.4 KIẾN TRÚC QUẢN LÍ MẠNG

1.4.1 Kiến trúc quản lý mạng

Quản lý mạng gồm một tập các chức năng để điều khiển, lập kế hoạch, liên kết, triển khai và giám sát tài nguyên mạng. Quản lý mạng có thể được nhìn nhận như một cấu trúc gồm nhiều lớp:

- Quản lý kinh doanh: Quản lý khía cạnh kinh doanh của mạng ví dụ như: ngân sách/ tài nguyên, kế hoạch và các thỏa thuận.
- Quản lý dịch vụ: Quản lý các dịch vụ cung cấp cho người sử dụng, ví dụ các dịch vụ cung cấp bao gồm việc quản lý băng thông truy nhập, lưu trữ dữ liệu và các ứng dụng cung cấp.
- Quản lý mạng: Quản lý toàn bộ thiết bị mạng trong mạng.
- Quản lý phần tử: Quản lý một tập hợp thiết bị mạng, ví dụ các bộ định tuyến truy nhập hoặc các hệ thống quản lý thuê bao.
- Quản lý phần tử mạng: Quản lý từng thiết bị đơn trong mạng, ví dụ bộ định tuyến, chuyển mạch, Hub.

Kiến trúc này là tiếp cận *top to down* với các thành phần trừu tượng nằm tại lớp cao của kiến trúc và các thành phần cụ thể nằm tại lớp thấp. Đối với các thành phần trìu tượng, các đặc tính quản lý cũng được thực hiện trong ngữ cảnh trừu tượng ví dụ như chính sách. Trong khi đó, các lớp thấp được quản lý qua các biến và tham số.



Hình 1.14: Phân cấp kiến trúc quản lý mạng

Quản lý mạng có thể chia thành hai chức năng cơ sở: truyền tải thông tin quản lý qua hệ thống và quản lý các phần tử thông tin quản lý mạng. Các chức năng này gồm

các nhiệm vụ khác nhau như: Giám sát, cấu hình, sửa lỗi và lập kế hoạch được thực hiện bởi nhà quản trị hoặc nhân viên quản lý mạng.

1.4.2 Cơ chế quản lý mạng

Cơ chế quản lý mạng bao gồm cả các giao thức quản lý mạng, các giao thức quản lý mạng cung cấp các cơ chế thu thập, thay đổi và truyền các dữ liệu quản lý mạng qua mạng. Hai giao thức thường được dùng phổ biến hiện nay là: giao thức quản lý mạng đơn giản SNMP và giao thức thông tin quản lý chung CMIP. Trong đó, giao thức quản lý mạng SNMP thường được sử dụng phổ biến hơn giao thức CMIP trong các hệ thống quản lý cho mạng công cộng và mạng thương mại. Thông qua các câu lệnh, giao thức SNMP thực hiện quá trình thu thập thông tin và đặt các bẫy cảnh báo cho thiết bị (các chức năng chi tiết của SNMP được thể hiện trong chương 2). Các tham số truy nhập qua SNMP được nhóm vào trong các bảng cơ sở thông tin quản lý MIB. CMIP cũng thực hiện quá trình thu thập và cài đặt tham số tương tự như SNMP nhưng cho phép nhiều kiểu điều hành hơn và vì vậy cũng phức tạp hơn SNMP.

Các cơ chế giám sát nhằm để xác định các đặc tính của thiết bị mạng, tiến trình giám sát bao gồm thu thập được và lưu trữ các tập con của dữ liệu đó. Dữ liệu thường được thu thập thông qua polling hoặc tiến trình giám sát gồm các giao thức quản lý mạng.

Xử lý dữ liệu sau quá trình thu thập thông tin quản lý mạng là bước loại bỏ bớt các thông tin dữ liệu không cần thiết đối với từng nhiệm vụ quản lý . Sự thể hiện các thông tin quản lý cho người quản lý cho phép người quản lý nắm bắt hiệu quả nhất các tính năng và đặc tính mạng cần quản lý . Một số kỹ thuật biểu diễn dữ liệu thường được sử dụng dưới dạng ký tự, đồ thị hoặc lưu đồ (tĩnh hoặc động).

Tại thời điểm xử lý thông tin dữ liệu, rất nhiều các thông tin chưa kịp xử lý được lưu trữ tại các vùng nhớ lưu trữ khác nhau. Các cơ chế dự phòng và cập nhật lưu trữ luôn được xác định trước trong các cơ chế quản lý mạng nhằm tránh tối đa tổn thất dữ liệu.

Các phân tích thời gian thực luôn yêu cầu thời gian hỏi đáp tới các thiết bị quản lý trong khoảng thời gian ngắn. Đây là điều kiện đánh đổi giữa số lượng đặc tính và thiết bị mạng với lượng tài nguyên (khả năng tính toán, số lượng thiết bị tính toán, bộ nhớ, lưu trữ) cần thiết để hỗ trợ các phân tích.

Thực hiện nhiệm vụ cấu hình chính là cài đặt các tham số trong một thiết bị mạng để điều hành và điều khiển các phần tử. Các cơ chế cấu hình bao gồm truy nhập trực tiếp tới các thiết bị, truy nhập từ xa và lấy các file cấu hình từ các thiết bị đó. Dữ liệu cấu hình được thông qua các cách sau:

- Các câu lệnh SET của SNMP
- Truy nhập qua telnet và giao diện dòng lệnh

- Truy nhập qua HTTP
- Truy nhập qua kiến trúc CORBA
- Sử dụng FTP/TFTP để lấy file cấu hình

1.5 MẠNG QUẢN LÍ VIỄN THÔNG

1.5.1 Giới thiệu chung

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 loạt khuyến nghị về các hệ thống quản lý điều hành mạng viễn thông M.3xxx. TMN được định nghĩa trong khuyến nghị của ITU-T M.3100 như sau: *"TMN là một mạng riêng liên kết các mạng viễn thông tại những điểm khác nhau để gửi/nhận thông tin đi/đến 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. Mạng quản lý viễn thông TMN gồm một hoặc nhiều hệ điều hành, mạng thông tin dữ liệu và những phần tử quản lý nhằm quản lý trạng thái thực hiện chức năng các phần tử mạngviễn thông (như hệ thống chuyển mạch, hệ thống truyền dẫn …). Mạng thông tin dữ liệu của TMN được sử dụng để truyền tải thông tin quản lý trong nội bộ mạng hoặc tới các mạng quản lý 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.

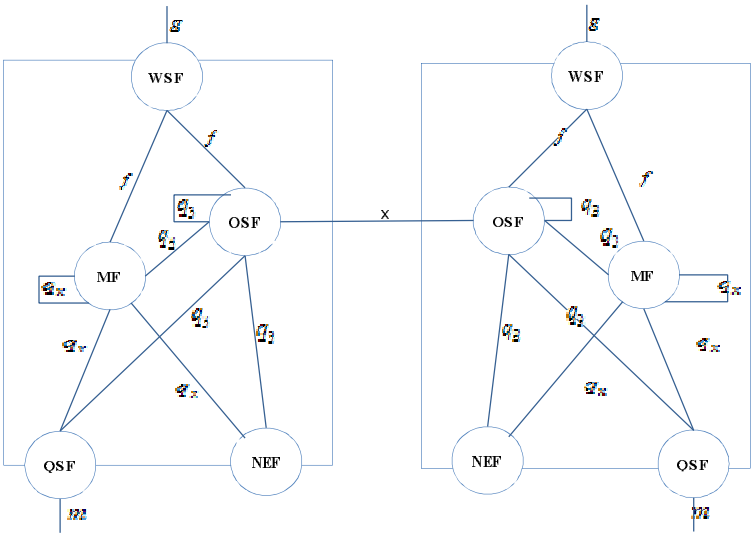
TMN không chỉ quản lý sự đa dạng của mạng viễn thông mà còn quản lý một phạm vi lớn về thiết bị, phần mềm và những dịch vụ trên mỗi mạng.

1.5.2 Kiến trúc chức năng

Kiến 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 chuẩn. 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.

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 phần tử mạng được quản lý .



Hình 1.15: Các khối chức năng và điểm tham chiếu của TMN

- Khả năng cho người sử dụng TMN truy nhập hoạt động quản lý và nhận được sự thể hiện về kết quả của hoạt động.

A, 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.

B, 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.

C, 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.

D, 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.

E, 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 gồm:

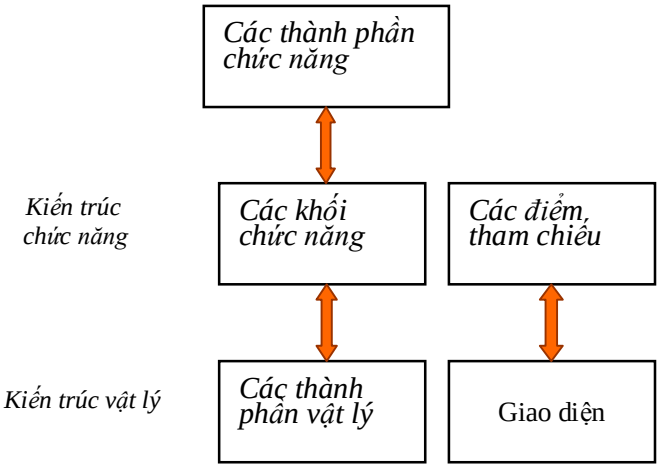
- Các chức năng truyền tải thông tin ITF (Information Tranfer Funtion) gồm: Biến đổi giao thức, biến đổi bản tin, biến đổi tín hiệu, dịch/ ánh xạ địa chỉ, định tuyến và tập trung dữ liệu.
- Các chức năng xử lý thông tin gồm: Thực hiện, hiển thị, lưu giữ, lọc thông tin.

1.5.3 Kiến trúc vật lí

Kiến trúc vật lí 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.

Nút trong TMN có thể là một hệ thống phần cứng, một hệ ứng dụng phần mềm

hoặc kết hợp cả hai.



Hình 1.16 : Quan hệ giữa mô hình chức năng và kiến trúc vật lí

Các chức năng quản lý có thể được thực hiện trong các thành phần khác nhau của các cấu hình vật lí. Mối quan hệ của các khối chức năng tới thiết bị vật lí được trình bày ở bảng 1.1. Nó định rõ các khối vật lí quản lý theo tập các khối chức năng mà mỗi khối này được cho phép để chứa đựng. Đối với mỗi khối vật lí, 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 tuỳ chọn cho các khối vật lí để bao hàm.

A, 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 tuỳ 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 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 qui 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 trúc vật lí 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 lí 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.

B, Phần tử mạng NE

Phần 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.

Bảng 1.1: Mối quan hệ của khối vật lí 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: Tuỳ chọn

Phần tử mạng NE có thể bao gồm bất kỳ tuỳ 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 tuỳ 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.

C, 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 phần tử mạng đảm bảo làm cho thông tin phù hợp. Chức năng tại những điểm này có thể là lưu trữ, chuyển đổi, lọc, xắp xếp và phân loại thông tin.

- 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 MIB 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, xắp 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.

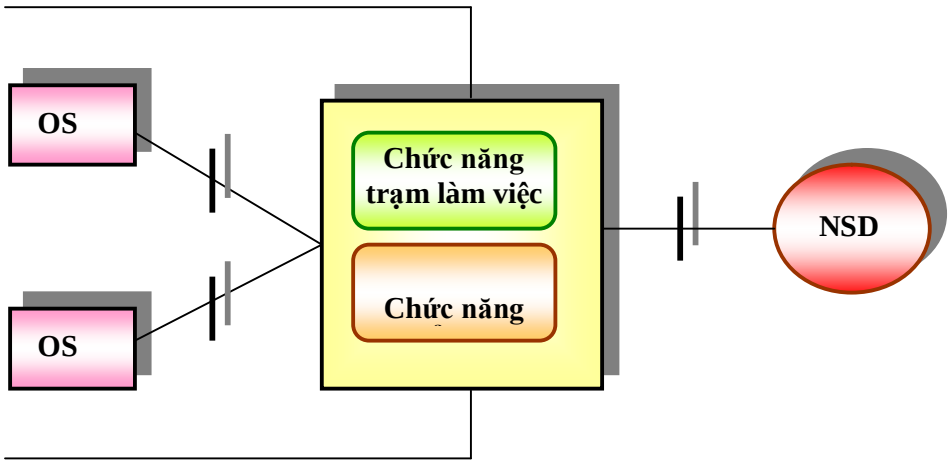
Chức năng trung gian có thể thực hiện như một thiết bị trung gian. Trong trường hợp đứng một mình, những giao diện trước của NE, QA, và OS là giao diện cơ bản của Qx và Q3. Khi trung gian là một phần của NE, chỉ những giao diện cụ thể trước OS sẽ là giao diện chuẩn. Chức năng trung gian có thể cũng được 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 thích ứng Q thường được đề cập tới như là thiết bị trung gian.

D, Trạm làm việc WS

WS là hệ thống thực hiện các chức năng trạm làm việc 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.

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. 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 lí và những phương tiện 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 dòng lệnh, đường dẫn hay cửa sổ cơ sở.



Hình 1.17: Trạm làm việc WS

Chức năng trạm làm việc 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 chứa chức năng OSF. Nếu OSF và WSF được kết hợp làm một thì trạm làm việc được coi là hệ điều hành OS.

E, Thành phần thích ứng QA

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

Thích 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 thích ứng Q do khó 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 thích ứng Q. Trên thực tế sự sử dụng đó rất thông dụng, thuật ngữ thiết bị trung gian bao hàm ý nghĩa của thích ứng Q. Một QAF thực hiện hai chức năng cơ bản: chuyển đổi thông tin và chuyển đổi giao thức.

F, 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, thích 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 thích ứng Q qua giao diện Qx. 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.

G, Các điểm tham chiếu

Điểm tham chiếu là điểm mang tính khái niệm để trao đổi thông tin giữa các chức năng không chồng lấn nhau. 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 lí. 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. 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

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.

1.6 TỔNG KẾT CHƯƠNG 1

Chương 1 giới thiệu các vấn đề cơ bản nhất của quản lý mạng, bao gồm các khái niệm, yêu cầu và các cách thức tiếp cận trong quản lý như quản lý hiện, quản lý ẩn, quản lý tập trung hay phân cấp, phân tán, hướng đối tượng hay tích hợp. Chương cũng đưa ra các kiến trúc quản lý mạng và giới thiệu về mạng quản lý viễn thông TMN với kiến trúc chức năng và vật lí điển hình.

CHƯƠNG 2

GIAO THỨC QUẢN LÍ MẠNG ĐƠN GIẢN SNMP

GIỚI THIỆU CHƯƠNG

Chương 2 giới thiệu về giao thức quản lý mạng đơn giản SNMP. SNMP là giao thức ứng dụng của IETF dành cho quản lý mạng đơn giản dựa trên nền giao thức TCP/IP (mạng Internet). Cho tới nay đã có nhiều phiên bản SNMP được ứng dụng rộng rãi, mới nhất là phiên bản thứ 3. Chương này cũng giới thiệu cụ thể về ứng dụng và phương thức hoạt động của giao thức quản lý mạng đơn giản SNMP nhằm đưa tới người đọc các kiến thức nền tảng của giao thức quản lý mạng trong môi trường IP và các môi trường mới trong lĩnh vực truyền thông như môi trường hội tụ trên nền IP. SNMP và RMON (thảo luận trong chương 3) là các chuẩn về mạng có mối liên hệ khá chặt chẽ, chúng cho phép bắt được những thông tin thời gian thực trên toàn bộ mạng lưới.

2.1 GIỚI THIỆU CHUNG VỀ SNMP

Vào đầu năm 1988, Tổ chức kiến trúc Internet IAB (Internet Architecture Board) nhận thấy sự cần thiết có bộ công cụ quản lý cho TCP/IP nên đã cho ra đời RFC 1052. RFC 1052 là các yêu cầu tiêu chuẩn hoá quản lý mạng và tập trung vào các vấn đề quản lý mạng phải thực hiện:

- Đảm bảo tính mở rộng
- Đảm bảo tính đa dạng để phát triển
- Đảm bảo tính đa dạng trong quản lý
- Bao trùm nhiều lớp giao thức

Dựa trên ý tưởng của giao thức điều khiển cổng đơn giản SGMP (Simple Gateway Protocol) một số RFC tiếp tục được ra đời trong năm 1988.

- RFC 1065 - Cấu trúc và nhận dạng thông tin quản lý cho TCP/IP dựa trên internet.
- RFC 1066- Cơ sở thông tin quản lý cho quản lý mạng TCP/IP.

- RFC 1067 – Giao thức quản lý mạng đơn giản.

Vào năm 1991, Phiên bản SNMPv1 được viết lại từ RFC 1067 và bổ sung thêm một số các chức năng gồm các RFC sau:

- RFC 1155
  - √ Cấu trúc và nhận dạng thông tin quản lý cho TCP/IP dựa trên Internet.
  - √ Cấu trúc và hướng dẫn nhận dạng thông tin thông tin quản lý cho các tên đối tượng.
  - √ Mô tả thông tin quản lý theo cấu trúc hình cây.
  - √ Đặt ra một số hạn chế cho phép giao thức đơn giản.
  - √ Đưa các luật đăng ký tên cho các đối tượng
- RFC 1212
  - √ Định nghĩa cơ sở thông tin quản lý và hoàn thiện các định nghĩa của 1155.
- RFC 1213
  - √ Cơ sở thông tin quản lý cho quản lý mạng của TCP/IP MIB-II.
  - √ Liệt kê các biến sử dụng trong mô hình quản lý mạng, trạng thái của các hệ thống điều hành mạng.
- RFC 1157
  - √ Định nghĩa các bản tin có thể trao đổi giữa hệ thống quản lý với các thực thể bị quản lý để đọc hoặc cập nhật giá trị.
  - √ Định nghĩa bản tin TRAP được gửi đi từ hệ thống.
  - √ Định nghĩa khuôn dạng bản tin và chi tiết giao thức truyền thông.

Các nhóm làm việc khác cũng phát triển và mở rộng các giao thức hỗ trợ MIB cho các kiểu thiết bị mạng (Cầu nối, chuyển mạch, bộ định tuyến, các giao diện WAN, DS1, DS3…) và các giao thức quản lý riêng của nhà cung cấp thiết bị.

Tháng 4 năm 1993, SNMPv2 trở thành tiêu chuẩn quản lý mạng đơn giản thay thế SNMPv1. SNMPv2 bổ sung một số vấn đề mà SNMPv1 còn thiếu như nhận thực và bảo mật. Tuy nhiên, SNMPv2 khá phức tạp và khó tương thích với SNMPv1.

Năm 1997, SNMPv3 ra đời nhằm tương thích với các giao thức đa phương tiện trong quản lý mạng, phát triển trên nền java và đưa ra kiến trúc và giao thức mới như

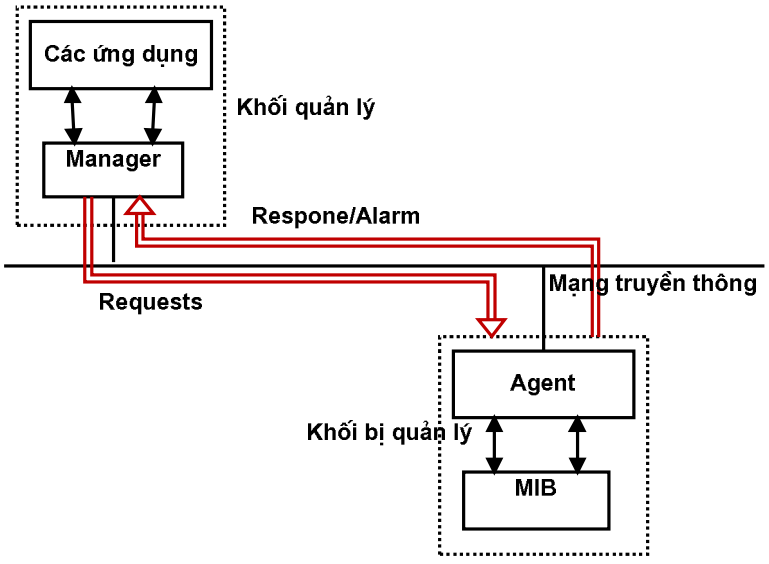
giao thức quản lý đa phương tiện HMMP (Hypermedia Management Protocol).

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 SNMPv3 hỗ trợ 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 như SNMPv2.

2.2 QUẢN LÍ TRUYỀN THÔNG TRONG SNMP

Hệ thống quản lý mạng dựa trên SNMP gồm ba thành phần: bộ phận quản lý (manager), thiết bị chịu sự quản lý – còn gọi là 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). Cơ sở dữ liệu do agent SNMP quản lý là đại diện cho MIB của SNMP. Hình 2.1 minh họa mối quan hệ giữa ba thành phần SNMP này.



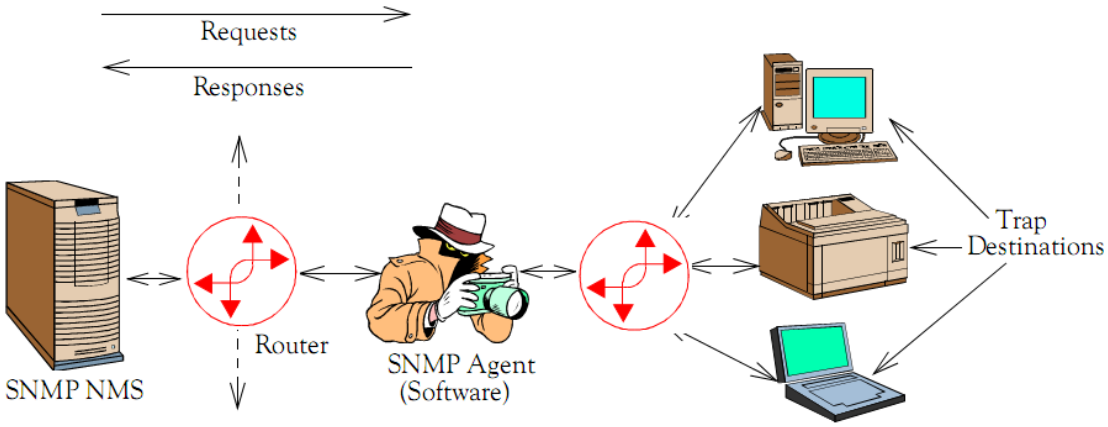
Hình 2.1: Mối quan hệ giữa các thành phần SNMP

2.2.1 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 sẽ cho ra giao diện sử dụng con trỏ và chuột để phối hợp hoạt động với bộ phận quản lý 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 (hình 2.2). 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.



Hình 2.2 Truyền thông giữa manager và agent trong SNMP [6]

2.2.2 Agent

Thiết bị chịu sự quản lý (Agent) 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 là những phần tử mạng, có thể là các bộ định tuyến và máy chủ truy nhập (Access Server), switch và bridge, hub, máy tính hay là 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 không tương thích với 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 phải có agent ủy nhiệm (proxy agent). Proxy agent này có thể được coi 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 đáp ứng này cảnh báo việc agent đã tới ngưỡng định trước. Dưới sự điều khiển SNMP, việc truyền cảnh báo này được gọi là cái bẫy (TRAP).

2.2.3 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 định nghĩa chức năng và khả năng vận hành của thiết bị. Thông tin này rất đa dạng, 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 cách cài đặt thiết bị mà hệ thống quản lý điều khiển.

2.2.4 Mô hình giao thức SNMP

SNMP sử dụng các dịch vụ chuyển tải dữ liệu thông qua 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 nhận dạng cổng UDP của nó. Khung UDP sẽ được gửi đi thông qua thực thể IP tới hệ thống chịu sự quản lý , tại đó khung UDP sẽ được phân phối bởi thực thể UDP tới Agent. Tương tự, các bản tin TRAP phải được các Manager nhận dạng. 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 (hình 2.3).

- *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 thiết bị cập nhật.

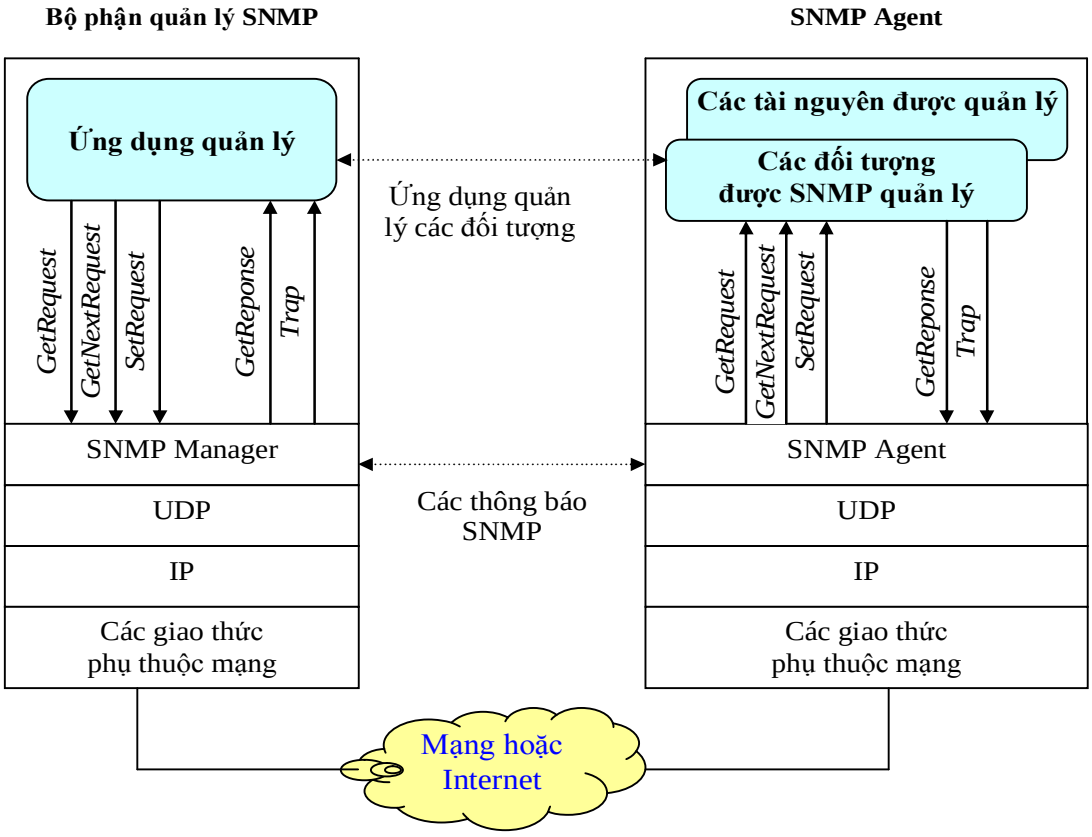
- *Lệnh Write:* Được SNMP dùng để ghi các thông tin điều khiển lên thiết bị bằng cách thay đổi giá trị các biến SNMP.

- *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.

Giao thức SNMP sử dụng kiểu kết nối vô hướng (connectionless) để trao đổi thông tin giữa các phần tử và hệ thống quản lý mạng (cụ thể là UDP - User Datagram Protolcol - Giao thức dữ liệu đồ người sử dụng). 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. Khi gửi các gói tin qua mạng, các phần tử mạng hay hệ thống quản lý mạng vẫn giữ nguyên định dạng của SNMP.



Hình 2.3 Mô hình giao thức hoạt động SNMP

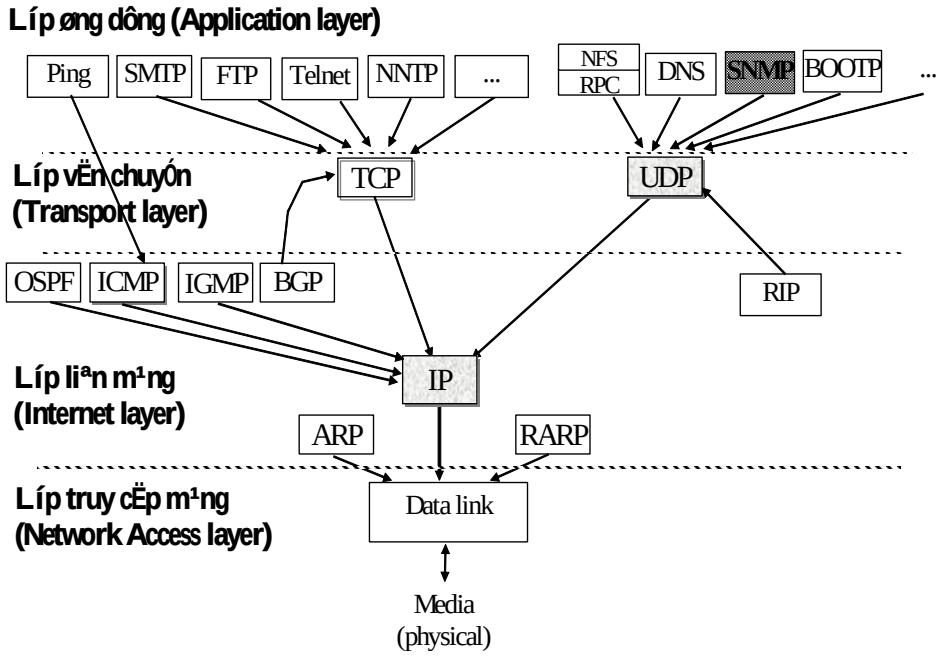
Hình 2.4 cho thấy vị trí giao thức SNMP trong mô hình chồng giao thức TCP/IP. Ta thấy, SNMP thuộc về lớp ứng dụng trong mô hình giao thức, nó sử dụng UDP làm giao thức lớp vận chuyển trên mạng IP.

Quản lý liên lạc giữa manager với các agent

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

Manager trước hết phải xác định được các agent mà nó muốn liên lạc. Có thể xác định được ứng dụng agent bằng địa chỉ IP của nó và cổng UDP được gán cho nó. Cổng UDP 161 được dành riêng cho các agent SNMP. Manager gói lệnh SNMP vào một tiêu đề UDP/IP. Tiêu đề này chứa cổng nguồn, địa chỉ IP đích và cổng 161. Một thực

thể IP tại chỗ sẽ chuyển giao gói UDP tới hệ thống bị quản lý . Tiếp đó, một thực thể UDP tại chỗ sẽ chuyển phát nó tới các agent. Tương tự như vậy, lệnh TRAP cũng cần xác định những manager mà nó cần liên hệ. Chúng sử dụng địa chỉ IP cũng như cổng UDP dành cho SNMP manager, đó là cổng 162.



Hình 2.4 Vị trí của SNMP trong chồng giao thức TCP/IP

Cơ chế vận chuyển thông tin giữa manager và agent

Việc lựa chọn cơ chế vận chuyển là độc lập với giao thức truyền thông đó. SNMP chỉ đòi hỏi cơ chế vận chuyển không tin cậy dữ liệu đồ (datagram) để truyền đưa các PDU (đơn vị dữ liệu giao thức) giữa manager và các agent. 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 có một số lựa chọn cho 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 đã 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 và điều này cũng được khuyến khích sử dụng cho bất cứ nhóm giao thức nào.

Bảo vệ truyền thông liên lạc giữa manager và các agent khỏi sự cố

Trong điều kiện mạng thiếu ổn định và tin cậy thì việc truyền thông quản lý càng trở nên quan trọng. Làm thế nào để các manager liên lạc với các agent một cách tin cậy? Việc SNMP sử dụng cơ chế UDP để liên lạc đã làm thiếu đi độ tin cậy vì UDP hoạt động theo kiểu dữ liệu đồ. SNMP để lại cho chương trình manager hoàn toàn 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 agent tạo ra lại không yêu cầu phúc đáp. Khi bị thất lạc bản tin TRAP, các chương trình agent sẽ không biết được điều đó (tất nhiên là manager cũng không hay biết về điều này). Thông thường các bản tin TRAP mang những thông tin hết sức quan trọng cho manager, do vậy manager cần chú ý và cần bảo đảm việc vận chuyển chúng một cách tin cậy.

Một câu hỏi đặt ra là làm thế nào để vận chuyển mà tránh được mất mát, thất lạc các bản tin TRAP? Ta có thể thiết kế cho các agent gửi lặp lại bản tin TRAP. Biến số MIB có thể đọc số lần lặp lại theo yêu cầu. Lệnh SET của manager có thể đặt cấu hình cho biến số này. Có một cách khác là agent có thể lặp lại lệnh TRAP cho đến khi manager đặt biến số MIB để chấm dứt sự cố. Tuy nhiên, 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 agent tạo ra chúng. Điều này làm cho sự cố mạng trở nên trầm trọng hơn. Trong cả hai trường hợp, nếu ta cần chuyển những bản tin TRAP tới nhiều manager thì có thể xảy ra tình trạng không nhất quán giữa các manager hoặc xảy ra hiện tượng thất lạc thông tin rất phức tạp. Nếu các agent phải chịu trách nhiệm thiết kế cho việc phục hồi những bản tin TRAP thì càng làm tăng thêm độ phức tạp trong việc quản lý các agent trong môi trường đa nhà chế tạo.

Người ta cũng đã cố gắng 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. Lệnh này do agent tạo ra và chuyển đến cho "manager bẫy" tại cổng UDP-162. Điều này phản ánh quan điểm là bộ phận 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 manager nhận bản tin về các sự cố này và việc lặp lại được thực hiện để cải thiện độ tin cậy trong việc vận chuyển thông tin.

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 độc lập với việc lựa chọn giao thức quản lý . Quản lý trong băng có thể dẫn đến tình trạng mất liên lạc với một agent đúng lúc agent 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 agent quản lý lại bảo vệ đường truy nhập tới các agent này.

Có một ảnh hưởng nhỏ về khả năng quản lý xuất hiện trong việc đánh địa chỉ tầng vận chuyển. Ví dụ: có thể xác định duy nhất một agent SNMP 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 agent duy nhất. Hơn thế nữa agent 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 agent 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 agent 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 làm tăng phức tạp 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 agent duy nhất trong một hệ thống có thể giữ vai trò như một proxy mở rộng cho các agent phụ đóng gói những cơ sở dữ liệu 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 manager. Các phiên bản mở rộng này cho phép agent đóng vai trò như một manager của các agent con tại chỗ, do vậy cho phép tiếp cận hàng loạt các agent con.

2.3 CẤU TRÚC VÀ ĐẶC ĐIỂM NHẬN DẠNG CỦA THÔNG TIN QUẢN LÍ MIB

Thông tin quản lý hệ thống SMI (System Management Information) 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 cơ sở dữ liệu thông tin quản lý MIB. SMI mô phỏng sáu loại dữ liệu, đó là bộ đếm, kiểu (gauge), tích tắc thời gian (Time Ticks), 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 bít 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.

SMI duy trì tính đơn giản và khả năng mở rộng trong MIB. Vì thế MIB chỉ lưu những loại dữ liệu đơn giản gồm các đối tượng vô hướng và các mảng hai chiều của các đối tượng vô hướng. 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. Thông tin quản lý hệ thống hỗ trợ cho liên điều hành trong quản lý mạng dựa trên các cơ sở

thông tin quản lý MIB, nó đặc tả và hiển thị các thông tin tài nguyên trong MIB cũng như tiêu chuẩn kỹ thuật định nghĩa cho các đối tượng đơn lẻ khác.

Để cung cấp phương pháp tiêu chuẩn biểu diễn thông tin quản trị, SMI cần thực hiện 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 gauge, 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.
- ***Access (Truy nhập):*** Phương pháp truy nhập có thể là: chỉ đọc, đọc-ghi hay không thể truy nhập.
- ***Status (Trạng thái):*** Có thể là cưỡng chế, tùy chọn hay không còn hiệu lực.

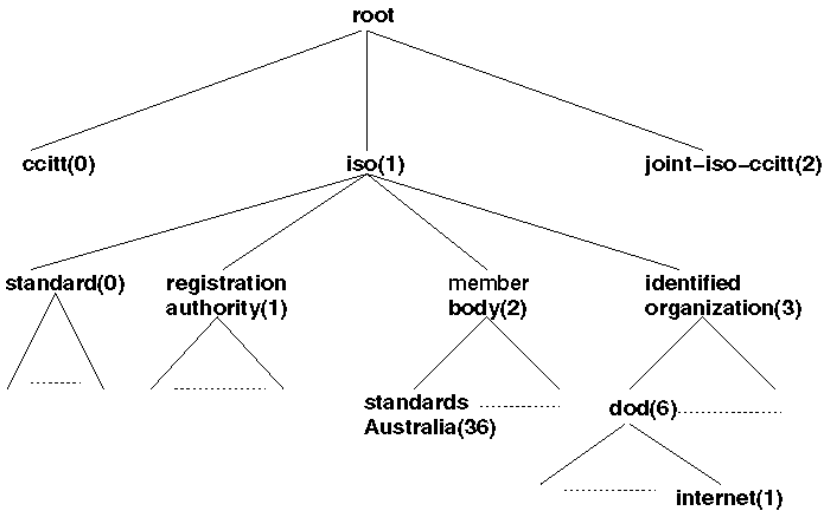
2.4 CƠ SỞ THÔNG TIN QUẢN LÍ MIB

2.4.1 Cấu trúc của MIB

Các đối tượng quản lý trong môi trường SNMP được sắp xếp theo cấu trúc hình cây có thứ bậc. Lá của cây là đối tượng quản lý thực, mỗi thành phần trong đối tượng này 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 biến số bị quản lý được lưu trữ tại các lá cây. Người ta sử dụng các biến 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. Còn sự thay đổi mở rộng chỉ có trong các giá trị của cơ sở dữ liệu và trong việc tạo ra hay xóa đi các hàng của bảng.

Như minh họa trên hình 2.5, người ta sử dụng cây đăng ký để đánh dấu các định

nghĩa của các tiêu chuẩn khác nhau. Mỗi nút của 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 con 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).



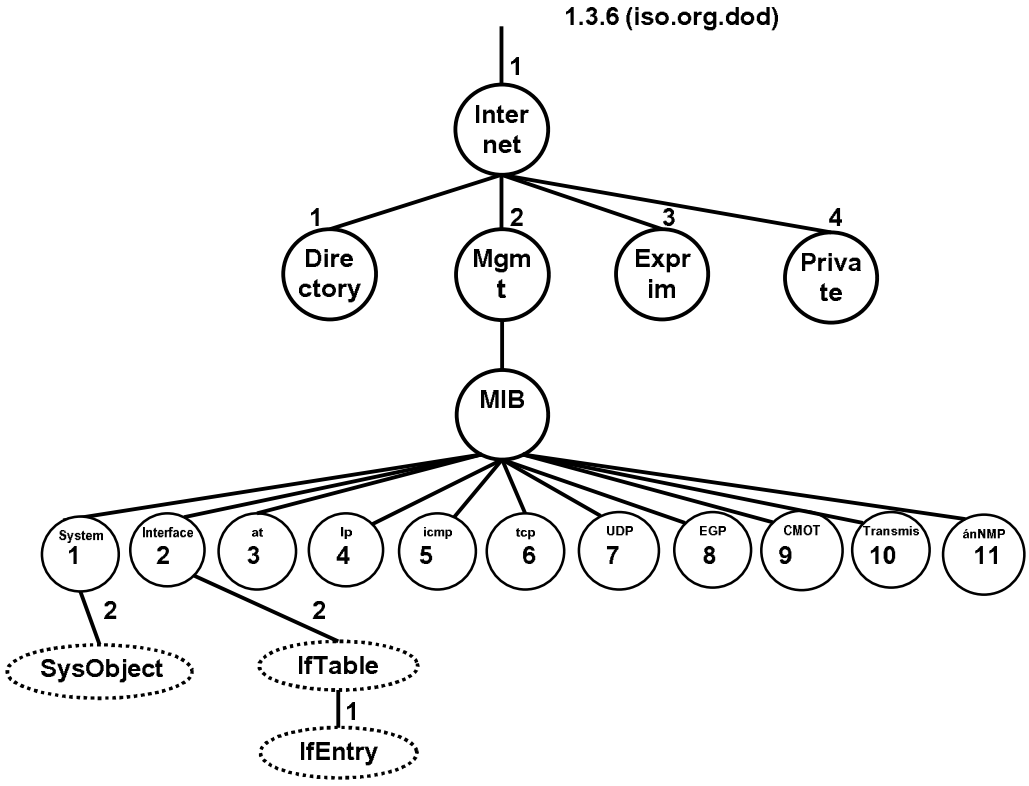
Hình 2.5: Cây đăng ký của OSI

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.

Với mục tiêu quản lý các nhóm giao thức trong mô hình TCP/IP và mạng Internet, một mô hình cây có tên gọi MIB II (RFC1213) có nhánh Internet được chia ra thành 4 nhóm lớn: Thư mục, quản lý , thực nghiệm và vùng chỉ số cá nhân.

- Nhóm thư mục (Directory): Hỗ trợ các thư mục trong OSI X.500
- Nhóm quản lý (Management): Gồm các đối tượng của Internet
- Nhóm thực nghiệm (Experimental): Sử dụng cho quá trình thực nghiệm trước khi chuyển sang nhóm quản lý .
- Nhóm cá nhân (Private) : Gồm các đặc tả của các nhà cung cấp thiết bị và các vùng gia tăng giá trị.



Hình 2.6 Cấu trúc cây MB-II

Theo nhánh nhóm quản lý , MIB-II đưa ra các biến số để quản lý các giao thức gồm 11 cây chức năng con (Hình 2.6). Các cây con này lại tiếp tục được chia ra thành các cây con cấp thấp hơn như đối tượng hệ thống và các bảng con tương ứng với các lá. Lá được sử dụng để đánh dấu các biến số bị quản lý thuộc một loại nhất định. Một số lá như mô tả hệ thống sysDesc chỉ đánh dấu một thời điểm duy nhất của biến số bị quản lý và chỉ đòi hỏi một phần tử lưu trữ duy nhất. Những lá khác như mô tả trạng thái một đường kết nối TCP tcpConnState 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).

Việc đánh số theo thứ tự hình cây đem lại lợi thế cho quá trình truy nhập thông tin trạng thái chính xác nhưng khá phức tạp về mặt chỉ dẫn do thể hiện trạng thái của cùng một đối tượng tại các thời điểm khác nhau là khác nhau. Vì vậy, phương pháp chỉ dẫn theo bảng sẽ hỗ trợ các chỉ dẫn đối với các đối tượng có sự thay đổi. Agent có thể bổ sung thêm hoặc xóa đi các đầu mục mới. Bằng các cột chìa khóa người ta có thể xác định duy nhất một đầu mục của bảng thông qua việc sử dụng nội dung của các cột chìa khóa làm chỉ dẫn. Bảng giao diện đưa ra một chỉ dẫn đặc biệt đóng vai trò như chìa khóa. Giá trị lưu trữ trong cột này cho phép ta xác định các hàng cột một cách duy nhất.

2.4.2 Truy nhập thông tin quản lý 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. Đáp lại hai đơn nguyên này là GET-RESPONSE trả lại dữ liệu dưới dạng cặp 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 cách ứng xử của thiết bị. SET thường được sử dụng để khởi tạo hành động của agent làm hiệu ứng bổ xung 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 agent 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 hợp các lệnh GET-NEXT để cải thiện thời gian truy cập đối với dữ liệu dạng bảng.

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. Trong môi trường agent 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 nút 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 nhãn 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. 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 phiên 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 truyền 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).

2.4.3 Các đối tượng của MIB

MIB-II phân tách đối tượng quản trị thành 11 nhóm đối tượng. Bảng 2.3 sẽ trình bày chi tiết về các nhóm đối tượng này.

Bảng 2.3: Các nhóm đối tượng trong MIB-II

STT	Nhóm	Đường đi	Vai trò
1	**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. Nhóm này bao gồm OID, độ dài thời gian từ thời điểm tái khởi động thực thể quản lý mạng và những chi tiết quản lý khác. Nhóm hệ thống gồm 7 đối tượng sử dụng để mô tả thông tin cấu hình các thiết bị bị quản lý . Các đối tượng đơn lẻ trong cùng một hệ thống có thể được nhận dạng nhóm theo hệ thống system n (n có giá trị:1..7). Các mô tả chi tiết về 7 đối tượng này có trong phụ lục A.1. ▪ sysDescr {1.3.6.1.2.1.1.1} Mô tả thiết bị ▪ sysObjectID {1.3.6.1.2.1.1.2} Nhận dạng phần cứng, phần mềm hoặc tài nguyên ▪ sysUptime {1.3.6.1.2.1.1.3} Độ dài thời

STT	Nhóm	Đường đi	Vai trò
			gian tính từ khi Agent khởi tạo ▪ sysContact {1.3.6.1.2.1.1.4} Tên đại diện của nút hoặc thiết bị ▪ sysName {1.3.6.1.2.1.1.5} Tên nút hoặc thiết bị ▪ sysLocation {1.3.6.1.2.1.1.6} Vị trí vật lí của thiết bị ▪ sysServices {1.3.6.1.2.1.1.7} Mã nhận dạng tập dịch vụ do thiết bị cung cấp.
2	**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. Nhóm giao diện gồm 23 nhận dạng đối tượng cung cấp các thông tin như: hiệu năng, cấu hình và trạng thái cho tất cả các loại giao diện. Mặc dù các thông tin chung có thể cung cấp trong chính hoạt động của các giao diện nhưng các thông tin này vẫn chưa được coi là đầy đủ trong bài toán quản lý , vì không thể hiện rõ được hiệu năng tổng thể của toàn bộ hệ thống. Khi mạng có rất nhiều thiết bị cần phải quản lý , một cơ chế nhận dạng thiết bị được thêm vào cây quản lý và 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 lí, trạng thái vận hành hiện thời và thống kê về gói tin qua giao diện (Mô tả chi tiết có trong phụ lục A.2).
3	**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 lí (phần cứng) để phiên dịch giữa hai địa chỉ này (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

STT	Nhóm	Đường đi	Vai trò
			phiên bản sau. Trong MIB-II và những phiên bản sau, mỗi nhóm giao thức sẽ chứa bảng phiên dịch riêng của nó. Bảng để chuyển đổi biên dịch gồm có 3 cột tương ứng với số giao diện, địa chỉ vật lí và địa chỉ mạng (IP). Trong mô hình TCP/IP sử dụng giao thức phân giải địa chỉ ARP (Address Resolution Protocol). Thực tế, nhóm biên dịch chứa cả bảng địa chỉ vật lí và địa chỉ mạng với các chỉ số tương đương cho phép tìm kiếm và ánh xạ từ bất kỳ bảng nào.
4	**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 19 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 lí (ipNetToMediaTable) và bảng hướng đi IP (ipForwardTable). RFC 1354 đã định nghĩa ipForwardTable, thay thế ipRoutingTable trong MIB-II. Nội dung chi tiết của các đối tượng nhóm IP có trong phụ lục A3.
5	**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 lý . 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. Do giao thức ICMP là kỹ thuật báo cáo lỗi, người quản lý mạng có thể sử dụng các giá trị đối tượng ICMP để xác định kiểu lỗi. Thêm vào đó, ICMP còn sử dụng các bản tin định kỳ để đặt lại ngưỡng cảnh báo dựa trên số lượng bản tin.
6	**TCP Group**	{1.3.6.1.2.1.6}	Nhóm giao thức điều khiển truyền tải là bắt buộc

STT	Nhóm	Đường đi	Vai trò
			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. Thêm vào đó, qua các phản hồi của đối tượng giao thức TCP, ta có thể xác định các thông tin về lỗi tại lớp 4 trong mô hình OSI và chỉ ra hướng đi tới các lỗi được xác định.
7	**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 thống 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.
8	**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 các số liệu thống kê bản tin liên quan tới EGP. Bảng egpNeighTable chứa thông tin EGP lân cận.
9	**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 SNMP được cố gắng sử dụng làm một bước chuyển tiếp trong hoàn cảnh thúc bách có chuẩn quản lý mạng, và để tạo Giao thức thông tin quản lý

STT	Nhóm	Đường đi	Vai trò
			chung (CMIP) trên nền TCP/IP (CMOT) với giải pháp dài hạn tương thích OSI (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 (OSI Internet Management) 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. . Hiện tại, RFC 1214 được xếp loại là giao thức "lịch sử".
10	**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, RFC 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 sử dụng trong nhóm quản lý .
11	**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 thống kê bản tin SNMP, số lượng đối tượng MIB khôi phục (retrieved) và số lượng bẫy (trap) SNMP đã gửi. Bẫy nhận thực: Khi một trạm được cấu hình đúng, nó cho phép mở một nhận dạng đối tượng bẫy nhận thực các đối tượng bản tin truy nhập. Các bản tin truy nhập bất hợp pháp sẽ bị ngăn ngừa tại các giao diện. Trong một số trường hợp, bẫy nhận thực tạo ra một số lượng lớn lưu lượng thông tin điều khiển giữa các nhà điều hành mạng. Đếm lưu lượng đến: SNMP gồm 17 nhận dạng đối tượng đếm lưu lượng đến, trong đó mô tả

STT	Nhóm	Đường đi	Vai trò
			các số lượng bản tin SNMP, hiển thị điều kiện lỗi, tổng kết các câu lệnh được xử lý và chấp nhận bởi Agent và hiển thị số lượng bẫy được chấp nhận và xử lý. Đếm lưu lượng đi: Tương tự như đếm lưu lượng đến, nhóm SNMP gồm 10 nhận dạng đối tượng được sử dụng để giám sát lưu lượng đi khỏi thiết bị. Các đối tượng chia thánh hai nhóm con: Nhóm con đếm lưu lượng và nhóm con đếm lỗi. Các đối tượng này cung cấp thông tin về số lượng bản tin đi, đo lưu lượng cho các kiểu điều kiện lỗi khác nhau và lưu lượng bản tin ra theo kiểu.

Mỗi nhóm đối tượng trên mô tả một cách tổng quan về thuộc tính đối tượng. Bảng 2.4 cho ta nội dung chi tiết về nhóm hệ thống .

Bảng 2.4: Nhóm hệ thống trong MIB-II

Cây con nhóm hệ thống 1.2.1.1.2 (SysObject)		**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

2.5 SNMPv2

SNMPv2 tích hợp khả năng liên điều hành từ manager tới manager và hai đơn vị dữ liệu giao thức mới. Khả năng liên kết điều hành manager-manager cho phép SNMP

hỗ trợ quản lý mạng phân tán trong một trạm và gửi báo cáo tới một trạm khác.

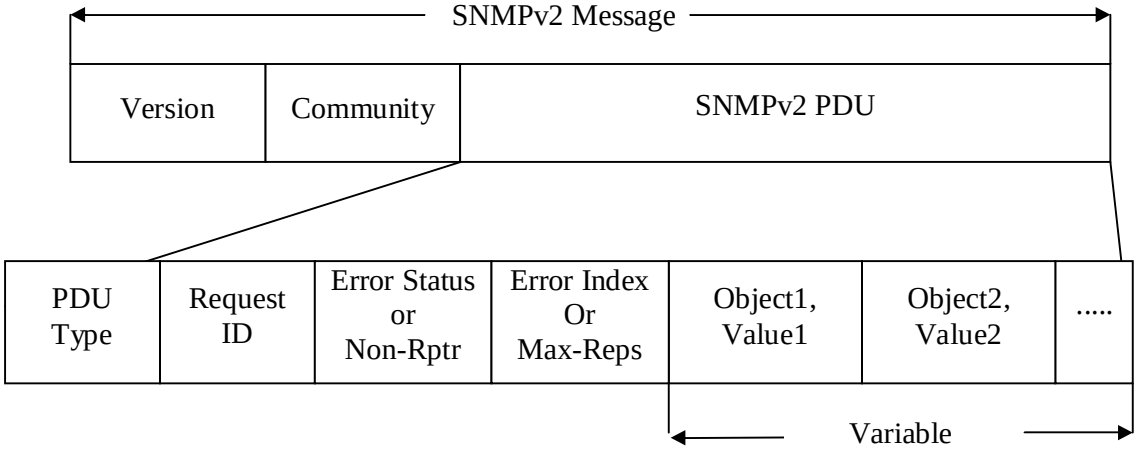
Để hỗ trợ tương tác tốt nhất, SNMPv2 thêm các nhóm cảnh báo và sự kiện vào trong cơ sở thông tin quản lý MIB. Nhóm cảnh báo cho phép đặt ngưỡng thiết lập cho các bản tin cảnh báo. Nhóm sự kiện được đưa ra khi thông tin Trap xác định các giá trị phần tử MIB.

Hai đơn vị dữ liệu giao thức PDU (Protocol Data Unit) là GetbulkRequest và InformRequest. Các PDU này liên quan tới xử lý lỗi và khả năng đếm của SNMPv2. Xử lý lỗi trong SNMPv2 đi kèm với các đối tượng yêu cầu cho phép trạm quản lý lập trình đặt các phương pháp khôi phục hoặc dừng truyền bản tin. Khả năng đếm trong SNMPv2 sử dụng bộ đếm 64 bit (hoặc 32) để duy trì trạng thái của các liên kết và giao diện.

2.5.1 Cấu trúc bản tin SNMPv2

Các bản tin trao đổi trong SNMPv2 chứa các đơn vị dữ liệu giao thức PDU. Hình 2.7 mô tả cấu trúc chung các bản tin này.

- Trường phiên bản (Version) thể hiện phiên bản của giao thức SNMPv2.
- Trường Community là một chuỗi password xác nhận cho cả tiến trình lấy và thay đổi dữ liệu. SNMP PDU chứa kiểu điều hành (get, set), yêu cầu đáp ứng (cùng số thứ tự với bản tin gửi đi) - cho phép người điều hành gửi đồng thời nhiều bản tin. Biến ghép gồm các thiết bị được đặc tả trong RFC 2358 và chứa cả giá trị đặt tới đối tượng.
- Trường đơn vị dữ liệu giao thức (PDU) gồm có các trường con: Kiểu đơn vị dữ liệu giao thức, nhận dạng các yêu cầu (Request ID), trạng thái lỗi, chỉ số lỗi, các giá trị và đối tượng.



Hình 2.7 Cấu trúc dạng bản tin SNMPv2

- Các kiểu đơn vị dữ liệu giao thức PDU thể hiện các bản tin sử dụng trong SNMPv2 gồm có:

GetRequest: Câu lệnh GetRequest được sử dụng giữa Manager tới Agent. Câu lệnh này được sử dụng để đọc biến MIB đơn hoặc danh sách các biến MIB từ các Agent đích. GetRequest yêu cầu sử dụng hai địa chỉ, địa chỉ đầu là địa chỉ của manger hoặc agent, địa chỉ thứ hai thể hiện vị trí của biến hoặc đối tượng. Cây cấu trúc MIB đã trình bày trong phần 2.4 định nghĩa các địa chỉ của biến MIB.

GetNextRequest: Câu lệnh GetNextRequest tương tự như câu lệnh GetRequest, tuy nhiên tuỳ thuộc vào agent trong khoản mục kế tiếp của MIB. Các biến được lưu trong thiết bị và được coi như đối tượng bị quản lý . Vì vậy, câu lệnh GetNextRequest mở rộng các biến và được đọc theo tuần tự.

SetRequest: Câu lệnh SetRequest là câu lệnh được gửi đi từ Manager tới Agent như hai câu lệnh trên. SetRequest tìm kiếm các thông tin mở rộng trong bảng MIB và yêu cầu Agent đặt giá trị cho các đối tượng quản lý hoặc các đối tượng chứa trong câu lệnh. Sự thành công của câu lệnh này phụ thuộc vào một số yếu tố gồm sự tồn tại của các đối tượng bị quản lý và các phương thức truy nhập.

GetResponse: Câu lệnh GetResponse là câu lệnh từ Agent tới Manager. Câu lệnh này cung cấp cơ chế đáp ứng cho các câu lệnh GetRequest, GetNextRequest và SetRequest. Các thông tin trong câu lệnh GetResponse gồm một số trường chức năng cho phép đáp ứng các câu lệnh đã nhận trước đó.

Trap: Trap là câu lệnh độc lập, không phụ thuộc vào đáp ứng hoặc yêu cầu từ các Manager hoặc các Agent. Trap đưa ra các thông tin liên quan tới các điều kiện được định nghĩa trước và được gửi từ các Agent tới Manager.

GetBulkRequest: Chức năng của câu lệnh GetBulkRequest tương tự như câu lệnh GetNextRequest ngoại trừ vấn đề liên quan tới số lượng dữ liệu được lấy ra. GetBulkRequest cho phép Agent gửi lại Manager dữ liệu liên quan tới nhiều đối tượng thay vì từng đối tượng bị quản lý . Như vậy, GetBulkRequest có thể giảm bớt lưu lượng truyền dẫn và các bản tin đáp ứng thông báo về các điều kiện vi phạm.

InformRequest: Câu lệnh InformRequest cung cấp khả năng hỗ trợ các Manager bố trí theo cấu hình phân cấp.Câu lệnh này cho phép một Manager trao đổi thông tin với các Manager khác. Các cảnh báo và sự kiện được gửi đi trong câu lệnh InformRequest để phát hiện và khởi tạo lại các tuyến truyền bản tin.

Một trạm quản lý có thể thông tin tới các trạm quản lý lân cận biết các điều kiện quan trọng trong vùng quản lý .

- Các câu lệnh được thể hiện trong trường PDU Type, các giá trị thể hiện như trong bảng 2.5:

Bảng 2.5: Câu lệnh và giá trị trong trường PDU

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

- Trường nhận dạng yêu cầu cho phép SNMP gửi và nhận đồng thời nhiều bản tin, phân biệt các bản tin thông qua các chỉ số nhận dạng.
- Trường error-status (trạng thái lỗi) được sử dụng trong các dạng bản tin như trong bảng 2.6 .

Bảng 2.6: Sử dụng trường trạng thái lỗi trong các 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	

SNMPv2 Error	Get	GetNext	GetBulk	Set	Inform
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	

Chú ý: *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 có chỉ mục 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 phần tử 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 số nhận dạng của 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.

2.5.2 Cơ sở thông tin quản lý 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. Các đối tượng mới trong phần mở rộng 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 tuỳ thuộc vào cấu hình động bởi một bộ phận quản lý .

- 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. Nó 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 (MIB objects group): một tập hợp các đối tượng liên quan đến các SNMPv2-Trap PDU và cho phép một vài phần tử SNMPv2 cùng hoạt động, thực hiện như trạm quản trị, phối hợp việc sử dụng của chúng trong toán tử Set của SNMPv2.

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 (variable binding) thứ hai trong mọi SNMPv2-Trap PDU và InformRequest PDU.
- snmpTrapEnterprise: là nhận dạng đối tượng của tổ chức liên quan đến Trap đ-ược gửi hiện thời. Khi một Agent uỷ quyền SNMPv2 ánh xạ

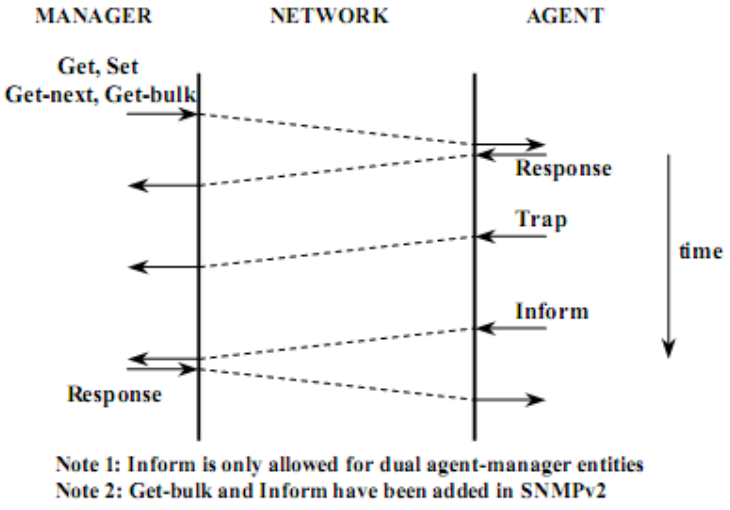
một Trap PDU sang một SNMPv2-Trap PDU, biến này xuất hiện như một varbind cuối cùng.

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 manager có thể gây ra một sự mâu thuẫn hoặc làm cho cơ sở dữ liệu bị sai.

Đối tượng snmpSet được sử dụng theo cách sau: Khi một manager 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 manager gửi các setRequestPDU sử dụng cùng một giá trị của snmpSet, bản tin đến Agent trước sẽ được thực hiện (giả sử không có lỗi), kết quả là làm tăng snmpSet; các toán tử set còn lại sẽ bị lỗi vì không phù hợp với giá trị snmpSet. Hơn nữa, nếu một manager 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.

2.5.3 Nguyên tắc hoạt động của SNMPv2

Hình 2.8 cho ta thấy nguyên tắc hoạt động của SNMPv2.



Hình 2.8 Gửi và nhận bản tin trong SNMPv2

i, Truyền một bản tin SNMPv2

Qui tắc gửi và nhận bản tin của Manager và Agent được thể hiện trong bảng 2.7.

Bảng 2.7 : Quy tắc truyền và nhận một bản tin trong SNMPv2

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 tạo ra 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 vận chuyển.

ii, 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 tiếp đến là xử lý PDU.

iii, 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 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 đối tượng được quản lý 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 4 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 tham chiếu qua 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.
  - Các mệnh đề STATUS, DESCRIPTION và REFERENCE: có ý nghĩa tương tự như trong macro OBJECTS-GROUP
- 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 NONTIFICATION-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 khả năng thể hiện những cải tiến hoặc biến đổi nhất định liên quan đến các macro OBJECT-TYPE trong các khối MIB.

2.6 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 nhập vào các thiết bị bằng cách kết hợp sự xác nhận và mã khoá các gói tin trên mạng. Những đặc điểm bảo mật cung cấp trong SNMPv3 là:

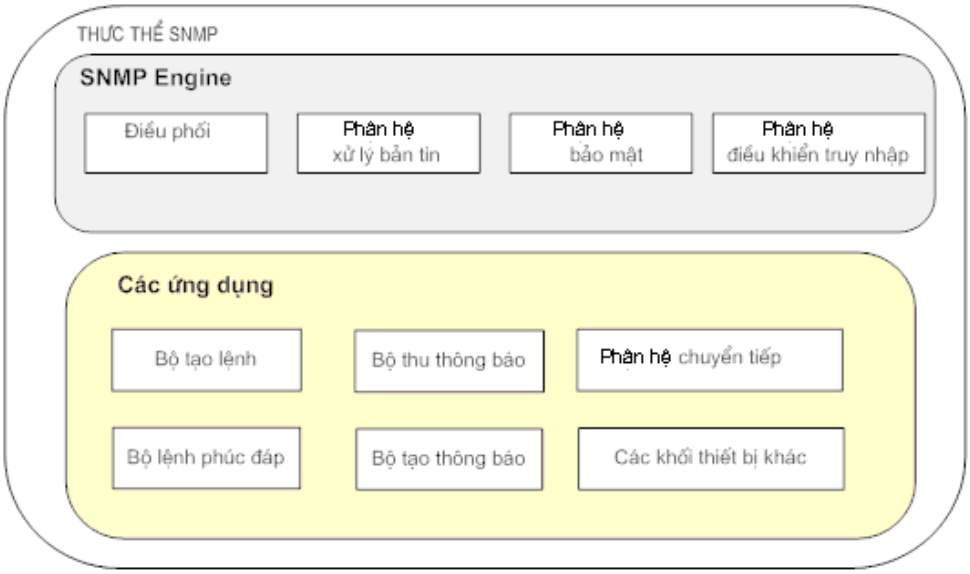
- Tính toàn vẹn thông tin : Đảm bảo các gói tin không bị sửa trong khi truyền.
- Sự xác nhận: Xác nhận nguồn của thông tin gửi đến.
- Mã khoá: Đảo nội dung của gói tin, ngăn cản việc gửi thông báo từ nguồn không được xác nhận.

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 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 dù nó là sự lựa chọn tốt nhất cho vấn đề bảo mật của mạng. Việc sử dụng sẽ tốn rất nhiều tài nguyên do trong mỗi bản tin truyền đi sẽ có phần mã hóa BER. Phần mã hóa này 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.

Kiến trúc thực thể SNMPv3 (RFC257) được thể hiện trên hình 2.9 gồm cơ cấu SNMP và các ứng dụng.

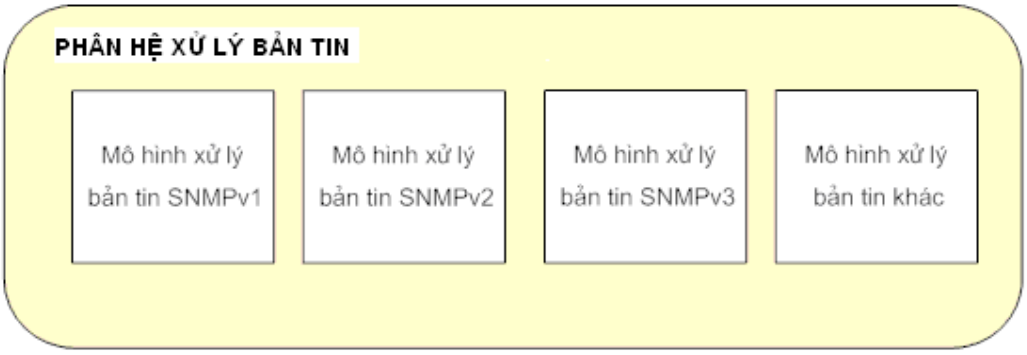


Hình 2.9 Kiến trúc thực thể của SNMPv3

Cơ cấu SNMPv3 gồm 4 thành phần:

- Điều phối (Dispatcher).
- Phân hệ xử lý bản tin (Message Processing Subsystem).
- Phân hệ bảo mật (Security Subsystem).
- Phân hệ điều khiển truy nhập (Access Control Subsystem).

Phân hệ điều phối bản tin xử lý bản tin gửi và nhận, khi nhận được bản tin phân hệ này sẽ xác nhận phiên bản của SNMP và gửi bản tin tới phân hệ xử lý bản tin tương ứng. Phân hệ xử lý bản tin chia thành 3 khối (module) như sau:

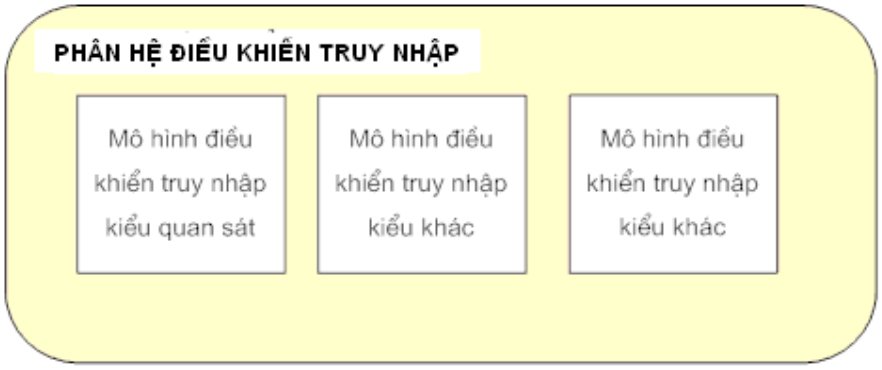


Hình 2.10 Phân hệ xử lý bản tin trong SNMPv3

Module SNMPv3 tách phần dữ liệu của bản tin gửi tới phân hệ bảo mật để giải nén và nhận thực. Phân hệ bảo mật cũng có nhiệm vụ nén dữ liệu. Cấu trúc module của phân hệ bảo mật như sau:

Hình 2.11 Cấu trúc module của phân hệ bảo mật trong SNMPv3

SNMPv3 tương thích hoàn toàn với SNMPv1 và SNMPv2, nó gồm mô hình bảo mật dựa trên người dùng và mô hình bảo mật chung để xử lý SNMPv1, SNMPv2. Cấu trúc module đơn giản khi thêm vào các module bảo mật dạng khác trong quá trình phát triển. Khi số liệu tách ra khỏi PDU và nó sẽ được gửi tới ứng dụng thích hợp qua phân hệ điều khiển truy nhập. Phân hệ điều khiển truy nhập chịu trách nhiệm xác định đối tượng bị quản lý và cách thức truy nhập tới nó. Hiện nay chỉ có một mô hình điều khiển truy nhập nhưng nó có thể mở rộng trong tương lai (RFC2575).



Hình 2.12 Cấu trúc phân hệ điều khiển truy nhập trong SNMPv3

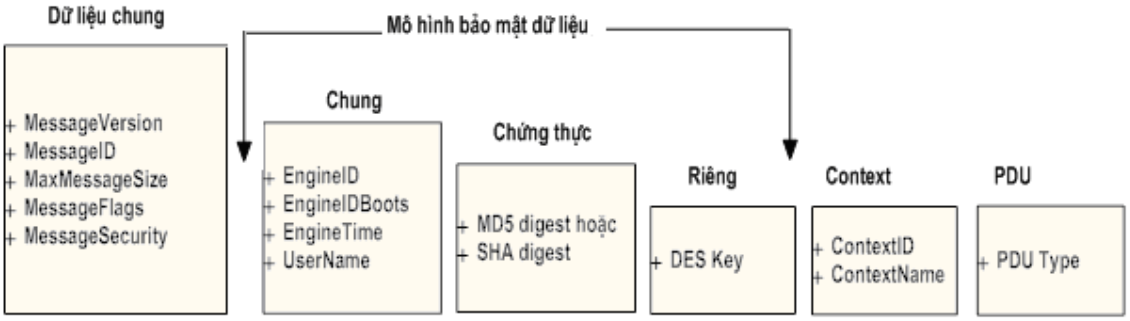
Mô hình điều khiển truy nhập có thể nhìn thấy (RFC 2575) quyết định người dùng có thể truy nhập (đọc hoặc đặt trạng thái) cho đối tượng quản lý .

2.6.1 Khuôn dạng bản tin SNMPv3

RFC 2572 định nghĩa các khuôn dạng bản tin SNMPv3. Khuôn dạng bản tin SNMPv3 được phân chia trong trong bốn phần (Hình 2.13).

- Dữ liệu chung (Common data)- Trường này xuất hiện trong tất cả các bản tin SNMPv3.
- Bảo mật mô hình dữ liệu (Security model data)- Vùng này có ba phần: phần chung, phần dành cho sự chứng thực và phần cho dữ liệu riêng.

- Context – Hai trường nhận dạng và tên được dùng để cung cấp context cho PDU nào sẽ phải xử lý.
- PDU –Vùng này chứa một SNMPv2c PDU.



Hình 2.13 Khuôn dạng bản tin SNMPv3

MessageVersion

Trường đầu tiên trong bản tin là trường phiên bản SNMP.Trường này cung cấp tính tương thích với các phiên bản khác nhau. Giá trị 3 trong trường này chỉ ra đây là một bản tin SNMPv3. Giá trị 2 và 1 tương ứng với SNMPv2 và SNMPv1.

MessageID

Nhận dạng bản tin là một số được sử dụng giữa hai thực thể cho bản tin tương quan. Đơn vị dữ liệu giao thức PDU chứa trường nhận dạng yêu cầu và được sử dụng nhận dạng trong SNMPv1 và SNMPv2c, nhưng từ SNMPv3 cả mã hóa PDUs, message ID đều nằm bên trong tiêu đề.

MaxMessageSize

Kích thước bản tin lớn nhất MaxMessageSize là kích thước lớn nhất của bản tin được hỗ trợ bởi bên gửi bản tin. Đây là gói kích thước lớn nhất để giao thức vận chuyển có thể mang mà không cần phân đoạn. Bên phía thu sử dụng giá trị MaxMessageSize để bảo đảm sự trả lời của nó vẫn nằm trong phạm vi kích thước cho phép.

MessageFlags

Cờ đánh dấu bản tin có độ dài 1 byte, xác định sự thiết lập chứng thực và đặt riêng cho bản tin. Nó cũng thông báo khi bản tin yêu cầu một sự đáp lại từ phía máy thu. Có ba bit được sử dụng khi việc mã hóa không thành công.

- Không có chứng thực và không có sự riêng lẻ (giá trị bit 000).
- Chứng thực và không có sự riêng lẻ (giá trị bit 001).
- Chứng thực và riêng lẻ (giá trị bit 011).

Cả ba trường hợp trên đều có thể đặt cảnh báo tùy chọn.

MessageSecurity

Bảo mật bản tin là một đối tượng số nguyên được đặt bảo mật cho bản tin. Phạm vi của những giá trị hỗ trợ như sau:

- 0 được dành cho " any " (bất kỳ).
- 1 được dành cho SNMPv1.
- 2 được dành cho SNMPv2c.
- 3 được dành cho USM (User-based Security Model).
- 4-555 được dành cho những mô hình bảo mật tiêu chuẩn khác.

Các giá trị ngoài 255 có thể được dùng cho mô hình bảo mật tiêu chuẩn. Bên thu cũng phải dùng cùng mô hình bảo mật đó khi xử lý bảo mật hoạt động. Phân hệ bảo mật điều khiển quá trình xử lý này của bản tin SNMPv3.

M*ô hình bảo mật dữ liệu chung*

Phần chung của mô hình bảo mật dữ liệu bao gồm các trường sau:

- EngineID: Sự nhận dạng duy nhất của engine SNMPv3.
- EngineBoots: là khoảng thời gian mà engine SNMP bắt đầu up hoặc reset giá trị của usmUserTable cuối cùng bị sửa đổi.
- EngineTime: Số giây mà giá trị EngineBoots cuối được sửa đổi.
- UserName: Tên của người dùng.

Những trường trên đi trước các vùng dữ liệu chứng thực và riêng lẻ. EngineID và UserName được dùng để tạo một chỉ số trong một bảng gọi là usmUserTable. Bảng này lưu giữ dữ liệu mô hình bảo mật cho EngineID và cặp người dùng.

Mô hình bảo mật dữ liệu qua chứng thực

Hai giao thức chứng thực hỗ trợ trong SNMPv3 là MD5 và SHA. Cả hai giao thức cùng phục vụ cho mục đích: xác nhận thông báo SNMPv3. Thuật toán MD5 tính toán 16 byte (128 bit) digest và 12 byte đầu tiên (96 bit) bao gồm các thành phần của bản tin bên trong các trường chứng thực. Người dùng phải chọn một chìa khóa bí mật 16-octet (byte) để dùng cho thuật toán MD5. Nếu người dùng chọn thuật toán chứng thực SHA thì thuật toán tính toán 20 byte (160 bit) digest và một lần nữa 12 byte đầu tiên (96 bit) bao gồm những thành phần của bản tin chứng thực. Người dùng phải chọn một chìa khóa bí mật 20-octet để dùng thuật toán SHA.

Dù giải thuật nào được dùng thì trường giao thức chứng thực là một chuỗi 12

byte được dùng làm nhận dạng để chứng thực bản tin. Khi một thực thể SNMPv3 (manager) muốn gửi một yêu cầu cho thực thể khác (agent) phải dùng một chìa khóa bí mật cho cả hai phía.

Mô hình bảo mật dữ liệu qua giao thức riêng

Trường của giao thức riêng lẻ là chuỗi 18 byte octet dùng cho thuật toán tiêu chuẩn mã hóa dữ liệu DES (Data Encryption Standard). Mã hóa dùng khóa 16 byte. 8 octet đầu tiên của khóa bí mật 16 octet dùng như khóa DES. 8 octet tiếp theo được dùng như một vector khởi tạo. Cả hai dùng một khóa riêng bí mật để mã hóa và giải mã bản tin.

2.6.2 Các ứng dụng nội bộ của SNMPv3

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.

2.6.3 Nguyên tắc hoạt động của giao thức SNMPv3

i, Gửi một bản tin hoặc một yêu cầu

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

- Tạo ra các yêu cầu ứng dụng
  - 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.

ii, 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 kết quả (result) là errorIndication thì errorIndication sẽ trả lại ứng dụng gọi tới và không có hành động nào được xử lý nữa.
- Nếu kết quả 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.

iii, 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, tuỳ vào giá trị của sendPduHandle là rỗng hay không rỗng ta có hai hướng xử lý tiếp.

iv, 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 kết quả 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 quan sendpduHandle.
- Nếu không có ứng dụng nào đợi, bản tin bị huỷ bỏ và quá trình xử lý kết thúc. stateReference được giải phóng. snmpUnknownPDUHandlers được tăng lên. Quá trình xử lý kết thúc.
- Nếu xuất hiện ứng dụng đang đợi thì đáp ứng được trả về.

2.6.4 Hỗ trợ bảo mật và nhận thực trong SNMPv3

Một trong những mục tiêu chính – nếu không coi là một mục đích chính chính – khi phát triển SNMPv3 đó là thêm đặc tính bảo mật cho quản lý SNMP. Xác thực và bảo vệ thông tin, cũng như xác thực và điều khiển truy cập, đã được nêu rõ ở trên.

Cấu trúc SNMPv3 cho phép sử dụng linh hoạt bất cứ một giao thức nào cho xác thực và bảo vệ thông tin. Dù sao, nhóm IETF SNMPv3 đã đưa ra mô hình bảo mật người dùng. Chúng ta sẽ tìm hiểu thêm về các khía cạnh chung về bảo mật kết hợp với các kiểu của các mối đe doạ bảo mật, mô hình bảo mật, định dạng dữ liệu bản tin để điều tiết các tham số bảo mật và sử dụng cũng như quản lý của các khoá trong phần này.

Các mối đe doạ bảo mật.

Có 4 mối đe doạ đến thông tin quản lý mạng khi một thực thể quản lý được truyền đến thực thể khác đó là:

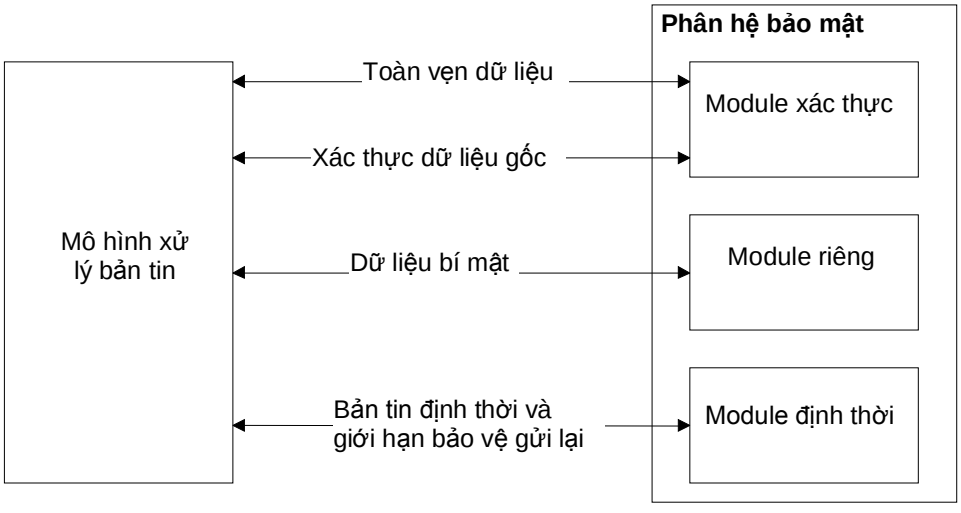
- Thông tin có thể bị thay đổi bởi một người dùng không được phép nào đó trong khi truyền.

- Người dùng không được phép cố gắng giả trang như người dùng được phép.
- Thông tin SNMP được chia làm nhiều gói nhỏ để truyền đi theo nhiều hướng và phía nhận phải sắp xếp lại. Vì vậy nó có thể bị người nào đó làm trễ 1 gói tin, bị gửi lại do một người không được phép tạo ra ... làm thay đổi thông tin của bản tin
- Bị ngăn chặn hoặc bị lộ bản tin.

Ít nhất có 2 mối đe doạ trên thường xảy ra với kết nối dữ liệu truyền thống, nhưng với mô hình bảo mật người dùng SNMP thì nó được coi là không có mối đe doạ. Thứ nhất là từ chối dịch vụ, một xác thực người dùng sẽ bị từ chối dịch vụ bởi thực thể quản lý . Nó không bị coi như mối đe doạ, khi mạng lỗi có thể là lý do của sự từ chối, và một giao thức sẽ thực thi mục đích này. Thứ hai là thống kê lưu lượng bởi một người dùng không xác thực. Nhóm IETF SNMv3 đã xác định rằng không có thuận lợi quan trọng nào đạt được bằng cách chống lại sự tấn công này.

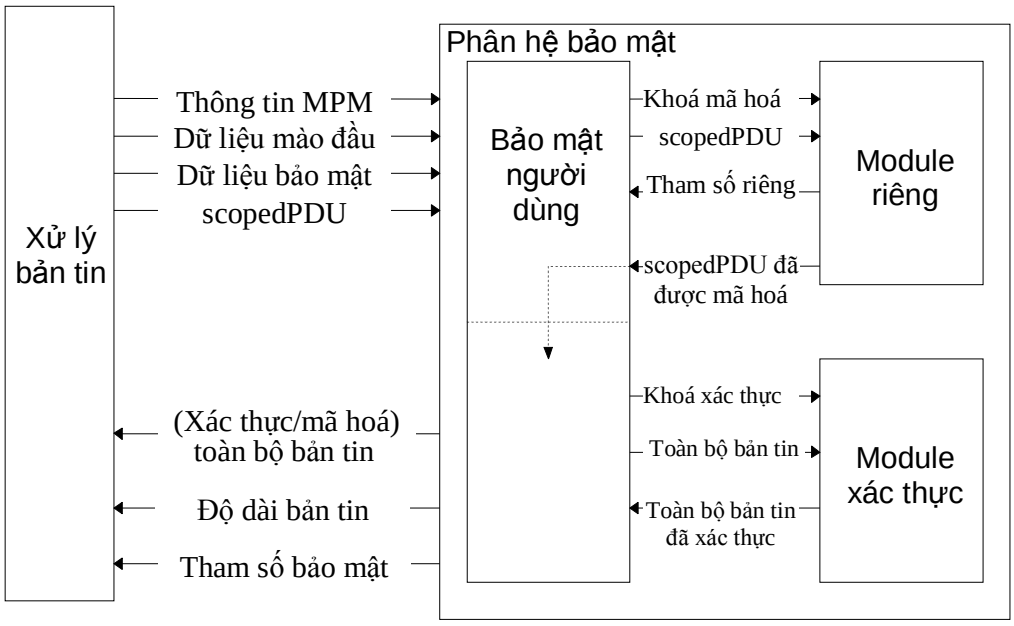
Mô hình bảo mật

Trong điều kiện hoạt động bình thường, mô hình xử lý bản tin tác động với mô hình phân hệ bảo mật. Ở ví dụ hình 2.9 về kiến trúc thực thể của SNMPv3, chúng ta thấy rằng bản tin gửi đi sẽ được tạo bởi một ứng dụng và kiểm soát đầu tiên bởi bộ giao vận, sau đó bởi mô hình xử lý bản tin, cuối cùng là mô hình bảo mật. Nếu bản tin cần được xác thực, mô hình bảo mật sẽ xác thực nó và chuyển tiếp đến mô hình xử lý bản tin. Tương tự với bản tin đến, mô hình xử lý bản tin yêu cầu dịch vụ này của mô hình bảo mật để xác thực chỉ số người dùng. Hình 2.14 chỉ ra các dịch vụ được cung cấp bởi 3 module – module xác thực, module riêng và module định thời – trong mô hình bảo mật tới mô hình xử lý bản tin.



Hình 2.14 Mô hình bảo mật

Mô hình bảo mật người dùng SNMPv3

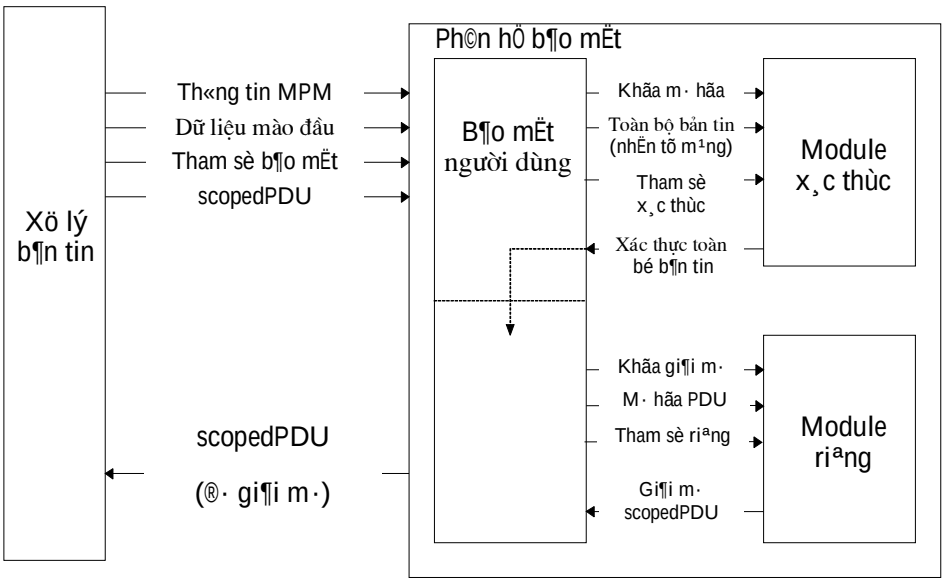


Hình 2.15 Dịch vụ riêng và xác thực cho bản tin đi

Mô hình bảo mật trong SNMPv3 là mô hình bảo mật người dùng (User-base Security Model viết tắt là USM). Nó phản ánh khái niệm tên người dùng truyền thống. Như chúng ta đã định nghĩa giao diện dịch vụ trừu tượng giữa các phân hệ khác nhau trong thực thể SNMP, bây giờ chúng ta sẽ định nghĩa giao diện dịch vụ trừu tượng trong USM. Các định nghĩa này bao trùm lên khái niệm về giao diện giữa dịch vụ giống USM và xác thực không phụ thuộc và dịch vụ riêng. Hai primitive được kết hợp với một dịch vụ xác thực, một tạo ra bản tin xác thực đi, và một để kiểm tra bản tin xác thực đến. Tương tự, 2 primitive được kết hợp với các dịch vụ riêng: *encryptData* để mã hoá bản tin đi và *decryptData* để giải mã bản tin đến.

Các dịch vụ được cung cấp bởi module xác thực và module riêng trong phân hệ bảo mật cho bản tin đi và bản tin đến. Mô hình xử lý bản tin dẫn chứng cho USM trong phân hệ bảo mật. Dựa trên mức bảo mật gắn trên bản tin, USM lần lượt được dẫn qua module xác thực và module riêng. Kết quả được đưa trở lại mô hình xử lý bản tin bởi USM.

Hình 2.15 chỉ ra sự xử lý một bản tin đi và hình 2.16 cho thấy sự xử lý ngược lại của 1 bản tin đến đi qua xác nhận hợp lệ trước sau đó sẽ được giải mã hoá bởi module riêng.



Hình 2.16 Dịch vụ riêng và xác thực cho bản tin đến

Các giao thức bảo mật.

Nền tảng cho bảo mật sử dụng xác thực và bảo vệ riêng là các khoá bí mật được dùng chung bởi người gửi và người dùng - một người xác thực và người kia mã hoá và giải mã. Ban đầu, các khoá bí mật của USM là mật khẩu. Hai thuật toán được khuyến nghị trong SNMPv3 đó là HMAC-MD5-96 và HMAC-SHA-96.

Khoá xác thực. Khoá bí mật cho xác thực được xuất phát từ mật khẩu được người dùng lựa chọn. Người dùng ở đây là các công cụ SNMP không xác thực, nó tạo ra hệ thống quản lý mạng. Trong hai thuật toán MD5 và SHA-1, mật khẩu được lặp lại cho đến khi có dạng 2^{20} octet (1048576 octet), xoá lần lặp cuối nếu thấy cần thiết.

Thủ tục mã hoá HMAC. Mã MAC dài 96 bit xuất phát từ việc sử dụng thủ tục HMAC (RFC 2104, RFC 2274).

Quản lý khoá. Người dùng (hệ thống quản lý mạng) chỉ có một mật khẩu và do đó chỉ có một khoá bí mật, digest1 (đã đề cập trong phần khoá xác thực). Tuy nhiên, nó kết nối với tất cả các công cụ SNMP xác thực (tất cả các agent trên mạng). Thông tin chia sẻ thêm vào sự bí mật giữa 2 công cụ kết nối. Khái niệm khoá cục bộ được đưa ra để tránh sự lưu trữ khoá khác nhau trên các công cụ xác thực với liên kết người dùng. Thuật toán băm - giống như sử dụng để tạo ra khoá bí mật - được sử dụng để tạo ra khoá cục bộ.

Phát hiện. Một trong những chức năng quan trọng của hệ thống quản lý mạng là phát hiện ra những agent trên mạng. Phát hiện được hoàn thành bằng cách ra các bản tin yêu cầu với mức bảo mật là không cần xác nhận và không có khoá riêng, có tên là khởi tạo (initial), một *SNMP engine ID* xác thực có độ dài bằng không và *varBin* là rỗng. Công cụ xác thực sẽ hồi đáp bằng bản tin hồi đáp bao gồm *engine ID* và điền vào tham số bảo mật. Thông tin thêm này có được qua bản tin *pair-wise*.

Giao thức mã khoá.

Mã khoá tạo ra các ký tự không đọc được (ciphertext) từ các từ đọc được (plaintext). SNMP khuyến nghị dữ liệu tin cậy nên sử dụng giao thức mã hoá ma trận CBC-DES (Cipher Block Chaining - Data Encryption Standard). USM chỉ rõ yêu cầu scopedPDU chia rõ phần bản tin cần mã khoá. Giá trị bí mật kết hợp với giá trị định thời sẽ tạo ra khoá mã hoá/giải mã và vecto khởi tạo (IV). Mặt khác, giá trị bí mật dựa trên người dùng, do đó sẽ kết hợp đặc thù với hệ thống quản lý mạng.

Điều khiển truy cập

Trong hai phần trước, chúng ta đã nói đến sự bảo mật trong quản lý mạng với sự quan tâm đến tính toàn vẹn dữ liệu, bản tin xác thực, dữ liệu tin cậy và định thời của bản tin. Bây giờ chúng ta sẽ đề cập đến điều khiển truy cập, nó giải quyết vấn đề ai có quyền truy cập vào các phần tử mạng và họ có thể truy cập những gì. Trong SNMP v1 và SNMPv2, vấn đề này đã được đề cập trong phần chính sách truy cập dựa trên truyền thông. Trong SNMPv3, điều khiển truy cập đã bảo mật hơn và mềm dẻo hơn bởi mô hình điều khiển kết nối dựa trên các View (View-based Access Control Model viết tắt là VACM).

VACM định nghĩa các giao diện mà ứng dụng trong một agent có thể sử dụng để hợp thức các câu lệnh yêu cầu và các bộ nhận thông báo. Nó hợp thức nguồn gửi và quyền truy cập đối với các lệnh yêu cầu. Một trong những giả định được tạo ra là xác thực của nguồn đã được thực hiện bởi module xác thực. Để thực hiện các dịch vụ này, dữ liệu cục bộ bao gồm các quyền và chính sách truy cập, được gọi là lưu trữ dữ liệu cấu hình cục bộ (LCD), đã được tạo ra trong thực thể SNMP. LCD này đặc trưng trong một agent hoặc trong một chức năng quản lý trong vai trò của một agent khi nó kết nối với một manager khác.

LCD cần thiết cho việc cấu hình từ xa và cân nhắc bảo mật cần được quan tâm, vì vậy module MIB cho VACM được đưa ra.

Các phần tử của mô hình

VACM gồm 5 phần tử: (1) các nhóm, (2) mức bảo mật, (3) ngữ cảnh, (4) các view MIB và họ các view, (5) chính sách truy cập.

Các nhóm. Một nhóm, *groupName*, gồm 1 cặp *vacmSecurityModel* và *vacmSecurityName* (mô hình bảo mật và tên bảo mật) đại diện cho các đối tượng quản

lý có thể truy cập. Một tên bảo mật là chủ độc lập với mô hình bảo mật được sử dụng. Tất cả các phần tử thuộc một nhóm có quyền truy cập giống nhau.

Mức bảo mật. Có các mức

Không xác thực – không bảo vệ

Có xác thực – không bảo vệ

Có xác thực – có bảo vệ

Ngữ cảnh. Ngữ cảnh SNMP là sự thu thập các thông tin quản lý có thể truy cập của các thực thể SNMP (agent). Một thực thể SNMP truy cập đến tiềm năng hơn một ngữ cảnh. Mỗi công cụ SNMP có một bảng ngữ cảnh liệt kê các ngữ cảnh cục bộ có thể bằng các *contextName*.

Các view MIB và họ các view. Trong SNMPv1 và SNMPv2, quyền truy cập tới ngữ cảnh được điều khiển bởi các view MIB. Một view MIB được định nghĩa cho mỗi nhóm và chi tiết của kiểu đối tượng quản lý (và tuỳ chọn, trường hợp rõ ràng của các kiểu đối tượng). Một view MIB phức tạp xảy ra khi tất cả các đối tượng của cột dựa trên khái niệm hàng của bảng xuất hiện trên các cây con khác nhau, mỗi cột một view với định dạng như nhau. Vì định dạng như nhau nên yêu cầu của cây con phải tập hợp vào một cấu trúc, được gọi là họ các cây con view. Một họ các cây con view là một cặp của giá trị OBJECT IDENTIFER (được gọi là tên của họ) cùng với một giá trị chuỗi bit (được gọi là mặt nạ họ). Mặt nạ họ cho biết nhận dạng con của tên họ kết hợp là dấu hiệu để định nghĩa họ. Một họ của các cây con view có thể bao gồm hoặc loại trừ một view MIB.

Quyền truy cập. Xác định quyền truy cập các đối tượng như quyền đọc, ghi và thông báo.

2.6.5 Ứng dụng thực tiễn của SNMPv3

Một số vấn đề thực tiễn quản lý mạng

Cùng với sự phát triển đa dạng của các công nghệ mạng, các thách thức đối với hệ thống quản lý mạng ngày càng lớn nhất là đối với các mạng lớn, các kiểu lưu lượng và sự tăng trưởng lưu lượng tiếp tục tăng không ngừng. Với các yêu cầu đảm bảo chất lượng dịch vụ trong môi trường đa dịch vụ, hệ thống quản lý mạng phải có khả năng quản lý từ đầu cuối tới đầu cuối, giảm giá thành quản lý qua các thoả thuận chất lượng dịch vụ SLA (Service Level Agreement), các hệ thống quản lý mạng của các nhà sản xuất thiết bị và sử dụng phần mềm quản lý hiệu quả. Dưới đây sẽ phân tích một số vấn đề này sinh khi sử dụng giao thức quản lý mạng đơn giản SNMP.

i, Chuyển các dữ liệu quản lý vào mã lệnh

Dữ liệu liên kết và mã là các khái niệm tính toán cơ bản, nó tập trung vào vùng quản lý mạng trên cơ sở các thực thể mạng NE (Network Element) chuyển dữ liệu quản lý tới trạm quản lý . Khi chuyển dữ liệu thành các mã có một số vấn đề sau:

- Các đối tượng bị quản lý nằm trên rất nhiều Agent
- Bản sao của các đối tượng quản lý nằm tại hệ thống manager
- Sự thay đổi dữ liệu trên các Agent sẽ làm thay đổi dữ liệu bản sao trên manager.

Cơ sở thông tin quản lý MIB cung cấp một hạ tầng quản lý và phải dự phòng các không gian nhớ cho những thay đổi của đối tượng quản lý . Mặt khác, sự phát triển và độ phức tạp của thực thể mạng (NE) tăng lên không ngừng trong khi quá trình truyền và nhận dữ liệu từ Agent là thủ tục bắt buộc của SNMP, vì vậy việc chuyển các dữ liệu thành mã như thế nào là một vấn đề thách thức của hệ thống quản lý mạng. Hơn nữa, hệ thống quản lý có nên đòi hỏi tất cả dữ liệu agent hay không? Trong thực tế, điều này chỉ chấp nhận được trên những mạng nhỏ nhưng không thể thực hiện được trên các mạng lớn. Khi các NE trở thành phức tạp hơn thì gánh nặng lại đặt lên hệ thống quản lý .

ii, Sự tăng trưởng của MIB

Các bảng cơ sở thông tin quản lý lưu trữ các tham số của đối tượng quản lý , khi số lượng NE lớn đồng nghĩa với việc mở rộng bảng MIB. Sự phức tạp gia tăng khi nhiều nhà cung cấp cung cấp những module MIB cho các NE của họ theo dạng file văn bản. Những file này có thể hợp nhất vào trong một hệ thống mạng quản lý NMS và dùng phối hợp với bộ duyệt MIB. MIB chứa định nghĩa đối tượng quản lý và dùng để dẫn xuất mô hình cơ sở dữ liệu cho NMS. Mô hình cơ sở dữ liệu NMS chứa số lượng lớn các bảng, ví dụ một bảng để cất giữ những đường dẫn chi tiết, bảng khác cho các mạch ảo,v.v. Hệ thống quản lý mạng NMS theo dõi và sửa đổi những giá trị của NE, quản lý các đối tượng và lưu giữ nó trong cơ sở dữ liệu của mình.

Việc tích hợp các hệ thống thiết bị thành các phần tử mạng lớn cũng mang lại một số khó khăn trong hệ thống quản lý mạng, vì các chức năng được tích hợp rất khó quản lý đồng thời các hệ thống quản lý phải hỗ trợ rất nhiều tương tác trong FCAPS.

iii, Độ phức tạp trong triển khai

Việc xây dựng hệ thống quản lý cho những thiết bị mạng hiện nay và trong tương lai ngày càng gặp nhiều khó khăn (điều này là đúng với việc phát triển thiết bị của những công nghệ mới như MPLS hay Ethernet Gigabit là việc thêm vào hoặc kế thừa các thực thể mạng-NE lớp 2). Một số nhà cung cấp có những nhóm được tách riêng dành cho thực thể mạng và việc phát triển hệ thống quản lý nên cần có sự truyền thông giữa những nhóm này. Ngoài ra việc thiết lập các kỹ năng yêu cầu của

người phát triển phần mềm NMS đang tăng và bao gồm:

- Việc phát triển và làm mô hình hướng đối tượng sử dụng UML (Unified Modeling Language) cho việc giữ những yêu cầu, định nghĩa các hoạt động và các trường hợp sử dụng để sắp xếp chúng vào trong các lớp phần mềm.
- Phát triển các phần mềm quản lý trên Java/C++.
- Phần mềm Server đa xử lý FCAPS.
- Đặc biệt hỗ trợ cho việc phát triển các đặc tính như ATM/MPLS.
- Cơ sở dữ liệu của việc thiết kế/nâng cấp phù hợp với MIB tới giản đồ cơ sở dữ liệu qua nhiều phiên bản phần mềm NMS/NE.
- Công nghệ lớp 2 như ATM, FR và Gigabit Ethernet.
- Công nghệ kế thừa như thoại qua TDM và X.25.
- Khả năng phát triển mô hình và thành phần phần mềm chung, hệ thống quản lý có thể giấu nhiều chi tiết nằm bên dưới của hoạt động mạng.
- Thiết kế Client/server.
- Quản lý việc thiết kế đối tượng, giai đoạn làm mô hình của hệ thống quản lý .
- Việc thiết kế MIB cần có đối tượng mới bên trong thiết bị quản lý để hỗ trợ hệ thống quản lý .

Sự di trú chung tới cơ sở hạ tầng lớp 3 là một lý do khác cho việc mở rộng giữa những kỹ năng phát triển sẵn có và các đặc tính sản phẩm yêu cầu. Đây là một cách tiếp cận khác cho việc phát triển hệ thống quản lý thông qua:

- Tập giải pháp tiêu chuẩn.
- Phân tán và giải quyết các vấn đề phát sinh.
- Xử lý thông tin thống kê.
- Bao quát những chu trình phát triển ngắn.
- Tối giản việc thay đổi mã.
- Tăng khả năng kiểm tra.

2.7 TỔNG KẾT CHƯƠNG 2

- SNMP cung cấp cách thức quản lý mạng các host như mạng của các máy tính trạm hoặc máy chủ, router, bridge và hub từ máy tính điều khiển tập trung chạy phần mềm quản lý mạng.
- Các chuẩn c ho SNMP và những giao thức khác như TCP/IP được ấn bản trong

các RFC.

- SNMP phiên bản 1 (SNMPv1) là phiên bản chuẩn của giao thức SNMP. Nó được định nghĩa trong RFC 1157 và đây là chuẩn đầy đủ của IETF. Độ bảo mật trong SNMPv1 chỉ dựa vào từ khóa (password).

- SNMP phiên bản 2 (SNMPv2) được phát triển để cung cấp chức năng bảo mật mà SNMP còn thiếu. Phiên bản này được định nghĩa trong các RFC 1905, 1906 và 1907.

- SNMP phiên bản 3 (SNMPv3) được phát triển để cung cấp độ bảo mật tốt nhất trong quản lý SNMP. Nó được định nghĩa trong các RFC 2571, 2572, 2573, 2574 và 2575.

- Thiết bị được quản lý là thiết bị có chạy phần mềm SNMP agent.

- Các đối tượng được quản lý là các đặc tính hoạt động của thiết bị được quản lý .

- Một đặc tính hoạt động đơn như phiên UDP trên một thiết bị quản lý đơn được coi là một biến đối tượng.

- Cơ sở thông tin quản lý (MIB) là cơ sở dữ liệu của các đối tượng được quản lý , nó được truy nhập thông qua các giao thức quản lý mạng.

- SNMP chứa hai chuẩn MIB. Chuẩn MIB I có trong RFC 1156 được định nghĩa để quản lý Internet dựa trên TCP/IP. Chuẩn MIB II định nghĩa trong RFC 1213, cơ bản vẫn dựa trên MIB I. MIB II là định nghĩa được dùng hiện nay. SNMPv2 bao gồm MIB II và bổ sung một số đối tượng mới khác.

- Các đối tượng MIB là các đối tượng được quản lý được phân loại theo công việc và mà chúng thực hiện, các đối tượng này nằm trong MIB.

- Số nhận dạng đối tượng là một sery số nguyên dựa trên nút trong cây, được tách bằng các dấu chấm (.). Vì thế iso(1).org(3).dod(6).internet(1) trong dạng số nhận dạng đối tượng được biểu diễn là 1.3.6.1 hay dưới dạng chữa là iso.org.dod.internet.

- Trong SNMP các vận hành yêu cầu tuân theo tuần tự.

- Cấu trúc thông tin quản lý (SMI) là chuẩn sử dụng ASN.1. SMI đặc tả cú pháp cho các loại dữ liệu như số nhận dạng đối tượng, bộ đếm, hàng, bảng, chuỗi, địa chỉ mạng và các thành tố SNMP khác sao cho độc lập với cơ cấu SNMP.

- Hai nhánh chính dựa trên gốc Internet là Quản lý và MIB cá nhân. Các chuẩn MIB công nghiệp là nhánh quản lý iso.org.dod.internet.mgmt.mib với số nhận dạng đối tượng là 1.3.6.1.2.1. Còn các MIB cá nhân là nhánh iso.org.dod.internet.private với số nhận dạng đối tượng là 1.3.6.1.4.

- Trap là các bản tin (unsolicited) gửi từ agent tới NMS.

- SNMPv1 sử dụng các hoạt động Get, Getnext, Set và Trap.
- SNMPv2 sử dụng các hoạt động Get, Getnext, Set, Trap, GetBulk và Inform.
- Các thỏa thuận số doanh nghiệp cá nhân của các các nhân, học viện và các tổ chức đều do IANA quản lý .
- Trong SMIv2 phần chú ý tương đương với trap trong SMIv1. Trong SMIv1, trap thường được đặc tả là macro ASN.1 TRAP-TYPE. Trong SMIv2 phần chú ý được đặc tả bằng macro ASN.1NOTIFICATION-TYPE.
- SNMPv2 cung cấp hoạt động inform để cho phép truyền thông từ NMS đến NMS. Khi inform được gửi từ một NMS đến NMS khác thì NMS bên nhận gửi đáp ứng tới NMS bên gửi để xác nhận việc nhận được bản tin.
- Chúng ta có thể sử dụng SNMP inform để gửi trap của SNMPv2 từ một agent tới một NMS. Trong trường hợp này, agent sẽ được NMS thông báo là trab đó đã được nhận.
- Hoạt động report được tăng cường cho SNMPv2 song nó lại không được triển khai. Tuy nhân nó được sử dụng trong SNMPv3 để cho phép các thiết bị sử dụng SNMP truyền thông với nhau và báo cáo lại những sự cố trong việc xử lý các bản tin SNMP.
- Trong SNMPv3, thiết bị được cấu thành từ 4 phần: Điều phối (Dispatcher), Phân hệ xử lý bản tin, Phân hệ bảo mật và Phân hệ điều khiển truy nhập.
- Điều phối là công việc gửi và nhận bản tin. Nó cố gắng xác định phiên bản của mỗi bản tin nhận được (ví dụ phiên bản 1, 2 hay 3) và nếu như phiên bản được hỗ trợ thì nó sẽ điều khiển bản tin tới Phân hệ xử lý bản tin. Phân hệ điều phối cũng gửi các bản tin SNMP tới các thực thể khác.
- Phân hệ xử lý bản tin chuẩn bị các bản tin để gửi đi và trích dữ liệu từ các bản tin nhận được. Một hệ thống xử lý bản tin có thể gồm nhiều khối (module) xử lý bản tin. Ví dụ: một phân hệ có thể có module xử lý các yêu cầu SNMPv1, SNMPv2 và SNMPv3. Nó cũng có thể có các module xử lý cho các mô hình khác trong tương lai.
- Phân hệ bảo mật cung cấp các dịch vụ cá nhân và nhận thực. Nhận thực sử dụng hoặc là các chuỗi truyền thông (SNMPv1 và v2) hoặc là nhận thực dựa trên người dùng SNMPv3. Nhận thực dựa trên người dùng sử dụng thuật toán MD5 hoặc SHA để nhận thực những người sử dụng mà không cần phải gửi từ khóa. Dịch vụ cá nhân sử dụng thuật toán DÉ để mã khóa và giải mã các bản tin SNMP.
- Phân hệ điều khiển truy nhập chịu trách nhiệm điều khiển truy nhập tới các đối tượng MIB. Chúng ta có thể điều khiển đối tượng nào mà người sử dụng có thể truy nhập cũng như những hoạt động nào mà người sử dụng đó cho phép trên những đối tượng này. Ví dụ: chúng ta có thể giới hạn truy nhập dạng đọc-ghi của người sử dụng

với một phần nào đó trong cây mib-2 trong khi vẫn cho phép truy nhập chỉ đọc với toàn bộ cây này.

- Trong SNMPv3, các bộ tạo lệnh tạo ra những yêu cầu get, get-next, getbulk, set và xử lý các đáp ứng. Ứng dụng này được NMS thực hiện, vì vậy nó có thể đưa ra những yêu cầu và thiết lập yêu cầu chống lại các thực thể trên các router, switch, các máy trạm Unix, v.v.

- Trong SNMPv3, bộ đáp ứng lệnh đáp lại các yêu cầu get, get-next, getbulk, set. Với SNMPv3, ứng dụng này được thực hiện bởi một thực thể như router của Cisco hoặc máy trạm Unix. (Với SNMPv1 và v2, bộ đáp ứng lệnh được agent SNMP thực hiện).

- Trong SNMPv3, bộ tạo các thông điệp chú ý tạo ra các chú ý và SNMP trap. Ứng dụng này được một thực thể trên router hoặc máy trạm Unix thực hiện. (Với phiên bản 1 và 2, bộ tạo các thông điệp chú ý này là một phần của agent SNMP).

- Trong SNMPv3, bộ thu thông điệp chú ý bắt và thông báo về các bản tin. Ứng dụng này do một NMS thực hiện.

- Trong SNMPv3, bộ chuyển tiếp proxy chuyển các bản tin giữa các thực thể.

CHƯƠNG 3

GIÁM SÁT TỪ XA RMON

3.1 NGUYÊN LÝ CHUNG

Giám sát mạng được tiếp cận theo hai phương pháp: giám sát từ xa mạng thụ động và giám sát mạng chủ động. Mục tiêu giám sát nhằm kiểm tra và giám sát hiệu năng thực tế của dịch vụ mạng với các thỏa thuận cung cấp chất lượng dịch vụ.

a. Giám sát mạng bị động

Các thiết bị mạng ghi lại các trạng thái lưu lượng mạng để cung cấp các thông tin của một phần tử mạng thực tế. Các bản tin thăm dò (polling) định kỳ được sử dụng để thu thập thông tin dữ liệu cho báo cáo và phân tích. Đây là một phép đo nhỏ tại các thiết bị độc lập. Thông tin trạng thái mạng có thể được suy luận từ tập các phép đo từ các phần tử mạng trên. Giám sát thụ động không yêu cầu bất cứ một lưu lượng phụ nào để sử dụng cho các mục đích đo.

b. Giám sát mạng chủ động

Phương pháp giám sát mạng chủ động gửi các thông tin giám sát vào mạng quản lý . Các luồng dữ liệu tổng hợp gồm các gói tin thăm dò được gửi vào mạng nhằm giám sát hiệu năng mạng. Các nhà phân tích thu thập các luồng dữ liệu để phân tích và đánh giá hiệu năng mạng. Phương pháp giám sát mạng chủ động cung cấp bài đo mang tính tổng thể qua một loạt các phần tử mạng trong hệ thống.

Các hệ thống giám sát bị động hoặc chủ động được phát triển do một số lý do sau:

Mục tiêu giám sát và báo cáo: Các dịch vụ mạng được cung cấp theo các mục tiêu thỏa thuận chất lượng dịch vụ ví dụ như: Các mạng chủ động và giám sát SLA; Chiến lược dài hạn liên quan tới sự thay đổi hiệu năng SLA và mức hiệu năng mạng với các mục tiêu chất lượng dịch vụ được yêu cầu và cảm nhận bởi người sử dụng.

Như một mạch vòng hồi tiếp cho tiến trình lập kế hoạch mạng, các kết quả giám sát chủ động và bị động là cơ sở cho các bài toán dự đoán, lập ngưỡng trong kế hoạch phát triển và quy hoạch mạng.

Đối với các nhà cung cấp dịch vụ, giám sát bị động và chủ động cung cấp các cơ hội cho dịch vụ gia tăng giá trị, hỗ trợ khách hàng có các thông tin nhằm đánh giá mức độ sử dụng mạng và cách thức thỏa mãn thỏa thuận chất lượng dịch vụ SLA.

3.2 CÁC PHƯƠNG PHÁP GIÁM SÁT MẠNG

3.2.1 Giám sát mạng bị động

Từ góc độ chất lượng dịch vụ, giám sát mạng bị động liên quan tới vấn đề gửi thông tin giám sát để giám sát trạng thái duy trì các chức năng QoS đang thực hiện. Phương pháp giám sát mạng bị động thường được sử dụng giao thức quản lý mạng đơn giản SNMP để thu thập các thông tin trong cơ sở dữ liệu thông tin quản lý MIB. Các khía cạnh của vấn đề thu thập thông tin gồm: Tần suất gửi thông tin, các trạng thái trên từng liên kết, giám sát hệ thống và ma trận lưu lượng lõi.

a. Tần suất gửi thông tin

Trên thực tế, tần suất gửi thông tin giám sát được xác định trong sự cân bằng giữa khả năng xử lý của hệ thống quản lý mạng, tải của các thiết bị và sự ảnh hưởng của lưu lượng giám sát trên mạng. Các thông tin trạng thái mạng thường nằm dưới dạng các gói tin và các byte, các thông tin này có thể được sử dụng để xác định các yêu cầu lưu lượng trung bình qua các mẫu lưu lượng. Chu kỳ giám sát lớn có kích thước mẫu lớn và có thể được sử dụng cho các mục tiêu mang tính chiến lược. Tuy nhiên, dữ liệu giám sát có thể có giá trị trung bình trong khoảng thời gian dài và không thể hiện được sự thay đổi trong hệ thống. Vì vậy, các chu kỳ ngắn được ưa chuộng hơn vì các phép đo đưa lại các kết quả tốt hơn mặc dù phải cân bằng với lưu lượng tải giám sát.

b. Các trạng thái trên từng liên kết

Các trạng thái trên từng liên kết có thể sử dụng với các mục đích khác nhau tùy thuộc vào vị trí trong mạng và chia thành hai kiểu: liên kết truy nhập và liên kết lõi. Các liên kết truy nhập có thể bao gồm cả vùng phân biệt dịch vụ (Differ) và cả cùng nhà cung cấp dịch vụ và khách hàng. Vì vậy, trạng thái của liên kết truy nhập được sử dụng cho cả mục đích phát hiện lỗi và báo cáo trạng thái tới khách hàng sử dụng dịch vụ cũng như tới các lớp QoS của thiết bị biên mạng. Trên các liên kết lõi, trạng thái chất lượng dịch vụ được sử dụng cho cả mục đích phát hiện lỗi và như một tham số đầu vào của tiến trình quy hoạch mạng lõi. Các trạng thái trên từng liên kết được xác định qua một số phương pháp như: giám sát lớp, giám sát chính sách, giám sát hàng đợi và mất gói.

Giám sát lớp : Mục đích sử dụng chính của các trạng thái phân lớp là để xác minh lưu lượng có nằm trong lớp thích hợp hay không. Các trạng thái lớp còn có thể được sử dụng để xác định hoặc suy luận tới các trạng thái khác. Giám sát phân lớp được thực hiện trên từng lớp hoặc tập hợp các lớp.

Giám sát chính sách : Giám sát chính sách trong phương pháp giám sát thụ động gồm kiểu ép buộc tốc độ tối đa cho dịch vụ thời gian thực và đánh dấu các lưu lượng trong hợp đồng lưu lượng.

Giám sát hàng đợi và tỉ lệ tổn thất : Phương pháp thông thường để giám sát hàng

đợi và tỉ lệ loại bỏ gói được thực hiện theo qua số lượng gói truyền phát và tổn thất. Việc giám sát tỷ lệ tổn thất có thể được thực hiện trên số lượng gói tin hủy bỏ theo trọng số tại phần đuôi của lưu lượng hoặc thông qua giám sát kỹ thuật loại bỏ gói sớm RED (Ramdom Early Detection).

c. Giám sát hệ thống

Về mặt nguyên tắc, các gói tin loại bỏ được thực hiện tại các nút mạng. Tùy theo kiến trúc của các nút mạng các gói tin có thể được loại bỏ ở các vị trí khác nhau theo các điều kiện ràng buộc của hệ thống. Các hệ thống luôn được thiết kế nhằm giảm thiểu các lưu lượng loại bỏ. Mặt khác, vấn đề loại bỏ gói tin là một luôn xảy ra trên thực tế. Vì vậy, việc giám sát các trường hợp như vậy là rất cần thiết nhằm cung cấp các thông tin về các vấn đề gây ảnh hưởng tới chất lượng dịch vụ cung cấp. Một vài kiểu hệ thống loại bỏ gói tin điển hình gồm : (1) Loại bỏ gói không lưu đệm khi bộ nhớ đệm được chia sẻ giữa các hàng đợi trong một hệ thống, tại đó có các gói tin đến và không đủ bộ nhớ cho các gói tin và gây tắc nghẽn lưu lượng ; (2) Loại bỏ gói tin tại đầu vào xảy ra khi không đủ không gian bộ nhớ đệm cho các gói tin đầu vào mặc dù các quyết định chuyển mạch và định tuyến đã được thực hiện. Loại bỏ gói tin đầu vào cho thấy năng lực chuyển tiếp gói tin trong hệ thống chưa đáp ứng được các yêu cầu của người sử dụng. Các hệ thống loại bỏ gói tin như trên cần được giám sát qua các cơ sở thông tin quản lý đặc biệt của nhà cung cấp thiết bị. Thông tin về các hiện tượng loại bỏ gói tin trên sẽ sử dụng để xác định nguyên nhân loại bỏ gói và tránh sự lặp lại.

d. Ma trận lưu lượng lõi

Ma trận lưu lượng lõi là một ma trận của các yêu cầu lưu lượng đầu vào và đầu ra trong mạng lõi. Ma trận lưu lượng có thể đo hoặc đánh giá từ các trạng thái thu thập được qua các kỹ thuật giám sát thụ động. Lợi ích chính của ma trận lưu lượng lõi là để lập kế hoạch mạng, dự đoán mức tăng trưởng lưu lượng và mô hình các kịch bản có thể xảy ra nhằm dự đoán sự ảnh hưởng của lỗi trong các thành phần mạng lõi tới hiệu năng toàn mạng.

3.2.2 Giám sát mạng chủ động

Về mặt nguyên tắc, hoàn toàn có thể đo và giám sát một loạt các tham số chất lượng từ phía người sử dụng qua các thông tin tại đầu cuối hệ thống. Tuy nhiên, sự đa dạng và khác biệt của các giao thức người sử dụng dẫn tới việc thu thập và xử lý thông tin giám sát này rất phức tạp. Một cách tiếp cận khác thường được sử dụng là giám sát từ mức mạng. Giám sát chủ động từ mức mạng sử dụng một số luồng lưu lượng trong đó có chứa các gói tin thăm dò (probe) để phỏng tạo lưu lượng mạng nhằm đánh giá các tham số hiệu năng mạng. Trong các môi trường phân biệt dịch vụ, giám sát mạng chủ động có thể sử dụng để đo hiệu năng của tất cả các phân lớp lưu lượng.

Giám sát mạng chủ động yêu cầu các hệ thống thăm dò tích cực có các agents để gửi và nhận các thông tin thăm dò. Các agent đo các luồng lưu lượng đến và giữ phân tích

trạng thái của các kết quả đo, kết quả này có thể lấy định kỳ từ các thiết bị đo chủ động qua giao thức SNMP. Thêm vào đó, các thiết bị giám sát chủ động có thể đưa ra các bẫy (trap) nếu có các ngưỡng xác định trước nhằm để giám sát hiệu năng khi các hệ thống quá tải các luồng lưu lượng. Các khía cạnh quan trọng của giám sát chủ động được trình bày dưới đây.

a. Các tham số luồng lưu lượng kiểm tra

Các đặc tính luồng lưu lượng kiểm tra trong phương pháp giám sát chủ động sẽ ảnh hưởng tới các đặc tính của mạng kiểm tra. Các kết quả đo chỉ hữu dụng khi nó thể hiện được chính xác hiệu năng của các ứng dụng hoặc lớp lưu lượng của mạng. Điều này dẫn tới vấn đề cần phải xác định các tham số luồng lưu lượng thích hợp để phản ánh chính xác các đặc tính mạng. Các phương pháp đo khác nhau sẽ dẫn tới các tham số khác nhau. Vì vậy, dưới đây sẽ mô tả các tham số chung nhất đối với giám sát chủ động.

Kích thước gói : Có hai cách tiếp cận nhằm xác định kích thước gói tin giám sát theo kích thước gói tin của lưu lượng giám sát (cũng kích thước và khác kích thước). Kích thước các gói tin giám sát có thể ảnh hưởng lớn tới trễ nối tiếp của các liên kết tốc độ thấp, các gói tin giám sát cùng kích thước phản ánh chính xác độ trễ của các đường dẫn. Các gói tin giám sát có kích thước lớn có thể bị loại bỏ tại các điểm tắc nghẽn do tràn bộ đệm. Trong môi trường có các liên kết tốc độ thấp, các gói tin giám sát có kích thước nhỏ được sử dụng vì mục tiêu kinh tế. Hơn nữa, khi tần suất các gói tin giám sát tăng nhằm tăng độ chính xác, sử dụng các gói tin giám sát kích thước lớn sẽ ảnh hưởng tới lưu lượng mạng cần giám sát.

Chiến lược lấy mẫu : Chiến lược lấy mẫu thăm dò xác đinh phân bố của trễ từ các gói tin giám sát liên tục gồm 3 kiểu : định kỳ, ngẫu nhiên và từng đợt. Kiểu lấy mẫu định kỳ gửi thông tin theo từng khoảng thời gian, trong tiếp cận này có thể không thu được các thông tin sự kiện trong khoảng thời gian giữa hai lần lấy mẫu. Thủ tục gửi gói tin giám sát ngẫu nhiên được phân bố theo một dạng hàm mật độ xác suất nhằm đưa ra các mức đo phù hợp hơn với sự phân bố lưu lượng mạng. Lấy mẫu theo từng đợt là sự kết hợp của các gói tin giám sát theo từng nhóm và khoảng cách giữa các nhóm có thể theo định kỳ hoặc ngẫu nhiên.

Tốc độ kiểm tra giám sát : Tốc độ kiểm tra, giám sát được xác định qua số lượng gói tin gửi đi trong chu trình kiểm tra giám sát, tốc độ kiểm tra có thể gây xáo trộn lưu lượng trong mạng nếu có một lượng lớn các gói tin được gửi qua các liên kết có băng thông thấp và gây ra kết quả đo sai. Việc xác định chính xác tốc độ kiểm tra thích hợp dựa trên tính cân bằng giữa độ chính xác của các phép đo và mức ảnh hưởng tới các luồng lưu lượng trên mạng. Trên thực tế, tốc độ này phụ thuộc vào các đặc tính của ứng dụng hoặc lớp ứng dụng bị giám sát.

Thời gian kiểm tra và tần suất : Thời gian kiểm tra và tần suất cần đủ lớn nhằm đảm bảo tính chính xác của phép đo. Ngưỡng thấp nhất của (thời gian x tần suất) chỉ ra một cửa sổ đáp ứng xác suất sự kiện cần giám sát, khung cửa sổ càng lớn dẫn tới xác suất mất sự kiện càng nhiều. Thêm vào đó, nếu các thiết bị giám sát chủ động lưu giữ thông tin trạng thái qua các chu kỳ kiểm tra, tốc độ kiểm tra ảnh hưởng rất lớn tới kết quả đo.

b. Các tham số đo chủ động

Các tham số đo lượng theo phương pháp chủ động có thể là một tham số đơn hoặc một tập tham số được xác định qua luồng lưu lượng giám sát. Các tham số thông dụng thường là : trễ, biến động trễ, tổn thất gói, băng thông và độ thông qua, sự sắp xếp lại, độ khả dụng và chất lượng cảm nhận từ phía người dùng QoE.

c. Các khía cạnh triển khai giám sát chủ động

Một hệ thống đo chủ động sử dụng các agent giám sát chủ động để gửi và nhận các gói tin giám sát. Các agent này có thể gắn hoặc nhúng với các thiết bị mạng. Các agent gắn ngoài có thể là phần cứng đặc biệt chạy phần mềm giám sát chủ động. Tiếp cận này đưa ra được cách nhìn khách quan nhất từ phía người sử dụng, tuy nhiên nó yêu cầu bổ sung các thiết bị và làm tăng giá thành. Đối ngược với cách tiếp cận trên, một số nhà cung cấp thiết bị đã hỗ trợ sẵn các agent giám sát chủ động trong các sản phẩm, cho phép triển khai nhanh các hệ thống giám sát mà không cần bổ sung thiết bị phụ trợ. Do các thông số đo từ giám sát chủ động thể hiện các đặc tính ứng dụng nên các thiết bị giám sát chủ động càng gần với các hệ thống ứng dụng đầu cuối càng tốt. Tuy nhiên, điều này tùy thuộc vào cấu hình mạng triển khai trong thực tiễn và thường có các dạng cấu hình như : cấu hình kết nối hình lưới đầy đủ, cấu hình kết nối hình lưới từng phần và cấu hình kết nối hình lưới phân cấp. Ngoài ra còn một số vấn đề ảnh hưởng tới mô hình triển khai hệ thống giám sát chủ động như : Đo các đường dẫn đa đường cân bằng giá và dồng hồ đồng bộ cũng là những vấn đề quan trọng ảnh hưởng tới hệ thống giám sát chủ động.

3.3 GIÁM SÁT TỪ XA RMON

3.3.1 Giới thiệu chung

Giám sát từ xa RMON (Remote MONitoring) là một cơ sở thông tin quản lý tiêu chuẩn khác với giao thức quản lý mạng đơn giản. Các thông tin quản lý , tập hợp và phân tích nội bộ, có thể truyền đến trạm quản lý từ xa và được giám sát. Tương tự giao thức quản lý mạng đơn giản SNMP, giám sát từ xa RMON là một tiêu chuẩn mở được định nghĩa bởi IETF (RFC-1757) và gồm hai phiên bản RMONv1 (RFC 2819), RMONv2 (RFC 2021). RMONv1 cung cấp các trạm quản lý mạng NMS với trạng thái mức gói của toàn bộ mạng LAN, MAN hoặc WAN. RMONv2 cải thiện RMONv1 trên cơ sở bổ sung, cung cấp trạng thái mức mạng và ứng dụng.

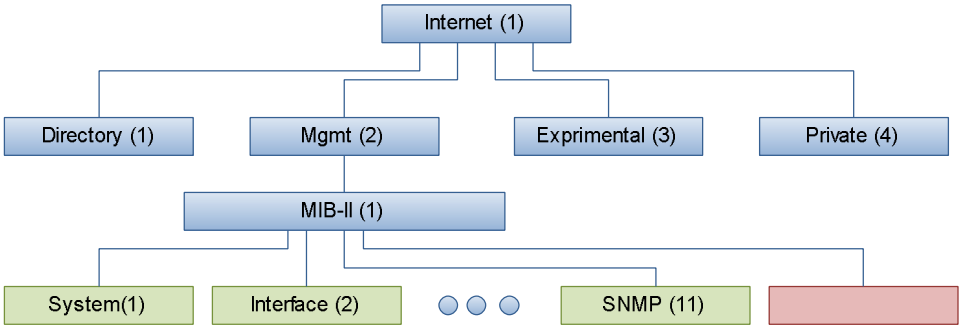
RMON cung cấp các thông tin tiêu chuẩn cho người quản trị mạng có thể sử dụng để giám sát, phân tích và sửa lỗi cho một nhóm mạng cục bộ phân tán và kết nối T1/E1, T2/E3 tới các trạm trung tâm. RMON định nghĩa các thông tin đặc tả cho các kiểu hệ thống giám sát mạng. Sự khác biệt của RMON và SNMP được chỉ ra dưới đây :

- RMON dựa trên thiết bị, trong đó sử dụng các phần cứng đặc biệt để điều hành.
- RMON gửi thông tin theo phương pháp chủ động nhằm sử dụng tối ưu băng thông và các sự kiện mạng.
- RMON có khả năng thu thập dữ liệu chi tiết.
- Thiết bị RMON cung cấp một hệ thống giám sát mạnh mẽ với chi phí thấp, các thăm dò RMON thường được cài đặt trong các liên kết đường trục và máy chủ.
- Hệ thống RMON có thể cấu hình để cung cấp dữ liệu như :
    - Các thông tin liên quan tới hiệu suất mạng;
    - Các thông tin thống kê cho phân tích trạng thái và chiến lược mạng;
    - Thông tin mô tả truyền thông giữa các hệ thống và lượng dữ liệu trao đổi.

RMON đã trở thành tiêu chuẩn năm 1992 với phiên bản RMONv1 cho mạng Ethernet. RMONv2 được hoàn thiện 1997. RMONv1 hoạt động chỉ trên lớp liên kết dữ liệu của mô hình OSI, RMONv2 thêm khả năng thu thập dữ liệu từ các lớp cao hơn và đưa ra nhiều khả năng báo cáo hơn. Ví dụ, RMONv2 có thể báo cáo các sự kiện xảy ra tại lớp lưu lượng TCP thay vì lớp IP trong phân đoạn LAN đa giao thức. Các nhà quản trị mạng sử dụng các bộ phân tích mạng để giám sát các vấn đề sử dụng mạng và các sự kiện liên quan. Nhằm đảm bảo độ chính xác dữ liệu lưu lượng mạng, các bộ phân tích mạng được gắn vào các mạng đích để tránh sự lọc bỏ thông tin của các cầu nối. Thêm vào đó, để cải thiện hiệu năng giám sát từ xa và chẩn đoán lưu lượng mạng, các bộ phân tích nối tiếp được đưa vào để chuyển tiếp lưu lượng dữ liệu tới trung tâm xử lý.

Cộng đồng người sử dụng với sự trợ giúp của IETF định nghĩa các đặc tính giám sát tiêu chuẩn cho phép giám sát các mạng khác nhau và các hệ thống điều hành khác nhau có thể trao đổi các thông tin giám sát mạng. Các đặc tính RMON này định nghĩa một tập các trạng thái và chức năng có thể trao đổi giữa các khối quản lý mạng và các phần tử thăm dò (probe). RMON đưa tới người quản lý mạng sự lựa chọn tùy ý các phần tử thăm dò và giám sát phụ hợp với môi trường ứng dụng.

Các phần tử thăm dò RMON thay thế các thiết bị phân tích mạng đắt tiền được gắn vào các vùng trọng yếu trong mạng. Các phần tử thăm dò RMON có nhiều dạng khác nhau phụ thuộc vào kích thước và kiểu thiết bị giám sát: Nhúng RMON MIB trên chính thiết bị chịu sự giám sát, card rời, thiết bị hoặc máy tính ngoài. Trong đó, các phần cứng đặc biệt gắn với các thiết bị chịu sự giám sát có lợi điểm như: Thu thập được các tham số đo chi tiết hơn agent SNMP và hoạt động như một bộ xử lý thời gian thực cho quá trình thu thập thông tin gửi tới NMS.



Hình 3.1: Vị trí RMON trong cây MIB-II

Thông tin quản lý hệ thống RMON và cơ sở thông tin quản lý MIB là cơ sở để các nhà cung cấp thiết bị khác nhau cùng được tham gia vào hệ thống giám sát. Trong hệ thống truyền thông của thông tin quản lý mạng, tiêu chuẩn chung cho RMON được định nghĩa tại RFC.1757 trên cơ sở cú pháp ASN.1. Các nhóm của RMON (RMONv1 và RMONv2) thuộc vào nút 16 của cây cơ sở thông tin quản lý MIB-II (hình 3.1). Các nhóm của RMONv1 gồm 9 nhóm được định nghĩa trong RFC 1757 và RMONv2 gồm 9 nhóm bổ sung được định nghĩa trong RFC 2021. RMONv1 định nghĩa các hoạt động tại lớp liên kết dữ liệu của mô hình OSI, trong khi đó RMONv2 mở rộng hoạt động tới các lớp cao hơn.

Một số đặc tính cơ bản của RMON như sau:

a. Điều hành ngoại tuyến

RMON cho phép một phần tử thăm dò thực hiện các công tác chẩn đoán và thu thập thông tin liên tục ngay cả khi truyền thông với trạm quản lý không kết nối. Phần tử thăm dò cố gắng thông báo với trạm quản lý khi có các điều kiện bất thường xảy ra. Tuy nhiên, khi xảy ra lỗi truyền thông, phần tử thăm dò lưu trữ thông tin và truyền lại trạm quản lý khi kết nối được khôi phục.

b. Giám sát chủ động

Với RMON, thiết bị giám sát từ xa (phần tử thăm dò) có một nguồn tài nguyên để thực hiện chẩn đoán và lưu giữ thông tin hiệu năng mạng. Vì vậy, phần tử thăm dò có thể thông báo tới trạm quản lý lỗi và lưu trữ thông tin trạng thái về lỗi. Thông tin này có thể được chuyển tới trạm quản lý để thực hiện các chẩn đoán xa hơn nhằm cách ly nguyên nhân lỗi.

c. Phát hiện và báo cáo lỗi

Phần tử thăm dò có thể được cấu hình nhằm nhận dạng các điều kiện lỗi và kiểm tra các lỗi. Khi một trong các điều kiện bị vi phạm, sự kiện được ghi lại và được thông báo tới các trạm quản lý theo một số cách thức khác nhau.

d. Dữ liệu gia tăng giá trị

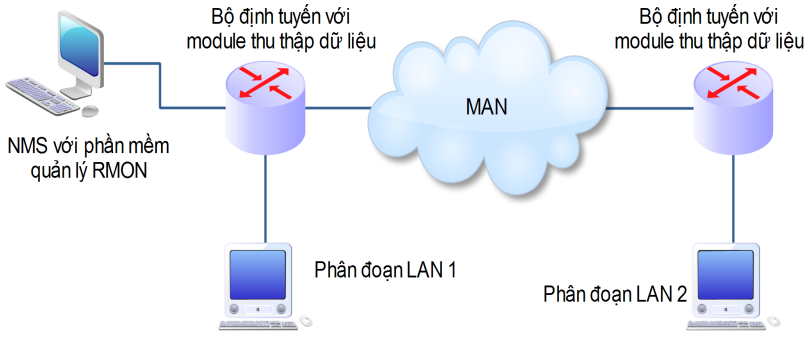
Một khi thiết bị giám sát từ xa thể hiện một nguồn tài nguyên mạng khác biệt với các chức năng quản lý mạng vì nó được xác định trực tiếp từ phần giám sát mạng, thiết bị giám sát từ xa có thể thêm các giá trị vào dữ liệu đã thu thập nhằm hỗ trợ các phần tử thăm dò đưa ra được các thông tin chính xác hơn tới thiết bị giám sát từ xa.

e. Đa quản lý

Một tổ chức có thể có nhiều trạm quản lý cho các đơn vị của tổ chức với các chức năng khác nhau nhằm cung cấp các thông tin tốt nhất để khôi phục lỗi. Do môi trường đa quản lý rất phổ biến trong thực tế, các thiết bị giám sát từ xa cần có chức năng phân phối thông tin tài nguyên tới các trạm quản lý khác nhau.

3.3.2 Các thành phần của RMON

Hình 3.2 chỉ ra một mô hình RMON điển hình. Tương tự SNMP, một kiểu cấu hình RMON gồm một trung tâm quản lý mạng NMS và một thiết bị giám sát từ xa RMON.

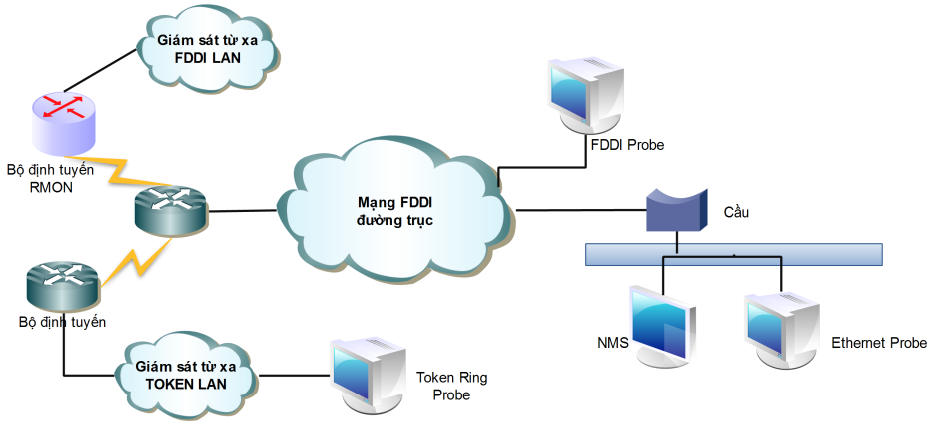


Hình 3.2: Cấu hình RMON điển hình

Trung tâm quản lý mạng NMS có thể hoạt động trên các máy chủ windows, unix hoặc máy PC chạy các ứng dụng quản lý mạng nhằm thực hiện các nhiệm vụ tập hợp trạng thái qua việc giám sát các gói tin dữ liệu trên mạng, lưu trữ các thông tin phù hợp với đặc tính của RMON.

Từ NMS, ta có thể đưa ra các câu lệnh yêu cầu thông tin từ RMON agent, RMON agent gửi thông tin yêu cầu tới NMS sẽ được xử lý và hiển thị thông tin trên bàn điều khiển.

Để chi tiết hơn các đặc tính hoạt động của RMON, ta xem xét một trường hợp giám sát mạng từ xa trên hình 3.3. Mạng được xây dựng dựa trên mạng đường trục FDDI và kết nối tới mạng LAN thông qua thiết bị cầu. Các bộ định tuyến chứa phần mềm giám sát RMON nhằm giám sát các thành phần trong các phân đoạn mạng. Khi xuất hiện các sự kiện bất bình thường trong các phân đoạn mạng quản lý , RMON gửi thông tin tới hệ thống giám sát mạng từ xa để báo cáo. Mô hình trên hình 3.2 cũng chỉ ra lợi ích của sử dụng RMON khi các agent không nhất thiết phải tồn tại trong toàn bộ thời gian quản lý hệ thống mạng.



Hình 3.3: Ví dụ về mạng giám sát từ xa RMON

Một số cơ chế xác nhận lỗi trong mạng IP như gói tin ICMP ping có thể bị tổn thất trong các đường truyền thông có khoảng cách lớn. Nhất là khi có hiện tượng tắc nghẽn lưu lượng. Vì vậy, các gói tin thăm dò RMON được thực hiện trong từng mạng nội bộ và giám sát liên tục làm tăng độ tin cậy của bài toán giám sát.

3.3.3 Điều khiển thiết bị RMON

Do tính phức tạp của các hàm chức năng trong các thiết bị, các chức năng điều khiển thường yêu cầu cấu hình từ phía người sử dụng. Trong rất nhiều trường hợp, chức năng này yêu cầu các tham số để thiết lập các điều hành thu thập dữ liệu và các điều hành chỉ có thể thực hiện khi các tham số được thiết lập đầy đủ. Nhiều nhóm chức năng trong cơ sở thông tin quản lý MIB có một vài bảng để thiết lập tham số điều khiển hoặc sử dụng để lưu kết quả của hoạt động điều hành. Các bảng cơ sở dữ liệu điều khiển là các bảng ghi đọc (readwrite) trong khi các bảng cơ sở dữ liệu kết quả là các bảng chỉ đọc (read only). Các tham số trong bảng điều khiển được sử dụng để mô tả dữ liệu kết quả trong bảng dữ liệu. Trong một số trường hợp, các khoản mục dữ liệu có thể không tồn tại. Vì vậy, các tham số điều khiển được yêu cầu sửa đổi nhằm nhận dạng các dữ liệu liên quan trong bảng dữ liệu và tạo ra các tham số điều khiển mới. Việc xóa khoản mục điều khiển cũng là một phương pháp thích hợp nhằm phản ánh lại nguồn tài nguyên sử dụng của các dữ liệu liên quan.

Một số đối tượng trong MIB cung cấp một cơ chế thực hiện các hoạt động của thiết bị giám sát từ xa. Các đối tượng này có thể thực hiện các hoạt động khi có sự thay đổi trạng thái của đối tượng.

a. Chia sẻ tài nguyên giữa các trạm quản lý

Khi sử dụng hệ thống đa trạm quản lý , nguồn tài nguyên được chia sẻ giữa các trạm quản lý . Ví dụ như bộ nhớ và nguồn tài nguyên tính toán phục vụ cho các yêu cầu chức năng. Một số vấn đề tranh chấp thường xảy ra gồm:

- Hai trạm quản lý cùng muốn sử dụng nguồn tài nguyên vượt quá khả năng của thiết bị.
- Một trạm quản lý sử dụng một lượng tài nguyên nhất định trong một khoảng thời gian dài.
- Một trạm quản lý sử dụng các tài nguyên và không giải phóng sau khi sử dụng.

Một cơ chế được cung cấp cho mỗi trạm quản lý tại MIB nhằm tránh các xung đột và giải quyết khi xung đột xảy ra. Mỗi một hàm chức năng có một nhãn nhận dạng khởi tạo. Nhãn này được đặt bởi bộ khởi tạo nhằm tương thích các khả năng sau:

- Một trạm quản lý có thể xác định rõ nguồn tài nguyên và yêu cầu sử dụng của nó.
- Người điều hành mạng có thể tìm thấy các trạm chiếm giữ tài nguyên và thỏa thuận để giải phóng tài nguyên.
- Người điều hành mạng có thể quyết định đơn phương giải phóng tài nguyên với các nhà điều hành mạng khác.
- Ngay sau khi khởi tạo, một trạm quản lý có thể nhận dạng các nguồn tài nguyên đã được sử dụng trước đó và có thể giải phóng khi không được sử dụng.

Các trạm quản lý và các phần tử thăm dò cần phải hỗ trợ tất cả định dạng của chuỗi đưa ra bởi các vùng mạng. Nó chứa một hoặc một vài tên sau: Địa chỉ IP, tên trạm quản lý , tên các nhà quản lý mạng, khu vực hoặc số điện thoại. Các thông tin này sẽ giúp người sử dụng chia sẻ tài nguyên hiệu quả.

Thông thường, một số chức năng của thiết bị và nhà quản lý phần tử thăm dò muốn được thiết lập ngầm định. Các tài nguyên gắn với các chức năng này được sở hữu bởi chính bản thân thiết bị hoặc nhà quản lý mạng trong thời gian hoạt động. Trong trường hợp này, thiết bị hoặc nhà quản lý sẽ đặt các đối tượng sở hữu liên quan vào một chuỗi bắt đầu với từ giám sát "monitor". Một trạm quản lý mạng chỉ thay đổi các đối tượng này dưới sự chỉ đạo của người quản lý phần tử thăm dò.

Các nguồn tài nguyên trên một phần tử thăm dò được chỉ định khi các hàng điều khiển được tạo ra bởi các ứng dụng. Khi có rất nhiều các ứng dụng cùng sử dụng phần tử thăm dò cùng một thời điểm, việc phân bổ tài nguyên không hiệu quả sẽ dẫn đến sự thiếu hụt tài nguyên trong phần tử thăm dò. Khi một trạm quản lý mạng muốn sử dụng một chức năng trong một khối giám sát từ xa, nó quét bảng điều khiển của chức năng đó để tìm các tham số tương tự để chia sẻ. Các tham số có độ biến động ít nhất là các tham số thuộc về khối giám sát. Nếu một trạm quản lý quyết định chia sẻ tài nguyên cho những trạm quản lý khác, nó cần hiểu rằng trạm quản lý sở hữu các tham số có thể không cho phép sửa đổi hoặc xóa bỏ. Vì vậy, một ứng dụng quản lý quan trọng thường được đặt trong hàng của khối giám sát do sự thay đổi trong hàng này ít khi xảy ra. Trong khi đó, một hàng của một ứng dụng quản lý có thời gian sống nhỏ vì nhà

quản lý mạng thường phân bổ lại tài nguyên từ đó hơn là một hàng thuộc về khối giám sát được sử dụng bởi nhiều người sử dụng.

b. Bổ sung hàng giữa các trạm quản lý

Cơ chế bổ sung thêm hàng được mô tả trong RFC 1212. Trong cơ sở thông tin quản lý MIB, các hàng thường xuyên được bổ sung vào trong một bảng để cấu hình một chức năng. Cấu hình này thường gồm các tham số để điều hành chức năng. Agent cần kiểm tra các tham số này để đảm bảo chúng phù hợp với các giới hạn được định nghĩa trong MIB cũng như giới hạn về tài nguyên. Các khối thực thi Agent có thể nhầm lẫn khi kiểm tra các tham số này và báo lại tới trạm quản lý rằng các tham số này không có giá trị do hai khả năng sau:

- Khi một trạm quản lý đặt riêng lẻ các đối tượng tham số.
- Khi trạm quản lý đặt một đối tượng trạng thái không chính xác.

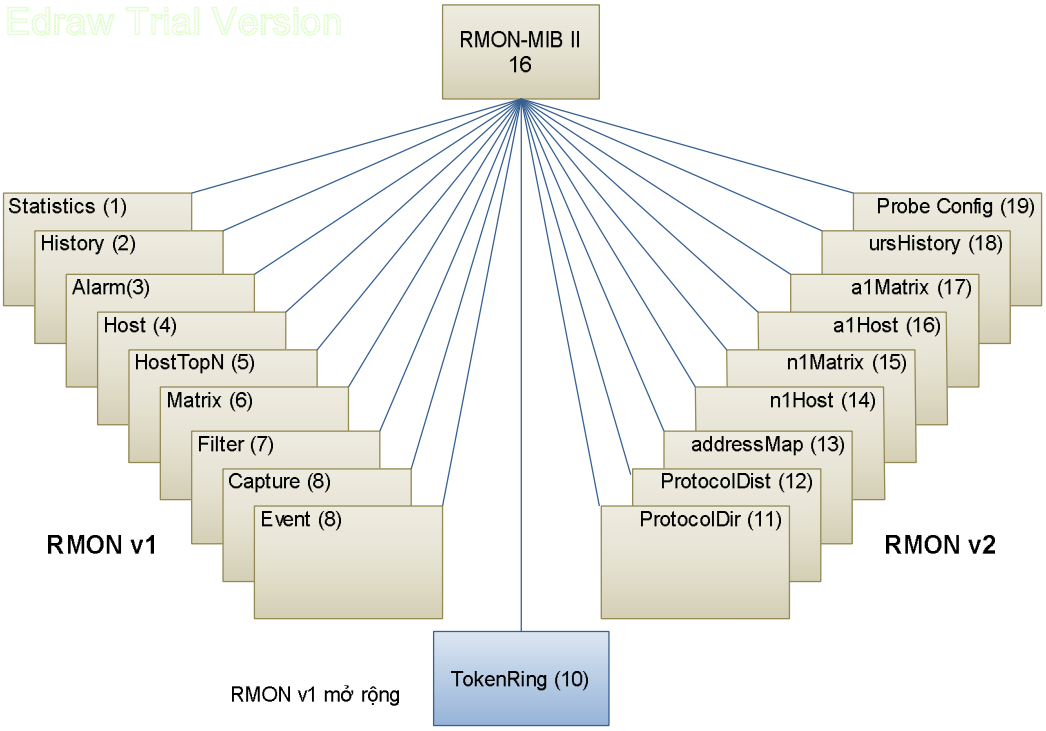
Trường hợp thứ hai xảy ra khi một trạm quản lý có một vài tham số không chính xác và gây ra lỗi, khối thực thi sẽ lựa chọn các tham số trước đó để có thêm thông tin về trạm quản lý . Thêm vào đó, một vấn đề nảy sinh khi nhiều trạm cùng quản lý cố gắng thiết lập các thông tin cấu hình bằng giao thức SNMP trong cùng một thời điểm. Khi đó, quá trình bổ sung một hàng mới trong cùng một bảng điều khiển có thể dẫn tới tranh chấp giữa các trạm quản lý khi các trạm này cùng muốn tạo cùng một khoản mục. Để tránh tranh chấp này, mỗi khoản mục điều khiển như vậy chứa một đối tượng trạng thái có một ngữ nghĩa đặc biệt để dàn xếp giữa các trạm quản lý . Nếu một cơ chế tạo hàng đưa ra một đối tượng trạng thái tương tự như đối tượng trạng thái tồn tại thì bản tin báo lỗi được gửi tới trạm quản lý . Khi nhiều trạm quản lý cùng muốn tạo ra một hàng, chỉ trạm quản lý đầu tiên thành công và các trạm còn lại sẽ nhận được thông báo lỗi.

Khi một trạm quản lý muốn tạo ra một khoản mục điều khiển mới, nó tạo ra một chỉ mục cho hàng đó. Lựa chọn chỉ mục có thể theo nhiều cách khác nhau nhưng đều nhằm hạn chế tối thiểu cơ hội của các trạm quản lý khác sử dụng chỉ mục này. Nếu chỉ mục đang được sử dụng, các kỹ thuật trên đây sẽ được sử dụng để chống tranh chấp.

Một số bảng trong cơ sở thông tin quản lý MIB này được tham chiếu tới các bảng khác trong cùng MIB. Khi tạo và xóa các khoản mục trong các bảng này, nó cho phép các tham chiếu không ổn định tồn tại và không định nghĩa thứ tự để tạo hoặc xóa các khoản mục trong bảng.

3.3.3 RMONv1

Như đã giới thiệu, RMONv1 gồm 9 nhóm được định nghĩa bởi RFC 1757 và một nhóm mở rộng cho TokenRing RFC 1513. Các nhóm trong RMONv1 được thể hiện qua hình 3.4.



Hình 3.4: Các nhóm của RMONv1 và RMONv2

Hai loại dữ liệu được định nghĩa trong RMON1 được quy ước là chuỗi dữ liệu của người quản lý (OwnerString) và trạng thái khoản mục (EntryStatus). Hai kiểu dữ liệu này được sử dụng bởi hệ thống quản lý giám sát và thiết bị chịu quản lý giám sát. Các thông tin dữ liệu được biểu diễn qua bảng tham số điều khiển giám sát. Bảng điều khiển giám sát cho phép tạo, sử dụng và xóa các tham số nhằm thực thi các hoạt động giám sát thông qua dữ liệu OwnerString, OwnerString còn được gọi là "monitor" khi một Agent tự quản lý chính nó.

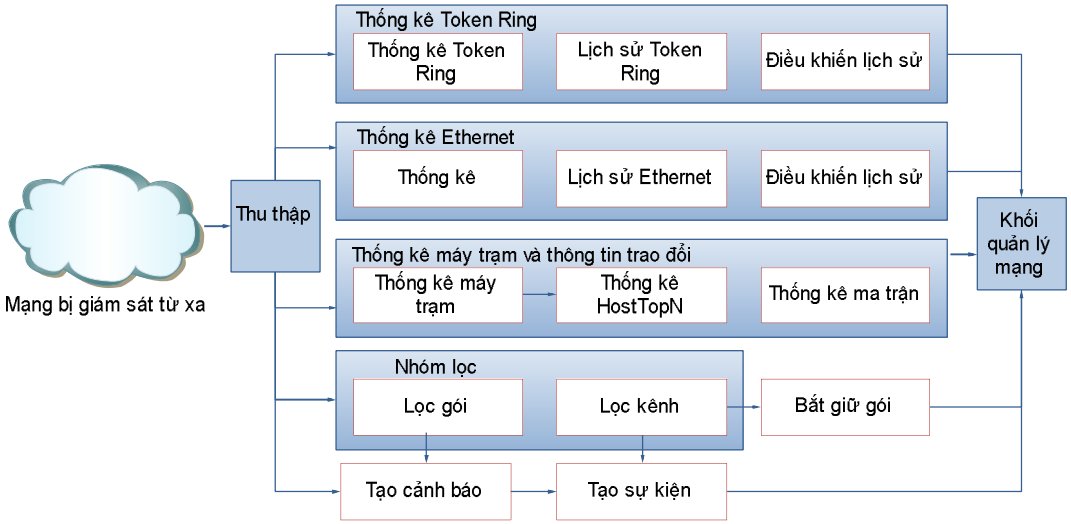
Dữ liệu trạng thái khoản mục EntryStatus được sử dụng để giải quyết xung đột có thể xuất hiện giữa hệ thống quản lý bằng phương pháp nhân công. Đối với một bảng điều khiển nhiều người sử dụng, một cột được sử dụng riêng cho dữ liệu trạng thái khoản mục EntryStatus và gồm 4 trạng thái: (1) valid, (2) createRequest, (3) underCreation, và (4) invalid; được biểu diễn trong bảng 3.1. Trong trạng thái điều khiển có hiệu lực (valid), tất cả các hệ thống quản lý sử dụng thiết bị RMON có thể sử dụng hàng dữ liệu. Nếu dữ liệu trạng thái khoản mục chỉ ra là không hiệu lực (invalid) hệ thống sẽ mất dữ liệu. Trạng thái không hiệu lực còn được được sử dụng để xóa hàng. Nếu hàng mong muốn của thông tin không tồn tại, hệ thống quản lý có thể tạo ra một hàng qua trạng thái createRequest. Trong quá trình trao đổi thông tin giữa khối quản lý và Agent, trạng thái của khoản mục được đặt vào trạng thái underCreation nhằm tránh sử sử dụng hàng của các khối quản lý khác. Sau khi quá trình tạo thông tin dữ liệu hoàn thành, trạng thái này được thiết lập về trạng thái có hiệu lực (valid).

Bảng 3.1. Quy ước EntryStatus

Trạng thái	**Thứ tự**	**Mô tả**
Valid	1	Hàng tồn tại và trong trạng thái hoạt động.
createRequest	2	Yêu cầu tạo hàng mới qua đối tượng này
underCreation	3	Hàng không trong trạng thái kích hoạt.
Invalid	4	Xóa hàng bằng cách ngắt các liên kết ánh xạ tới khoản mục.

Các nhóm và chức năng RMONv1

RMONv1 thực thi các chức năng ở lớp liên kết dữ liệu, trong hình 3.5 mô tả chi tiết hơn về nhóm và chức năng RMONv1.



Hình 3.5: Các nhóm của RMONv1

Từ mạng bị giám sát từ xa, module thu thập dữ liệu nhận các thông tin giám sát và chuyển tới từng khối chức năng quản lý . Các dữ liệu được đưa vào 5 khối chức năng trong đó có 3 khối sử dụng để giám sát lưu lượng thống kê cho các kiểu mạng và thiết bị (tokenRing, Ethernet và máy trạm). Khối chức năng điều khiển lịch sử của tokenRing được sử dụng chung với Ethernet. Các đầu ra của các module này đưa ra phía quản lý mạng các thông tin thống kê dưới dạng bảng biểu hoặc biểu đồ. Nhóm chức năng lọc bao gồm chức năng lọc gói theo chuỗi và lựa chọn các kênh tương ứng, khối lọc đưa ra các thông tin cảnh báo hoặc các sự kiện khi các dữ liệu vượt quá giới hạn hoặc không hợp lệ. Các thông tin của nhóm lọc có thể được lưu trữ trong module bắt giữ gói tin để phân tích các mẫu lưu lượng hoặc các sự kiện bất thường trong mạng. Các nhóm đối tượng của RMONv1 là các đơn vị cơ sở thống nhất, thiết bị giám

sát từ xa sử dụng một nhóm đối tượng đồng nghĩa với việc sử dụng toàn bộ đối tượng trong nhóm. Tất cả các nhóm trong cơ sở thông tin quản lý MIB này đều là tùy chọn, bổ sung của MIB này đều kéo theo sự bổ sung nhóm giao diện và hệ thống của MIB-II. MIB-II cũng có thể ủy thác sử bổ sung của các nhóm phụ. Các nhóm này được định nghĩa để cung cấp một phương tiện gán nhận dạng đối tượng và cung cấp một phương pháp cho các agents quản lý biết đối tượng nào cần được bổ sung.

Chức năng của các nhóm đối tượng của RMONv1 được chỉ ra trên bảng 3.2 gồm: Thống kê trạng thái Ethernet (ethernet statistics); điều kiển lịch sử (history control); lịch sử Ethernet (ethernet history); cảnh báo (alarm); máy trạm (host); máy trạm phân cấp cao nhất (hostTopN); ma trận (matrix); bộ lọc (filter); bắt gói tin (packet capture); sự kiện (event).

Bảng 3.2. Các bảng và nhóm MIB RMON1

Nhóm	**OID**	**Chức năng**	**Bảng**
Statistics	rmon 1	Trạng thái mức liên kết	-etherStatsTable -etherStats2Table
History	rmon 2	Thu thập dữ liệu trạng thái định kỳ và lưu trữ thông tin.	-historyControlTable -etherHistoryTable -historyControl2Table -etherHistory2Table
Alarm	rmon 3	Tạo các sự kiện khi mẫu thu thập vượt ngưỡng.	-alarmTable
Host	rmon 4	Thu thập dữ liệu trên máy trạm.	-hostControlTable -hostTable -hostTimeTable -hostControl2Table
HostTopN	rmon 5	Số lượng các máy trạm sắp xếp theo số liệu thống kê thu thập được.	-hostTopNcontrolTable
Matrix	rmon 6	Thống kê lưu lượng giữa cặp máy trạm.	-matrixControlTable -matrixSDTable -matrixDSTable -matrixControl2Table
Filter	rmon 7	Chức năng lọc cho phép bắt giữ các	-filterTable

		thông tin cần thiết.	-channelTable -filter2Table -channel2Table
Packet Capture	rmon 8	Bắt gói tin qua các kênh.	-buffercontrolTable -captureBufferTable
Event	rmon 9	Điều khiển tạo sự kiện và cảnh báo.	-eventTable

Chức năng chi tiết của các nhóm được liệt kê dưới đây:

a. Nhóm thống kê Ethernet

Nhóm thống kê Ethernet chứa các dữ liệu thống kê đo bởi các phần tử thăm dò trên mỗi giao diện Ethernet của thiết bị. Nhóm này gồm bảng dữ liệu thống kê ethernet (etherStatsTable). Dựa trên cùng mô hình này, các nhóm khác có thể được định nghĩa cho các kiểu phương tiện khác như FDDI và TokenRing.

b. Nhóm điều khiển lịch sử

Nhóm điều khiển lịch sử điều khiển mẫu trạng thái thống kê định kỳ của dữ liệu từ các kiểu mạng khác nhau. Trong nhóm này gồm bảng điều khiển lịch sử (historyControlTable).

c. Nhóm lịch sử Ethernet

Nhóm lịch sử Ethernet ghi lại các mẫu thống kê định kỳ từ mạng Ethernet và lưu trữ từ các lần lấy dữ liệu sau cùng. Nhóm này gồm bảng lịch sử ethernet (ethHistoryTable). Các nhóm này có thể định nghĩa cho các kiểu phương tiện khác như FDDI và TokenRing.

d. Nhóm cảnh báo

Nhóm cảnh báo định kỳ đưa ra các mẫu thống kê từ các biến trong dữ liệu thăm dò và so sánh chúng với các ngưỡng đã được cấu hình. Một sự kiện được tạo ra nếu các biến vượt quá ngưỡng định sẵn. Một cơ chế gây trễ được thực hiện nhằm giới hạn các bản tin cảnh báo, tránh sự gia tăng của các bản tin cảnh báo gây tác động xấu tới hiệu năng mạng. Nhóm này gồm bảng cảnh báo (alarmTable) và các cơ chế thực thi sự kiện.

e. Nhóm máy trạm

Nhóm máy trạm chứa các dữ liệu thống kê liên quan tới các sự kiện phát hiện máy trạm trong mạng, chứa danh sách các địa chỉ MAC nguồn/đích từ các gói tin trong mạng. Nhóm này gồm các bảng: bảng điều khiển máy trạm (hostControlTable); Bảng máy trạm (hostTable) và bảng thời gian máy trạm (hostTimeTable).

f. Nhóm máy trạm đỉnh N

Nhóm hostTopN được sử dụng cho các báo cáo mô tả giám sát các máy trạm trên từ trên xuống dưới theo thứ tự thống kê gồm N máy trạm. Các thống kê khả dụng là các mẫu thống kê thu được theo thời gian xác lập bởi trạm quản lý . Vì vậy, mẫu thống kê này dựa trên tốc độ lấy mẫu. Trạm quản lý cũng lựa chọn số lượng các máy trạm báo cáo (N). Nhóm này gồm bảng điều khiển máy trạm đỉnh (hostTopControlTable), bảng máy trạm đỉnh (hostTopTable) và yêu cầu thực hiện trong nhóm máy trạm (host group).

g. Nhóm ma trận

Nhóm ma trận lưu trữ dữ liệu thống kê lưu lượng sử dụng cho nhiệm vụ trao đổi thông tin giữa hai tập địa chỉ. Một khoản mục mới trong bảng định tuyến được tạo ra khi một thiết bị nhận dạng được một quá trình trao đổi. Nhóm này gồm bảng điều khiển ma trận (matrixControlTable), bảng ma trận nguồn (matrixSDTable) và bảng ma trận đích (matrixDSTable).

h. Nhóm lọc

Nhóm lọc cho phép lọc các gói thích hợp nhằm phục vụ cho quá trình giám sát. Nhóm này gồm bảng lọc gói (filterTable) nhằm cho phép các gói tin thích hợp được chuyển qua kênh truyền và bảng kênh (channelTable) thể hiện kênh thông tin truyền các gói tin giám sát.

i. Nhóm bắt gói

Nhóm bắt gói cho phép các gói được thu thập sau khi chuyển qua kênh truyền. Nhóm này gồm bảng điều khiển đệm (bufferControlTable), bảng bộ đệm bắt gói (captureBufferTable), các nhiệm vụ bắt giữ gói tin trong bộ đệm được thực thi trong nhóm lọc gói.

j. Nhóm sự kiện

Nhóm sự kiện điều khiển chức năng tạo và thông báo các sự kiện từ các thiết bị. Nhóm này gồm bảng sự kiện (eventTable) mô tả các sự kiện sẽ được thông báo và bảng lưu vết (logTable) lưu lại lịch sử các sự kiện.

3.3.4 RMONv2

RMONv1 cơ bản đã giám sát được dữ liệu tích hợp tại lớp liên kết dữ liệu trong mô hình OSI. RMONv2 mở rộng khả năng giám sát cho các mức cao hơn, từ lớp mạng tới lớp ứng dụng. Mức ứng dụng được sử dụng trong khái niệm SNMP RMON mô tả một lớp các giao thức, và không hoàn toàn tuân thủ theo mô hình 7 lớp OSI. Các thống kê lỗi trong lớp cao bất kì đều được chuyển xuống tới lớp mạng. Ví dụ, các lỗi lớp mạng không bao gồm các lỗi lớp liên kết dữ liệu, nhưng các lỗi lớp truyền tải bao trùm và thể hiện tại lớp mạng.

Kiến trúc cơ sở thông tin quản lý của RMONv2 gồm 10 nhóm chức năng được chỉ ra trên hình 3.4 và được tóm tắt trong bảng 3.3 dưới đây.

Bảng 3.3. Các nhóm và bảng MIB RMONv2

Nhóm	**OID**	**Chức năng**	**Bảng**
Protocol directory	Rmon 11	Tóm tắt các giao thức	protocolDirTable
Protocol distribution	Rmon 12	Thống kê lưu lượng tương quan giao thức trên cơ sở octet và các gói	protocolDistControlTable
Address map	Rmon 13	Bản đồ ánh xạ địa chỉ MAC và địa chỉ mạng trên các giao diện	protocolDistStatsTable addressMapControlTable
Network layer host	Rmon 14	Lưu lượng dữ liệu đi và đến mỗi máy trạm	addressMapTable n1HostControlTable
Network layer matrix	Rmon 15	Dữ liệu lưu lượng giữa các cặp máy trạm	n1Host Table n1MatrixControlTable
Application layer host	Rmon 16	Lưu lượng dữ liệu giao thức đi và đến mỗi máy trạm	n1MatrixSDTable n1MatrixDSTable n1MatrixTopNControlTable n1MatrixTopNTable a1HostTable
Application layer matrix	Rmon 17	Lưu lượng dữ liệu giao thức giữa 2 máy trạm	a1MatrixSDTable
User history collection	Rmon 18	Dữ liệu lịch sử của người sử dụng trên cơ sở các cảnh báo và thống kê	usrHistoryObjectTable usrHistoryTable serialConfigTable
Probe Configuration	Rmon 19	Cấu hình các tham số phần tử giám sát	netConfigTable trapDestTable serialConnectionTable

Các nhóm trên đây dựa trên các đơn vị cơ sở của phần tử giám sát. Nếu một thiết bị giám sát từ xa thực hiện triển khai trong một nhóm, thiết bị đó phải thực thi với tất cả các đối tượng trong nhóm đó. Các chức năng sơ lược của các nhóm gồm:

a, Nhóm thư mục giao thức

Thư mục giao thức là một phương pháp cho phép một ứng dụng RMONv2 dễ dàng liên kết điều hành với các giao thức được triển khai trong các agent. Nhóm thư mục giao thức mô tả nhận dạng các giao thức thông qua các tham số được phần tử giám sát thu thập (ví dụ, chỉ số cổng UDP) cho tất cả các giao thức lớp phía trên lớp IP. Các tham số cấu hình cho phần tử giám sát được thay đổi trong bảng thư mục giao thức (ProtocolDirTalbe), mỗi giao thức được nhận dạng thông qua một chỉ số ID trên cột duy nhất trong bảng. Các giao thức thể hiện trong thư mục giao thức được định nghĩa trong RFC 2074.

b, Nhóm phân phối giao thức

Nhóm phân phối giao thức cung cấp thông tin về lưu lượng tương quan giữa các giao thức khác nhau trên cơ sở các octet hoặc các gói. Thên vào đó, nhóm phân phối giao thức thực hiện việc ánh xạ các dữ liệu thu thập được bởi phần tử giám sát và tới tên giao thức để hiển thị cho người quản lý mạng. Bảng dữ liệu phân phối giao thức (protocolDistControlTable) được cấu hình theo dữ liệu được tập hợp và lưu trữ tại bảng thống kê phân phối giao thức (protocolDistStatsTable).

c, Nhóm ánh xạ địa chỉ

Nhóm ánh xạ địa chỉ thực hiện biên dịch địa chỉ lớp MAC và lớp mạng thông qua phần tử giám sát nhằm cung cấp thông tin tới người quản lý mạng và nền tảng quản lý . Ánh xạ địa chỉ được thực hiện trên các giao diện thông qua hai bảng dữ liệu: bảng thống kê phân phối giao thức (protocolDistStatsTable) và bảng điều khiển ánh xạ địa chỉ (addressMapControlTable).

d, Nhóm máy trạm lớp mạng

Nhóm máy trạm lớp mạng cung cấp thống kê thông tin lớp mạng được phân loại theo địa chỉ mạng. Nhóm này giám sát và thống kê lưu lượng đi/đến các địa chỉ mạng thông qua phần tử thăm dò. Nhóm gồm một bảng ánh xạ địa chỉ lớp mạng (addressMapTable) và bảng điều khiển máy trạm (HostControlTable).

e, Nhóm ma trận lớp mạng

Nhóm ma trận lớp mạng lưu trữ các thống kê lưu lượng ứng dụng được truyền thông giữa các tập địa chỉ lớp mạng. Nhóm này gồm bảng điều khiển ma trận lưu lượng (matrixHostTable) và bảng dữ liệu lưu lượng giữa các cặp máy chủ (hostTable).

f, Nhóm lớp ứng dụng của máy trạm

Các chức năng lớp ứng dụng trong máy trạm được chia thành hai nhóm gồm nhóm lớp ứng dụng máy trạm và nhóm ma trận lớp ứng dụng. Các thông tin về ứng dụng và lưu lượng dữ liệu giao thức được thể hiện qua các bảng của lớp ứng dụng lưu trữ số liệu thống kê về địa chỉ, lưu lượng đi và đến máy trạm và bảng điều khiển.

g, Nhóm ma trận lớp ứng dụng

Nhóm ma trận lớp ứng dụng thống kê lưu lượng giao thức được chuyển giữa các cặp máy trạm.

h, Nhóm thu thập thông tin lịch sử người sử dụng

Các thông tin cảnh báo và lịch sử người sử dụng được thu thập trong nhóm thu thập thông tin lịch sử người sử dụng. Các chức năng này được thực hiện bởi các hệ thống quản lý mạng. Các đối tượng dữ liệu được tập hợp trong các nhóm bucket, mỗi nhóm bucket gắn liền với một đối tượng MIB và các phần tử trong nhóm là các trường hợp của đối tượng MIB. Người dùng có thể thay đổi dữ liệu được tập hợp bằng việc nhập dữ liệu trong bảng điều khiển lịch sử người sử dụng (usrHistoryControlTable), khi đó sẽ được kết hợp với các hàng của các trường hợp trong bảng đối tượng lịch sử người sử dụng (usrHistoryObjectTable).

h, Nhóm cấu hình phần tử thăm dò

Chức năng của nhóm cho phép một ứng dụng RMON của một nhà cung cấp thiết bị có thể cấu hình từ xa các tham số của phần tử thăm dò thuộc về nhà cung cấp thiết bị khác. RMONv2 bổ sung thêm tính năng tương thích với các đặc tính bắt buộc hoặc tùy chọn nhằm hỗ trợ các nhà cung cấp thiết bị bổ sung các tham số giám sát cho các hệ thống giám sát từ xa. Các chức năng cấu hình gồm: Cấu hình truy nhập nối tiếp (modem); cấu hình địa chỉ IP; cấu hình các kết nối nối tiếp cho bẫy (trap) và cấu hình các tham số bẫy.

3.4 TỔNG KẾT CHƯƠNG 3

Trong chương 3 đã trình bày một số đặc điểm cơ bản của phương pháp giám sát từ xa. Trên cơ sở nguyên tắc chung về giám sát từ xa, hai phiên bản giám sát từ xa RMONv1 và RMONv2 đã được mô tả trên các khía cạnh nguyên lý hoạt động, vị trí và chức năng của các nhóm trong cây cơ sở thông tin quản lý . Mặc dù giám sát từ xa có được một loạt các lợi điểm như đã trình bày, RMON hiện vẫn còn một số vấn đề cần tiếp tục cải thiện như: Độ phức tạp triển khai RMON trên các thiết bị quản lý và agent rất lớn, khả năng tùy biến và mở rộng kém và mức độ phổ biến còn hạn chế.

CHƯƠNG 4

QUẢN LÍ CÁC MẠNG THỰC TIỄN

4.1 QUẢN LÍ MẠNG IP

4.1.1 Lựa chọn phương pháp quản lý

Trong thực tế, các thiết bị trong mạng IP là rất đa dạng và phức tạp dẫn tới việc cần thiết phải có một số lượng lớn tham số cấu hình. Thêm vào đó, mỗi mức thiết bị mạng đều yêu cầu các đặc tính quản lý riêng và khác nhau. Trong phần lớn các kịch bản quản lý , các tham số này được đặt ở giá trị ngầm định, các phương pháp quản lý mạng hướng tới sự thay đổi các tham số này để tối ưu các chức năng mạng trong các mô hình cụ thể. Tại một thời điểm, rất nhiều các tác vụ cần được thực hiện như: giám sát chức năng và hành vi các nút, nguồn tài nguyên kích hoạt, lưu lượng chuyển tiếp và các trạng thái tắc nghẽn. Các vấn đề quản lý trên có một miền rộng từ thông tin trạng thái cơ bản của thiết bị tới các dữ liệu chi tiết liên quan tới các chức năng bên trong của thiết bị. Các thông tin cần thiết được lấy ra từ các thiết bị được chiết xuất theo các module chức năng hoặc các thành phần logic.

Khả năng cung cấp các dịch vụ mới cũng là một yêu cầu quản lý quan trọng, yêu cầu này có thể cần các nguồn tài nguyên chắc chắn tại mỗi nút dọc theo đường dẫn quản lý mạng. Mạng IP có thể sử dụng giao thức báo hiệu dành trước tài nguyên RSVP (Resource ReSerVation Protocol) để thực hiện nhiệm vụ này.

Quản lý mạng là một miền trong đó hầu hết các nhà cung cấp dịch vụ Internet quan tâm, đặc tính của các mạng này là thường xuyên thay đổi và động lực thúc đẩy các loại hình dịch vụ mới luôn được người sử dụng yêu cầu. Sự thay đổi này dẫn tới một loạt sự thay đổi các bộ công cụ quản lý mạng và yêu cầu các nhà cung cấp dịch vụ Internet đưa ra các giải pháp kỹ thuật nhằm đáp ứng các yêu cầu của khách hàng. Thêm vào đó, những khách hàng doanh nghiệp hiện nay thường yêu cầu cung cấp các dịch vụ riêng ảo, loại hình dịch vụ chia sẻ tài nguyên kiểu này đặt ra một loạt các thách thức mới đối với khả năng quản lý mạng.

4.1.2 Lựa chọn phương pháp cấu hình

Có rất nhiều cách để cấu hình thiết bị trong mạng IP, từ các phương pháp cấu hình tự động qua các giao thức BOOTP và DHCP, tới các giao diện dòng lệnh, file cấu hình và các giao diện người dùng đồ họa. Các kỹ thuật này có thể sử dụng tổ hợp thông tin và kỹ thuật của nhà sản xuất, các giao thức tiêu chuẩn và các khuôn dạng dữ liệu tiêu chuẩn.

Các giao diện dòng lệnh: Công cụ quản lý đơn giản nhất đối với các thiết bị mạng là sử dụng công cụ dòng lệnh CLI (Command Line Interface). CLI là một tập dòng lệnh dựa trên text đưa ra bởi người điều hành tại thiết bị kết cuối quản lý . Các dòng lệnh có các cú pháp đặc biệt được định nghĩa bởi nhà cung cấp thiết bị, các thiết bị của cùng nhà cung cấp thường có chung các bộ câu lệnh và ngữ nghĩa câu lệnh. Điều này có nghĩa rằng các nhà vận hành khi quản lý các nút mạng từ các nhà sản xuất khác nhau phải nhận thức được các ngôn ngữ lệnh cho nút đó.

Do các thiết bị thực hiện cùng chung các chức năng cần được thực hiện cùng phương pháp cấu hình, cũng như các nhà cung cấp thiết bị nhận thấy các vấn đề phức tạp của các mạng quản lý xây dựng trên cấu trúc phần cứng của các nhà cung cấp khác nhau. Khuynh hướng của CLI thường sử dụng là hội tụ các cú pháp câu lệnh từ các nhà công nghiệp lớn. Điều này có lợi ích rõ ràng nhưng cũng tạo ra tính phức tạp khi phải ghi nhớ câu lệnh. Trong mô hình đơn giản nhất, CLI yêu cầu người điều hành tại thiết bị quản lý được kết nối trực tiếp với thiết bị bị quản lý . Điều này không khả thi trong các trường hợp mạng lớn, trong đó các bộ định tuyến và chuyển mạch được phân tán trong các vùng địa lý rộng. Truy nhập qua bàn điều khiển từ xa có thể đóng vai trò như một máy chủ kết cuối mà người sử dụng kết nối telnet qua nó tới thiết bị được quản lý .

Một phương pháp khác được sử dụng khi thiết bị hỗ trợ giao thức điều khiển truyền tải TCP (Transport Control Protocol) và chạy máy chủ Telnet, người điều hành có thể truy nhập bằng Telnet và chạy CLI.

Một trường hợp có thể xảy ra và cần được tính đến khi người điều hành phải cấu hình thiết bị trong thời gian thiết bị khởi tạo lại, vì vậy hầu hết các thiết bị đều lưu trữ dữ liệu của cấu hình trong một số dạng khác nhau, ví dụ trong ổ cứng, bộ nhớ flash, trên các máy chủ, v..v. Các thông tin thường được lưu trữ dưới dạng mã nhị phân để dễ dàng truy nhập và sử dụng bởi các phần mềm quản lý . Dạng thông tin này còn rất thuận lợi để ghi các câu lệnh cấu hình từ phía người quản lý hệ thống. Tệp cấu hình dựa trên các câu lệnh có ưu điểm lớn nhất là có thể kiểm tra và quản lý từ người điều hành và sửa đổi khi cần thiết.

Một lợi ích khác của CLI là dễ dàng đưa ra các mức điều khiển tinh qua các thiết bị và cho phép người sử dụng kiểm tra chi tiết các hoạt động gần nhất của thiết bị.

Giao diện người dùng đồ họa: Các giao diện người dùng đồ họa (GUI) là các công cụ cấu hình thân thiện với người dùng. Người sử dụng không cần nhớ ngôn ngữ câu lệnh mà thông qua các khoảng trống tham số để thực hiện cấu hình. Các giá trị ngầm định được cung cấp tự động trên cơ sở các trợ giúp ngữ cảnh có sẵn. Các giao diện đồ họa cung cấp phương thức (point-and-click) để kích hoạt các mức quản lý , chuột để lựa chọn thiết bị và để kéo thả các đối tượng cấu hình.

Lợi ích lớn nhất của GIU là phương pháp thu thập dữ liệu từ các thiết bị có thể hiển thị. Mặc dù ta có thể hiển thị bảng cơ sở dữ liệu như trong CLI, nhưng trong chế độ đồ họa của GUI ta có thể dễ dàng xem chi tiết các thông tin và thậm chí thể hiện động theo tiến trình và thời gian.

Các giao diện đồ họa có khả năng truy nhập và điều hành từ xa thông qua các giao diện điều hành mở X/open nhưng yêu cầu các thao tác đồ họa và thể hiện phức tạp trên các thiết bị bị quản lý .

GUI có thể được triển khai qua các CLI, khi đó tất cả các câu lệnh đưa ra bởi GUI được ánh xạ vào CLI và gửi tới thiết bị qua telnet. Các thông tin dữ liệu được thu thập bởi CLI và hiển thị trên màn hình đồ họa thích hợp. Mặt khác, GUI có thể sử dụng các giao thức truyền thông và các khuôn dạng dữ liệu riêng để trao đổi với các thiết bị nhằm giảm độ dài các câu lệnh điều khiển và dữ liệu ra.

Giao diện đồ họa cũng có khả năng xử lý các file cấu hình hệ thống. Nếu GUI được triển khai trên CLI thì việc lưu giữ file cấu hình được thực hiện qua các câu lệnh CLI. Mặt khác, GUI có thể được sử dụng trực tiếp thông qua các truy nhập tới các cấu trúc dữ liệu cấu hình để lưu trữ file cấu hình dưới dạng nhị phân. Tuy nhiên, phương pháp này phức tạp hơn nhiều so với phương pháp sử dụng các câu lệnh CLI.

Mặc dù giao diện đồ họa đưa ra các thể hiện thân thiện với người quản trị hệ thống. Nhưng các nhà quản trị hệ thống có kinh nghiệm thường sử dụng CLI vì CLI có thể đưa ra các mức điều khiển chi tiết hơn và đưa ra lượng thông tin lớn hơn, thậm chí là phương pháp nhập lệnh CLI cũng nhanh hơn.

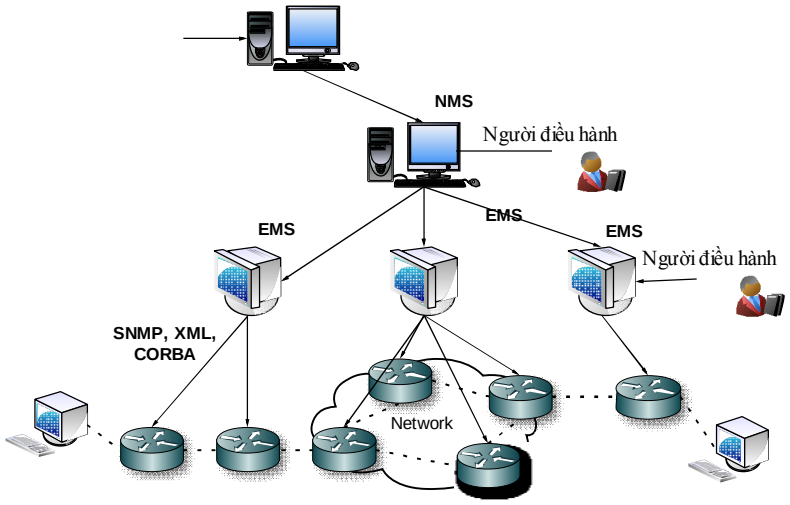
4.1.3 Truy nhập và thể hiện dữ liệu tiêu chuẩn hóa

Các nhà quản lý mạng mong muốn có một ứng dụng đơn để quản lý toàn bộ mạng. Ứng dụng này phải có khả năng điều khiển tất cả các thiết bị trong mạng, thu thập và tích hợp các thông tin và trạng thái lưu trữ trên các thiết bị. Như vậy, người quản trị mạng có được thông tin tổng thể một cách logic và giảm thiểu các nhiệm vụ quản lý mạng phức tạp do không cần sử dụng nhiều ngôn ngữ lệnh đối với các nhà cung cấp thiết bị khác nhau.

Một cách tiếp cận vấn đề này được theo hướng xây dựng công cụ quản lý tổng thể để phối hợp các module trong các thành phần riêng biệt và ánh xạ vào một thành phần điều khiển và hiển thị chung. Điều này dẫn tới sự khó khăn khi viết các ứng dụng quản lý khi phải cập nhật thường xuyên các câu lệnh mới từ mỗi nhà cung cấp thiết bị. Tuy nhiên, giải pháp này khả thi khi sử dụng tiếp cận theo module.

Một tiếp cận khác để tạo ra một công cụ quản lý tổng thể là tạo ra các module do các nhà cung cấp thiết bị chịu trách nhiệm quản lý toàn bộ các thiết bị của họ và tạo ra các giao diện tới ứng dụng chung. Trong ví dụ được chỉ ra trên hình 4.1, người điều hành thực hiện nhiệm vụ quản lý tại một hệ thống quản lý mạng NMS hoặc qua hệ thống hỗ trợ điều hành OSS (Telcordia). Sử dụng OSS cho phép người điều hành

ứng dụng các dịch vụ cung cấp và tính toán một cách chuyên biệt, OS sử dụng ngôn ngữ Scrip như TL1 để chuyển qua các câu lệnh CLI tới NMS.



Hình 4.1: Mô hình quản lý mạng IP

NMS là một ứng dụng quản lý tổng thể có thể thông tin tới nhiều hệ thống quản lý phần tử EMS, mỗi EMS được hỗ trợ bởi nhà cung cấp thiết bị như một module riêng để tổ hợp các thông tin tới mạng quản lý tổng thể. Như trên hình 4.1 chỉ ra, người điều hành có thể phải truy nhập tới các EMS bằng các giao diện CLI và GUI thích hợp để điều khiển thiết bị. Nếu người điều hành thực hiện tại NMS hoặc OSS thì tại đó phải có một kênh truyền thông giữa NMS và mỗi EMS. Hai yêu cầu cơ bản của truyền thông này gồm: các bản tin phải đảm bảo tính tổng thể và các dữ liệu phải được thể hiện trên khuôn dạng chung. Tiêu chuẩn phổ biến cho giao tiếp truyền thông từ NMS tới EMS là CORBA. CORBA cung cấp một phương thức tiêu chuẩn hóa để NMS truy nhập tới các đối tượng dữ liệu được quản lý bởi mỗi EMS, và cách thức cho các nhà cung cấp thiết bị hoặc EMS công khai khuôn dạng cơ sở dữ liệu tới NMS. Các khuôn dạng này được tiêu chuẩn hóa nhằm trợ giúp công việc quản lý giảm thiểu độ phức tạp. Ba kỹ thuật cấu hình dựa trên các tiêu chuẩn thông dụng thường được sử dụng là: CORBA, SNMP và XML. Nếu CORBA được sử dụng bởi EMS để quản lý các thiết bị của nó, ánh xạ giữa NMS và EMS. Tuy nhiên, một khi các thiết bị hỗ trợ giao thức cấu hình tiêu chuẩn hóa thì rất ít khi sử dụng EMS, các thiết bị này bổ sung các đặc tính quản lý đặc biệt của các nhà cung cấp thiết bị và nhận các lệnh trực tiếp từ NMS.

4.1.4 Một số vấn đề thách thức của quản lý mạng IP

Cùng với sự phát triển đa dạng của các công nghệ mạng, những thách thức đối với hệ thống quản lý mạng ngày càng lớn nhất là đối với các mạng lớn như mạng IP, trong đó các kiểu lưu lượng và sự tăng trưởng lưu lượng tiếp tục gia tăng không ngừng. Với những yêu cầu đảm bảo chất lượng dịch vụ trong môi trường đa dịch vụ, hệ thống quản lý mạng phải có khả năng quản lý từ đầu cuối tới đầu cuối, giảm giá

thành quản lý qua các thoả thuận chất lượng dịch vụ SLA (Service Level Agreement) nhằm nâng cao hiệu quả quản lý . Phần sau sẽ phân tích một số vấn đề này sinh khi sử dụng giao thức quản lý mạng đơn giản SNMP.

- *Chuyển các dữ liệu quản lý vào mã lệnh*

Dữ liệu liên kết và mã là những vấn đề liên quan tới các vấn đề tính toán, bảo mật và tối ưu trong quản lý mạng, các vấn đề này thường tập trung vào vùng quản lý mạng trên cơ sở các thực thể mạng NE (Network Element). Việc chuyển dữ liệu quản lý tới trạm quản lý thông qua cơ chế chuyển dữ liệu thành các mã gặp một số vấn đề sau:

- Các đối tượng bị quản lý nằm trên rất nhiều Agent
- Bản sao của các đối tượng quản lý nằm tại hệ thống Manager
- Sự thay đổi dữ liệu trên các Agent sẽ làm thay đổi dữ liệu bản sao trên Manager.

Như vậy, cơ sở thông tin quản lý MIB cung cấp một hạ tầng quản lý và phải dự phòng các không gian nhớ cho các thay đổi của đối tượng quản lý . Mặt khác, sự phát triển và độ phức tạp của NE tăng lên không ngừng trong khi quá trình truyền và nhận dữ liệu từ Agent là thủ tục bắt buộc của SNMP, vì vậy việc chuyển các dữ liệu thành mã như thế nào là một vấn đề thách thức của hệ thống quản lý mạng. Hơn nữa, hệ thống quản lý có nên đòi hỏi tất cả dữ liệu agent hay không? Trong thực tế, điều này chỉ chấp nhận được trên những mạng nhỏ nhưng không thể thực hiện được trên các mạng lớn. Khi các NE trở nên phức tạp hơn thì gánh nặng lại đặt lên hệ thống quản lý .

- *Sự tăng trưởng của MIB*

Các bảng cơ sở thông tin quản lý lưu trữ các tham số của đối tượng quản lý , khi số lượng NE lớn đồng nghĩa với việc mở rộng bảng MIB. Sự phức tạp gia tăng khi nhiều nhà cung cấp cung cấp những module MIB cho NEs của họ theo dạng file văn bản. Những file này có thể hợp nhất vào trong một hệ thống mạng quản lý NMS và dùng phối hợp với bộ duyệt MIB. MIB chứa định nghĩa đối tượng quản lý và dùng để dẫn xuất mô hình cơ sở dữ liệu cho NMS. Mô hình cơ sở dữ liệu NMS chứa số lượng lớn các bảng trong đó có một bảng để cất giữ những đường dẫn chi tiết, bảng khác cho các mạch ảo,v.v. Hệ thống quản lý mạng NMS theo dõi và sửa đổi những giá trị của NE, quản lý những đối tượng và lưu giữ nó trong cơ sở dữ liệu của mình.

Việc tích hợp các hệ thống thiết bị thành các phần tử mạng lớn cũng đem lại một số khó khăn trong hệ thống quản lý mạng, vì các chức năng được tích hợp rất khó quản lý đồng thời các hệ thống quản lý phải hỗ trợ rất nhiều tương tác trong phần mềm server đa xử lý FCAPS.

- *Độ phức tạp trong triển khai*

Việc xây dựng hệ thống quản lý cho những thiết bị mạng hiện nay và trong tương lai ngày càng gặp nhiều khó khăn (điều này là đúng với việc phát triển thiết bị của những công nghệ mới như MPLS hay Ethernet Gigabit là việc thêm vào hoặc kế thừa các NE lớp 2). Một số nhà cung cấp có những nhóm được tách riêng dành cho NE và việc phát triển hệ thống quản lý nên cần có sự truyền thông giữa những nhóm này. Ngoài ra việc thiết lập các kỹ năng yêu cầu của người phát triển phần mềm NMS đang tăng và bao gồm:

- Việc phát triển và làm mô hình hướng đối tượng sử dụng UML (Unified Modeling Language) cho việc giữ những yêu cầu, định nghĩa các hoạt động và các trường hợp sử dụng để sắp xếp chúng vào trong những lớp phần mềm.
- Phát triển các phần mềm quản lý trên Java/C++.
- Phần mềm Server đa xử lý FCAPS.
- Đặc biệt hỗ trợ cho việc phát triển các đặc tính như ATM/MPLS.
- Cơ sở dữ liệu của việc thiết kế/nâng cấp phù hợp với MIB tới giản đồ cơ sở dữ liệu qua nhiều phiên bản phần mềm NMS/NE.
- Công nghệ lớp 2 như ATM, FR và Gigabit Ethernet.
- Công nghệ kế thừa như thoại qua TDM và X.25.
- Khả năng phát triển mô hình và thành phần phần mềm chung, hệ thống quản lý có thể giấu nhiều chi tiết nằm bên dưới của hoạt động mạng.
- Thiết kế Client/server.
- Quản lý việc thiết kế đối tượng, giai đoạn làm mô hình của hệ thống quản lý .
- Việc thiết kế MIB cần có đối tượng mới bên trong thiết bị quản lý để hỗ trợ hệ thống quản lý .

Sự di trú chung tới cơ sở hạ tầng lớp 3 là một lý do khác cho việc mở rộng giữa những kỹ năng phát triển sẵn có và các đặc tính sản phẩm yêu cầu. Đây là một cách tiếp cận khác cho việc phát triển hệ thống quản lý thông qua:

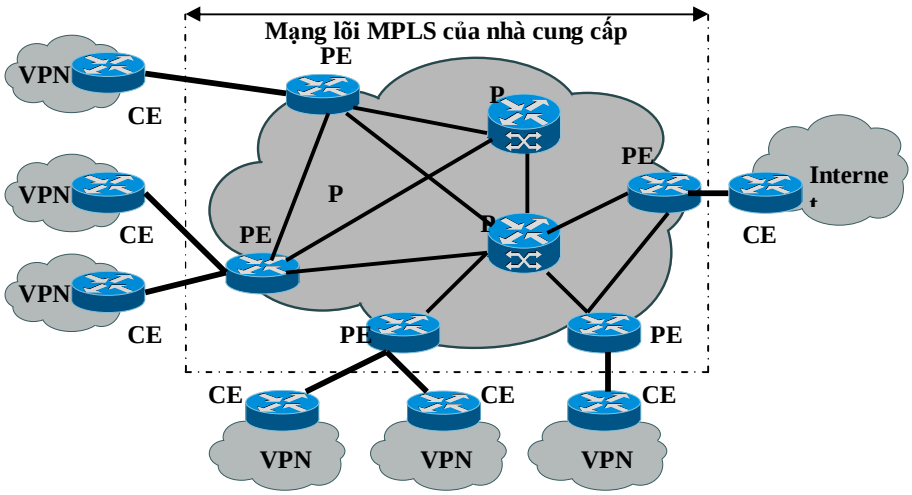
- Tập giải pháp tiêu chuẩn.
- Phân tán và giải quyết các vấn đề phát sinh.
- Xử lý thông tin thống kê.
- Bao quát những chu trình phát triển ngắn.
- Tối giản việc thay đổi mã.
- Tăng khả năng kiểm tra.

4.2 QUẢN LÍ MẠNG MPLS

4.2.1 Các ứng dụng cơ bản của MPLS

Hiện thời, hai ứng dụng quan trọng nhất của MPLS là kỹ thuật lưu lượng và mạng riêng ảo. Tuy nhiên các ứng dụng triển vọng khác của MPLS như VoIP, các dịch vụ mô phỏng kênh ảo và dịch vụ mạng LAN ảo qua MPLS cũng sẽ cùng tồn tại. Mặc dù một số ứng dụng của MPLS như TE và VPN hiện đang được phát triển trên một số giao thức không dựa trên MPLS, nhưng MPLS vẫn thỏa mãn được các mục tiêu của các ứng dụng do sự tách biệt của mặt bằng định tuyến và mặt bằng chuyển tiếp cùng với các cơ chế báo hiệu tích hợp trong MPLS. Ví dụ, với việc cung cấp dịch vụ mạng riêng ảo, MPLS có thể thực hiện đơn giản hoạt động cấu hình VPN bởi yêu cầu của người quản lý thông qua các thiết bị biên kết nối tới mạng biên khách hàng. Báo hiệu MPLS quản lý các kết nối thực tế trong VPN.

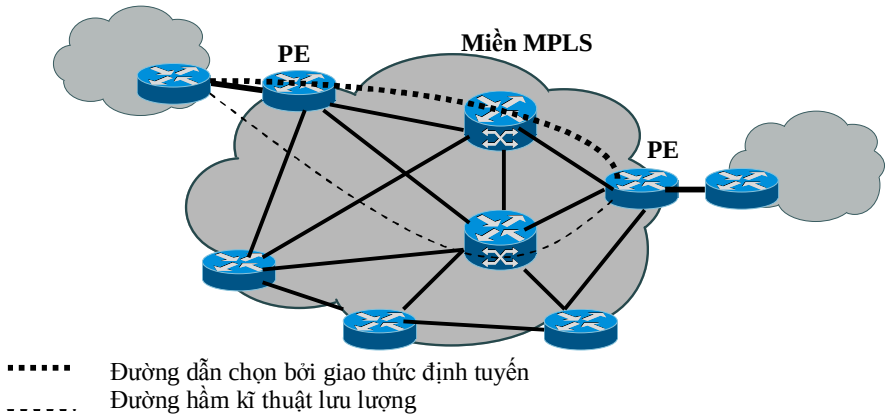
Một ví dụ của mạng MPLS hỗ trợ VPN được trình bày trong hình 4.2.



Hình 4.2: Ví dụ về cung cấp dịch vụ VPN trên MPLS

MPLS hỗ trợ kỹ thuật lưu lượng thông qua các tuyến hiện trong quá trình định tuyến để tạo ra một đường dẫn có một số đặc tính dữ liệu đặc biệt qua mạng. Các công nghệ hiện thời sử dụng các giao thức định tuyến để tìm ra các đường dẫn có trọng số thấp nhất. Như vậy, có thể xảy ra trường hợp tồn tại nhiều đường dẫn có trọng số bằng nhau và chỉ một đường được chọn. Mặt khác, các giao thức định tuyến thường chuyển tất cả các lưu lượng vào một đường dẫn đơn được chọn và có thể gây ra các điểm tập trung lưu lượng tại các nút khi có rất nhiều đường dẫn xuyên qua đó. Giải pháp kỹ thuật lưu lượng được sử dụng để giải quyết hai vấn đề còn tồn tại trên thông qua các tuyến hiện được điều hành bởi người quản lý . Người quản lý có thể phân các luồng lưu lượng trong mạng theo các tuyến khác nhau không phụ thuộc vào tiến trình định tuyến. Hơn nữa, kỹ thuật lưu lượng cho phép người quản lý mạng có thể tạo ra các

tuyến dự phòng cho các đường dẫn. Để thực hiện các cơ chế này, các đường hầm MPLS TE được thiết lập để truyền tải các gói qua mạng MPLS. Một ví dụ về MPLS TE được mô tả trên hình 4.3.



Hình 4.3: Đường hầm kỹ thuật lưu lượng trong MPLS-TE

Với giả thiết các liên kết có cùng giá trị trọng số thì hai đường dẫn có trọng số bằng nhau sẽ được thực hiện cho truyền tải dữ liệu. Đường chấm đậm thể hiện đường dẫn tối ưu được chọn bởi giao thức định tuyến, đường chấm nhạt thể hiện đường hầm MPLS TE đã được cấu hình qua đường dẫn chọn bởi giao thức định tuyến. Điều này cho phép một số lưu lượng đi qua các đường dẫn ngầm định chuyển hướng sang các đường luân phiên. Đường hầm TE đã được cấu hình để sử dụng đường dẫn luân phiên và chưa sử dụng để tối ưu nguồn tài nguyên mạng.

4.2.2 Các đối tượng quản lý trong MPLS

Một trong các thách thức lớn nhất của vấn đề quản lý mạng MPLS nảy sinh từ cơ chế báo hiệu của giải pháp công nghệ này. MPLS sử dụng các kỹ thuật định tuyến khác nhau để thiết lập các đường dẫn thông qua các điều kiện ràng buộc để tạo ra các đường chuyển mạch nhãn LSP. LSP được tạo ra không nhất thiết phải tồn tại các cơ chế báo hiệu như trong mạng IP thuần cho dù các phần tử mạng của MPLS có thể hỗ trợ các giao thức báo hiệu. Thêm vào đó, số lượng phần tử cần quản lý trong mạng MPLS là rất lớn và đưa tới các thủ tục quản lý có độ phức tạp cao. Các đối tượng quản lý được chỉ ra dưới đây là các đối tượng quan trọng nhất của vấn đề quản lý mạng MPLS.

A. Đối tượng định tuyến hiện (ERO)

Đối tượng định tuyến hiện ERO (Explicit Route Object) là một danh sách các địa chỉ lớp 3 trong một vùng mạng MPLS. Tương tự như danh sách chuyển tiếp mong muốn DTL (Designated Transit List) trong ATM, ERO mô tả một danh sách các nút MPLS có đường hầm đi qua. ERO được thiết lập thông qua giao thức báo hiệu dành trước tài nguyên hỗ trợ kỹ thuật lưu lượng RSVP-TE nhằm chỉ rõ đường dẫn chứa đường hầm. Trên khía cạnh định tuyến, tuyến hiện còn thể hiện đặc tính ràng buộc của

đường dẫn, vì vậy đối tượng tuyến hiện cho phép người quản lý có thể cưỡng bức các đường dẫn theo từng bước nhảy trên LSP. Một đối tượng tuyến hiện ERO lưu trữ trong bảng MIB trên nút khởi đầu LSP và có thể dùng cho nhiều đường hầm của nút đó. Do đặc tính hỗ trợ lưu lượng tự động, các đối tượng tuyến hiện thường không sử dụng phương pháp cấu hình nhân công cho các LSP mà thông qua các giao thức báo hiệu như RSVP-TE.

B. Đối tượng tài nguyên

Các giải pháp hỗ trợ kỹ thuật lưu lượng và QoS trong MPLS cho phép sự dành trước tài nguyên trong mạng. Đối tượng tài nguyên trong MPLS được cung cấp thông qua các bản tin dành trước tài nguyên, đường hầm ưu tiên hoặc các đường dẫn LSP ngắn nhất. Trên góc độ quản lý lưu lượng LSP cho mạng MPLS, đối tượng tài nguyên của LSP thường gồm một số thành phần sau:

- Băng tần thu phát lớn nhất.
- Kích cỡ bó lưu lượng lớn nhất.
- Độ dài gói.

C. Đường hầm và đường chuyển mạch nhãn

Các đường hầm trong MPLS được thể hiện qua các đối tượng gồm phân đoạn vào (In-segment), kết nối chéo (Cross connect) và phân đoạn ra (Out-segment). Một gói tin được chuyển qua đường hầm trên cơ sở của các phương pháp sau:

- Chuyển tiếp dựa trên cơ sở tra cứu nhãn MPLS.
- Chuyển tiếp trên cơ sở tài nguyên có sẵn cố định.
- Chuyển tiếp theo trên cơ sở ràng buộc theo kỹ thuật lưu lượng.

Các đường hầm và LSP đều dựa trên kỹ thuật lưu lượng xác lập qua các địa chỉ IP đặc biệt, các gói tin trong đường hầm được phân biệt qua các địa chỉ IP tại phía đầu vào và đầu ra của đường hầm nhằm hỗ trợ kỹ thuật lưu lượng. Các đối tượng phân đoạn vào và ra là các điểm đầu vào và đầu ra lưu lượng của một nút. Từ các đối tượng này, nút MPLS sử dụng đối tượng kết nối chéo nhằm quyết định chuyển mạch lưu lượng qua nút. Một bảng đấu nối chéo trong một nút MPLS hỗ trợ 3 kiểu kết nối gồm: Điểm - điểm, điểm - đa điểm và đa điểm - điểm.

D. Các giao thức báo hiệu

Các đường dẫn chuyển mạch nhãn LSP và đường hầm trong MPLS có thể sử dụng bằng phương pháp nhân công hoặc tự động thông qua giao thức báo hiệu. Các giao thức báo hiệu trong MPLS có thể được sử dụng để thiết lập các LSP bao gồm hai giao thức cơ bản: Giao thức dành trước tài nguyên hỗ trợ kỹ thuật lưu lượng RSVP-TE và giao thức phân phối nhãn ràng buộc CR-LDP. Các giao thức báo hiệu này thể hiện tài nguyên quản lý thông qua các hoạt động cấp phát nhãn, chọn đường dẫn và thiết lập các đặc tính đường dẫn.

4.2.3 Đặc điểm MIB trong quản lý mạng MPLS

A. Một số vấn đề của cơ sở thông tin quản lý trong MPLS

Cơ sở thông tin định tuyến MIB thể hiện sự phân chia không gian giữa các đại diện quản lý và các nhà quản lý mạng. MIB đóng vai trò trung tâm trong mạng quản lý của các kiểu mạng viễn thông bao gồm cả MPLS, nếu MIB đưa ra cấu hình quản lý thích hợp thì các tác vụ như cài đặt, cấu hình và hoạt động các phần tử mạng NE trong một hệ thống quản lý mạng NMS sẽ giảm thiểu được độ phức tạp.

Thông qua giao thức quản lý mạng đơn giản, các khoản mục dữ liệu được tạo ra trong các bảng MIB dưới dạng các hàng. Mối liên hệ với các cột trong bảng cơ sở thông tin quản lý sẽ thể hiện các đối tượng quản lý liên quan. Thứ tự các cột trong bảng và mức độ kết hợp giữa cột thể hiện khả năng kết hợp các khối đặc tính của đối tượng. Mặt khác, một khoản mục có thể được sử dụng lại tại các bảng khác nhằm tối ưu hóa tài nguyên của các bảng cơ sở dữ liệu. Ví dụ, trong một bảng thể hiện các đường hầm MPLS gồm các bảng bước nhảy tuyến hiện ERO và bảng tài nguyên được dành trước đều được sử dụng bởi bảng đường hầm.

Trong kết cấu đa bảng MIB, các bảng được liên kết với nhau thông qua các chỉ mục số nguyên nhằm chia sẻ các khoản mục trong các bảng khác nhau dựa trên các cột. Vì vậy, các hệ thống quản lý mạng thường lưu trữ dữ liệu các phần tử dưới dạng các lưu đồ cơ sở dữ liệu quan hệ.

Các giá trị đối tượng trong bảng MIB có thể được thiết lập mặc định nhằm tạo điều kiện thuận lợi trong quá trình quản lý các kết nối. Một kết nối thường được đặc trưng bởi mối liên hệ giữa các bảng và có một số giá trị mặc định được xác định trước. Các giá trị này được có sẵn tại các bảng MIB của các phần tử mạng NE và được xác minh qua các thủ tục kiểm tra nhanh.

Các giá trị mặc định có thể được đưa vào MIB từ các đối tượng bên ngoài thông qua giao thức SNMP. Ví dụ, đối tượng đường hầm MPLS gồm các đặc tính liên quan mplstunnelIncludeAffinity trong bảng đường hầm MPLS. Đối tượng này được sử dụng khi tạo ra một đường hầm trong đó người sử dụng muốn cưỡng bức các lưu lượng qua một vùng MPLS. Do một loạt các yếu tố xác định đặc tính từ phía nhận dịch vụ nên việc cung cấp các giá trị mặc định cho đối tượng này có thể giảm bớt sự tác động từ các Agent, khi xảy ra trường hợp phía thu nhận sử dụng một giá trị không hiệu lực của một cột thì giá trị ngoại lệ đó sẽ được xác lập bằng nhân công. Mỗi giá giá trị cho phép của mplstunnelIncludeAffinity được xác định bằng mặt nạ bít nguyên mô tả một giá trị mã màu giao diện, ví dụ: 0x00001 cho vàng, 0x00010 cho bạc, và 0x00100 cho đồng. Mạng quản lý phải cấu hình các màu này trên tất cả các phần tử mạng NE liên quan. Có thể cấu hình để hỗ trợ cho màu bạc và đồng trên một giao diện vào của NE. Sau đó một đường hầm có thể tạo ra một đường cưỡng bức sử dụng chỉ với giao diện với màu

bạc và đồng bởi sự thiết lập mplstunnelIncludeAffinity vào mặt nạ 0x00110. Giá trị mặc định để không sử dụng đối tượng mplstunnelIncludeAffinity trong bảng MIB là 0.

Một bảng đường hầm trong MPLS có tính năng tập trung các mối quan hệ các đặc tính của đường hầm. Các bảng đơn lẻ bên ngoài được sử dụng để tạo, sửa đổi và quản lý các đường hầm thông qua các quan hệ với bảng đường hầm. Vì vậy, các lệnh cung cấp và và xác lập kết nối được thực hiện đơn lẻ tại các bảng và giảm thiểu các trường MIB trong hệ thống quản lý mạng NMS.

B. Các trình duyệt MIB

Các trình duyệt MIB là các công cụ đặc biệt để kiểm tra các giá trị của các trường hợp đối tượng MIB trên một Agent đưa ra. Một trình duyệt có thể là một ứng dụng có giao diện đồ họa hoặc giao diện dòng lệnh. Trình duyệt MIB có thể sử dụng kiểu biên dịch để chỉ ra cấu trúc các file MIB và thống kê giá trị cho các đối tượng kết hợp. Các đặc tính và hành vi đối tượng được đưa ra bởi NMS được người sử dụng tường minh qua trình duyệt MIB.

C. Các đối tượng quản lý MPLS trong MIB

Thông tin quản lý MIB cho MPLS chia các đối tượng quản lý thành hai loại:

- Các đối tượng mức thấp: Giao diện, kết nối chéo, các bảng phân đoạn và LSP;
- Các đối tượng mức cao: Đối tượng kỹ thuật lưu lượng đường hầm, các tuyến hiện và tài nguyên.

Các đối tượng MIB trong các bộ định tuyến chuyển mạch nhãn LSR gồm các bảng mô tả: Cấu hình giao diện MPLS, in-segments, out-segments, đấu nối chéo, các giới hạn lưu lượng, các giới hạn thực thi.

Các đối tượng kỹ thuật lưu lượng MIB gồm các bảng mô tả: đường hầm kỹ thuật lưu lượng, các tài nguyên đường hầm, các đường hầm và bộ đếm thực thi đường hầm.

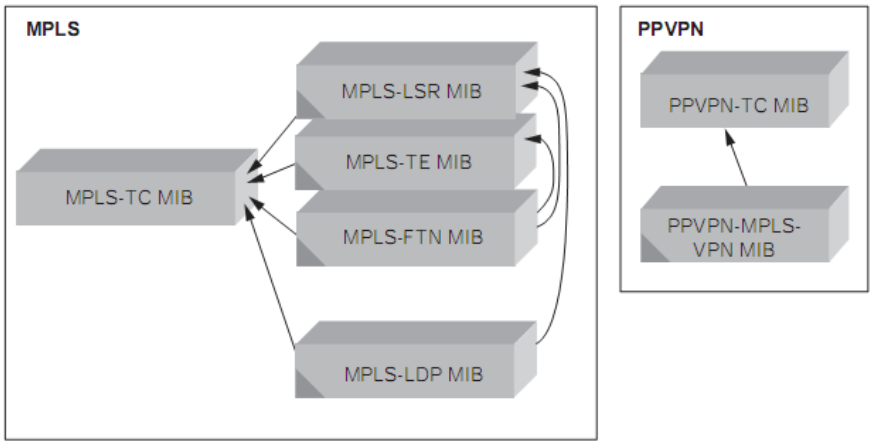
Các đối tượng thiết bị MPLS gồm các bộ định tuyến chuyển mạch nhãn, các bộ định tuyến IP, các thiết bị chuyển mạch ATM trong chế độ luân phiên và các chuyển mạch đa dịch vụ.

Giao diện MPLS được cấu hình trên thiết bị gồm các thành phần sau:

- Giao diện tới bộ định tuyến IP
- Giao thức định tuyến nội miền IGP (bao gồm cả giao thức định tuyến hỗ trợ kỹ thuật lưu lượng)
- Giao thức định tuyến ngoại miền EGP (không cấu hình cùng với IGP nhằm tránh lỗ hổng thông tin định tuyến)
- Giao thức báo hiệu LDP hoặc RSVP-TE.

D. Các module quản lý MPLS trong MIB

Để quản lý các đối tượng trong MPLS, một số các module cơ sở thông tin quản lý đã được các tổ chức tiêu chuẩn đưa ra nhằm đáp ứng các yêu cầu quản lý mạng MPLS. Cơ cấu tổ chức của các cơ sở thông tin quản lý được mô tả trên hình 4.4.



Hình 4.4: Cơ cấu tổ chức của các module MIB cho MPLS

MPLS-TC MIB: cơ sở thông tin quản lý MPLS-TC MIB mô tả chuyển đổi chuẩn tắc cho các bảng cơ sở thông tin quản lý liên quan.

MPLS-LSR MIB: MPLS-LSR MIB mô tả các hoạt động chuyển tiếp nhãn cơ bản của một bộ định tuyến chuyển mạch nhãn LSR. MPLS-LSR MIB cũng mô tả các giao diện mà LSR cho phép tham chiếu chéo tới các giao diện MPLS có trong bảng cơ sở thông tin quản lý giao diện IF-MIB. Cơ sở thông tin quản lý này thể hiện căn cứ thiết lập các đối tượng thực tế (đối ngược với TC trong MPLS-TC MIB) được sử dụng bởi các MIB khác.

MPLS-TE MIB: Cơ sở thông tin quản lý TE cung cấp tới người quản lý các khía cạnh của các đường hầm kỹ thuật lưu lượng để cấu hình và quản lý các đặc tính. Nếu một đường hầm cũng thể hiện như một giao diện trong bảng cơ sở thông tin quản lý giao diện IF-MIB thì tại đó sẽ tồn tại một khoản mục sử dụng cho tham chiếu. MPLS-TE MIB phụ thuộc bảo bảng MPLS-LSR MIB, trong đó phần mềm hệ thống trong một thiết bị có thể được lập trình để liên kết các LSP hoạt động với một đường hầm.

MPLS-LDP MIB: Cơ sở thông tin quản lý giao thức phân phối nhãn cung cấp thông tin về các hoạt động của giao thức LDP trên một LSR. MPLS-LDP MIB phụ thuộc vào MPLS-LSR MIB để ánh xạ các bảng dữ liệu sử dụng để liên kết các phiên LDP và các LSP hoạt động. MPLS-LDP MIB cũng phụ thuộc vào bảng IF-MIB nhằm thể hiện miền nhãn được cấu hình trên các giao diện MPLS.

MPLS-FTN MIB: cơ sở thông tin quản lý ghép các lớp lưu lượng tương đương vào bước nhảy kế tiếp thể hiện cách thức và hành vi của lưu lượng IP đi vào mạng

MPLS, và cách thức ánh xạ các luồng lưu lượng IP vào trong các LSP hoặc các giao diện đường hầm TE. MPLS-FTN MIB phụ thuộc vào MPLS-LSR-MIB và MPLS-TE MIB trên quan hệ ghép luồng lưu lượng IP tới LSP và đường hầm TE.

MPLS-FTN MIB cũng phụ thuộc vào bảng cơ sở thông tin quản lý giao diện MPLS do nó cho phép người điều hành cấu hình FEC- to- NHLFE theo từng giao diện.

PPVPN-MPLS-VPN MIB: cơ sở thông tin quản lý mạng riêng ảo của các nhà cung cấp dịch vụ chỉ phụ thuộc vào bảng chuyển đổi dữ liệu MPLS-TC MIB. Bảng này chứa các biến đổi text chung được sử dụng bởi các PPVPN-MPLS-VPN MIB và các cơ sở thông tin quản lý khác. PPVPN-MPLS-VPN MIB cung cấp cho người điều hành khía cạnh cấu hình VPN trên các thiết bị của nhà cung cấp PE. Cũng như là các thông tin liên quan như: thống kê, BGP và giao diện. Thông tin giao diện được thể hiện trong bảng cơ sở thông tin quản lý IF-MIB và vì vậy PPVPN-MPLS-VPN MIB phụ thuộc vào bảng IF-MIB.

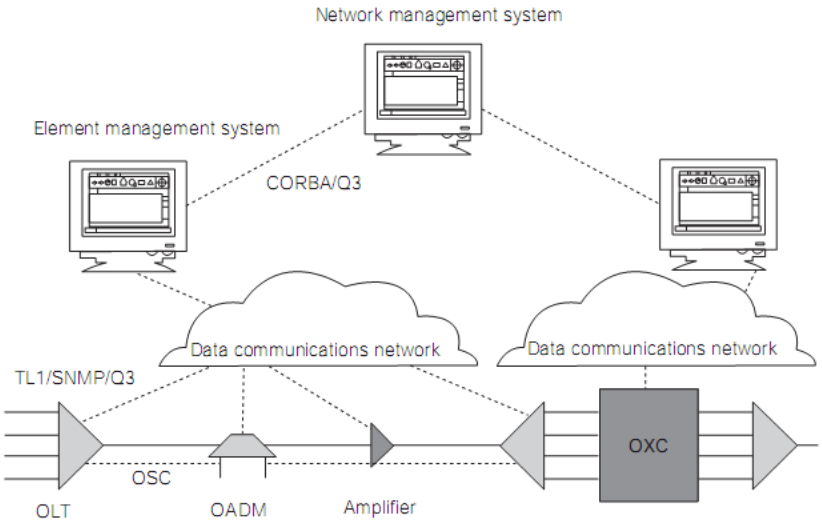
4.3 QUẢN LÍ MẠNG QUANG

4.3.1 Khung làm việc của quản lý mạng quang

Trên cơ sở hàng loạt các phương pháp quản lý mạng được giới thiệu trong chương 1 của bài giảng, các chức năng quản lý mạng có thể được thực hiện theo các cấu hình tập trung, phân tán và phân cấp. Với yêu cầu tốc độ cao trong vấn đề quản lý , các phương pháp điều khiển tập trung và phân cấp rất khó đáp ứng được các yêu cầu của mạng quang nhất là đối với các mạng lớn. Thêm vào đó, các mạng lớn thường được quản lý theo từng vùng bởi các nhà quản lý riêng và các nhà quản lý thông tin với các nhà quản lý của vùng khác thông qua chức năng phối hợp. Hình 4.5 chỉ ra tổng quan của các chức năng quản lý mạng điển hình sử dụng cho mạng quang. Các chức năng quản lý được phân cấp theo nhiều hệ thống quản lý , các thành phần riêng biệt được quản lý gọi là các phần tử mạng. Các phần tử mạng gồm: các đầu cuối đường quang OLT (Optical Line Terminal), các khối ghép/tách quang OADM (Optical Add/Drop Multiplexer), Các bộ khuếch đại quang, các thiết bị kết nối chéo quang OXC (Optical cross-connect). Mỗi phần tử mạng được quản lý bởi hệ thống quản lý phần tử EMS. Các Agent được thường trú trong phần mềm của vi xử lý trong phần tử mạng.

Hệ thống quản lý phần tử mạng EMS thường được kết nối tới một hoặc nhiều phần tử mạng và truyền thông với các phần tử mạng khác trong mạng qua mạng truyền thông dữ liệu DCN (data communication network). Kênh truyền thông báo hiệu được thiết lập trong DCN thường được tách biệt nhằm truyền tải các thông tin quản lý thời gian thực ví dụ như kênh giám sát quang OSC (Optical Supervisory Channel).

Để quản lý toàn mạng, một số hệ thống quản lý phần tử EMS được xây dựng cho các hệ thống thông tin quang phục vụ cho công tác quản lý . Ví dụ, một nhà khai thác sử dụng hệ thống ghép kênh phân chia theo bước sóng WDM (wavelength division multiplexing) của nhà cung cấp thiết bị A và kết nối chéo tới nhà cung cấp thiết bị B thường sẽ sử dụng hai EMS: một sử dụng để quản lý hệ thống đường cáp quang và một cho kết nối chéo. Như trên hình 4.5, một EMS thường chỉ quản lý một phần tử mạng tại một thời điểm và không bao hàm quản lý toàn mạng, vì vậy các kiểu phần tử mạng khác không được quản lý . EMS thực hiện truyền thông với hệ thống quản lý mạng NMS hoặc hệ thống hỗ trợ điều hành để trao đổi thông tin và quản lý tới các phần tử khác đó.



Hình 4.5: Mô hình tổng quan của quản lý mạng quang

4.3.2 Giao diện và các dịch vụ lớp quang

Lớp quang cung cấp các đường dẫn quang tới các lớp khác như SONET, IP hoặc ATM. Trong ngữ cảnh này, lớp quang có thể nhìn nhận như một lớp phục vụ cho các dịch vụ từ các lớp khác đưa tới, lớp quang đóng vai trò "server" và các lớp dịch vụ đóng vai trò "client". Từ góc độ này, một số đặc tính then chốt của lớp quang liên quan tới vấn đề quản lý được đưa ra như sau:

- Các đường dẫn quang cần được thiết lập và giải pháp bởi các lớp client cũng như là đáp ứng các yêu cầu duy trì mạng.
- Băng thông các đường dẫn quang cần được thỏa thuận giữa các lớp client và lớp quang. Thông thường các lớp client đưa ra các lượng băng thông cần thiết tới lớp quang.
- Chức năng tương thích có thể được yêu cầu tại đầu vào và đầu ra của mạng quang để biến đổi các báo hiệu client thành các tín hiệu tương thích với lớp quang. Chức năng này thường được thực hiện bởi bộ chuyển đổi

tín hiệu (transponder) bao gồm cả kiểu tín hiệu, tốc độ bit và các giao thức hỗ trợ cho kết nối giữa client và lớp quang.

- Các đường dẫn quang cần được cung cấp các mức đảm bảo hiệu năng, điển hình là tỉ lệ lỗi bít không vượt quá 10^{-12}.
- Các mức bảo vệ khác nhau cho mạng quang cần phải được triển khai và quản lý bao gồm cả mức ưu tiên, độ dự phòng và yêu cầu thời gian khôi phục cho các dịch vụ khác nhau.
- Hầu hết các đường dẫn quang hiện nay đều thiết kế song hướng mặc dù các đường dẫn quang có thể đơn hướng hoặc song hướng. Tuy nhiên, khi có yêu cầu khác biệt về băng thông, mạng vẫn cần có cấu hình đơn hướng.
- Các yêu cầu về biến động trễ thường được đưa ra đối với các kết nối SONET/SDH, cũng như yêu cầu về độ trễ tối đa cho một số kiểu lưu lượng cũng là các vấn đề cần quản lý trong các đường dẫn quang.
- Quản lý lỗi mở rộng cần được hỗ trợ để tìm tới gốc của nguyên nhân gây ra cảnh báo. Điều này rất quan trọng vì một số lỗi đơn có thể kích hoạt thêm nhiều lỗi và tạo ra nhiều cảnh báo khác nhau.

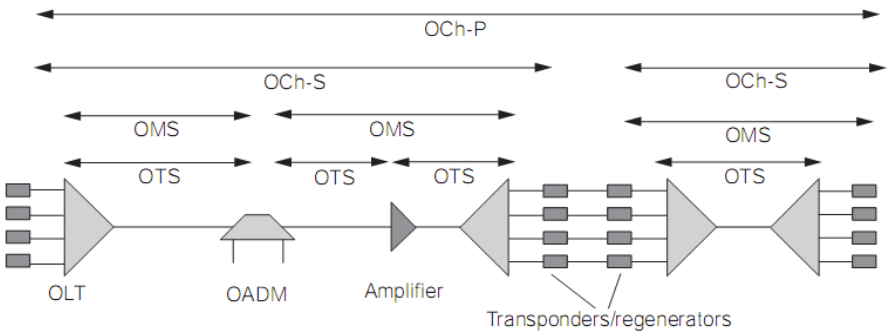
Giữa các lớp client và lớp quang hình thành một giao diện quản lý và điều khiển, giao diện này cho phép client chỉ rõ tập đường dẫn quang được thiết lập hoặc giải phóng cùng với một số tham số dịch vụ liên quan. Ngoài ra, giao diện này cho phép lớp quang cung cấp các thông tin quản lý lỗi và hiệu năng tới lớp client.

Giao diện đơn giản nhất thường sử dụng hiện nay là thông qua hệ thống quản lý . Một hệ thống quản lý tách biệt truyền thông với EMS của lớp đường dẫn quang và EMS quản lý lớp quang.

Do các đường dẫn quang hiện nay thường được thiết lập trong các khoảng thời gian dài, nhưng trong tương lai các đường dẫn quang sẽ được thiết lập động dẫn tới vấn đề giao diện báo hiệu giữa lớp client và lớp quang sẽ trở nên phức tạp. Ví dụ, các bộ định tuyến IP có thể báo hiệu để liên kết tới kết nối quang nhằm thiết lập và giải phóng các đường dẫn quang cũng như áp các đặc tính bảo vệ thông qua giao diện báo hiệu này.

Việc tồn tại giao diện như giao diện báo hiệu phụ thuộc vào cách tiếp cận của các nhà khai thác. Một số nhà khai thác cho rằng cần phải tách biệt cơ chế quản lý mạng quang ra khỏi các lớp client khác. Tiếp cận này hữu ích khi lớp quang phải phục vụ nhiều đối tượng dịch vụ khác nhau trong lớp client. Ngược lại, khi lớp quang chỉ phục vụ số ít lớp client thì các cơ chế kết hợp quản lý sẽ đem lại hiệu quả cao, nhất là về thời gian thực hiện quản lý .

Lớp quang là một thực thể phức tạp để thực hiện một số chức năng như: ghép kênh bước sóng, chuyển mạch và định tuyến bước sóng và giám sát hiệu năng mạng tại các mức khác nhau trong mạng. Kiến trúc phân lớp trong lớp quang được chỉ ra trên hình 4.6 được ITU đưa ra gồm 3 lớp:



Hình 4.6: Các phân lớp trong lớp quang

Lớp trên cùng là lớp kênh quang Och liên quan tới định tuyến từ đầu cuối tới đầu cuối của các đường dẫn quang. Thuật ngữ đường dẫn quang mô tả một chuỗi các kênh kết nối giữa các nút quang. Một đường dẫn quang chuyển qua trên nhiều liên kết quang và các bộ ghép kênh mang các đường dẫn quang.

Mỗi liên kết giữa OLT hoặc OADM thể hiện qua một vùng truyền tải đa bước sóng OMS (carrying multiple wavelength) mang các bước sóng. Mỗi một vùng truyền tải đa bước sóng OMS gồm một vài đoạn liên kết, mỗi đoạn là một phần của liên kết giữa hai điểm kết nối quang, các đoạn này hợp thành phân đoạn truyền dẫn quang OTS (optical transmission section). OTS gồm vùng truyền tải đa bước sóng và các thiết bị kết nối chéo quang.

Trên chính lớp kênh quang cũng được chia thành các phân lớp nhỏ hơn, một đoạn trong suốt kênh quang Och-TS thể hiện một đoạn của đường dẫn quang trong một phân mạng toàn quang. Trong đoạn này, các đường dẫn quang được mang trên các cáp quang mà không có sự hiện diện của vùng điện.

Ngay phía trên của Och-TS là lớp đoạn kênh quang Och-S, lớp này thêm các tiêu đề cho đường dẫn quang để thực hiện báo hiệu cho các phân mạng quang.

Cuối cùng, lớp đường dẫn kênh quang Och-P thể hiện truyền tải từ đầu cuối tới đầu cuối của một đường dẫn quang qua các miền quang.

Về mặt nguyên tắc, khi các giao diện giữa các lớp khác nhau được định nghĩa để cung cấp cho các nhà cung cấp thiết bị cung cấp các thiết bị tiêu chuẩn hóa. Hơn nữa, các lớp này tạo ra các tiếp cận quản lý tốt nhất tới các thiết bị mạng.

4.3.3 Quản lý lỗi và hiệu năng mạng quang

Mục tiêu của quản lý hiệu năng mạng là cung cấp đảm bảo chất lượng dịch vụ tới người sử dụng của mạng. Điều này thường yêu cầu giám sát các tham số hiệu năng cho tất cả các kết nối trong mạng và đưa ra các hoạt động cần thiết để đảm bảo các yêu cầu hiệu năng. Vấn đề quản lý hiệu năng mạng gần với vấn đề quản lý lỗi. Quản lý lỗi gồm tiến trình xác định lỗi và cảnh báo tới hệ thống quản lý khi có một hoặc vài

tham số nào đó vượt ngưỡng. Quản lý lỗi cũng gồm các dịch vụ khôi phục các sự kiện lỗi. Chức năng này được coi như chức năng điều khiển mạng tự trị vì thông thường các ứng dụng khôi phục lỗi được phân tán trong mạng.

A. Quản lý tỷ lệ lỗi bit

Tỷ lệ lỗi bit là đặc tính hiệu năng then chốt của các đường dẫn quang. Các khung tín hiệu trong SONET và SDH bao gồm các byte tiêu đề trong đó có chưa các byte kiểm tra chẵn lẻ để tính toán tỷ lệ lỗi bít. Các tiêu đề này cung cấp phép đo trực tiếp tỷ lệ lỗi bit. Các dữ liệu báo hiệu cho client được đóng gói trong các khung tiêu đề của khung tin SONET/SDH và ta có thể đo BER và đảm bảo hiệu năng trong lớp quang.

Khi lớp quang có thiết kế phức tạp, rất khó để đánh giá chính xác BER dựa trên các phép đo gián tiếp các tham số như công suất tín hiệu quang hoặc tỷ lệ tín hiệu trên nhiễu. Các tham số này có thể được sử dụng để đánh giá chất lượng tín hiệu và có thể để sử dụng làm căn cứ phát hiện cảnh báo nhưng không nên sử dụng để đánh giá BER.

B. Giám sát vết đường quang

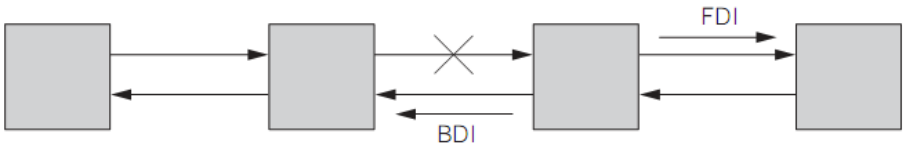
Các đường dẫn quang đi qua nhiều nút và qua nhiều card thiết bị trong mỗi nút. Việc giám sát vết đường quang nhằm chỉ ra các nhận dạng duy nhất cho mỗi đường dẫn quang. Ví dụ, nhận dạng này gồm địa chỉ IP của phần tử mạng nguồn phát cùng với các nhận dạng của card chuyển đổi trong các phần tử mạng mà đường dẫn quang đi qua. Nhận dạng này được gọi là giám sát vết đường quang. Vết đường quang cho phép hệ thống quản lý nhận dạng, kiểm tra và quản lý các kết nối trong đường dẫn quang. Thêm vào đó, nó cung cấp khả năng cách ly lỗi cho hệ thống quản lý mạng.

Giám sát vết đường dẫn quang có thể sử dụng trong nhiều lớp khác nhau trong lớp quang. Ví dụ, một đường dẫn quang đi qua nhiều nút và các bộ tái tạo tín hiệu quang, ta có thể xác định kết nối từ đầu cuối tới đầu cuối của đường dẫn quang thông qua giám sát vết đường dẫn kênh quang. Giám sát vết này được đưa tại đầu vào của đường dẫn quang và giám sát tại các vị trí khác nhau trên đường dẫn. Để xác định vị trí và xác định kết nối giữa các vùng tái tạo tín hiệu quang, ta sử dụng thêm nhận dạng giám sát vết cho đoạn kênh quang. Trong một mạng con toàn quang, ta có thể sử dụng giám sát vết phân đoạn trong suốt cho kênh quang. Hai kiểu giám sát vết cuối này được chèn vào và lấy ra tại các bộ tái tạo tín hiệu quang.

C. Quản lý cảnh báo

Trong một mạng, một sự kiện lỗi đơn lẻ có thể là nguyên nhân tạo ra rất nhiều cảnh báo qua mạng và dẫn tới các điều kiện lỗi khác. Ví dụ, khi một liên kết hỏng, tất cả các đường dẫn quang qua đó đều lỗi. Sự kiện này có thể được các nút tại cuối của liên kết lỗi phát hiện và các nút này sẽ đưa ra các cảnh báo cho các đường dẫn quang cũng như là báo cáo sự kiện lối tới hệ thống quản lý mạng. Thêm vào đó, tất cả các

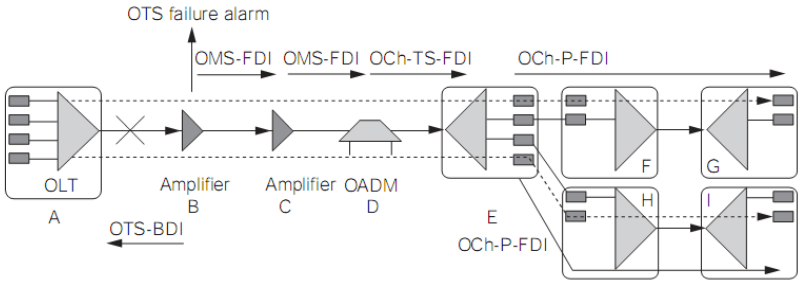
nút mà đường dẫn quang đi qua sẽ nhận được các cảnh báo này. Vì vậy, số lượng bản tin cảnh báo rất lớn. Việc loại bỏ bớt các cảnh báo không cần thiết được sử dụng qua một tập các tín hiệu đặc biệt được gọi là chỉ thị lỗi hướng đi FDI (forward defect indicator) và chỉ thị lỗi hướng về BDI (backward defect indicator).



Hình 4.7: Ví dụ về các tín hiệu FDI và BDI trong mạng quang

Hình 4.7 chỉ ra hoạt động điều hành của tín hiệu FDI và BDI. Khi một liên kết lỗi, nút hướng xuống của liên kết lỗi sẽ phát hiện ra lỗi liên kết và tạo ra điều kiện lỗi. Điều kiện lỗi có thể được tạo ra do tỷ lệ lỗi bit lớn trên luồng tín hiệu đến hoặc mất luồng tín hiệu. Nếu lỗi tiếp tục xuất hiện trong một chu kỳ thời gian (vài giây) thì nút sẽ phát cảnh báo.

Ngay sau khi xác định lỗi, nút chèn một tín hiệu FDI hướng xuống nút kế tiếp. tín hiệu FDI cũng thường được gọi là tín hiệu chỉ thị cảnh báo AIS (alarm indication signal). Một nút phát hiện lỗi cũng gửi tín hiệu BDI tới các nút phía trên nó để thông báo chính nó đang lỗi. Nếu một nút không thể gửi đi được FDI thì liên kết giữa nút đó và nút đường xuống cũng bị lỗi. Việc tách các tín hiệu FDI và BDI rất hữu ích cho các lớp khác nhau trong lớp quang. Ví dụ, để phân biệt các lỗi trên các đường dẫn quang tách biệt hoặc lỗi trên các phân đoạn liên kết quang giữa các vùng khuếch đại quang. Hình 4.8 chỉ ra một trường hợp cụ thể của các báo hiệu này trong một mạng quang. Giả thiết ở đây có một liên kết đứt giữa thiết bị kết cuối quang OLT A và thiết bị kết cuối quang OLT B, khối khuếch đại quang B phát hiện ra lỗi đứt liên kết, nó lập tức chèn tín hiệu OMS-FDI hướng xuống chỉ ra rằng tất cả các kênh trong nhóm ghép kênh lỗi, và gửi tín hiệu OTS-BDI hướng lên tới OLT A. Tín hiệu OMS-FDI được truyền như một phần của tiêu đề liên kết với lớp OMS và OTS - BDI được truyền trong lớp OTS.



Hình 4.8: Phân cấp tín hiệu chỉ thị lỗi trong mạng quang

Tín hiệu OMS-FDI chỉ được truyền theo hướng xuống do các thông tin lỗi cần được truyền lan tới các phần tử mạng có lớp OMS cuối cùng, trong trường hợp này là

OADM D. Bộ khuếch đại C đường xuống nhận OMS-FDI và chuyển tới OADM D là nút kế tiếp trên đường xuống nhận OMS-FDI và xác định lỗi của các đường dẫn quang nhằm loại bỏ các đường dẫn quang lỗi.

Đối với một đường dẫn quang chuyển qua, OADM tạo ra các tín hiệu OCh-TS-FDI và gửi theo đường xuống. Các tín hiệu OCh-TS-FDI được truyền trong tiêu đề Och-TS. Tại điểm cuối của mạng con quang OLT E, các bước sóng được tách và kết cuối tại các bộ tách sóng và tái tạo tín hiệu quang (transponders/regenerators), vì vậy lớp Och-TS được kết cuối tại đây. OLT E nhận các tín hiệu OCh-TS-FDI và tạo ra các chỉ thị cảnh báo cho tường đường dẫn quang lỗi, gửi trên đường xuống tới đích của các đường dẫn quang trong tiêu đề OCh-P. Nút cuối cùng sẽ là nơi đưa ra các cảnh báo tới hệ thống quản lý mạng.

Một lý do quan trọng khác để sử dụng các tín hiệu chỉ thị lỗi là để sử dụng chuyển mạch bảo vệ. Ví dụ, một nút gần nhất nơi xảy ra sự kiện lỗi sẽ phát hiện lỗi và thực hiện việc chuyển mạch bảo vệ tới các đường dẫn khác. Tại cùng thời điểm đó, các nút phía trên và phía dưới liên kết lỗi cũng sẽ thực hiện các phương pháp tái định tuyến lưu lượng nhằm tránh đi qua liên kết lỗi. Một nút nhận được tín hiệu FDI sẽ quyết định có khởi tạo hoặc không khởi tạo chuyển mạch bảo vệ. Ví dụ, một phương pháp chuyển mạch bảo vệ yêu cầu các nút gần nhất liên kết lỗi ngay lập tức tái định tuyến lưu lượng thì các nút khác nhận tín hiệu FDI sẽ không thực hiện chuyển mạch bảo vệ. Mặt khác, nếu chuyển mạch bảo vệ được thực hiện bởi các nút kết cuối đường dẫn quang thì một nút nhận được FDI sẽ khởi tạo chuyển mạch bảo vệ nếu nút đó là nút kết cuối đường dẫn quang.

4.3.4 Mạng truyền thông dữ liệu và báo hiệu

Hệ thống quản lý phần tử mạng truyền thông với các phần tử mạng khác thông qua mạng truyền thông dữ liệu DCN. DCN thường sử dụng trên một mạng tiêu chuẩn như mạng TCP/IP hoặc OSI. Nếu DCN thỏa mãn điều kiện đảm bảo kết nối ngay cả khi có lỗi đơn xảy ra trong mạng thì DCN có thể truyền tải theo một số phương thức sau:

- Qua các mạng ngoài băng lớp quang. Các nhà khai thác có thể tạo ra mạng TCP/IP riêng để phục vụ mục đích quản lý mạng này. Nếu một mạng như vậy không được thiết lập thì có thể thay thế bằng các đường dây riêng (leased line). Phương thức này cho phép các phần tử mạng trong một trung tâm văn phòng lớn có sẵn các kiểu kết nối như vậy mà không qua các phần tử mạng như các bộ khuếch đại quang.
- Qua kênh giám sát quang OSC trên các bước sóng riêng. Phương thức này có sẵn trong các thiết bị WDM, tại nơi xử lý các phân đoạn quang và các lớp phân đoạn ghép kênh có các kênh giám sát quang. Các bộ khuếch đại quang được quản lý theo tiếp cận này. Trong khi đó các thiết bị thuộc lớp quang như thiết bị kết nối chéo quang sẽ không được quản lý .

- Qua các kênh quan trong băng dành riêng. Phương thức này được sử dụng chó các thiết bị thuộc lớp quang là không xử lý tại các lớp phân đoạn truyền dẫn và ghép kênh quang như các kết nối chéo quang. Thông qua các báo hiệu số trong tiêu đề khung quang, tiếp cận này chỉ tồn tại khi mạng quang có các vùng điện ví dụ như các bộ tái tạo tín hiệu quang và tách sóng quang.

Bảng 4.1 tổng kết các tùy chọn mạng truyền thông dữ liệu DCN khả dụng cho mỗi kiểu phần tử mạng quang. Ta giả thiết các OADM là một phần của hệ thống sợi quang chứa các thiết bị kết cuối quang OLT và các bộ khuếch đại quang.

Bảng 4.1: Các phương pháp ứng dụng DCN cho các phần tử mạng

Phần tử mạng	***Ngoài băng***	***OSC***	***Tiêu đề***
OLT với bộ tách sóng	Có	Có	Có
OADM	Có	Có	Có
Bộ khuếch đại	Không	Có	Không
OXC với tái tạo quang	Có	Không	Có
OXC toàn quang	Có	Không	Có

Trong rất nhiều trường hợp đối với DCN, các phần tử mạng quang cần có một kiểu báo hiệu nhanh. Điều này cho phép các phần tử mạng trao đổi các thông tin quan trọng với nhau theo thời gian thực. Ví dụ, các tín hiệu báo hiệu FDI và BDI cần phải truyền lan nhanh tới các nút dọc đường dẫn quang, hay các tín hiệu báo hiệu sử dụng cho chuyển mạch bảo vệ. Thông thường, mạng báo hiệu được thiết lập trong DCN có thể sử dụng các kết nối cố định ngoài băng, kênh giám sát quang hoặc qua một trong các kỹ thuật xử lý tiêu đề.

4.4 QUẢN LÍ MẠNG GMPLS

4.4.1 Giới thiệu chung về hệ thống quản lý mạng GMPLS

Công nghệ chuyển mạch nhãn đa giao thức tổng quát GMPLS chia sẻ một loạt chức năng quản lý trong mặt bằng truyền tải sang mặt bằng điều khiển. Ví dụ, việc thu thập thông tin và hiệu chỉnh thông tin về trạng thái và dung lượng liên kết được xử lý tự động bởi các giao thức định tuyến trong GMPLS. Tương tự, các giao thức báo hiệu trong GMPLS tạo ra các nhãn để cung cấp các đường dẫn chuyển mạch nhãn LSP và quản lý các LSP đó. Từ góc độ của người điều hành quản lý hệ thống, có thể có một số điểm khác nhau rất nhỏ giữa các công cụ được sử dụng cho bài toán quản lý mạng truyền thống với GMPLS. Nhưng hiệu quả hoặc phương thức điều hành trong lớp

truyền tải là khác biệt nhau. Mặt bằng điều khiển GMPLS tạo sự chắc chắn cho người điều hành về thông tin cập nhật cũng như các dịch vụ được quản lý bởi mặt bằng quản lý . Vì vậy, mặt bằng quản lý là một phần chính yếu và quan trọng trong các mạng GMPLS.

Một mạng truyền tải điển hình được cấu trúc từ các thiết bị của một số nhà cung cấp thiết bị khác nhau. Tùy thuộc vào các mục tiêu dài hạn và khả năng liên điều hành của các thiết bị mà người quản lý mạng xây dựng các vùng thiết bị có cùng nhà cung cấp thiết bị và đưa ra các cơ chế quản lý riêng. Các thiết bị của các nhà cung cấp thiết bị khác nhau có các đặc tính quản lý khác nhau thậm chí khi cùng thực hiện chức năng mạng tương tự nhau. Vì vậy, các giao diện chuẩn hoán và các giao thức chuẩn hóa là các điều kiện quan trọng nhất để quản lý các thiết bị truyền tải. Điều đó có nghĩa người điều hành cần sử dụng nhiều ứng dụng khác nhau hoặc ghi nhớ một số loại cú pháp câu lệnh khác nhau để điều hành mạng. Trong bối cảnh đó các đặc tính quản lý thường được chia sẻ vào các vùng quản lý , người quản lý có thể điều khiển theo từng vùng. Mặc dù các tương tác giữa các người quản lý phải được sử dụng để mở rộng vùng, các tương tác này được quản lý một cách trừu tượng tại lớp cao và không yêu cầu hiểu rõ các kỹ thuật cấu hình trong từng vùng.

Một thực tế khác ảnh hưởng tới vấn đề phân tán các thiết bị của người quản lý trong mạng chính là sự hội tụ mạng. Các mạng nhỏ thường có tài nguyên được cung cấp bởi hai nhà cung cấp thiết bị và dẫn tới các phân nhánh mạng. Tuy nhiên, chiến lược này làm tăng kích thước của mạng do số lượng kết nối các mạng nhỏ tăng lên để cung cấp các thỏa thuận dịch vụ giữa các nhà cung cấp. Thêm vào đó, tiếp cận này tạo ra các đảo hoặc các vùng quản lý thiết bị riêng từ một nhà cung cấp dịch vụ.

4.4.2 Các module MIB của GMPLS

Giao thức quản lý mạng đơn giản GMPLS là giao thức quản lý được IETF lựa chọn, nhưng điều đó không có nghĩa là GMPLS buộc phải theo hoặc không theo do GMPLS có rất nhiều các kiểu giao diện người quản lý có thể được sử dụng. Mặt khác, cơ sở thông tin quản lý MIB là cơ sở dữ liệu phân tán tổng thể cho quản lý và điều khiển các thiết bị có khả năng hoạt động với SNMP. Thêm vào đó, cơ sở thông tin quản lý MIB của GMPLS được phát triển trên kỹ thuật lưu lượng trong MPLS và mở rộng cho GMPLS.

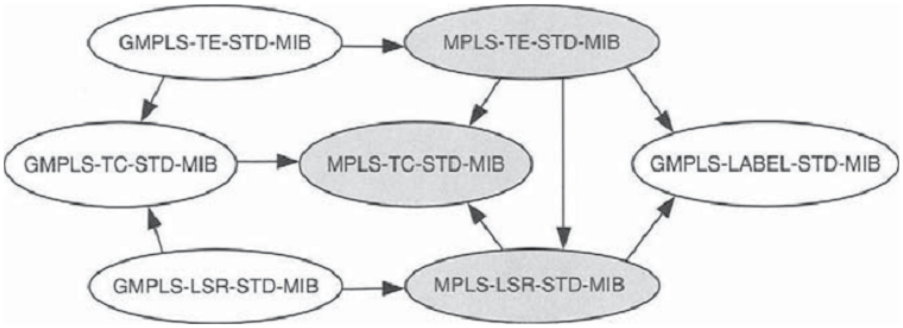
A. Quản lý cơ sở thông tin quản lý MPLS-TE

Ba module MIB thuộc vấn đề quản lý thiết bị trong mạng MPLS-TE gồm: Module cơ sở thông tin quản lý chuyển đổi chính tắc, module cơ sở thông tin quản lý bộ định tuyến chuyển mạch nhãn và module cơ sở thông tin quản lý kỹ thuật lưu lượng MPLS.

- Module cơ sở thông tin quản lý chuyển đổi chính tắc (MPLS TC MIB) chứa các định nghĩa được phân loại để sử dụng cho các module cơ sở thông tin

quản lý khác. Theo nghĩa hẹp, đó là một file tiêu đề định nghĩa các kiểu và kiến trúc cơ sở dữ liệu sử dụng trong file dữ liệu khác. Nó gồm các định nghĩa như tốc độ bít, nguyên tắc chuyển đổi kiểu khi thể hiện các giá trị nhận dạng đường hầm, giá trị nhận dạng đường hầm mở rộng, nhận dạng đường chuyển mạch nhãn và các nhãn MPLS.

- Module cơ sở thông tin quản lý MPLS được sử dụng để mô hình hóa và điều khiển các bộ định tuyến chuyển mạch nhãn MPLS. MIB này chứa các chức năng lõi của một bộ định tuyến chuyển mạch nhãn LSR (chuyển tiếp các gói có nhãn, giao thức phân phối nhãn, giao thức dành trước tài nguyên hỗ trợ kỹ thuật lưu lượng). Trong thực tế, cơ sở thông tin quản lý MIB có thể được sử dụng để cấu hình nhân công khi không có giao thức báo hiệu. Có 4 khối cơ sở trong cơ sở thông tin quản lý MIB. Ở đó có một bảng giao diện cho MPLS thể hiện thông tin gửi gói và nhận gói. Một bảng phân đoạn đầu vào tương ứng với các nhãn nhận được trên các giao diện hoặc hướng lên của các đường LSP. Một bảng phân đoạn đầu ra mô hình hóa các đoạn liên kết đường xuống của LSP, nhận dạng qua một chồng nhãn đầu ra và chỉ thị giao diện mà gói tin sẽ chuyển qua. Bảng cuối cùng là bảng kết nối chéo chỉ ra môi quan hệ giữa các phân đoạn đầu vào và phân đoạn đầu ra.
- Module cơ sở thông tin quản lý kỹ thuật lưu lượng MPLS-TE được sử dụng để mô hình và điều khiển các đường chuyển mạch nhãn LSP. Mục tiêu chính của module này cho phép người quản lý cấu hình và kích hoạt các đường dẫn chuyển mạch nhãn LSP tại các đầu vào LSR, đồng thời giám sát tất cả các LSP đi qua bộ định tuyến chuyển mạch nhãn LSR. Cơ sở thông tin quản lý MPLS-TE chứa các bảng sử dụng để cấu hình các đường hầm LSP đồng thời cho nhiệm vụ chia tải hoặc tuần tự cho chức năng khôi phục. Vì vậy, một đường hầm có một điểm gốc trong mplsTunelTable và liên quan tới các LSP khác. Mỗi một LSP trong bảng mplsTunelTable được thể hiện như một trường hợp của đường hầm.

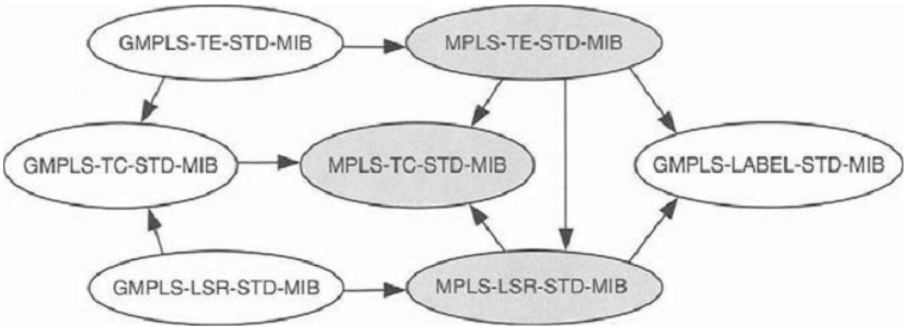


Hình 4.9: Mối quan hệ giữa các bảng dữ liệu trong MPLS-TE MIB

Các bảng khác cho phép cấu hình và kiểm tra tài nguyên sử dụng cho LSP, tính toán, yêu cầu và xác định các đường đi của một LSP. Sự phụ thuộc giữa các module trong MPLS-TE được thể hiện trên hình 4.9.

B. Quản lý cơ sở thông tin quản lý GMPLS

Quản lý cơ sở thông tin quản lý GMPLS được xây dựng trên cơ sở quản lý MPLS-TE nhằm tái sử dụng lại một loạt các đặc tính của MPLS-TE. Hình 4.10 chỉ ra một số module được tái sử dụng (màu xám) và các module mới (màu trắng). Như trên hình vẽ thể hiện, 4 module mới được bổ sung gồm: GMPLS-TC-STD-MIB, GMPLS-LSR-STD-MIB, GMPLS-TE-STD-MIB và GMPLS-LABEL-STD-MIB.



Hình 4.10: Mối quan hệ giữa các bảng dữ liệu trong MPLS-TE MIB

Trong đó, GMPLS-TC-STD-MIB được bổ sung một số chuyển đổi chuẩn tắc cho GMPLS; GMPLS-LSR-STD-MIB và GMPLS-TE-STD-MIB được sử dụng để mở rộng cho MPLS-TE, cung cấp thêm một loạt các đối tượng quản lý ; GMPLS-LABEL-STD-MIB là module mới nhằm xử lý các nhãn có độ dài vượt quá 20 bit được sử dụng trong MPLS. Nó chứa một bảng nhãn với các chỉ mục đơn giản nhưng có khuôn dạng phức tạp vì được tham chiếu từ các module khác.

C. Quản lý bộ định tuyến chuyển mạch nhãn GMPLS

GMPLS LSR được quản lý qua các bảng trong MPLS-LSR-MIB với một số chức năng mở rộng. Bảng giao diện MPLS (mplsInterfaceTable) được mở rộng thành bảng gmplsInterfaceTable. Một khoản mục trong bảng cũ chỉ ra giao diện sử dụng RSVP-TE cho MPLS cũng có ý nghĩa tương tự trong bảng mới. Trong trường hợp này, một đối tượng ttrong bảng gmplsInterfaceTable định nghĩa giao thức báo hiệu GMPLS sử dụng và một đối tượng khác định nghĩa chu kỳ bản tin Hello được sử dụng cho giao diện đó.

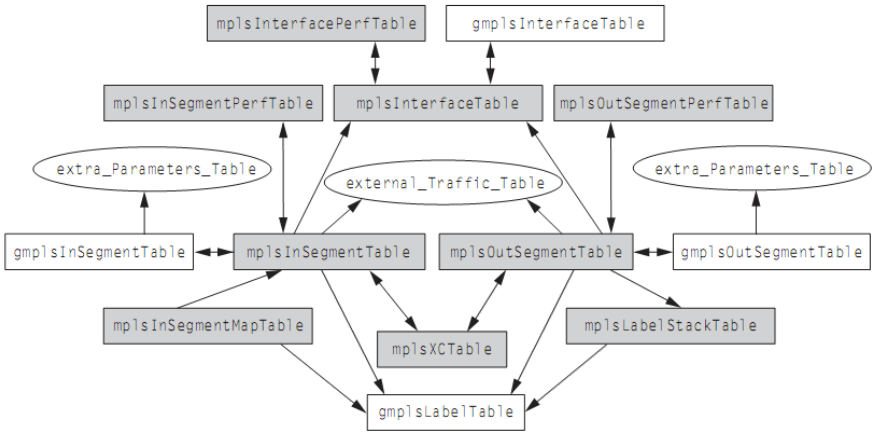
Hiệu năng của chuyển mạch nhãn trên giao diện được ghi lại trong bảng mplsInterfacePerfTable và giữ nguyên đối với GMPLS. Trong thực tế, hai bộ đếm được sử dụng để đếm tiến trình xử lý gói và đếm tuần tự số lần xử lý gói khi GMPLS hoạt động trong môi trường gói.

Các phân đoạn đầu vào trong MPLS được lưu trong bảng mplsInSegmentTable. Trong GMPLS bảng này có thê gây nhầm lẫn các khoản mục khi các LSP song hướng được thiết lập. Vì vậy, nó gồm các khoản mục tham chiếu tới các hướng của luồng dữ liệu không mang thông tin báo hiệu thiết lập LSP. Hai hướng

LSP gồm hai bảng: Bảng phân đoạn đầu vào In-segment trên giao diện đường lên (cho hướng đi) và bảng phân đoạn đầu ra trên giao diện đường xuống (cho hướng về). Bảng in-segment được mở rộng cho GMPLS có tên gọi gmplsInSegmentTable sẽ chỉ ra khi nào một đoạn được sử dụng cho hướng đi hoặc hướng về của đường dẫn LSP song hướng. Bảng này còn chứa một con trỏ tới bảng gmplsLableTable để xử lý mã hóa các nhãn phức hợp.

Bảng ánh xạ phân đoạn đầu vào mplsInSegmentMapTable cho phép người quản lý điều hành tạo ra các giám sát ngược {giao diện, nhãn} để tìm kiếm phân đoạn đầu vào thích hợp trong bảng mplsInSegmentTable. Chức năng này được tái sử dụng trong GMPLS nhưng sẽ phức tạp hơn một chút do nhãn có thể được tìm thấy trong một hướng của gmplsLabelTable. Các mở rộng tương tự được thực hiện với mplsOutSegmentTable và được bổ sung thêm một đối tượng kiểm soát mức độ giảm của trường thời gian sống của gói tin TTL (Time to live).

Bảng chồng nhãn MPLS (mplsLabelStackTable) được dự phòng cho GMPLS, nó cũng chỉ được áp dụng trong các môi trường mạng gói. Bảng này liệt kê chồng nhãn bổ sung được áp dụng cho các gói ra dưới nhãn ở bậc cao nhất. Bảng chồng nhãn MPLS được tái sử dụng cho GMPLS chứa danh sách các nhãn bổ sung cho môi trường GMPLS. Các nhãn này được lấy từ bảng nhãn GMPLS (gmplsLabelTable). Mối quan hệ giữa các bảng cơ sở thông tin quản lý để quản lý bộ định tuyến GMPLS được thể hiện trên hình 4.11.



Hình 4.11: Mối quan hệ giữa các bảng quản lý bộ định tuyến GMPLS

Cả hai bảng phân đoạn đầu vào và phân đoạn đầu ra đều chứa các con trỏ để mở rộng các bảng có chứa các tham số mô tả lưu lượng của LSP. Con trỏ này có thể chỉ thị một khoản mục trong bảng tài nguyên đường hầm MPLS trong cơ sở thông tin quản lý MPLS-TE, hoặc trỏ tới một khoản mục trong một cơ sở thông tin quản lý có nhiệm vụ quản lý LSP (bảng kết nối chéo MPLS). Chức năng này được tái sử dụng trong GMPLS và có xu hướng quản lý chặt chẽ hơn các phân đoạn đầu vào và phân đoạn đầu ra để cung cấp các đường LSP qua thiết bị.

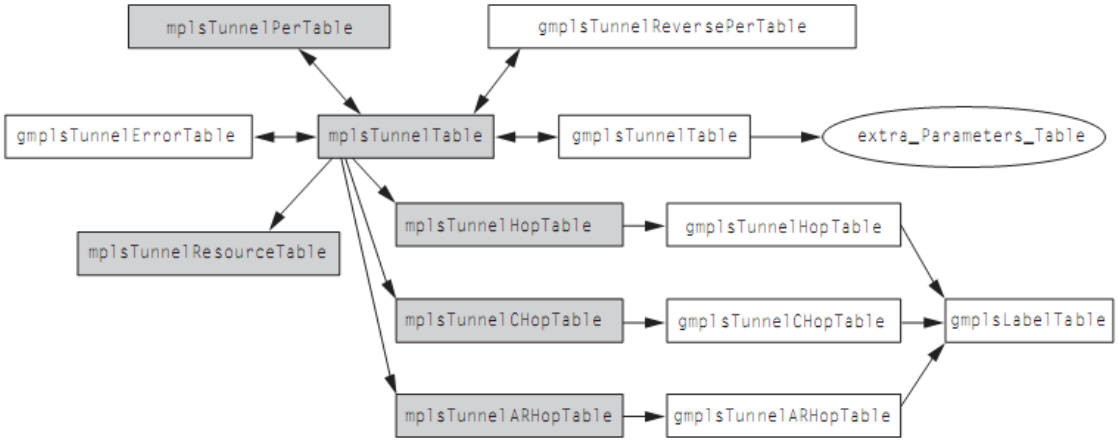
D. Quản lý đường dẫn chuyển mạch nhãn GMPLS-TE

Vấn đề quản lý các đường dẫn chuyển mạch nhãn MSP-TE yêu cầu số lượng bảng cơ sở dữ liệu ít hơn so với việc quản lý bộ định tuyến chuyển mạch nhãn GMPLS. Nguyên tắc chung của bài toán quản lý các LSP là được thực hiện trên bảng đường hầm MPLS (mplsTunnelTable), trong đó có chứa các tham số để khởi tạo, kết thúc hoặc chuyển tiếp các đường hầm. Các khoản mục trong bảng đường hầm không đánh số theo nhóm 5 cặp (five-tuple) như trong định nghĩa LSP (gồm {nguồn, đích, chỉ số nhận dạng đường hầm, chỉ số nhận dạng đường hầm mở rộng, và chỉ số nhận dạng LSP}) mà theo một tập tham số gồm {chỉ số đường hầm, sự kiện đường hầm, chỉ số nhận dạng LSR đầu vào, chỉ số nhận dạng LSR đầu ra}. Chỉ số đường hầm được ánh xạ tới nhận dạng địa chỉ đường hầm đã được gán, sự kiện đường hầm thể hiện sự phân biệt các LSP ghép thành đường hầm và chỉ ra các nhận dạng LSP được gán. Module cơ sở thông tin quản lý giả thiết rằng nguồn và đích của một LSP sẽ được mô tả bởi các nhận dạng LSR và nhận dạng đường hầm mở rộng sẽ được gán vào chỉ số nhận dạng LSR đầu vào nhằm cho phép hoạt động mở rộng môi trường trong GMPLS.

Mục đích của module cơ sở thông tin quản lý GMPLS-TE là để cho phép các LSP có thể cấu hình và quản lý tại các đầu vào, cũng như cho phép các LSP được giám sát tại bất kỳ một điểm nào trong mạng. Để cấu hình một LSP ta cần có các tham số gán phù hợp với các yêu cầu ràng buộc và tùy chọn của lưu lượng trong đó. Một tập đối tượng chính đã được thể hiện trong mplsTunelTable và mở rộng cho GMPLS nhằm hỗ trợ một số đặc tính sau:

- Thể hiện đường hầm trong LSR như một giao diện không đánh số;
- Lựa chọn phương pháp ghi nhãn;
- Kiểu mã hóa cho LSP;
- Kiểu chuyển mạch cho LSP;
- Kiểu bảo vệ liên kết cho LSP;
- Nhận dạng tải trong LSP;
- Lựa chọn LSP dự phòng;
- Lựa chọn kiểu LSP (đơn hướng, song hướng);
- Điều kiển cảnh báo và các đặc tính khác của LSP;
- Phương pháp tính toán đường dẫn cho các LSR đầu vào.

Một số đặc tính chung được sử dụng trong cả MPLS và GMPLS sẽ được đặt giá trị cho kiểu mã hóa bằng ZERO trong bảng gmplsTunnelTable để chỉ thị đó là LSP của MPLS. Tất cả các đối tượng được liệt kê trước khi LSP được xác định tại điểm chuyển tiếp hoặc đầu ra LSR. Từ đó, có thể xác định các thiết bị nhận thông báo và cờ trạng thái của người quản trị hệ thống.



Hình 4.12: Mối quan hệ giữa các bảng MIB trong quản lý GMPLS-TE LSP

Để thực hiện ghi lại hiệu năng của các LSP trong GMPLS, một module được bổ sung trong bảng cơ sở thông tin quản lý GMPLS-TE gọi là gmplsTunnelReversePerfTable. Điều này xuất phát từ các LSP trong GMPLS được thiết lập song hướng trong các môi trường không chỉ là môi trường gói.

Các yêu cầu và lượng tài nguyên sử dụng trong GMPLS được lưu trong bảng mplsTunnelResourceTable.

Vấn đề quản lý LSP-TE liên quan tới đặc tính, tính toán và ghi lại các đường dẫn chuyển mạch nhãn LSP được cung cấp trong 3 bảng của module cơ sở thông tin quản lý MPLS-TE gồm: mplsTunnelHopTable, mplsTunnelCHopTable, mplsTunnelARHopTable. Các bảng này được giữ nguyên trong GMPLS.

Mở rộng cuối cùng trong module cơ sở thông tin quản lý GMPLS-TE là bảng chỉ thị lỗi đường hầm GMPLS (gmplsTunnelErrorTable). Bảng này ghi lại các lỗi xảy ra khi thiết lập LSP hoặc khi LSP hoạt động lỗi. Hình 4.12 chỉ ra các bảng MIB sử dụng để quản lý các đường dẫn chuyển mạch nhãn trong GMPLS-TE cũng như mối quan hệ giữa chúng.

4.4 TỔNG KẾT CHƯƠNG 4

Trong chương này đã lần lượt trình bày về các đặc điểm cơ sở của các bài toán quản lý trong mạng IP, MPLS, mạng quang và GMPLS. Mỗi kiểu kiến trúc và công nghệ mạng yêu cầu các phương pháp quản lý khác nhau, nhưng tiếp cận phổ biến nhất được thực hiện trên nguyên tắc tiêu chuẩn hóa và tái sử dụng các hệ thống cơ sở dữ liệu cũng như giao thức quản lý mạng đã tồn tại. Những yêu cầu sửa đổi và mở rộng của các module cơ sở thông tin quản lý MIB được thực hiện trên các yêu cầu thực tế của các môi trường mạng. Đối với các mạng diện rộng, phương pháp phân vùng chức năng quản lý nhằm thích ứng với các kiểu cấu hình thiết bị và tính đặc thù của môi

trường quản lý đã và đang được phát triển và hoàn thiện với các cơ chế quản lý liên vùng thích hợp. Tiếp cận này đã và sẽ đưa đến một loạt thách thức trong bài toán quản lý mạng hiện nay và trong tương lai.

TÀI LIỆU THAM KHẢO

[1] NGN FC books Proceeding, Part II, 2005.

[2] Gilbert Held: *Managing TCP/IP Networks*. John Wiley & Sons, 2000.

[3] Douglas Mauro, Kevin Schmidt: *Essential SNMP*, 2nd Edition, O'Reilly, 2005.

[4] Stephen, B.Moris: *Network management*, MIBs and MPLS, Prentice Hall 2003.

[5] Sebastian Abeck, et all. : *Network Management: Know It All*, Morgan Kaufman, 2009.

[6] Steven T.Karris: *NETWORKS Design and Management*, 2nd ed., Orchard Publications, ISBN 978-1-934404-16-4, 2009.