TRƯỜNG ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

Luận Văn Tốt nghiệp cử nhân khoa học

NGUYỄN MINH SÁNG

Đề tài:

QUẢN TRỊ MẠNG VÀ NGHI THỨC QUẢN TRỊ MẠNG

Hà Nội 1997
TRƯỜNG ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

LUẬN VĂN TỐT NGHIỆP CỬ NHÂN KHOA HỌC

NGUYỄN MINH SÁNG

Đề tài:

QUẢN TRỊ MẠNG VÀ NGHI THỨC QUẢN TRỊ MẠNG

Giáo viên hướng dẫn:

Nguyễn Nam Hải

Đào Kiến Quốc

Giáo viên phản biện:

Phạm Giang Lâm

Hà Nội 1997

MỤC LỤC

LỜI NÓI ĐẦU

Những năm qua chúng ta đã và đang sống trong thời kỳ phát triển rất nhanh chống và sôi động của công nghệ thông tin. Chiếc máy vi tính đa năng, tiện lợi và hiệu quả mà chúng ta đang dùng, giờ đây đã trở nên chật hẹp và bất tiện so với các máy vi tính nối mạng.

Từ khi xuất hiện mạng máy tính, tính hiệu quả tiện lợi của mạng đã làm thay đổi phương thức khai thác máy tính cổ điển. Mạng và công nghệ về mạng mặc dù ra đời cách đây không lâu nhưng nó đã được triển khai ứng dụng ở hầu hết khắp mọi nơi trên hành tinh chúng ta.

Chính vì vậy chẳng bao lâu nữa những kiến thức về tin học viễn thông nói chung và về mạng nói riêng sẽ trở nên kiến thức phổ thông không thể thiếu được cho những người khai thác máy vi tính, ở nước ta việc lắp đặt và khai thác mạng máy tính trong vòng mấy năm trở lại đây, đến nay số các cơ quan, trường học, đơn vị có nhu cầu khai thác các thông tin trên mạng ngày càng gia tăng. Đồng thời cùng với việc khai thác các thông tin mạng, người kỹ sư cũng cần phải quản lý mạng nhằm khai thác mạng hiệu quả và an toàn.

Quản lý mạng là một công việc rất phức tạp, có liên quan đến hàng loạt vấn đề như:

- Quản lý lỗi.
- Quản lý cấu hình.
- Quản lý an ninh mạng
- Quản lý hiệu quả.
- Quản lý tài khoản.

Để làm được điều này một cách có hiệu quả phải theo dõi một cách toàn diện tình trạng hoạt động của mạng bằng cách sử dụng các nghi thức quản trị mạng.

Trong khuôn khổ một bản luận văn tốt nghiệp, không thể đề cập được toàn bộ các vấn đề kể trên. ở đây chúng tôi tự giới hạn trong nội dung như sau:

Chương 1. Tổng quan về quản lý mạng. Nội dung chính của chương này là vẽ ra được một bức tranh chung về quản lý mạng

Chương 2 sẽ đề cập đến các nghi thức quản trị mạng cơ bản. Đây là vấn đề quan trọng nhất vì nó là cơ sở cho mọi hoạt động quản trị mạng.

Chương 3 sẽ đề cập đến nghi thức quản trị mạng SNMP.

Các nghi thức quản trị mạng chuẩn hoá chủ yếu là tạo những giao tiếp chuẩn giữa các phần mềm quản trị với các nguồn tin liên quan đến hoạt động của mạng từ các nút mạng chuyển tới. Thông tin từ các thiết bị thực ra chỉ cung cấp được các thông tin liên quan đến quản trị cấu hình, quản trị lỗi, quản trị hiệu quả, một chút về quản trị an ninh và tài khoản. Vì vậy trong năm khía cạnh quản trị mạng nêu trên, các nghi thức quản trị mạng đáp ứng trực tiếp hơn cho hai khía cạnh là quản trị lỗi và quản trị cấu hình. Vì vậy để làm rõ hơn ý nghĩa của các nghi thức quản trị mạng, các chương sau sẽ trình bày chi tiết hơn quản lý cấu hình.

CHƯƠNG I.
TỔNG QUAN QUẢN LÝ MẠNG

1. 1. Định nghĩa mạng

Một mạng dữ liệu (DataNetwork viết tắt là DN) là một tập hợp các thiết bị và các mạch, nhờ đó có thể cung cấp các phương tiện để chuyển giao thông tin và dữ liệu giữa các máy tính, cho phép người dùng ở các khu vực khác nhau dùng chung các nguồn tài nguyên trên một máy khác một nơi nào đó.

Ở các nước phát triển, hàng ngày hầu hết mọi người đều có công việc liên quan đến DN mà không nhận ra chúng. Một ví dụ điển hình của DN là máy rút tiền tự động (ATM). Một ATM quản lý một nhà băng và chuyển giao các thẻ tín dụng như sau: Ta có thể rút tiền từ tài khoản của mình hay yêu cầu hoặc tới tài khoản của ta với các thẻ tín dụng. Tuy nhiên, ATM thường điều hành tại các trạm từ xa (remote sites), có nghĩa là tại các trạm rút tiền, các liên lạc cần thiết sẽ được thiết lập để lấy các thông tin về tài khoản của ta. Dù sao các trạm cũng không có đầy đủ các khả năng như máy chủ vì để làm như vậy thì lãng phí và đắt. Thay vào đó, ATM sử dụng một DN để thiết lập một kết nối tuyền tin giữa nó và máy chủ, cho phép ATM chia sẻ các tài nguyên tài khoản với máy chủ và lấy các thông tin cần thiết. ATM dùng liên kết này để gửi các thông tin chuyển giao của ta. Ví dụ như số tài khoản, số tiền định rút hay số tiền định gửi đến cho máy chủ, mà ở đó sẽ gửi lại các kết quả kiểm tra về tài khoản của ta.

Một ví dụ khác, một nhà khoa học tại một phòng nghiên cứu ở Chicago muốn chạy một chương trình, máy tính cục bộ phòng máy này sẽ mất 8 giờ để hoàn thành chương trình. Tuy nhiên máy này cũng được kết nối với một DN của một máy chủ ở Miami mà nó chỉ cần 3 giờ để chạy chương trình. Trong trường hợp này, sử dụng DN để lấy tin tức từ máy chủ nó sẽ tiết kiệm được 5 giờ tính toán và cho nhà khoa học kết quả tính toán nhanh hơn.

Như chúng ta thấy, liên kết thông tin qua máy tính với DN cho phép các tổ chức có thể chia sẽ các thông tin nguồn giữa các máy với nhau và nhờ đó giúp cho các tổ chức trở nên có năng suất và đạt hiệu quả hơn.

1. 2. Vai trò của một kỹ sư mạng:

Do tầm quan trọng của DN nên một số chuyên gia hệ thống gọi là các kỹ sư mạng (Network Engineer viết tắt là NE) được giao trách nhiệm cài đặt, bảo trì thông tin, giải quyết các sai hỏng của mạng.

Công việc của họ có thể là đơn giản như trả lời các câu hỏi hoặc các yêu cầu của người sử dụng hoặc phức tạp hơn như thay thế thiết bị hỏng hóc, hoặc tiến hành các thủ tục phục hồi sai hỏng do một sự kiện hỏng hóc nào đó.

Thêm vào đó, khi mạng được mở rộng, các vấn đề cũng tăng lên, Để hoàn tất các tác vụ NE phải hiểu rất rõ và nắm bắt một số thông tin về mạng. Khối lượng thông tin có thể lớn và phức tạp đến nỗi họ không thể quản lý được, đặc biệt là khi mạng được mở rộng hay thường xuyên thay đổi. Để giúp đỡ NE làm các công việc của họ, các nhà nghiên cứu đã đưa ra các quan niệm về quản lý mạng và xây dựng các công cụ quản lý mạng.

1. 3. Cài đặt một mạng

Cài đặt một DN, không có nghĩa là bảo đảm rằng tất cả mọi người trong tổ chức có thể thâm nhập vào các thông tin nguồn. Điều trước tiên NE phải đáp ứng được yêu cầu trao đổi thông tin của tổ chức, để thành công thì người kỹ sư mạng phải thiết lập kế hoạch toàn diện. Họ phải lập một DN để làm thỏa mãn yêu cầu của từng người sử dụng trên hệ thống máy tính, các nhà phân tích cũng cần đánh giá xem hệ thống có hoạt động tốt với các kế hoạch thiết kế DN hay không.

Khi xây dựng một kế hoạch NE phải luôn luôn tham khảo cộng đồng người sử dụng để giúp họ tìm ra cách cài đặt tốt nhất. Việc thiết kế có thể kèm theo việc thêm vào một số bộ phận mới, trên một mạng đã có thể tạo ra một nhánh cho bộ phận mới khác. Tuy nhiên sẽ phải mất nhiều lần để kiểm tra các ứng dụng và nghi thức sử dụng một mạng.

Để có một mạng người kỹ sư phải thực hiện các tác vụ sau:

a. Thiết kế và xây dựng.

b. Bảo trì

c. Mở rộng.

d. Tối ưu hoá.

g. Xử lý sự cố

Trước tiên người kỹ sư sử dụng sơ đồ mạng phải quyết định cái gì là cần thiết để xây dựng mạng như thiết bị, phần mềm và phương thức kết nối.

Có hai kiểu kỹ thuật kết nối truyền tin giữa các điểm của DN là: mạng cục bộ (LAN) và mạng rộng (WAN). Một LAN kết nối các máy chủ với nhau với tốc độ từ khoảng 4 đến 1000 megabit/giây. Với mục tiêu là cung cấp các kết nối có liên quan trong khoảng cách ngắn.

Một WAN thường xử lý ở tốc độ khoảng từ 9,6 kilobit/giây đến 45 mêgabit/giây, và hơn nữa để thực hiện các việc truyền thông tin trong khoảng cách xa. Có nhiều công nghệ để kết nối các LAN một cách trong suốt với người sử dụng.

Sau khi xây dựng mạng, người kỹ sư sau đó phải tiến hành bảo trì mạng. Bất kể là người kỹ sư đã phải làm những gì trong việc xây dựng mạng, mạng vẫn cần được bảo trì. Ví dụ phần mềm đang chạy cần được đổi mới, một số bộ phận của mạng cần được nâng cấp hay một số thiết bị bị hỏng cần được thay thế.

Những thay đổi trong yêu cầu của người sử dụng cũng luôn luôn có ảnh hưởng tới toàn bộ sơ đồ tổng thể mạng. Do đó nẩy sinh ra vấn đề thứ ba cho người kỹ sư mạng là việc mở rộng mạng, bởi vì việc mở rộng một mạng đang tồn tại luôn tối ưu hơn việc thiết kế và xây dựng một mạng mới. Người kỹ sư cần phải cung cấp những giải pháp sửa chữa, thay đổi một cách đúng nhất.

Tác vụ thứ tư của người kỹ sư là phải tối ưu hoá DN, đây không phải là tác vụ đơn giản, nên chú ý một mạng thông thường có hàng trăm các thiết bị khác nhau, mỗi thiết bị có tính chất riêng của chúng và tất cả đều làm việc một cách hài hoà, thông qua một sơ đồ tỉ mỉ người kỹ sư mới có thể đảm bảo được chúng làm việc một cách tốt nhất với các chức năng của chúng trong DN, khi thay đổi hay sửa chữa người kỹ sư phải lập kế hoạch triển khai với các loại thiết bị mới, phải biết thông số nào cần thiết phải cài đặt, thông số nào không phù hợp với tình huống hiện tại, người kỹ sư có thể hoàn thành việc tối ưu hoá mạng của mình.

Qua các bước thực hiện trên, NE có thể giảm tối thiểu các lỗi trên mạng. Tuy nhiên không phải mạng nào cũng hoàn hảo, các lỗi có thể xẩy ta bất cứ lúc nào cho dù mạng được thiết kế tối ưu. Chính vì thế nên có tác vụ thứ năm: dàn xếp các tranh chấp bởi vì nó luôn tồn tại với những lý do không thể biết trước.

1. 4. Tổng quan về quản lý mạng:

Các tổ chức đã đầu tư rất nhiều thời gian và tiền của để xây dựng một hệ DN phức tạp mà nó rât cần được bảo trì tốt. Các công ty thường có một vài kỹ sư mạng để bảo trì máy, thật là tiện lợi khi các máy có thể tự kiểm tra bảo quản trong việc điều hành và xử lý thay cho các công việc buồn tẻ hàng ngày của các kỹ sư.

Quản lý mạng (NM: Network Management) là quá trình điều khiển các DN phức tạp, nhằm tối ưu hoá tính năng suất và hiệu quả của máy dựa trên các khả năng của chính hệ thống để thực thi việc quản lý mạng. Qúa trình này bao gồm:

Thu thập dữ kiện, hoặc là tự động hoặc là thông qua sự nỗ lực của các kỹ sư. Nó có thể bao gồm cả việc phân tích các dữ liệu và đưa ra các giải pháp và có thể còn giải quyết các tình huống mà không cần đến người kỹ sư.

Thêm vào đó nó có thể làm các bản báo cáo có ích cho các kỹ sư trong việc quản lý mạng. Để hoàn tất các công việc một hệ quản lý mạng cần có 5 chức năng sau.

- Quản lý lỗi.
- Quản lý cấu hình.
- Quản lý an toàn.
- Quản lý hiệu quả.
- Quản lý tài khoản.

Năm chức năng trên được định nghĩa bởi ISO trong hội nghị về mạng.

a. Quản lý lỗi: (FM:Fault Management)

FM là một quá trình định vị các lỗi , nó bao gồm cácvấn đề sau:

- Tìm ra các lỗi.
- Cô lập lỗi
- Sửa chữa nếu có thể.

Sử dụng kỹ thuật FM, các kỹ sư mạng có thể định vị và giải quyết các vấn đề nhanh hơn. Ví dụ, trong một quá trình cài đặt, một người sử dụng thâm nhập vào một hệ thống từ xa qua một đường đi với rất nhiều thiết bị mạng. Đột nhiên liên lạc bị cắt đứt, người sử dụng thông báo cho kỹ sư mạng. Với một công cụ quản lý lỗi kém hiệu quả muốn biết lỗi này có phải do người sử dụng gây ra không người quản trị phải thực hiện các test, ví dụ như đưa vào một lệnh sai hoặc cố ý vào một hệ mạng không cho phép. Nếu thấy người sử dụng không có lỗi thì sau đó cần phải kiểm tra các phương tiện nối giữa người sử dụng và hệ thống từ xa đó, bắt đầu từ thiết bị gần người sử dụng nhất. Giả sử ta không tìm ra lỗi trong thiết bị kết nối. Khi vào vùng dữ liệu trung tâm, ta thấy mọi đèn hiệu đều tắt và có thể xem thêm các ổ cắm, lúc đó phích cắm rời ra ta kết luận rằng có một ai đó đã ngẫu nhiên rút phích cắm ra, sau khi cắm lại ta sẽ thấy mạng làm việc bình thường. Ví dụ trên là một lỗi thuộc loại đơn giản. Nhiều lỗi không dễ dàng tìm như thế.

Với sự giúp đỡ của FM ta có thể tìm ra cách giải quyết các vấn đề nhanh hơn. Thực ra, ta có thể tìm và sửa các sai hỏng trước khi người sử dụng thông báo.

b. Quản lý về cấu hình (Configuration Management - CM)

Hình trạng các thiết bị trong một mạng có ảnh hưởng quan trọng đến hoạt động của mạng. CM là quá trình xác định và cài đặt lại cấu hình của các thiết bị đã bị có vấn đề.

Gỉa sử một version A của phần mềm chạy trên một cầu Ethernet có một vấn đề nào đó làm giảm hiệu năng của mạng. Để giải quyết các dị thường này nhà sản xuất đưa ra một bản nâng cấp lên version B mà nó sẽ phải đòi hỏi chúng ta phải cài đặt mới đối với từng cầu trong số hàng trăm cầu trong mạng. Theo đó ta phải lập một kế hoạch triển khai việc nâng cấp version B vào tất cả các cầu trên mạng đó. Trước tiên ta phải xác định loại phần mềm hiện tại được cài đặt trên các cầu đó. Để làm được điều đó nếu không có CM thì người kỹ sư cần phải kiểm tra từng cầu nối một bằng phương pháp vật lý nếu không có một công cụ quản trị cấu hình

Một bộ CM có thể đưa ra cho người kỹ sư tất cả các version hiện hành trên từng cầu nối. Do đó, nó sẽ làm cho người quản trị dễ dàng xác định được chỗ nào cần nâng cấp

c. Quản lý an ninh mạng (security management - SM)

Qủan lý an ninh là quá trình kiểm tra quyền truy nhập vào các thông tin trên mạng. Một vài thông tin được lưu trong các máy nối mạng có thể không cho phép tất cả những người sử dụng được xem. Những thông tin này được gọi là các thông tin nhạy cảm (sensitive information) ví dụ như thông tin về sản phẩm mới hoặc các khách hàng của công tyg tin đó.

Giả sử một tổ chức quyết định quản lý an ninh đối với việc truy nhập từ xa tới mạng thông qua đường điện thoại quay số trên một server phuc vụ các trạm cuối cho một nhóm các kỹ sư.

Mỗi lần các kỹ sư máy tính muốn làm việc trên mạng thì có thể đăng nhập vào hệ thống để làm việc.

Cổng dịch vụ cho phép truy nhập các thông tin từ nhiều máy tính ở trong mạng truy nhập tới trung tâm bảo mật để bảo vệ các thông tin cần thiết.

Để quản lý an ninh thì bước đâu tiên ta phải làm là dùng công cụ quản lý cấu hình để giới hạn các việc truy nhập vào máy từ các cổng dịch vụ. Tuy nhiên để biết ai đã truy nhập mạng thì người quản trị mạng phải định kỳ vào mạng để ghi lại những ai đang sử dụng nó.

Các hệ quản trị an ninh cung cấp cách theo dõi các điểm truy nhập mạng và ghi nhận ai đã sử dụng những tài nguyên nào trên mạng

d. Quản lý hiệu quả: (Performance management:PM)

PM liên quan đến việc đo hiệu quả của mạng về phần cứng phần mềm và phương tiện làm việc. Các hoạt động đó là các biện pháp kiểm tra ví dụ như kiểm tra năng lực thông qua (khối lượng công việc hoàn thành được trong một đơn vị thời gian), bao nhiêu % tài nguyên được sử dụng, tỷ lệ các lỗi xẩy ra hoặc thời gian trả lời.

Dùng các thông tin về PM, kỹ sư hệ thống có thể đảm bảo rằng mạng sẽ kiểm tra được mạng có thỏa mãn các yêu cầu của người dùng hay không và thoả mãn ở mức độ nào.

Xét một ví dụ, một người sử dụng phàn nàn về khả năng truyền tệp qua một mạng rất tồi. Nếu không có công cụ, đầu tiên nhân viên quản trị sẽ phải xem xét lỗi của mạng. Giả sử không tìm thấy lỗi, bước tiếp theo ta phải kiểm tra đánh giá hiệu quả làm việc của các đường kết nối giữa trạm làm việc của người sử dụng và thiết bị nối vào mạng. Trong quá trình điều tra, giả sử ta thấy thông lượng trung bình của đường kết nối là quá chật hẹp so với yêu cầu. Điều đó có thể dẫn ta đến giải pháp nâng cấp việc nối kết hiện thời hoặc cài đặt một kết nối mới với thông lượng lớn hơn.

Như vậy nếu ta có sẵn một công cụ quản lý chế độ làm việc thì ta có thể sớm phát hiện ra kết nối cần được nâng cấp thông qua các báo cáo định kỳ.

e. Quản lý tài khoản (accounting management - AM)

AM bao gồm các việc theo dõi việc sử dụng của mỗi thành viên trong mạng hay một nhóm thành viên để có thể đảm bảo đáp ứng tốt hơn yêu cầu của họ. Mặt khác AM cũng có quyền cấp phát hay thu lại việc truy nhập vào mạng.

1. 5. Định nghĩa một hệ quản lý mạng (network management system - NMS)

NMS là một bộ phần mềm được thiết kế để cải hiệu quả và năng suất việc quản lý mạng. Cho dù một kỹ sư mạng có thể thực hiện các công việc với các dịch vụ tương tự giống như hệ quản lý mạng thì vẫn có thể làm nó tốt hơn nếu có một phần mềm thực hiện các tác vụ đó. Do vậy nó có thể giải phóng các kỹ sư mạng ra khỏi các công việc phức tạp đã được định sẵn. Bởi vì một hệ NMS được dự kiến hoàn tất nhiều tác vụ đồng thời cùng một lúc và nó có đầy đủ khả năng tính toán.

a. Lợi ích của một hệ quản lý mạng:

NMS có thể giúp cho các kỹ sư mạng làm việc trong nhiều môi trường khác nhau. Gỉa sử ta có một kỹ sư mạng làm việc trong phòng thí nghiệm của một trường đại học, mạng có thể có 10 máy được nối kết thông qua LAN, một môi trường đủ nhỏ mà ở đó một kỹ sư mạng biết

được tất cả các khía cạnh của mạng một cách rõ ràng để có thể triển khai, bảo trì, điều khiển nó. Cũng trên hệ thống nay, một NMS còn có thể giúp đỡ cho các kỹ sư mạng nhiều vấn đề khác nhau. NMS sẽ thực hiện các công việc phân tích phức tạp, xem xét các xu hướng qua các mẫu truyền tin. Nó có thể kiểm tra các lỗi do người sử dụng gây mất an toàn thông tin, nó còn tìm ra các thông tin sai cấu hình trong hệ thống để cô lập khu vực có lỗi, từ đó đưa cách giải quyết cho các vấn đề đó. Với một NMS thực hiện các tác vụ trên, người kỹ sư mạng sẽ có thêm thời gian đẻ hoàn thiện hệ thống hỏi đáp với người sử dụng theo các nhu cầu của họ và giúp họ hoàn thành các dự án.

Bây giờ ta xét đến một mạng phức tạp hơn. Mạng có thể được mở rộng với các điểm nối ở Bắc mỹ, châu Âu, viễn đông và Úc, nó có thể chạy trên nhiều nghi thức mạng như IBM SNA (standard network architecture), XeroxXNS (xerox network service), appletalk, TCP/IP (transmission control protocol/internet protocol), và DECnet.

Các Host (một trạm có địa chỉ trên mạng) có thể lên tới nhiều ngàn bao gồm các trạm làm việc, các máy tính mini và các máy cá nhân với một vài thiết bị kết nối khác. Thật không thích hợp nếu trông chờ vào một người thậm chí một ê kip có khả năng bảo trì toàn bộ. Một môi trường như vậy đòi hỏi quản trị đồng thời cả LAN và WAN. Sự khác nhau giữa môi trường lớn như trên với môi trường một LAB của đại học ở chỗ phải quản lý cả các kết nối đường dài ví dụ như các modem tốc độ cao như DSU/CSU hay một ROUTER có thể hiểu được các nghi thức của cả LAN và WAN. Với nhiều thiết bị như vậy, kỹ sư hệ thống phải dựa trên các thông tin cung cấp từ hệ quản trị mạng để theo dõi một khối lượng lớn các thông tin sống còn đòi hỏi phải có quyết định cho "sức khoẻ" của mạng.

Tóm lại trong cả hai môi trường mạng nêu trên thì các khái niệm, chức năng của NMS là giống nhau, về mặt bản chất một môi trường lớn hơn sẽ luôn luôn đòi hỏi hệ thống phải thực hiện nhiều tác vụ và trợ giúp cho người kỹ mạng ở các mức độ phức tạp cao hơn. Tuy nhiên, với dữ liệu mạng ở bất kỳ cỡ nào thì NMS cũng có thể cho phép các kỹ sư làm việc trong mạng một cách tối ưu và hiệu quả hơn trong việc phục vụ các nhu cầu của người dùng.

b. Cấu trúc của một hệ quản lý mạng:

Để xây dựng một hệ NMS thì ta phải kết hợp chặt chẽ tất cả các chức năng cần thiết để cung cấp một hệ quản lý hoàn hảo, đó là nhiêm vụ phức tạp, người kỹ sư phần mềm phải hiểu mức độ làm việc và các yêu cầu của các kỹ sư mạng. Về mặt cơ bản họ phải bắt đầu thực hiện thiết kế một bản cấu trúc cho hệ thống, khi cấu trúc hệ thống được cài đặt kỹ sư phần mềm lúc đó sẽ phải xây dựng một loạt các công cụ hay ứng dụng để

trợ giúp người kỹ sư mạng hoàn tất các công việc quản lý. Ta thấy không có quy luật nhất định nào cho cấu trúc của hệ NMS, tuy nhiên khi quan tâm tới tất cả các chức năng mà hệ thống đòi hỏi thì ta có thể yêu cầu một vài điểm mà một NMS phải có là:

- Hệ thống phải cung cấp một giao diện đồ họa mà tại đó nó có thể đưa ra được hình ảnh của mạng theo từng cấp và nối kết logic giữa các hệ thống, nó cần phải giải thích rõ ràng các nối kết trong biểu đồ phân cấp chức năng và quan hệ của chúng như thế nào hiệu quả của mạng. Một giao diện đồ họa phải trùng với cấu trúc phân cấp chức năng. Một bản đồ mạng phải cung cấp hình ảnh chính xác hình trạng mạng (networrk topology).

- Hệ thống phải cung cấp một cơ sở dữ liệu, CSDL này có khả năng lưu giữ và cung cấp bất kỳ thông tin nào liên quan đến hoạt động và sử dụng mạng, đặc biệt để có thể quản lý cấu hình và quản lý tài khoản một cách có hiệu quả.

- Hệ thống phải cung cấp một phương tiện thu thập thông tin từ tất cả các thiết bị mạng. Trường hợp lý tưởng cho người dùng là thông qua một nghi thức quản lý mạng đơn giản.

- Hệ thống phải dễ dàng mở rộng và nâng cấp cũng như thay đổi theo yêu cầu. Hệ thống phải dễ dàng khi thêm vào các ứng dụng và các đặc điểm yêu cầu của người kỹ sư mạng.

- Hệ thống phải có khả năng theo dõi các đề phát sinh hoặc hậu quả từ bên ngoài. Khi kích cỡ và độ phức tạp của mạng tăng lên thì ứng dụng này trở nên vô giá.

c. Một số kiểu kiến trúc NMS

Có 3 phương pháp được đề cập đến việc làm thế nào để xây dựng một kiến trúc quản lý mạng đang phổ biến ở hiện nay.

- Xây dựng một hệ thống tập trung để điều khiển toàn mạng.

- Xây dựng một hệ thống mà có thể phân chia được chức năng quản lý mạng.

- Kết hợp cả hai phương pháp trên vào một hệ thống phân cấp chức năng.

Một kiến trúc tập trung sẽ sử dụng một CSDL chung trên một máy trung tâm nào đó, mọi thông tin liên quan đến hoạt động của mạng do các ứng dụng gửi về đây sẽ được sử dụng chung trong các ứng dụng quản lý mạng.

Một kiến trúc phân tán có thể sử dụng nhiều mạng ngang hàng (peer network) cùng thực hiện các chúc năng quản trị một cách riêng rẽ.

Thật khó đòi hỏi hơn nếu một số thiết bị nào đó chỉ thích hợp một số ứng dụng quản trị. Tuy nhiên rất có lợi nếu có một CSDL tập trung để lưu trữ các thông tin này.

Cấu trúc khả dụng thứ ba là kết hợp các phương pháp phân cấp và tập trung vào trong một hệ thống phân cấp chức năng. Vùng hệ thống trung tâm chính của cấu trúc sẽ còn tồn tại như là gốc của cấu trúc phân cấp, thu thập các thông tin từ các mạng cấp dưới và cho phép truy nhập từ các phần của mạng. Khi thiết lập các hệ thống đồng mức (peer system) từ cấu trúc phân cấp, hệ thống trung tâm này có thể giao quyền điều hành mạng cho chức năng đó giống như là các mức con trong hệ phân cấp.

Sự kết hợp tất cả các phương pháp này là có ưu điểm rất lớn. cung cấp rất nhiều sự lựa chọn linh động để xây dựng một cấu trúc NMS. Trong trường hợp lý tưởng nhất là bản kiến trúc có thể đối chiếu với cấu trúc tổ chức đang dùng nó, nếu hầu hết các việc quản lý của tổ chức là tập trung tại một khu vực thì một NMS sẽ có nhiều thuận lợi.

CHƯƠNG II.
NGHI THỨC QUẢN TRỊ MẠNG

Như đã trình bày quản lý mạng một cách có hiệu quả phụ thuộc vào người kỹ sư quản trị mạng có khả năng giám sát và điều khiển mạng được hay không. Thiếu những thông tin về tình trạng hoạt động của mạng, người kỹ sư có thể buộc phải đưa ra các quyết định không xác đáng do không tính đến số liệu đo định tính và định lượng được cung cấp bởi các phương tiện đo lường hoạt động mạng. Vì vậy, điều rất cơ bản là các kỹ sư mạng phải hiểu được các phương pháp sẵn có trong ngành công nghiệp máy tính về việc giám sát và điều khiển mạng.

Trong phần này chúng ta sẽ tổng kết một số các nghi thức quản trị mạng và nêu ra quá trình phát triển của các nghi thức. Mặt khác ta cũng đề cập tới các phương pháp sẵn có trong việc lấy và thiết lập các thông tin quản trị trên một mạng.

2.1. Lịch sử các nghi thức quản lý mạng.

Cho tới gần đây, việc thu thập thông tin từ các thiết bị mạng khác nhau đã đòi hỏi các kỹ sư phải học một loạt các phương pháp để lấy được các dữ liệu. Lý do đối với điều này là các sản phẩm nối mạng mới đã được phát triển, các nhà chế tạo chúng đã thiết lập các cơ chế thích hợp để có thể thu thập dữ liệu từ các sản phẩm của họ : kết quả là có hai công cụ có cùng chức năng nhưng được đưa ra từ các nhà chế tạo khác nhau, có thể cung cấp các phương pháp khác nhau để thu thập dữ liệu.

Ví dụ : giả sử một công ty sử dụng hai loại router của DEC để nối với các máy mini của Digital. Loại đầu tiên được sản xuất bởi một công ty được gọi là RoutMe và loại thứ hai bởi một công ty khác có tên là FastRoute.

Cả hai loại đều cho phép đăng nhập mạng từ xa. Tuy nhiên, phương pháp mà bạn sẽ phải sử dụng để tiếp cận thực sự tới các dữ liệu là khác nhau đáng kể. Để hỏi router RouteMe về số hiệu của thiết bị giao tiếp và các thông số hoạt động, ta sẽ phải sử dụng một thực đơn Trong khi để hỏi các thông tin đó đối với router FastRoute rất có thể lại phải sử dụng ba lệnh nào đó trên một giao diện theo kiểu lệnh.

Như đã thấy , trong một môi trường mạng hỗn tạp - việc sử dụng thông tin bằng những phương pháp triêng biệt do từng nhà sản xuất quy định gây chậm chạp và nặng nề. Các kỹ sư mạng đòi hỏi một phương pháp nhất quán để thu thập thông tin về tất cả các bộ phận hợp thành trên mạng. Vì vậy, các kỹ sư đã muốn sử dụng các công cụ chung như là các công cụ tiêu chuẩn. Tuy nhiên, dù rằng các công cụ này là đơn giản hơn nhiều phương pháp được cung cấp bởi các nhà chế tạo - chúng không được thiết kế riêng biệt cho quản lý mạng và như vậy đã có các mặt hạn chế của chúng như được bàn luận dưới đây.

Đối với các mạng theo nghi thức Internet (IP), các kỹ sư mạng có thể sử dụng chức năng lặp lại nghi thức thông báo điều khiển Internet (ICMP: Internet Control Message Protocol) Echo và Echo Reply để thu thập một số thông tin hạn chế nhưng hữu ích cho quản lý mạng. Dự định ban đầu là gửi thông báo điều khiển giữa hai thiết bị mạng, nhưng phần lớn các thông báo ICMP không dễ đọc. Tuy nhiên, cả hai chức năng trên tồn tại trên bất kỳ thiết bị nào với bộ nghi thức IP, chúng cung cấp một phương pháp kiểm tra liên tục của hệ thống đối với một thiết bị ở xa.

Với việc sử dụng các thông báo này, một thiết bị trên mạng khi tiếp nhận một thông báo ICMP (gọi là Echo) phải chuyển lại một báo đáp lại (Echo Reply) cho thiết bị nguồn. Nếu không thấy thông báo đáp lại có nghĩa là có một lỗi trên mạng. Ứng dụng đó được gọi là Ping (Packet Internet Groper). Nó kiểm tra hai thiết bị có kết nối được hay không bằng cách gửi đi một ICMP Echo và đợi Echo Reply.

Phần lớn các phiên bản của Ping cũng có thể đếm thời gian phản hồi tính theo miligiây giữa thông báo được gửi và báo đáp nhận được, cùng như tỷ lệ % của các thông báo đáp. TCP/IP không phải là bộ nghi thức duy nhất cung cấp công cụ như Ping. Mẫu báo đáp này còn tồn tại trong một vài nghi thức khác như Appletalk, Novell/ IPX, Xerox XNS và Banyan Vines.

Tuy nhiên, mẫu này có các mặt hạn chế sau đây :

1. Giao nhận không tin cậy.

2. Cần phải thăm dò.

3. Thông tin hạn chế.

Phần lớn các ứng dụng ICMP này sử dụng tầng network của mạng chứ không sử dụng tầng transport. Như vậy việc không nhận được Echo Reply không hẳn là không kết nối được. Có thể chỉ ra là một thiết bị mạng đã bỏ rơi báo đáp hay chỉ do thiếu vùng đệm tạm thời. Cũng có thể là hỏng bởi sự tắc nghẽn tại một mạch dữ liệu ở một thời điểm truyền dữ liệu.

Để tìm ra thông tin hiện hành bằng việc tìm chức năng Echo/Echo Reply ta phải thăm dò liên tục các thiết bị mạng. Việc thực hiện thăm dò này là một phương pháp cô lập lỗi thông dụng và có thể thực hiện nhanh chóng và dễ dàng và không đòi hỏi bất kỳ ưu tiên nào hoặc phần cứng hỗ trợ. Một tỉ lệ phần trăm lớn các báo đáp mất có thể cho biết có vấn đề về kết nối mạng. Một khi được xác định, kỹ sư mạng cần phải dựa vào các phương pháp khác để cô lập và xác định nguyên nhân. Một thủ tục quản lý mạng nên cung cấp khả năng để các thiết bị tự gửi các thông báo tới một hệ thống quản lý. Điều này có thể gây thêm công việc thăm dò, nhưng nó là một phương pháp rất hiệu quả để thu thập thông tin quản lý mạng.

Một lý do sơ đẳng của sự khiếm khuyết này là phép thử Echo/Echo Reply không được thiết kế để cung cấp nhiều thông tin quản trị mạng. Thông tin thu được thường không đủ để xác định tình trạng mạng và do đó không thể có các quyết định đúng đắn đối với việc quản trị mạng. Đối với mục đích này, cần sử dụng một thủ tục được viết riêng.

Những khó khăn trên đã làm nhu cầu cần có các nghi thức quản trị mạng tiêu chuẩn trở nên bức xúc. Các nhà phát triển đã đưa ra hai hướng khác nhau để tạo ra các nghi thức quản trị mạng. Giải pháp thứ nhất là SMNP (Simple Network Management Protocol) mà sau này đã chứng tỏ là rất thành công. Giải pháp thứ hai là CMIS/SMIP (Common Management Information Services/ Common Management Information Protocol) được phát triển bởi Tổ chức quốc tế về tiêu chuẩn (ISO) cũng có một ảnh hưởng nhất định trong cộng đồng mạng. Cả hai nghi thức này đều cung cấp các phương tiện thu thập các thông tin từ các thiết bị mạng và gửi các lệnh đến các thiết bị mạng. Hơn nữa cả hai nghi thức này đều được xây dựng trên cơ sở mô hình tham chiếu mạng 7 tầng đã được chuẩn hoá bởi ISO

2.2. Sự phát triển của các nghi thức chuẩn :

Các ví dụ và một số vấn đề mà ta đã thảo luận trong phần trên không làm rõ được các giải pháp liên quan đến quản lý một mạng phức tạp. Mặt khác nói chung không một mạng nào đó có thể hoàn toàn được

xây dựng từ các thiết bị (hubs, bridges, routers, hosts) được cung cấp bởi một công ty duy nhất. Do đó khi người kỹ sư mạng có kế hoạch thay đổi và phát triển mạng thì họ cũng phải tính ngay đến việc quản trị mạng với một tiêu chuẩn nào đó.

Gần đây để giải quyết các vấn đề đó thì các nhà chế tạo đã đưa ra các nghi thức quản lý mạng chuẩn, các nghi thức này cho phép thu thập và lấy các thông tin từ thiết bị mạng. Mặt khác các nghi thức này có thể cung cấp một kiểu truy nhập tới thiết bị mạng. Có thể ta phải hỏi

- Tên của thiết bị.
- Version phần mềm trong thiết bị.
- Số của giao diện trong thiết bị.
- Số của các gói tin đi qua một thiết bị trong một khoảng thời gian.

Các tham số có thể thiết lập được đối với thiết bị mạng có thể bao gồm :

- Tên của thiết bị.
- Địa chỉ của một giao diện mạng.
- Trạng thái hoạt động của một thiết bị giao tiếp mạng.

Các nghi thức mạng được chuẩn hoá mang thêm đến những lợi ích mới ở chỗ dữ liệu truyền đến và thu nhận về từ các thiết bị mạng là nhất quán.

Trước khi đi tới 2 nghi thức quản trị mạng tiêu chuẩn là CMIP và SNMP ta cũng nên điểm qua một vài sự kiện. Trước hết là Hội đồng Công tác Internet (Internet Activities Board viết tắt là IAB). Hội đồng này xem xét chung công nghệ cũng như nghi thức trong cộng đồng các mạng dựa trên TCP/IP. IAB gồm 2 nhóm đặc nhiệm là IETF (Internet Engineering Task Force) và IRTF (Internet Researche Task Force). IETF hướng vào xác định các vấn đề và phối hợp giải quyết vấn đề trong lĩnh vực quản trị, công nghệ và hoạt động của Internet. Còn IRTF chịu trách nhiệm nghiên cứu các vấn đề liên quan đến cộng đồng mạng TCP/IP và Internet.

Vào 1988 đã có ba nghi thức quản lý mạng khác nhau như sau:

- Hệ thống quản lý thực thể ở mức cao (HEMS:High-level Entity Management System).

- Nghi thức giám sát cổng đơn (SGMP: Simple Gateway Monitoring Protocol).

- Nghi thức thông tin quản lý chung trên TCP (CMIP : Common Management Information Protocol).

Như một giải pháp tạm thời, IAB đã khuyến cáo cài đặt ngay nghi thức quản lý mạng đơn giản (SNMP) dựa trên nghi thức giám sát cổng đơn (SGMP) như một nghi thức quản lý mạng chung (CNMP) với các mạng dựa trên TCP/IP.

IETF đã chịu trách nhiệm thiết lập SNMP. IAB cũng đã nhấn mạnh rằng SNMP trong tương lại phải tập trung vào quản lý lỗi và quản lý cấu hình. Dẫu sao thì tại thời điểm đó, SNMP được nhiều tổ chức sử dụng trong tất cả các lĩnh vực về quản lý mạng.

Trong thời gian dài, IAB đã khuyến cáo cộng đồng nghiên cứu Internet rà soát nghi thức CMIS/CMIP như một nền tảng cho việc quản trị mạng có thể đáp ứng được các nhu cầu trong tương lai. CMIS/CMIP được phát triển bởi chuẩn ISO với mục đích khác với nghi thức SNMP. SNMP chỉ nhằm vào mục đích quản trị các thiết bị kiểu IP còn CMIS / CMIP được mở rộng để trở thành một đặc tả không thủ tục để có thể quản trị toàn bộ các thiết bị mạng.

Khi IAB xem xét CMIS/CMIP, CMIS/CMIP đã được cài đặt trên nền tảng của TCP. Sự kết hợp này đã đưa tới nghi thức có tên là CMOT. Ngày nay CMOT không còn đượcc sử dụng rộng rãi nữa.

2.3. MIB (Management Information Base)

MIB là sự định nghĩa chính xác các thông tin truy nhập được thông qua nghi thức quản lý mạng. Trong RFC 1052, IAB đã khuyến cáo cần tiên cao cho việc xác định một MIB mở rộng dùng cho cả nghi thức SNMP và CMIS/CMIP mặc dù việc tạo một MIB như vậy không khả thi.

MIB định nghĩa những thông tin quản trị sẵn có trong các thiết bị mạng theo một cấu trúc phân cấp. Mỗi thiết bị muốn được xem xét trong công việc quản trị mạng phải sử dụng và cung cấp được những thông tin được MIB định dạng theo một tiêu chuẩn chung.

RFC 1065 miêu tả cú pháp và kiểu của thông tin có sẵn trong MIB để quản lý các mạng TCP/IP gọi là SMI (viết tắt từ Structure and Identification of management information for TCP/IP base Internets). Chính RFC 1065 đã định nghĩa các quy tắc đơn giản để đặt tên và tạo các kiểu thông tin. Ví dụ *Gauge* được định nghĩa như một số nguyên có thể tăng hoặc giảm hay *Time Ticks* là bộ đếm theo đơn vị 1/100 giây. Sau này RFC 1065 được IAB chấp nhận như một tiêu chuẩn đầy đủ trong RFC 1155.

Sử dụng qui tắc SMI, RFC 1066 đã đưa ra version đầu của MIB cho việc sử dụng bộ nghi thức TCP/IP. Chuẩn này đã được biết đến như

là MIB - I, nó giải thích và định nghĩa một cách chính xác những thông tin cơ sở cần thiết cho điều khiển và giám sát mạngTCP/IP.

RFC 1066 được chấp nhận bởi IAB như là một tiêu chuẩn đầy đủ trong RFC 1156.

RFC 1158 đã đề nghị một version thứ hai cho MIB, MIB - II được sử dụng cùng với nghi thức tiếp theo của TCP/IP. Đề nghị này đã được chính thức hóa như là tiêu chuẩn và đã được phê duyệt bởi IAB trong RFC 1213. MIB II đã mở rộng thông tin cơ sở đã được định nghĩa trong MIB - I.

Để dễ dàng chuyển dịch thành các version thương mại RFC-1156 cho phép các nhà phát triển mở rộng MIB. Vi dụ một công ty muốn tạo ra một đối tượng gọi là "sử dụng CPU" của một cầu Ethernet sẵn có mà MIB II chưa sẵn có. MIB II cho phép tạo thêm những đối tượng mới như vậy theo chuẩn SMI nói trên.

Các nhà nghiên cứu quản trị mạng cũng nghiên cứu các MIB không phụ thuộc vào môi trường TCP/IP. Mỗi MIB như vậy có thể tập trung vào một môi trường cụ thể và các thiết bị cụ thể. Chẳng hạn MIB cho Token Ring theo tiêu chuẩn IEEE 802.5 cho trong RFC 1231, RMON (Remote Network Monitoring MIB) cho trong RFC 1271, FDDI Interface cho trong RFC 1285...

a. ASN. 1 Syntax :

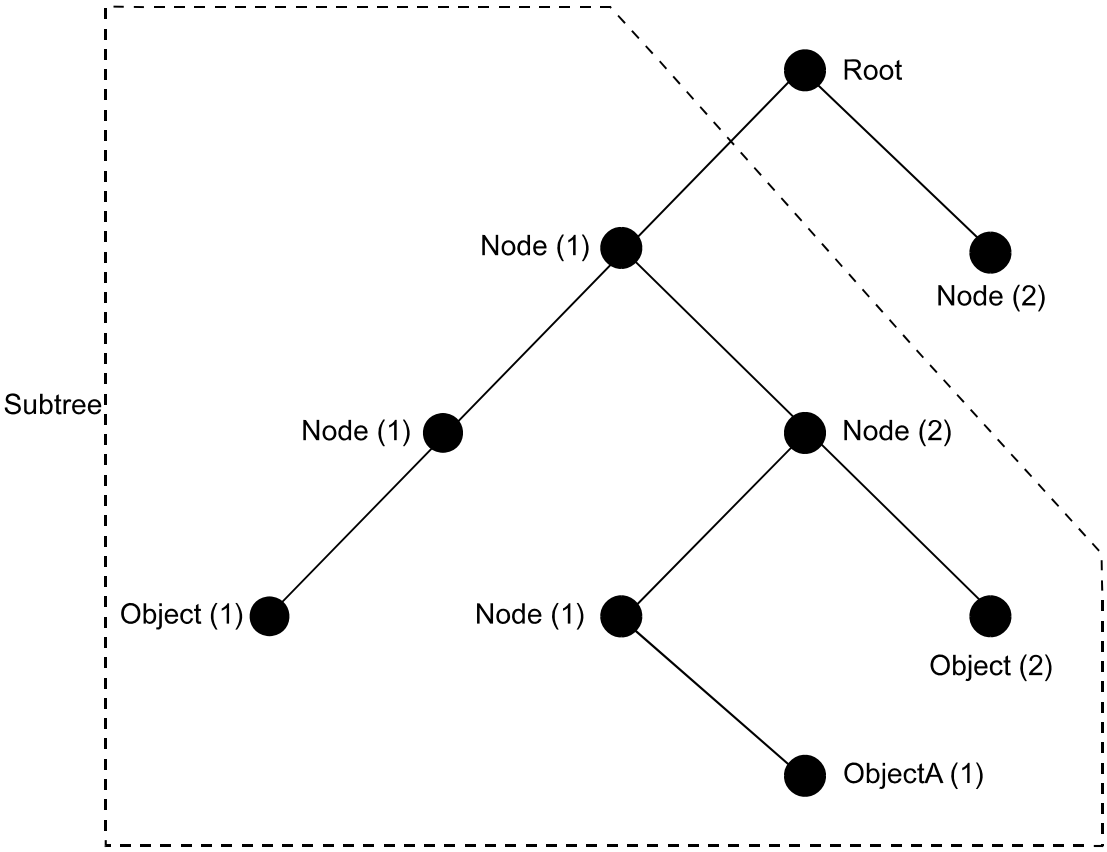
Một tập con các kí pháp cú pháp rút gọn của ISO (Abstract Syntax Notation one viết tắt là ISO ASN.1) đã định nghĩa cú pháp cho MIB. Mỗi MIB sử dụng cấu trúc cây được định nghĩa trong ASN.1 để tạo nên tất cả các thông tin sẵn có. Mỗi mẩu thông tin trong cây là một nút có nhãn (*Labeled node)*. Mỗi nút có nhãn gồm:

- Tên đối tượng (O*bject Identifier* - OID).

- Một mô tả ngắn dưới dạng văn bản.

Ổ đây OID là một dãy số nguyên được tách ra bởi các dấu chấm chỉ tên nút đó và biểu thị chính xác nhánh của cây ASN.1.

Một nút có nhãn có thể có các cây con chứa đựng các nút có nhãn khác hoặc là một nút lá (leaf node) không có cây con. Mỗi nút là chứa đựng một giá trị và được hiểu là một đối tượng. Hình vẽ sau là một cây MIB định nghĩa theo kiểu ASN.1



Một ví dụ của cây ASN.1

Theo hình vẽ này thì đối tượng A1 sẽ có OID là 1.2.1.1

b. Các nhánh của cây MIB :

Cây MIB nói ở đây hiểu như một sự phân nhánh các dạng thông tin cơ bản trong quản trị mạng. Nó cũng liên quan đến các tổ chức nghiên cứu chuẩn hoá các thông tin quản trị mạng.

Nút gốc của cây MIB không có tên nhưng có 3 cây con như sau:

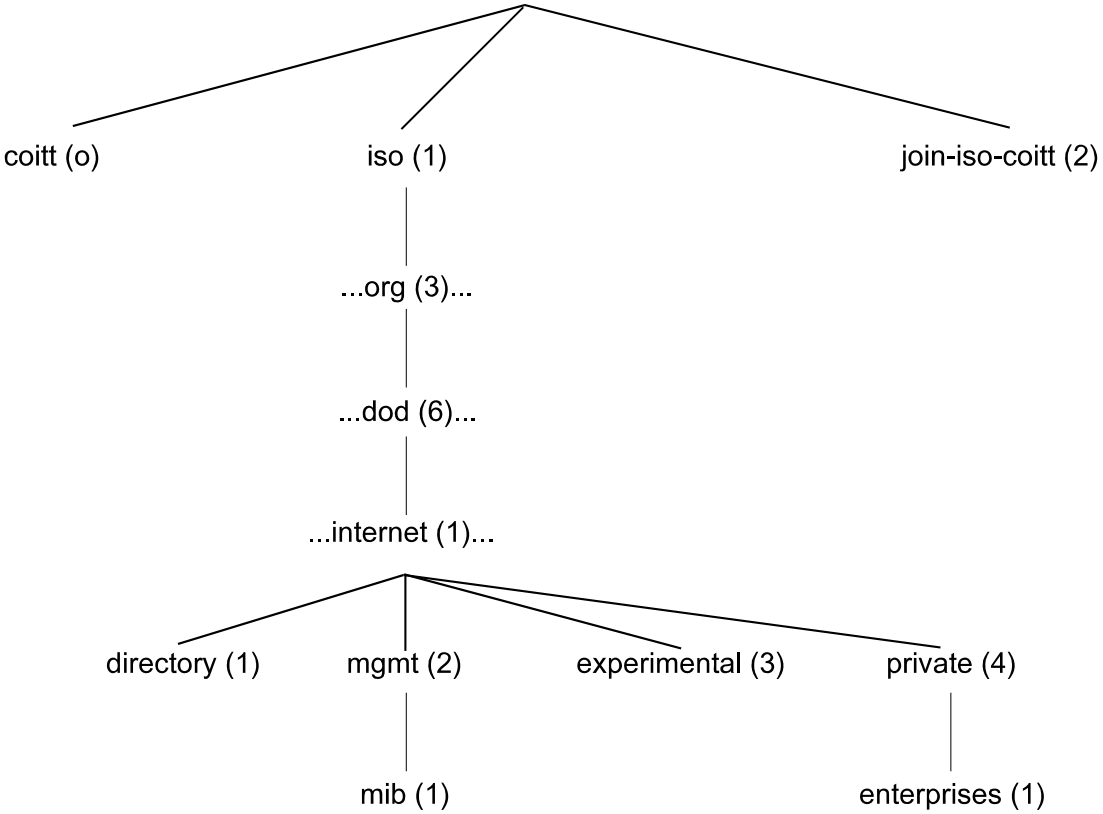
+ CCITT(0), được quản trị bởi CCITT (International Telephone and Telegraph Consultative Committee).

+ ISO(1), được quản trị bởi ISO.

+ Joint-CCITT - ISO(2), được quản trị bởi ISO và CCITT.

Dưới nút ISO (1) có một số cây con, trong đó có cả cây con mà ISO đã xác định cho các tổ chức khác gọi là org (3). Dưới tổ chức org(3) cây con, một nút đặc biệt được Bộ Quốc Phòng Mỹ sử dụng (United States Department of Defence - DOD) ký hiệu là dod(6). Tất cả các thông tin được thu thập từ các thiết bị qua các nghi thức kiểu DOD ví dụ như TCP/IP có trong cây con đó mà OID của nó là 1.3.6.1.

Các OID này chính là Internet. Nguyên bản chuẩn cho ID này là {ISO org (3)dod (6) 1}.



Cây ASN.1 được dùng cho quản lý mạng.

Có 4 cây con được định nghĩa dưới OID Internet như sau :

- Directory (1)
- Mgmt (2)
- Experimental (3)
- Private (4)

Cây con Directory (1) : Hiện tại cây con Directory (1) là được dành cho tương lai. Cây con này sẽ chứa các thông tin về dịch vụ thư mục OSI (X. 500).

- *Cây con Mgmt (2)* : Cây con Mgmt (2) là được dành cho thông tin quản lý theo nghi thức DOD. Tại thời điểm làm việc này, các đối tượng trong cây con hầu hết được sử dụng rộng rãi. MIB - I (RFC 1156) mới được đặt trong OID 1.3.6.1.2.1.

Dưới cây con Mgmt (2) là các đối tượng được sử dụng để lấy các thông tin cụ thể từ các thiết bị mạng. Các đối tượng đó được phân rã thành 11 loại như trong bảng dưới đây.

11 LOẠI CÂY CON MGMT(2)	LOẠI THÔNG TIN TRONG CÂY
System (1)	Hệ điều hành mạng
Interfaces(2)	Đặc tả giao tiếp mạng
Address tranlation(3)	Ánh xạ địa chỉ
IP(4)	Đặc tả nghi thức Internet
ICMP(5)	Đặc tả nghi thức điều khiển thông báo liên mạng
Tcp(6)	Đặc tả nghi thức truyền
UDP(7)	Đặc tả nghi thức Datagram cho người dùng
EGP(8)	Đặc tả nghi thức cổng ngoài
CMOT(9)	Dịch vụ thông tin quản lý chung
Tranmission(10)	Đặc tả Nghi thức truyền
SNMP(11)	Đặc tả nghi thức quản lý mạng đơn giản

-Cây con Experimental (3):

Các nghi thức thử nghiệm đặt trong cây con Experimental

- Cây con Private (4)

Cây con Private (4) là được dùng để định nghĩa các đối tượng cụ thể riêng biệt

2.4. Nghi thức SNMP

Hầu hết nghi thức quản lý mạng dùng cho mạng là nghi thức quản trị mạng đơn giản. Thực ra đầu tiên RFC 1067 đã đưa ra và đã định nghĩa các thông tin được truyền qua giữa hệ thống quản lý mạng và các Agent đối với SNMP. Tiếp đó RFC 1098 được tạo ra và làm cho RFC 1067 bị lỗi thời. Sau đó với RFC 1157 thì IAB đã chấp nhận đề nghị của RFC 1098 và chấp nhận nghi thức SNMP như là một nghi thức chuẩn.

RFC 1157 mô tả mô hình Agent/Station được dùng trong SNMP. Một agent của SNMP là phần mềm có khả năng trả lời một số câu hỏi

hợp thức từ một trạm SNMP. Một trạm SNMP có thể là hệ thống quản lý mạng . Một thiết bị mạng có thể cung cấp các thông tin về MIB tới trạm là một agent SNMP. Để mô hình Agent/Station làm việc được bình thường thì Agent và Station phải có cùng một ngôn ngữ giống nhau.

Các agent và station liên kết nhau thông qua một thông báo chuẩn. Mỗi một thông báo là sự trao đổi một gói thông tin. Vì vậy nghi thức SNMP sử dụng tầng 4 (tầng UDP (user datagram protocol) - chính là tầng vận chuyển (transport) trong mô hình tham chiếu OSI của mạng)

Nghi thức SNMP có 5 kiểu thông báo :

* *Get-Request.*

* *Get-Response.*

* *Get-Next-Request.*

* *Set-Request.*

* *Trap.*

Trạm SNMP dùng *Get-Request* để lấy thông tin từ một thiết bị mạng mà nó có một Agent SNMP. Agent đến lượt mình thông qua *Get-Respond* sẽ gửi trả lại một thông báo có thể mang thông tin về tên của hệ thống, hệ thống chạy trong bao lâu và số hiệu của thiết bị giao tiếp mạng trong hệ thống.

Get-Next-Request được dùng để hỏi tiếp các thông tin như Get-Request đã hỏi

Set-Request cho phép thiết lập từ xa các tham số cấu hình trong một thiết bị. Ví dụ thông báo *Set-Request* có thể thiết lập tên một thiết bị, giao diện ngắt hoặc xóa một địa chỉ phân giải bảng.

SNMP Trap (bẫy) là một thông báo không phải tạo ra theo yêu cầu mà do một Agent tự gửi tới một Station. Thường các bẫy là các thông báo bất thường ví dụ như một mạch bị hỏng, không gian đĩa không còn đủ cho hoạt động của hệ thống

Hiện tại có bảy kiểu Trap SNMP được MIB-II định nghĩa. Đó là:

**Coldstart of system.*

**Warmstart of a system.*

**Link down.*

**Link up.*

**Failure of authentication.*

**Exterior Gateway Protocol (EGP) neighbor loss.*

**Enterprise-specific.*

Trong đó:

Coldstart trap cho biết Agent đang do đó cấu hình hoặc nghi thức đã bị thay đổi. Một *Coldstart trap* xẩy ra khi một thiết bị bắt đầu được cấp nguồn điện. Trong khi đó một*Warmstart trap* cho biết thiết bị tự khởi động lại nhưng cấu hình và nghi thức không bị thay đổi

Link down Trap thông báo quá trình kết nối bị thất bại còn *Link up Trap* thông báo việc kết nối đã đượo thực hiện trở lại

Thông báo *Failure of authentication Trap* là gửi tới hệ thống quản lý mạng thông báo rằng station nhận được một thông báo không phù hợp

Exterior Gateway Protocol (EGP) neighbor loss Trap là được dùng bởi một Agent SNMP để báo cáo mất đối tác EGP. Khi đó EGP có thể được nạp lại

Các chuỗi chung (Community strings) SNMP không cung cấp thông tin cũng như phương tiện thay đổi cấu hình nếu không có các biện pháp an ninh cần thiết. Một SNMP agent có thể yêu cầu một SNMP station gửi thông báo có kèm mật khẩu sau đó nó kiểm tra quyền hạn sử dụng các thông tin MIB. Mật khẩu đó gọi là chuỗi chung. Một sô bản SNMP có quy định các mức an ninh khác nhau trong định dạng của chuỗi chung

2.5. Nghi thức CMIS/CMIP :

Nhiều người cho rằng nghi thức này có thể là tốt nhất đối vơi nhu cầu quản lý mạng theo mô hình tham chiếu OSI.

Ở đây CMIS định nghĩa dịch vụ cung cấp bởi mỗi thành phần trong mạng nhằm phục vụ quản lý mạng. Dịch vụ này thường là chung. Còn nghi thức CMIP là nghi thức thực thi dịch vụ CMIS.

Các nghi thức mạng OSI được dùng để cung cấp một kiến trúc mạng chung cho tất cả các thiết bị trên mỗi tầng của mô hình ISO. Tương tự, CMIS/CMIP cũng cung cấp một bộ nghi thức quản lý mạng trọn vẹn để dùng với nhiều thiết bị mạng. Với CMIS/CMIP một hệ thống (các thiết bị mạng) được xem là một hệ thống mở và bình đẳng

Quản trị mạng là một ứng dụng trên mạng, và nằm trên tầng 7 trong mô hình tham chiếu về kiến trúc mạng. Ở đây các đơn vị dịch vụ thông tin quản trị chung (Common Management Information Service Element, viết tắt là CMISE) cung cấp các phương tiện ứng dụng cho việc dùng CMIP. Cũng trong tầng này còn 2 nghi thức ứng dụng ISO là ACSE

(Association control service element và ROSE (Remote Opreration Service Element).

Như vậy trong mô hình tham chiếu ISO về mạng ta có thể hình dùng vị trí của các CMISE được ISO chuẩn hoá như sau.

	Các tiến trình quản trị mạng	
Lớp 7	CMISE ISO.....	
	ACSE	ROSE
Lớp 6	Presentation	
Lớp 5	Session	
Lớp 4	Transport	
Lớp 3	Network	
Lớp 2	Datalink	
Lớp 1	Physical	

Lấy thông tin nhờ CMIS.

Dịch vụ CMIS cung cấp việc xây dựng các mô đun cơ bản (một ứng dụng thành phần) để hệ thống có thể giải quyết các vấn đề rắc rối trong việc quản lý mạng. Mỗi một ứng dụng như vậy ta gọi là một CMISE-service-user mà ta tạm dịch là đối tượng sử dụng dịch vụ CMISE (ĐTSDDV CMISE)

CMIS đã định nghĩa 3 lớp dịch vụ như sau :

- Phối hợp quản lý (Management Association).
- Thông báo quản lý(Management Notification).
- Thi hành quản lý (Management Operation)

Dịch vụ phối hợp quản lý:

Lớp dịch vụ phối hợp quản lý kiểm soát sự phối hợp của các hệ thống mở bình đẳng. Dịch vụ này được dùng chủ yếu cho sự thiết lập hay hủy bỏ liên kết giữa các hệ thống. Chúng điều khiển các ứng dụng với các dịch vụ sau:

M-INITIALIZE.

M-TERMINATE.

M-ABORT.

Dịch vụ M-INITIALIZE thiết lập một sự kết hợp với một ĐTSDDV CMISE cho việc quản lý hệ thống. Dịch vụ M-TERMINATE kết thúc một kết nối giữa các ĐTSDDV CMISE cùng mức. Dịch vụ M-ABORT là được sử dụng khi một kết nối giữa ĐTSDDV CMISE bị kết thúc không bình thường (trường hợp có lỗi).

Mỗi dịch vụ của Management Association này đảm nhiệm việc sử dụng dịch vụ của ACSE cho thao tác. Một dịch vụ CMIS khác thao tác với ROSE.

Dịch vụ Thông báo quản lý

Kiểu thứ hai của dịch vụ CMIS là thông báo quản lý. Dịch vụ này tương tự như thông báo bẫy mà SNMP dùng để cung cấp thông tin về các sự kiện trên một mạng. Dịch vụ thông báo quản lý cung cấp các thông tin này thông qua dịch vụ M-EVENT-REPORT - nó báo cho một ĐTSDDV CMISE cùng mức về một sự kiện nào đó được xảy ra ở một ĐTSDDV CMISE khác. Nếu ĐTSDDV CMISE trong một hệ thống cần thay đổi giá trị (như là trạng thái của một thiết bị giao tiếp mạng) thì nó có thể khai báo vơi hệ thống nhờ dịch vụ M-EVENT-REPORT. Tuy nhiên, so với dịch vụ bẫy của nghi thức SNMP, các sự kiện ở đây không được xác định chặt chẽ. Đây là một yếu tố mở để các nhà phát triển định ra các thông báo phù hợp với yêu cầu.

Dịch vụ thi hành quản lý

Dịch vụ thao tác quản lý gồm các nhóm như sau :

- M-GET
- M-SET
- M-ACTION
- M-CREATE
- M-DELETE

Trong đó :

- Dịch vụ M-GET là được sử dụng bởi ĐTSDDV CMISE để lấy thông tin quản lý từ một ĐTSDDV CMISE khác cùng mức. Nó tương tự như trong thông báo GET-REQUEST của nghi thức SNMP.

- Dịch vụ M-SET của CMIS cho phép một ĐTSDDV CMISE sửa đổi thông tin quản lý của ĐTSDDV CMISE cùng mức. Dịch vụ này cũng

tương tự như thông báo SET-REQUEST của nghi thức SNMP cho phép sửa đổi thông tin trên một thiết bị mạng.

- Dịch vụ M-ACTION là được nêu ra bởi một ĐTSDDV CMISE để yêu cầu một ĐTSDDV CMISE cùng mức thực hiện một hành động mong muốn. VD : Một hệ thống có thể gửi ICMP Echoes (pings) tới một địa điểm khác và yêu cầu gửi trả lại phản hồi để kiểm tra việc kết nối tới một thiết bị IP khác có thành công hay không. Đây là một trong nhiều hoạt động mà một hệ thống mở có thể yêu cầu một hệ thống mở khác thực hiện.

- Dịch vụ M-CREATE được dùng bởi một ĐTSDDV CMISE để cung cấp một ĐTSDDV CMISE cùng mức cho việc tạo lập phiên bản để quản lý. Phiên bản này sẽ đại diện cho ĐTSDDV CMISE trên một hệ thống quản lý.

- Dịch vụ cuối cùng là M-DELETE cho phép xoá phiên bản đã tạo ra bởi M-CREATE

Cũng giống như chuỗi chung trong SNMP để kiểm soát quyền sử dụng thông tin quản lý, CMISE sử dụng danh sách truy nhập

Kết hợp quản lý (Management Associations)

Một kết hợp quản lý là một liên kết giữa hai hệ thống mở cùng mức đối với quản lý hệ thống. Quá trình kết nối dựa trên CMISE để tạo ra một giao tiếp với các nghi thức.

Với CMIS có 4 kiểu phối hợp có thể tồn tại giữa các hệ thống mở cùng mức như sau :

- Sự kiện (Event)
- Sự kiện và giám sát (Event/Monitor)
- Giám sát và điều khiển (Monitor/Control)
- Quản lý toàn diện và đối tác (Full Manager/Agent)

Một kết hợp theo kiểu sự kiện Event cho phép hai hệ thống mở gửi thông báo M-EVENT- REPORT.

Một kết hợp theo kiểu Event/Monitor là giống như phối hợp 1 Event, ngoài ra mỗi hệ thống cũng có thể thu nhận và vận hành thông báo M-GET.

Một kết hợp theo kiểu Monitor/Control cho phép liên kết M-GET, M-SET, M-CREATE, M-DELETE và M-ACTION yêu cầu, mặc dầu không cho phép sinh báo cáo.

Một kết hợp theo kiểu Full Manager/AGent hỗ trợ tất cả các dịch vụ của CMIS.

2. 6. Nghi thức CMOT :

CMOT là chữ viết tắt của Common Management information Services and Protocol over TCP/IP.

Nghi thức này thực chất là dùng các dịch vụ của CMIS trên nghi thức TCP/IP. RFC 1189 định nghĩa cho nghi thức CMOT và được minh hoạ trên mô hình ISO như bảng dưới đây.

Management Application Processes		
CMISE ISO 9595/9596		Layer 7
ACSE ISO 8649/8650	ROSE ISO 9072 - 1/2	
Lightweight Presentation Protocol (LPP) RFC 1085		Layer 6
ISO Session		Layer 5
TCP	UDP	Layer 4
IP		Layer 3
ISO data link		Layer 2
Physical		Layer 1

Các nghi thức ứng dụng được dùng bởi CMIS không thay đổi chế độ thi hành của CMOT. Nghi thức CMOT thường dựa vào các nghi thức CMISE, ACSE và ROSE như trước khi được miêu tả với CMIS. Tuy nhiên trong khi chờ đợi ISO thiết lập nghi thức ở mức 6 thì sử dụng nghi thức khác gọi là *Lightweight presentation protocol* (LPP) ở Layer 6 và nó được định nghĩa trong RFC 1085. Nghi thức này cung cấp giao tiếp chung cho cả hai nghi thức được dùng ngày nay là UDP và TCP.

CHƯƠNG III.

NGHI THỨC QUẢN TRỊ MẠNG SNMP

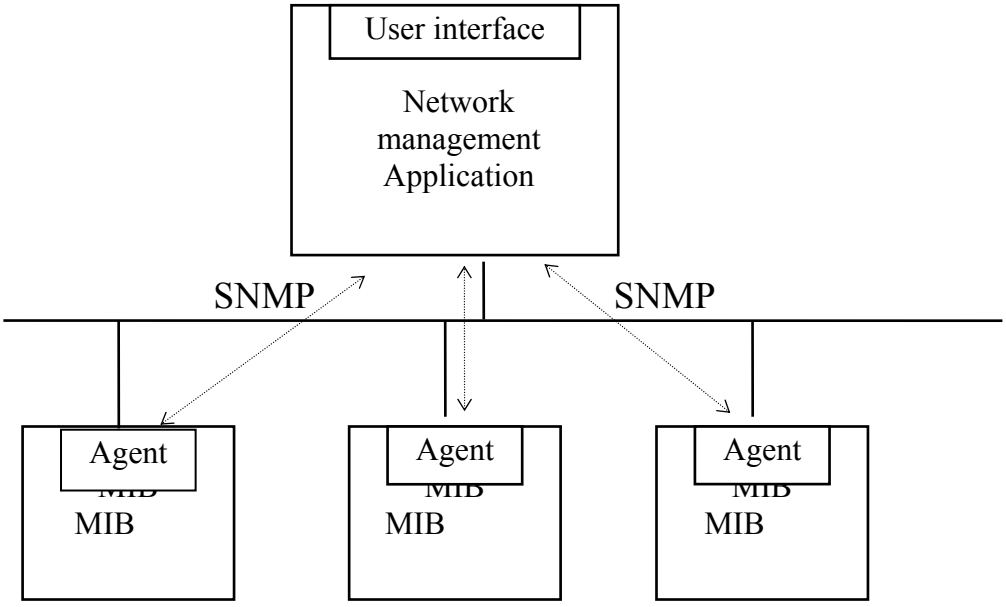
Như đã biết, nghi thức quản lý mạng đơn giản SNMP là một nghi thức ở tầng ứng dụng, nó cho phép dễ dàng trao đổi các thông tin quản lý giữa các thiết bị trong mạng. Trong chương này ta sẽ mô tả chi tiết nghi thức quản trị mạng SNMP.

3.1. SNMP Version. 1

Trong SNMP V.1 agent là các mô đun phần mềm chạy trong các thiết bị, agent truy cập tới các thông tin trên thiết bị, mà ở đó agent có thể lấy và tạo lập các thông tin này từ hệ thống quản lý mạng NMS (NMS : Network Management System) thông qua SNMP V.1

Một thiết bị được quản lý có thể là bất kỳ một nút trên mạng, bao gồm các máy chủ, card giao tiếp mạng, các print server, router, host, bridge và các hub.

Vì các thiết bị này có thể có khả năng rất hạn chế (VD : có thể do tốc độ của CPU hoặc bộ nhớ nhỏ) nên các phần mềm quản lý được giả định phải hoạt động ở mức chiếm tài nguyên thấp nhất có thể để ít gây ảnh hưởng nhất cho hoạt động của thiết bị được quản lý



Thiết bị được quản lý Thiết bị được quản lý Thiết bị được quản lý

Một hoặc nhiều NMS có thể tồn tại trên bất kỳ một mạng được quản lý nào. NMS có thể chạy các ứng dụng quản trị mạng mà kết quả là các thông tin quản lý mạng được đưa ra cho người quản trị. Giao diện người sử dụng thông thường là giao diện đồ hoạ (GUI : Graphical user interface).

Liên lạc giữa thiết bị được quản lý và NMS được quản trị bằng một nghi thức quản lý mạng. Khung chung của một hệ quản lý mạng theo chuẩn Internet dựa trên giả định rằng ta có thể tìm và sửa lỗi từ xa. Như vậy các thiết bị mạng phải sử dụng một số biến để duy trì các thông tin về thiết bị cũng như tình trạng hoạt động của thiết bị. Căn cứ vào đó NMS có thể kiểm tra và điều chỉnh các thông tin cần thiết phục vụ cho hoạt động của mạng. VD ta phải theo dõi các thông tin sau :

- Số hiệu và trạng thái của các mạch (Virtual circuit) của thiết bị.

- Thống kê số lượng một số loại thông báo lỗi.

- Số lượng byte và các gói đi và đến thiết bị.

- Độ dài lớn nhất của hàng đợi (cho các router và các thiết bị liên mạng khác).

- Các thông điệp phát đi và thu nhận.

- Các thiết bị giao tiếp mạng bị ngừng hoạt động hay hoạt động trở lại

a. Kiểu lệnh :

NMS điều khiển một thiết bị mạng bằng cách gửi một thông báo, yêu cầu thiết bị thay đổi giá trị một hoặc nhiều biến. Thiết bị sẽ đáp ứng hoặc khởi động bằng một trong 4 kiểu lệnh khác nhau sau:

 Kiểu đọc : Được NMS dùng để giám sát các thiết bị mạng. NMS đọc các biến đã được thiết bị ghi nhớ.

 Kiểu viết : Được NMS dùng để điều khiển các thiết bị. NMS viết giá trị các biến vào bộ nhớ, lưu giữ bên trong các thiết bị

 Kiểu các phép toán traversal : Được NMS dùng để qui định những biến mà thiết bị hỗ trợ cũng như là thu thập các thông tin từ một bảng biến (ví dụ bảng chọn đường trong IP)

 Kiểu bẫy : Được NMS dùng thu thập các sự kiện bất thường từ các thiết bị mạng.

b. Cơ sở dữ liệu quản lý:

Như đã biết, tất cả các đối tượng được quản lý đều được chứa trong MIB. Về bản chất, MIB là một cơ sở dữ liệu của các đối tượng, một MIB được miêu tả như là một cây với các mục dữ liệu riêng, tách rời nhau, mỗi một mục dữ liệu của thông tin trong cây là một nút có nhãn tuân thủ OSI ANS 1 mà ta đã nói trong chương trước. Bản thân MIB dùng đối với SNMP cũng dùng cây MIB này, nó cho trong nhánh 11 của nút MIB II.

Cấu trúc thông tin quản lý (Structure of Management of information - SMI) cho phép dùng kiểu dữ liệu chuẩn ASN.1 với các kiểu như sau: INTEGER, OCTET STRING và OBJECT IDENTIFIER. Ngoài ra nó cũng định nghĩa các kiểu dữ liệu như sau :

- *Network addressers* (Địa chỉ mạng) : Mô tả hay trình bày một địa chỉ của một họ nghi thức điển hình. SNMP V.1 chỉ hỗ trợ loại địa chỉ IP 32 bit

- *Counters* : Kiểu nguyên dương tăng cho đến giá trị lớn nhất thì quay trở lại 0. Tổng số byte nhận được trong một thiết bị giao tiếp mạng là một ví dụ của counter.

- *Gauges* : Kiểu nguyên dương có thể tăng hoặc giảm nhưng luôn duy trì giá trị lớn nhất đã đạt. Ví dụ : độ dài của một hàng đợi cần gửi đi (trong packet) là một ví dụ điển hình của gauges.

- *Time ticks* : Là một bộ đếm thời gian theo đơn vị 1/100 giây

- *Opaque* : mã hóa ngẫu nhiên, được sử dụng để chuyển các thông tin ra ngoài SMI.

c. Các phép toán.

Bản thân SNMPV. 1 là một nghi thức đơn giản vừa yêu cầu vừa đáp ứng. Ta nhắc lại 4 phép toán đã đề cập trong chương II

- *Get* : Lấy thông tin từ một đối tượng mà Agent cung cấp.

- *Getnext* : Lấy thông tin tiếp theo trong bảng hoặc danh sách

-*Set* : Thiết lập tham số cho một đối tượng

-*Trap* : NMS thông báo một vài sự kiện không đồng bộ

d. Định dạng thông báo :

Nội dung thông báo của SNMP V. 1 gồm có hai phần : header và phần dữ liệu (Protocol Data Unit - PDU)

Phần đầu thông báo là header trong đó nội dung có số version và *community name*. *Community name* có hai chức năng : Chức năng trước tiên là định nghĩa môi trường truy nhập cùng dùng chung cho một nhóm các hệ quản trị mạng . Chức năng thứ hai là để xác nhận bởi vì một số thiết bị không đượcSNMP V.1 hỗ trợ nên cần có một biện pháp ngăn ngừa, vì thề Community name được dùng để xác nhận .

Còn phần dữ liệu của nội dung thông báo SNMP V.1 chỉ ra tên phép toán *get, set*,... và các thể hiện của đối tượng của các giao tác này.

PDU định dạng thông báo của SNMP V. 1 như sau :

Request - ID	Error status	Error Index	Variable bindings

Get, getnext, set và response format

Enterprise	Agents Address	Generic Trap Type	Specific Trap code	Time stamp	Variable bindings

Trap format

SNMP Ver. 1. *get, getnext, response* có các trường sau:

+ *Requets ID* : Số hiệu chỉ định kết hợp các yêu cầu với đáp ứng.

+ *Error status* : Báo hiệu trạng thái lỗi và kiểu lỗi.

+ *Error Index* : Kết hợp lỗi với một biến đặc biệt ở trong variable building nói ở phần dưới đây

+ *Variable binding* : chứa dữ liệu của PDU của SNMP V.1. Mỗi *variable bindings* kết hợp một biến đặc biệt với giá trị hiện tại của nó. Biến này sẽ không dùng trong trường hợp yêu cầu là Get, GetNext

Còn dữ liệu bẫy đối với *get, getnext, response* và *set* có khác nhau đôi chút. Chúng có các trường sau :

- *Enterprise* : Chỉ định kiểu đối tượng phát sinh ra bẫy.

- *Agent address* : Cung cấp địa chỉ của đối tượng phát sinh ra bẫy.

- *Generic trap type* : Cung cấp kiểu bẫy tạo ra.

- *Specific trap code* : Cung cấp mã bẫy cụ thể.

- *Time stamp* : Cung cấp tổng số thời gian trôi qua kể từ khi khởi động lại mạng lần cuối tới khi bẫy phát sinh.

- *Variable bindings* : Cung cấp một danh sách các biến với nội dung các thông tin cần quan tâm về bẫy.

3.2. SNMP Version 2. 0 :

Nghi thức quản lý mạng SNMP V.2 là phát triển tiếp theo từ nghi thức quản lý mạng SNMP V.1, vào tháng 7 năm 1992. So với version 1, version 2 có hai đặc điểm mới là cơ chế an ninh và nghi thức quản lý đơn giản (SMP: simple Management protocol).

Cơ chế an ninh không có trong SNMP V.1. Vì vậy thông tin cơ sở trong SNMP V2 không tương thích với thông tin cơ sở trong SNMP V1.

Cộng đồng những người nghiên cứu Internet đã phân tích các đặc tả cho SNMP mới và tich hợp các yếu tố bảo mật cho version SNMP mới Mùa xuân năm 1993 version 2 của SNMP được công bố.

Để hiểu rõ hơn về nghi thức SNMP V. 2 này chúng ta hãy xem chi tiết các đặc điểm của nghi thức như sau :

a. Cấu trúc thông tin quản lý (Structure of Management Information - SMI).

Cấu trúc của thông tin quản lý SNMP V. 2 đã hỗ trợ cho một vài kiểu dữ liệu mới và được đưa vào để tạo lập và xóa dựa trên các hàng ở trong một bảng. Dữ liệu địa chỉ mạng cũng ngoài địa chỉ IP còn hỗ trợ cho địa chỉ OSI NSAP . Về mặt kiểu dữ liệu SNMP V2 đã đưa vào các loại bộ đếm (counter) 64 bit đếm và 32 bit đếm.

Nghi thức SNMP V. 2 đã đưa vào quan niệm về khối thông tin mà chúng cho dùng để liên kết một nhóm các thông tin có liên quan với nhau. Có 3 loại khối thông tin sau:

- *Khối MIB* : chứa định nghĩa các đối tượng quản lý có quan hệ qua lại với nhau.

- *Lệnh quy ước cho khối MIB* Cung cấp cách mô tả các nhóm đối tượng quản lý mà ta bắt buộc phải cài đặt

- *Lệnh thiết lập khả năng để cài đặt các agent.* Các thông tin này định nghĩa chính xác mức hỗ trợ mà một agent có quyền đòi hỏi theo quy cách của MIB (ví dụ mức truy nhập được phép)

b. Các phép toán của nghi thức

SNMP V. 2 định nghĩa thêm 2 phép toán mới như sau :

- Dạng *Inform* : Cho phép một chủ thể quản lý gửi một thông tin kiểu bẫy đến một chủ thể quản lý khác và yêu cầu một đáp ứng.

- Dạng *Getbulk* : Cho phép một chủ thể quản lý đọc các khối dữ liệu lớn một cách hiệu quả hơn, ví dụ như đọc các hàng trong một bảng dữ liệu.

c. Định dạng thông báo trong SNMPV. 2:

Để đơn giản hóa quá trình xử lý PDU thì tất cả các thao tác trừ thao tác *get-bulk* thì tất cả các phép toán khác như get, getnext, set, respond, trap đều dùng chung một định dạng PDU.

Sau đây là định dạng PDU cho *get, getnext, set*, *response* và *trap.*

PDU type	Request ID	Error status	Error Index	Variable bindings

Trong đó các trường của các thao tác như sau :

- *PDU type* : Chỉ định kiểu định dạng PDU, các kiểu đó có thể là *get, getnext, set, response* hoặc *trap.*

- *Request ID* : Một số hiệu kết hợp các yêu cầu với trả lời.

- *Error status* : Cho biết một lỗi và một kiểu lỗi.

- *Error Index* : Kết hợp lỗi với một biến cá biệt ở trong sự liên kết biến.

- *Variable bindings* : Kết hợp biến cá biệt với giá trị hiện tại của nó.

Khi dùng vớii các thao tác *get, getnext, set, trap* và *inform,* các trường *Error status, Error Index* được đặt giá trị 0.

Định dạng PDU cho phép toán getbulk như sau

PDU type	request ID	nonrepeater	Max repeatition	variable binding

trong đó:

-Ba trường PDU type, request ID và variable binding có ý giống như trong thao tác get, getnext, set, response và trap.

-Nonrepeaters: Chỉ định số của biến trong danh sách bó biến, mà nó được trả lại.

-Max-repetition: Đặc tả số của biến tiếp theo được trả lại cho biến còn lại trong danh sách bó biến.

d. Kiến trúc quản lý:

Nghi thức SNMP V. 2 hỗ trợ cho việc quản lý mạng tập trung giống như SNMP V1 cũng như là quản lý mạng theo kiểu phân tán dựa trên MIB mới theo kiểu "từ chủ thể quản lý đến chủ thể quản lý" (from manager to manager ")

Trong một kiến trúc phân tán, một số hệ thống thực hiện với cả hai tư cách : chủ thể quản lý và Agent (Các agent thực tế là các đối tượng bị quản lý) . Khi hoạt động như một Agent thì hệ thống chấp hành các lệnh từ một chủ thể quản lý giám sát. Còn khi đóng vai trò một chủ thể quản lý nó lại có thể ra lệnh cho các agent khác. Hơn nữa các chủ thể quản lý trung gian có thể phát ra một thông tin bẫy tới một chủ thể cấp cao hơn.

Một trong các khiếm khuyết trầm trọng của v.1 là không có cơ chế xác nhận, do đó không hỗ trợ được cho tính bảo mật. SNMP V2 đã khắc phục các khiếm khuyết này bằng cách đưa ra một số quan niệm như sau:

Masquerades: Một thực thể không có quyền, chỉ có thể thi các lệnh nếu có sự ủy quyền của các thực thể có quyền.

Modification of information: Một thực thể có thể thay đổi một thông báo được một thực thể có quyền tạo ra.

Message sequence and timing modification: Nghi thức SNMP V.1 được thiết kế cho vận chuyển không liên kết. Vì vậy SNMP V2 cho phép

một thực thể có thể sắp xếp lại, sao chép, gửi chậm các thông báo thuộc lớp SNMP V.1.

Disclosures: Thông qua việc trao đổi giữa một đối tượng quản lý và một Agent, một thực thể có thể biết được các giá tri của các đối tượng được quản lý và biết được các sự kiện có thể thông báo được.

Một thay đổi trong định dạng thông báo là cho phép nghi thức SNMP V.2 khả năng bảo mật trong việc trao đổi thông báo.

Định dạng thông báo mới trong SMNP V2 gồm ba loại như sau: *không bảo đảm (Nonsecure) :* Định dạng thông báo theo kiểu này không được bảo mật.

Destination	Unused	Destination	Source	Context	PDU

Định dạng thông báo trong trường hợp không bảo đảm

Được xác nhận nhưng không riêng*(Authenticated but not private*):

Nghi thức SNMP V.2 dùng một giá trị bí mật, chỉ chủ thể gửi và chủ thể nhận biết người nhận để xác nhận thông báo. Chủ thể gửi lấy một giá trị bí mật, giá trị này đã được chủ thể nhận biết rồi thực hiện một thuật toán mã hoá digest trên thông báo và ghi đè vào trường digest. Và gửi thông báo đó đi.

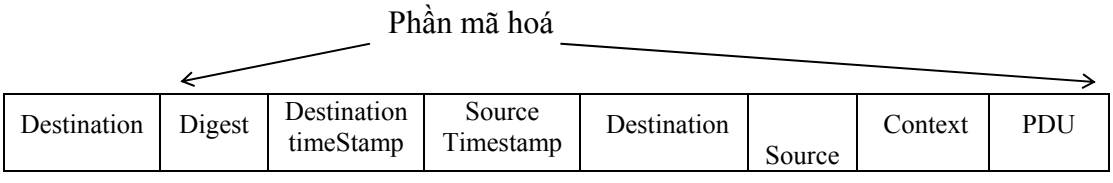
Khi chủ thể nhận được thông báo, nó giải mã lại để so sánh phải chăng thông tin trong trường digest có trùng với số hiệu nó đã biết chưa. Nếu trùng nhau chứng tỏ thông báo đã được xác nhận. Tuy nhiên, phương pháp định dạng này không riêng biệt bởi vì chủ thể nào cũng có thể biết được giá trị bí mật đó.

Destination	Digest	Destination timeStamp	source Timestamp	Destination	Source	Context	PDU

Định dạng thông báo trong trường hợp phải xác nhận nhưng không sử dụng riêng

*Private and authenticated (*có tính chất riêng biệt):

Phương pháp định dạng này thì thông báo sẽ được mã hoá và xác định rõ, có nghĩa là chỉ những người nào có quyền thì mới được sử dụng và nó có tính chất riêng biệt.



Định dạng thông báo trong trường hợp riêng và phải xác nhận

Các trường của kiểu định dạng thông báo SNMP V. 2 như sau:

Destination (nơi đến): Chỉ định đối tượng nhận thông báo. Trường này xuất hiện hai lần trong định dạng thông báo SNMP V.2. ở trường đầu tiên nó không được mã hoá cốt để thông báo không bị che địa chỉ đến. Phần còn lại đực mã hóa.

Source: Chỉ định đối tượng gửi thông báo.

Context: Chỉ định tập hợp tài nguyên của các đối tượng được quản lý bởi nghi thức SNMP V2. Trường *Context* này thay thế cho *community name* trong version 1 của nghi thức SNMP.

PDU: Chỉ định các phép toán quản lý mong muốn trong thông báo.

Digest: Chứa kết quả tính toán của thông báo thuật toán Digest trên một phần của định dạng thông báo đó.

Destination timestamp :Chứa thời gian theo đồng hồ của chủ thể gửi trong lần trao đổi thông báo trước.

Source timestamp: Chứa thời gian theo đồng hồ của chủ thể gửi thông báo.

Thông qua thuật toán xác nhận trong SMNP V2 có thể đảm bảo thông báo đã được gửi và được nhận không bị sửa đổi. Thuật toán digest tính ra một mã digest dài 128 bit trên một phần thích hợp nào đó của thông báo . Sau đó digest vừa tính được gửi kèm theo thông báo . Khi nhận được, chủ thể nhận tính lại digest của thông báo và so sánh với digest nhận được kèm theo thông báo. Nếu thấy trùng nhau thì thông báo nhận được có thể tin cậy được. Timestamp nói trên được xem như dấu ấn thời gian. Nó cho biết có duy trì được hay không đồng bộ về thời gian theo đồng hồ giữa chủ thể quản lý và các agent . Chủ thể nhận có thể căn cứ vào thông tin thời gian để kiểm tra thông báo là mới , hay bị lặp lại.

CHƯƠNG IV.
QUẢN LÝ CẤU HÌNH

Như đã trình bày, quản lý cấu hình là quá trình thu thập các dữ liệu lấy được từ mạng và dùng dữ liệu đó để định hình tất cả các thiết bị và là một trong các khía cạnh quản lý mạng

Quản lý cấu hình bao gồm việc :

- Thu thập các thông tin về cấu hình mạng hiện thời.

- Sử dụng các thông tin đó để sửa đổi (modify) cấu hình mạng :

- Lưu giữ dữ liệu , lập các bảng kiểm kê và sinh ra các báo cáo về tình hình hoạt động của mạng dựa trên các dữ liệu thu thập được.

Trong chương này chúng ta sẽ đề cập đến các lợi ích của quá trình quản lý cấu hình và nêu ra 3 mức công cụ quản lý cấu hình từ đơn giản đến phức tạp.

4. 1. Các lợi ích của quản lý cấu hình :

Lợi ích đầu tiên của công việc quản lý cấu hình là nó có thể tăng cường khả năng kiểm soát thiết bị mạng. Người kỹ sư mạng điều khiển có thể nhanh chóng truy cập tới các dữ liệu cấu hình để có thể thiết lập nhanh chóng cấu hình theo nhu cầu. Điều này càng quan trọng đối với các hệ thống phức tạp.

Xét ví dụ , dữ liệu cấu hình thường chưa cả các thông tin về trạng thái setup hiện thời cho mỗi thiết bị mạng. Giả sử ta cần phải thêm vào một thiết bị giao tiếp mới (một card mạng, một bộ chuyển mạch...) lúc đó ta cần phải biết trước số hiệu của của thiết bị đó về phương diện vật lý. Ta cũng có thể phải biết địa chỉ mạng được gán cho giao diện đó. Các dữ liệu thông tin này sẽ giúp ta xác định cấu hình cho phần mềm trên thiết bị. Với công cụ quản lý cấu hình, ta có thể dễ dàng xác định đúng các thông tin này.

Ví dụ : Xét một thiết bị giao tiếp có lỗi trên segment của LAN. Lúc đó ta có thể dùng công cụ quản lý cấu hình để tạm đình chỉ hoạt động của thiết bị đó (thậm chí có thể làm từ xa). Sau khi xem xét nguyên nhân, giả sử thấy rằng các tham số thiết lập không đúng, ta có thể đặt lại sau đó kích hoạt thiết bị hoạt động trở lại.

- Quản lý cấu hình có thể trợ giúp cho người kỹ sư mạng cung cấp một bảng kiểm kê mới nhất đối với các thành phần mạng. Ví dụ : có bao nhiêu thiết bị thuộc một loại nào đó hiện thời đang tồn tại trên mạng.

Bảng kiểm kê cũng có thể là danh sách các hệ điều hành đang sử dụng trên mạng.

4. 2. Thực hiện quản lý cấu hình :

Quản lý cấu hình bao gồm các bước sau :

- Thu thập các thông tin về môi trường mạng hiện thời : điều này có thể thực hiện một cách thủ công hay tự động. Trong trường hợp thu thập một cách thủ công, người quản trị có thể thất bại chỉ vì mất quá nhiều thời gian mà nguyên nhân lại lac có một lỗi cấu hình đơn giản.

- Dùng dữ liệu đó để sửa đổi cấu hình của thiết bị mạng.

Môi trường dữ liệu mạng là luôn luôn thay đổi. Khả năng để sửa đổi cấu hình hiện thời đó trong trong thời gian thực (Real time) cần thiết. Việc sửa đổi này có thể là thủ công nếu phương pháp thu thập thông tin là thủ công hay tự động nếu phương pháp thu thập thông tin là tự động.

- Dữ liệu thu thập được luôn được lưu trữ, cho phép sinh các bảng kiểm kê mới tất cả các thành phần mạng hay các báo cáo khác về từng thành phần của mạng.

a. Thu thập các dữ liệu một cách thủ công.

Thu nhận thông tin từ mạng thường là bắt đầu với một sự cố gắng bằng một thao tác thủ công. Ta có thể đăng nhập mạng từ xa để tìm mỗi thiết bị trên mạng và sau đó ghi các số serial cũng như địa chỉ của chúng trong một bảng tính hoặc trong file văn bản. Sẽ rất tốn thời gian và khó khăn để theo dõi và ghi nhận thường xuyên cấu hình mạng. Đó là chưa kể công việc này rất đơn điệu và buồn tẻ.

Thực ra để cho dễ theo dõi ta có thể sắp xếp các bảng này để dễ dàng tra cứu. Nhưng điều đó lại đòi hỏi ta phải thường xuyên xem xét lại danh mục các thiết bị mới và sắp xếp lại.

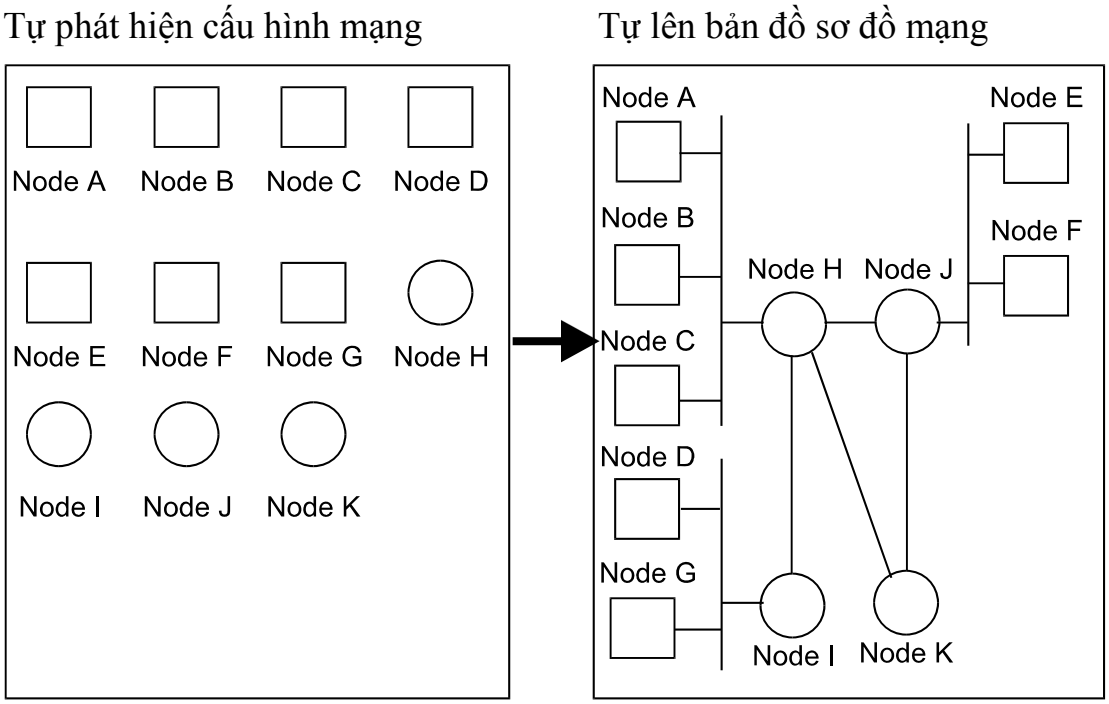
Việc thu thập số liệu thủ công đặc biệt khó khăn khi mạng phức tạp.

b. Thu thập tự động

Các công việc khó khăn của việc thu thập các thông tin và cập nhật dữ liệu cấu hình có thể được loại trừ nếu dùng các phương pháp tự động. VD : người kỹ sư có thể dùng một nghi thức quản lý mạng để lấy các dữ liệu đều đặn về các thiết bị mạng và tự động ghi lại các dữ liệu đó trong thiết bị nhớ.

Một công cụ khác ta có thể dùng là được công cụ tự phát hiện (Auto-discovery), cho phép sinh ra một danh sách tất cả các thiết bị hiện có trên mạng. Thông qua bộ tự phát hiện cũng có thể tạo ra một sơ đồ

hình học (graphical map) của mạng hiện thời đang dùng với một quá trình được gọi là tự động vẽ sơ đồ (automapping).



c. Sửa đổi dữ liệu cấu hình.

Thông tin quản lý cấu hình cần được cập nhật thường xuyên. Xét trường hợp một mạng có 5000 nút. Nếu chỉ cần1% các máy đó phải đặt địa chỉ một tuần thì người kỹ sư đã phải thực hiện tới 50 sửa đổi trong một tuần. Thế mà vấn đề cấp địa chỉ chỉ là một phần trong những công việc thiết lập cấu hình. Khi setup một thiết bị có khi phải đặt đến một tá tham số. Ta thấy rằng khó có thể làm công việc này một cách thủ công ngoại trừ khi các kỹ sư thực hiện từng bước để ghi lại các bước thực hiện của họ. Nếu các thay đổi của cấu hình sẽ không được lưu giữ có thể dẫn tới sự lộn xộn, rắc rối khi mà một người kỹ sư mạng khác kiểm tra cấu hình của thiết bị đã được thay đổi.

Nếu hệ quản lý cấu hình cho phép thay đổi cấu hình thiết bị trên toàn bộ hệ thống quản lý mạng thì các thay đổi đó có thể được ghi lại tự động trước khi chúng được gửi cho thiết bị. Một lợi ích khác khi quản lý tự động là hệ thống có thể xác định những thay đổi cấu hình nào là thích hợp với thiết bị mạng và phải báo cho người kỹ sư trước khi anh ta vô tình định dạng sai thiết bị.

d. Lưu giữ các thông tin :

Quản lý cấu hình cũng phải cung cấp một phương tiện cho để lưu giữ các thông tin. Một hệ quản lý có hiệu quả phải lưu trữ toàn bộ cấu hình của một dữ liệu mạng tại một vị trí trung tâm, mà ở đó người kỹ sư mạng có thể truy nhập được một cách nhanh chóng các dữ liệu cấu hình. Các thông tin này được lưu giữ vào trong một notebook hoặc là một bảng tính trên một máy PC tại trung tâm điều khiển mạng.

- Một dạng chung nhất để lưu giữ các thông tin cấu hình trong bộ nhớ của máy tính là các file dạng ASCII, dạng này có ưu điểm là dễ đọc và cấu trúc của các file đó thường là dễ hiểu và dễ quản lý. Hầu như các chương trình ứng dụng có khả năng đọc được các file ở dạng mã ASCII này. Tuy nhiên giải pháp này không phải là hoàn toàn tốt. Các tệp ASCII thường có kích thước lớn. Hơn nữa việc tìm kiếm thông tin trên tệp ASCII thường là phải duyệt nên sẽ mất thời gian hơn theo kiểu lưu trữ có cấu trúc. Một khiếm khuyết nghiêm trọng của dạng ASCII này là khó cung cấp những mối liên hệ phức tạp.

Vì các file ở dạng mã ASCII có những thiếu sót hay bất lợi trong việc lưu trữ và sử dụng thông tin nên để đạt được hiệu quả tốt sau này người ta thường dùng các hệ quản trị cơ sở dữ liệu quan hệ (RDBMS : Relational Database Management System), một RDBM thường có nhiều lợi thế hơn các file dạng ASCII trong lưu trữ dữ liệu.

 Nó lưu trữ dữ liệu hiệu quả, cho phép 1 số lượng lớn dữ liệu lưu trữ trên một máy.

 Nó lưu trữ dữ liệu trên khuôn dạng của nó, điều đó cho phép tìm kiếm nhanh các dữ liệu riêng biệt.

 Nó có thể sắp xếp một cách tự động các dữ liệu lưu giữ theo nhiều cách khác nhau.

 Nó có thể khôi phục tự động các dữ liệu bị mất.

 Nó cho phép người dùng liên kết nhiều kiểu dữ liệu khác nhau.

4.3. Quản lý cấu hình trên một hệ quản lý mạng.

Công cụ quản lý cấu hình có thể trợ giúp cho kỹ sư mạng đạt hiệu quả tốt trong việc quản lý bằng cách :

 Tự động thu thập và cập nhật dữ liệu trên thiết bị mạng.

 Cung cấp dữ liệu cấu hình cho bộ nhớ trung tâm.

 Cho phép sửa đổi dữ liệu mạng.

 Dễ dàng sinh ra các báo cáo.

Để quản lý cấu hình một hệ quản lý mạng chúng ta xét 3 kiểu công cụ từ đơn giản đến phức tạp sau.

a. Công cụ đơn giản:

Một công cụ quản lý cấu hình đơn giản ít nhất là phải cung cấp đầy đủ các thông tin của mạng để lưu giữ một cách tập trung. Các thông tin đó bao gồm sự gán địa chỉ trên mạng, các số hiệu thiết bị (serial number), địa chỉ vật lý và các dữ liệu khác về thiết bị. Một công cụ đơn giản cũng có thể cung cấp một phương tiện quan trọng khác là tìm kiếm. Chức năng tìm kiếm này cho phép người kỹ sư mạng xác định được các thông tin một cách dễ dàng trong việc quản lý cấu hình.

b. Công cụ phức tạp hơn :

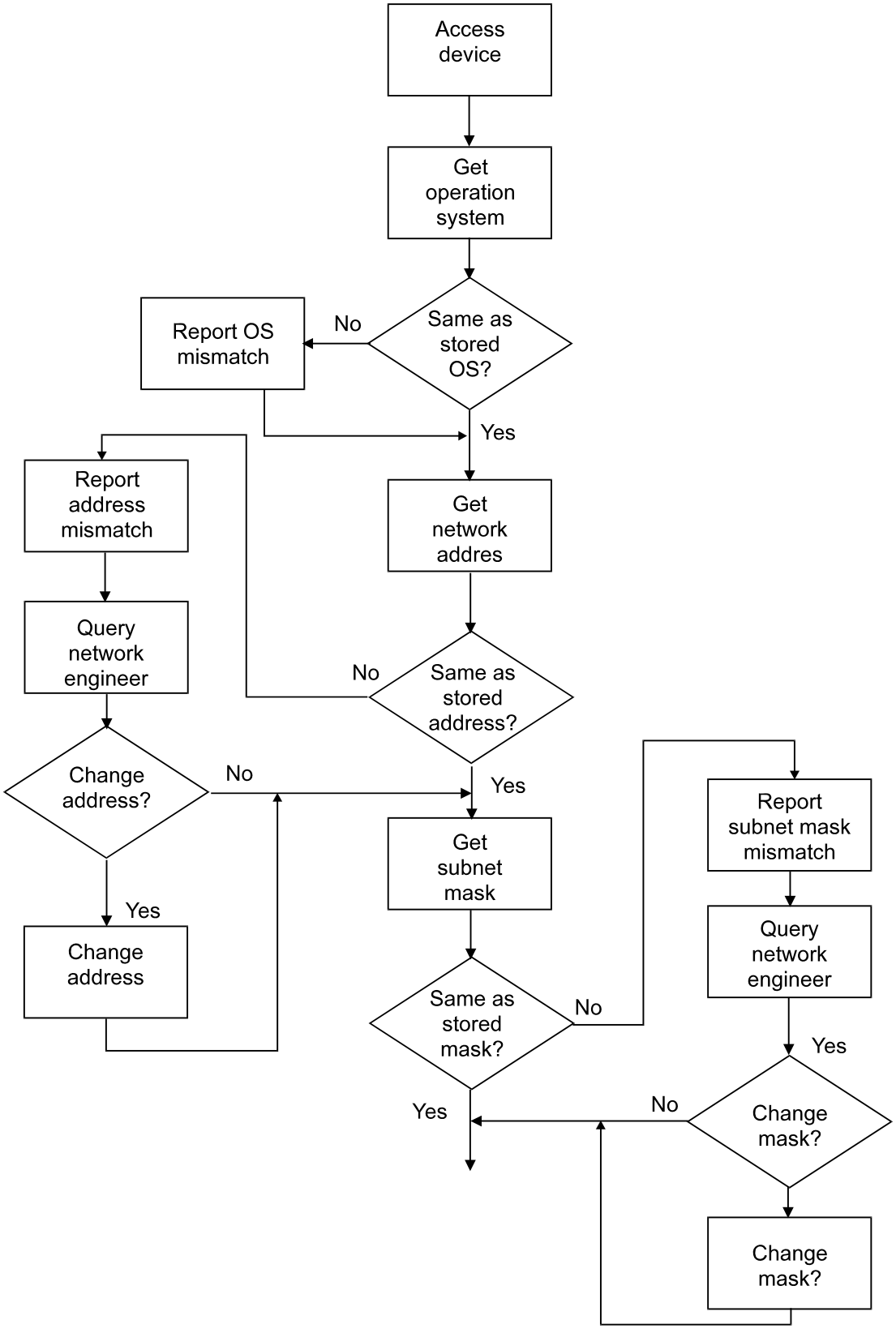
Một công cụ đơn giản đôi khi chỉ giải quyết hoặc quản lý được một số cấu hình đơn giản. Còn đối với những cấu hình phức tạp thì phải dùng đến công cụ phức tạp hơn để quản lý. Công cụ phức tạp hơn có thể được phát triển bằng cách thêm vào các đặc điểm thu thập tự động và lưu giữ các thông tin từ tất cả các thiết bị mạng. Công cụ phức tạp này cũng phải có thể so sánh cấu hình hiện tại của thiết bị với cấu hình đã nhớ. Công cụ phức tạp này cũng có thể cho phép người kỹ sư mạng thay đổi cấu hình đang chạy của thiết bị và quyết định giống như công cụ đơn giản. Một version phức tạp hơn sẽ phải cung cấp việc lưu trữ các dữ liệu vào bộ nhớ, tập hợp tất cả các dữ liệu vào bộ nhớ trung tâm và dễ dàng cho phép khôi phục lại hoặc lấy các dữ liệu một cách dễ dàng hơn.

Có thể đưa ra một số các đặc điểm của công cụ loại này như sau :

- Đặc điểm tự động thu nhận dữ liệu của công cụ quản lý cấu hình là một đặc điểm rất quan trọng bởi vì công cụ này cho phép người kỹ sư so sánh tự động một cấu hình đang chạy với cấu hình lưu giữ và cũng có thể cho phép thay đổi cấu hình hoặc chế độ làm việc tự động của cấu hình thiết bị đó. Công cụ còn kiểm tra xem cấu hình cài đặt của thiết bị có khác với cấu hình đã được lưu giữ không nếu như công cụ tìm thấy sự khác nhau thì có thể hỏi người kỹ sư có cần thay đổi cấu hình thiết bị hay không ?

Tuy nhiên để làm việc trong các môi trường khác nhau của mạng thì công cụ sẽ phải cung cấp các phương tiện khác nhau mà người kỹ sư có thể định rõ các lỗi cấu hình nào phát sinh thông báo lỗi và có thể nhắc nhở với một lời cảnh báo. Ví dụ một server cho terminal có khả năng làm việc được với nhiều thiết bị có tốc độ truyền khác nhau đang được đặt tốc độ truyền ở 9600 bps nhưng thiết bị chỉ làm việc ở tốc độ 2400 bps. Trong trường hợp này chỉ cần thông báo để người quản trị mạng biết. Ngược lại nếu công cụ phát hiện ra rằng một đường bảo mật nối với server cho terminal không được đặt mật khẩu, nó phải báo động cho

người quản trị và đặt lại cấu hình cho phù hợp. Ở đây đã có sự can thiệp để đặt lại cấu hình. Hình sau :



c. Công cụ cao cấp :

Công cụ ở mức nói trên chỉ có thể cho phép thay đổi cấu hình đang dùng của một thiết bị. Một công cụ cao cấp sẽ có có hiệu quả cao hơn nhiều nếu như nó dùng một cơ sở dữ liệu quan hệ (RDBMS) để lưu giữ, thiết lập quan hệ, hỏi, và kiểm kê thông tin mạng. Để hoạt động tối ưu, công cụ này cần có thể có khả năng đánh giá các cấu hình của thiết bị.

- Khả năng của công cụ cao cấp này cho phép thiết lập quan hệ giữa một tập dữ liệu này quan hệ với một tập dữ liệu khác là rất quan trọng để quản lý cấu hình.

- Một RDBMS không chỉ cho phép thao tác các dữ liệu phức tạp mà còn cho phép hỏi các dữ liệu phức tạp. Các câu hỏi đó thường viết bằng ngôn ngữ hỏi có cấu trúc (SQL: structured query language). dùng SQL người kỹ sư có thể tìm các thông tin được lưu trong cơ sở dữ liệu. Ví dụ người quản trị phát hiện ra version A của một phần mềm chạy trên cầu Ethernet đang gây lỗi. Để sửa chữa tình trạng này, ta cần tìm ra tất cả các cầu khác cũng chạy version này. Có thể hỏi bằng một câu hỏi trên một bảng tên là DEVICES như sau:

SELECT * FROM DEVICES WHERE TYPE = Bridge AND Software = A

SQL còn có khả năng sinh ra các báo cáo kiểm kê. Các báo cáo này có thể là:

- Báo cáo về số hiệu thiết bị.
- Nhà sản xuất và model.
- Hệ điều hành.
- Khả năng của RAM.
- Địa chỉ mạng.
- Khả năng thiết bị.

Ví dụ có thể sinh một báo cáo bằng câu hỏi SQL sau đây:

SELECT Devices, sn FROM devices, vendos WHERE vendors.name = Banzai AND devices.month <= 11

Kết quả ta sẽ được danh sách các thiết bị trong mạng do hãng Banzai cung cấp và vẫn còn trong hạn bảo hành trong vòng một năm.

Như vậy có thể chỉ ra các đặc trưng của một hệ quản trị cấu hình tiên tiến là:

 Có khả năng tự động lưu trữ các thông tin cần thiết.

 Có khả năng so sánh cấu hình để sửa đổi cấu hình.

 Có khả năng xử lý câu hỏi.

 Có khả năng đánh giá cấu hình.

Bây giờ ta xét kỹ hơn chức năng cuối cùng.

Việc đánh giá cấu hình cần thực hiện định kỳ, nó có thể phát hiện những vấn đề đại loại như địa chỉ được gán trùng nhau, các chức năng đã được sử dụng. Giả sử như một LAN đã được mở rộng. Trong LAN có nhiều server. Khi đó một công cụ quản trị tiên tiến cần phát hiện được và báo lại cho người quản trị ví dụ như có 2 server cùng cung cấp một loại dịch vụ, điều đó có thể gây trùng chéo.

Một ví dụ khác, công cụ quản trị có thể tính toán khả năng truyền thông của cấu hình mạng. Thiết bị của mạng rộng như bộ điều khiển cluster và các bộ xử lý đòi hỏi đặt lại cấu hình các thiết bị kết nối để đạt tốc độ cao trong truyền thông.

d. Sinh báo cáo cấu hình.

Ta đã biết, sinh báo cáo cấu hình là điều không bắt buộc nhưng rất nên có trong các hệ quản trị cấu hình mạnh. ít nhất thì một số các lỗi cấu hình quan trọng như sự kiện như trùng địa chỉ phải được báo cáo. Có thể chức năng trình bày trên giao diện đồ hoạ với mầu là không bắt buộc nhưng toàn bộ khả năng sinh báo cáo có thể kiểm soát được từ một terminal text.

Một kiểu báo cáo phải làm chi tiết cấu hình chung của mỗi nút mạng như tên, địa chỉ, số hiệu thiết bị, nhà sản xuất, hệ điều hành, người bảo trì. Một vài thông tin phụ như tên nhà cung cấp, địa chỉ vật lý của thiết bị cũng nên có. Tần số sinh báo cáo có thể là hàng tuần, hàng tháng tuỳ theo tính trạng ổn định của mạng.

Một báo cáo khác cần có liên quan đến lần sửa đổi cấu hình mạng gần nhất như danh sách các thiết bị mới và các thiết bị có thay đổi cấu hình, ai thay đổi và thay đổi khi nào.

Cuối cùng, cần có một bản kiểm kê tóm tắt về toàn bộ mạng gồm danh sách các thiết bị mạng với các thông tin về số hiệu thiết bị , vị trí vật lý, ngày cung cấp dịch vụ, bảo hành, lịch sử nâng cấp... Bản này có thể sinh không cần thiết phải định kỳ.

KẾT LUẬN

Như đã thấy, tầm quan trọng của quản lý mạng là nâng cao hiệu quả sử dụng mạng, cho phép phát hiện và xử lý lỗi, quản lý tốt an ninh mạng.

Đối với tôi, đây là một vấn đề khá mới mẻ so với kiến thức được trang bị trong các giáo trình về mạng vì nó vừa là vấn đề kỹ thuật, vừa là vấn đề chuẩn nên chắc chắc bản luận văn còn nhiều khiếm khuyết. Hy vọng rằng đây cũng chỉ là bước đầu để chuẩn bị cho những bước tiếp theo.

Một lần nữa tôi xin cảm ơn các thầy, cô giáo trong khoa Công nghệ Thông tin, đặc biệt là thầy Đào Kiến Quốc và thầy Nguyễn Nam Hải. Tôi cũng xin cảm ơn các bạn cùng làm việc trong nhóm làm luận văn về Intranet của khoa Công nghệ Thông tin.

TÀI LIỆU THAM KHẢO

[1]. Karen Fang Allan Leinwand. Network Management A Practical Perspective.

[2] Network Management System Protocol.

[3] Smoot Carl-Mitchell, John S. Quarterman. Practical Internetworking with TCP/IP and UNIX.