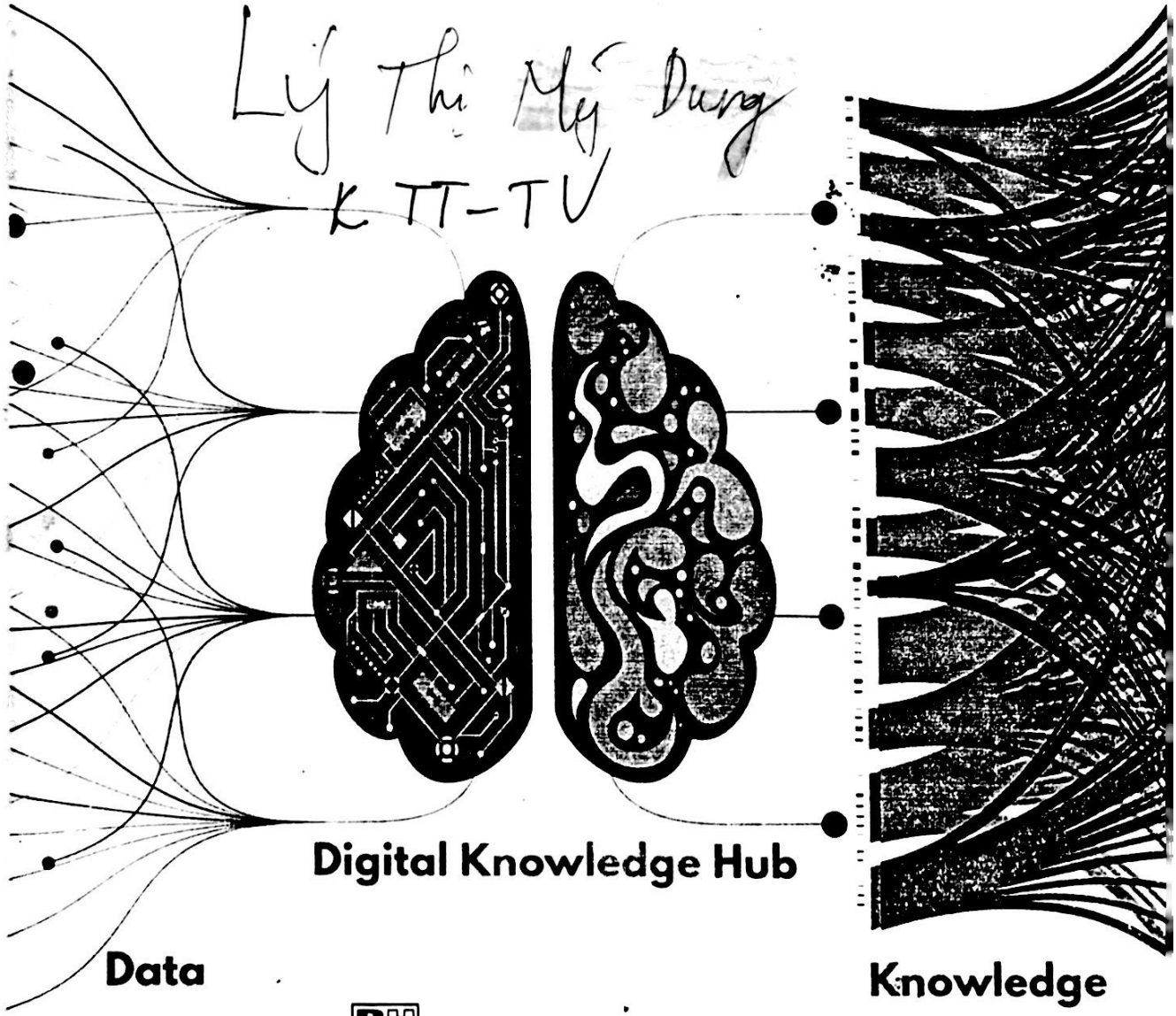
+ITQGia

① PHÁT TRIỂN MÔ HÌNH TRUNG TÂM TRI THỨC SỐ CHO CÁC THƯ VIỆN VIỆT NAM

Lý Thị Mỹ Dung
KTT-TV



NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA HÀ NỘI

GIẢI PHÁP KỸ THUẬT QUẢN LÝ MẠNG INTERNET VỚI VIỆC PHÁT TRIỂN TRUNG TÂM TRI THỨC SỐ TRONG THƯ VIỆN HIỆN NAY

Lý Thị Mỹ Dung*

Tóm tắt: *Những năm gần đây, việc phát triển nguồn tài nguyên số trong hệ thống thư viện trên cả nước ngày càng được đầu tư đáng kể. Các thư viện đang nỗ lực đẩy mạnh ứng dụng công nghệ thông tin nhằm đáp ứng nhu cầu sử dụng mạnh mẽ của người dùng tin trực tuyến hiện nay. Vì thế việc liên kết, chia sẻ thông tin giữa các thư viện là hết sức cần thiết, giúp người dùng được nhiều tài liệu quý giá mà không phải thư viện nào đưa ra một giải pháp kỹ thuật quản lý tập chung giúp cho việc kết nối hạn và đẩy*

17. the
A: Schema.
gue. The stra-
wledge: A collec-
18. Liy
tion and
management
19. Mehta, N. (2008),
global software cos.
20. Miltiadis, D. L., & Ath
edge management prin
intensive organizations: pr
yond. *The Learning Organisatio*.
21. Nonaka, I., & Takeuchi, H. (1995),
nese companies create the dynamics of in.

i học, giáo dục,
i rất lớn phục vụ
g với sự phát triển
; đang dần chuyển
; nhu cầu của người
lịnh và khai thác dữ
iần mềm và hệ thống

in hóa Hà Nội.

quản trị mạng. Có một số mô hình khả thi kèm theo các giải pháp thực hiện việc quản trị mạng TCP/IP như: HP Open-View Network Node Manager, Salawinds, Ciscoworks Network Connectivity Monitor, giúp cho việc giám sát chất lượng mạng trên cơ sở giao thức ICMP và SNMP, tạo được tính chủ động cho việc theo dõi và điều chuyển lưu lượng mạng kịp thời đảm bảo chất lượng dịch vụ truyền tải dữ liệu trong thư viện số hiện nay. Các giao thức trên đóng vai trò chẩn đoán tình trạng của mạng và giúp cho các chuyên gia có được những cảnh báo và đưa ra các giải pháp khắc phục kịp thời, đảm bảo hoạt động của hệ thống thư viện số luôn thông suốt, tránh tình trạng nghẽn mạng, không tìm được tài liệu hoặc không kết nối, lưu trữ, chia sẻ được tài liệu.

2. GIAO THỨC SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) TRONG QUẢN TRỊ MẠNG

Hiện nay các thư viện trên thế giới đã sử dụng hệ thống kết nối mạng lưới thư viện toàn cầu, còn ở Việt Nam mới đang dần hình thành ở những thư viện lớn. Các dịch vụ thư viện trực tuyến ngày càng phát triển như dịch vụ hướng dẫn tìm tin theo chủ đề, môn loại (LibGuides) giúp bạn đọc tiếp cận tài liệu một cách nhanh nhất. Việc quản lý truy cập theo địa chỉ IP giúp việc tạo và quản lý trực tuyến được dễ dàng. Và còn nhiều dịch vụ khác như công cụ thống kê các dịch vụ thư viện, hỗ trợ, tương tác với bạn đọc, quản lý thư viện với người dùng tin,... Như vậy, nhà quản lý về thư viện cần nắm được tình hình hoạt động của hệ thống thư viện số như thế nào? Mức độ truyền tải cở sở dữ liệu đến đâu? Dưới đây chính là giải pháp tối ưu cho việc quản lý này: Tất cả các thiết bị mạng quản lý được chạy giao thức Simple Network Management Protocol (SNMP). SNMP cung cấp một cơ chế cho việc lưu trữ dữ liệu mạng trong một cơ sở dữ liệu phân cấp trên các thiết bị mạng, và là một giao thức để truy vấn cơ sở dữ liệu từ một thiết bị từ xa.

Tất cả các thiết bị SNMP bao gồm một cơ sở thông tin quản lý chung (MIB _ Management Information Base) lưu trữ thông tin cơ bản về lưu lượng truy cập trên thiết bị. Những thông tin này bao gồm các byte truyền đi và nhận trên mỗi giao diện, số lượng và các loại lỗi trên các giao diện, và mức độ sử dụng mạng trên mỗi giao diện. Thông tin

này là vô giá để xác định chất lượng mạng trên các phân đoạn khác nhau của mạng.

Ngoài các đối tượng MIB cơ sở dữ liệu chung, hầu hết các thiết bị SNMP cũng bao gồm các đối tượng MIB độc quyền theo dõi thông tin cụ thể cho các thiết bị mạng. SNMP cung cấp một trong những cơ sở dữ liệu phân cấp cho các công ty để tạo ra các mục riêng của họ để theo dõi thông tin cụ thể đến các thiết bị mạng của họ. Khu vực cơ sở dữ liệu này được gọi là MIB doanh nghiệp. Truy xuất vào MIB doanh nghiệp thường được kiểm soát bởi các tên cộng đồng SNMP. Một tên cộng đồng là một mật khẩu được sử dụng để cấp quyền truy cập đến các phần cụ thể của cơ sở dữ liệu MIB. Khi sử dụng SNMP để truy vấn các thiết bị mạng, bạn phải biết được đúng vị trí giá trị về thông tin chất lượng mạng.

Cơ sở dữ liệu chung MIB cung cấp nhiều dữ liệu chất lượng mạng cơ bản được sử dụng để theo dõi chất lượng của một thiết bị mạng. Phiên bản thứ hai của cơ sở dữ liệu chung MIB (được gọi là MIB-2) đã được cập nhật các số liệu thống kê lỗi cho các thiết bị mạng. Các đối tượng cơ sở dữ liệu MIB-2 cung cấp nhiều trường hữu ích có thể được sử dụng để xác định lượng lưu lượng truy cập mạng và các lỗi trên một thiết bị mạng. Truy vấn các giá trị này có thể cung cấp cho bạn rất nhiều thông tin liên quan đến lưu lượng mạng trên thiết bị.

Hầu hết giá trị MIB-2 là những bộ đếm liên tục. Ví dụ, đối tượng ifInOctets đếm số byte (octet) nhận được trên giao diện kể từ khi nó được hỗ trợ (hoặc cơ sở dữ liệu MIB-2 đã được thiết lập lại). Giá trị này có thể đạt được một giá trị tối đa, và sau đó quay về không và bắt đầu lại từ đầu. Để xác định tốc độ dữ liệu, hầu hết các công cụ đo chất lượng mạng truy vấn các giá trị trong khoảng thời gian cụ thể ngoại trừ sự khác biệt. Cần phải cẩn thận khi làm điều này, để đảm bảo rằng giá trị không trở về không giữa các lần đo, ảnh hưởng đến dữ liệu kết quả.

Các thiết bị mạng có nhiều cổng (như switch và hub) duy trì một bảng MIB-2 riêng biệt cho mỗi giao diện trên thiết bị, như một hệ thống toàn bảng MIB-2. Các bảng cổng riêng biệt được truy cập bằng cách lập chỉ mục đặc biệt trong giá trị MIB. Mục "Sử dụng thiết bị mạng" mô tả làm thế nào cho một kỹ thuật phổ biến được sử dụng để thu thập dữ liệu chất lượng mạng là theo dõi lưu lượng đang tồn tại trên mạng. Rất

nhiều thông tin có thể được thu thập từ mạng chỉ bằng cách theo dõi các gói tin đang di chuyển giữa các thiết bị mạng.

Để nắm bắt tất cả các lưu lượng đang di chuyển trên mạng, giao diện mạng của thiết bị phải được đặt ở chế độ phức hợp (promiscuous mode). Mặc định, một giao diện mạng chỉ chấp nhận các gói tin đã được chỉ định cho thiết bị, hoặc được gửi ra trên một địa chỉ multicast hoặc broadcast. Chế độ Promiscuous cho phép giao diện mạng đọc tất cả các gói tin trên mạng, bất kể điểm đến của chúng. Tính năng này cho phép các thiết bị mạng để kiểm tra từng gói tin trên mạng, không quan tâm nó đến từ đâu, và nó được gửi từ đâu.

Sau khi các gói dữ liệu mạng đã được nắm bắt, chúng phải được giải mã và phân tích để xem những xu hướng và /hoặc các vấn đề tồn tại trên mạng. Một vài mục có thể được chỉ ra bằng cách phân tích lưu lượng mạng là:

- Gói tin được gửi lại;
- Kích cỡ cửa sổ Frozen TCP;
- Tấn công Broadcast (Broadcast storms);
- Quảng cáo mạng (Network advertisements);
- Các ứng dụng tán gẫu (CHAT);
- Các ứng dụng về chất lượng dịch vụ.

Mỗi mục này có thể tiềm ẩn một vấn đề về chất lượng mạng và nên được xem xét trong việc giám sát mạng, để truy cập thông tin này bằng cách sử dụng các công cụ mạng SNMP.

SNMP (Simple Network Management Protocol): là giao thức được sử dụng rất phổ biến để giám sát và điều khiển thiết bị mạng như switch, router... Với các hệ thống mạng lớn, như hệ thống thư viện số trong các hệ thống mạng của các nhà cung cấp dịch vụ với mô hình quản lý tập trung thì việc sử dụng SNMP dường như là bắt buộc. Giao thức SNMP được thiết kế để cung cấp một phương thức đơn giản để quản lý tập trung mạng TCP/IP. Nếu muốn quản lý các thiết bị từ 1 vị trí tập trung, giao thức SNMP sẽ vận chuyển dữ liệu từ client (thiết bị mà đang giám sát) đến Server nơi mà dữ liệu được lưu trong log file

nhằm phân tích dễ dàng hơn. Các phần mềm ứng dụng dựa trên giao thức SNMP như: MOM của Microsft và HP Openview v.v...

Bản chất của SNMP là tập hợp một số lệnh đơn giản và các thông tin mà lệnh cần thu thập để giúp người quản trị thu thập dữ liệu và thay đổi cấu hình của các thiết bị tương thích với SNMP. Ví dụ, SNMP có thể dùng để kiểm tra tốc độ hay ra lệnh shutdown một cổng Ethernet, theo dõi nhiệt độ của switch và cảnh báo khi nó lên quá cao.... SNMP có thể quản trị rất nhiều thiết bị, từ phần cứng đến phần mềm như Web Server hay cơ sở dữ liệu, từ thiết bị đắt tiền như router đến một số hub rẻ tiền, hay các hệ thống Unix, Windows, các máy in, nguồn điện... miễn là các thiết bị đó hỗ trợ SNMP. Các thiết bị được gọi là hỗ trợ hay tương thích SNMP tức là nó được cài đặt một phần mềm để có thể thu thập một số thông tin và trả lời các yêu cầu của người quản trị.

Giao thức Simple Netwok Management Protocol (SNMP) ra đời vào năm 1988 để đáp ứng đòi hỏi cấp bách về một chuẩn chung cho quản trị mạng Internet. SNMP cung cấp cho người dùng một tập các lệnh đơn giản nhất để có thể quản trị được các thiết bị từ xa. Được phát triển từ giao thức Simple Gateway Monitoring Protocol (SGMP), SNMP đã được mở rộng cho phù hợp với các yêu cầu của một hệ thống quản trị mạng đa dụng. Ban đầu, SNMP chỉ được xem như là một giải pháp tạm thời cho việc quản trị các mạng máy tính dựa trên nền TCP/IP trong khi chờ đợi chuyển hẳn sang một giao thức dựa trên kiến trúc mạng của OSI.

Các hoạt động và quy cách dữ liệu của SNMP được chỉ định dựa trên các tiêu chuẩn được đưa ra trong các bộ RFC (Request For Comment) và hiện chúng vẫn đang được phát triển. Trong số các RFC xây dựng nên chuẩn SNMP, có ba bộ tiêu chuẩn quan trọng được dùng làm cơ sở cho SNMP.

• RFC 1156 - Cấu trúc và định danh của các thông tin quản trị của Internet trên nền TCP/IP (Structure and Identification of Management Information for TCP/IP based Internets).

• RFC 1157 - A Simple Network Management Protocol (SNMP).

• RFC 1213 - Cơ sở thông tin quản trị mạng cho Internet trên nền TCP/IP (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II).

Phiên bản đầu tiên của SNMP (SNMPv1) ra đời năm 1988 được quy định trong RFC 1157. Ở phiên bản đầu tiên này, tiêu chí của SNMP đúng như tên gọi của nó, đó là sự đơn giản trong thực thi [Stallings 96]. Đó là lý do chính khiến cho tính bảo mật trong SNMPv1 rất lỏng lẻo, phụ thuộc vào một xâu chia sẻ tương tự như mật khẩu ở dạng thuần văn bản gọi là "commutitiy string". Điều này cho phép tất cả các ứng dụng SNMP nếu biết xâu này có thể truy cập thông tin quản trị trên thiết bị.

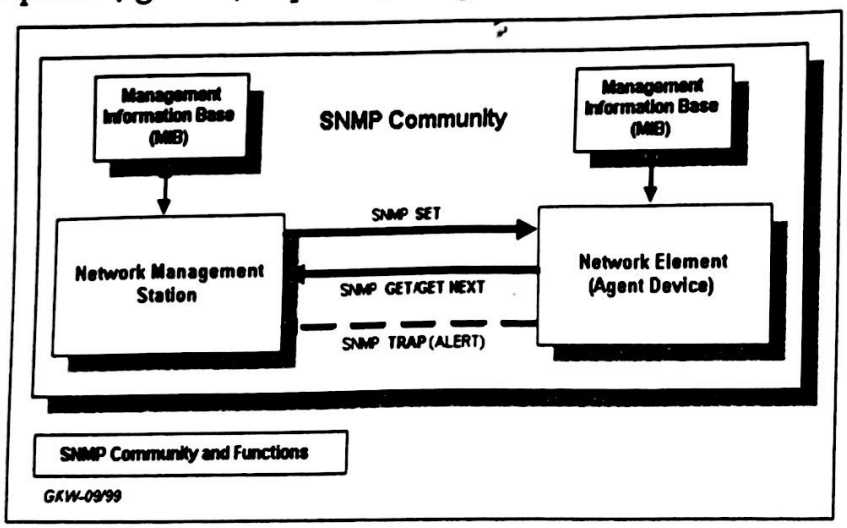
Mặc dù chuẩn SNMPv1 đã thuộc về quá khứ (historical standard) nhưng hiện nay nó vẫn là phiên bản mà rất nhiều các nhà sản xuất hỗ trợ. Phiên bản tiếp theo của SNMP là SNMPv2 hay SNMPv2c. Được quy định trong RFC 3416, RFC 3417 và RFC 3418, SNMPv2 thêm các khuôn dạng dữ liệu, các MIB và PDU mới, làm tăng khả năng cho giao thức.

Tuy nhiên hai phiên bản đầu tiên này của SNMP vẫn thiếu các tính năng bảo mật, xác thực cần thiết nên vẫn có thể dễ dàng bị khai thác. SNMPv3 là phiên bản cuối cùng, chủ yếu tăng cường bảo mật trong quản trị mạng [Stallings 98]. Phiên bản này hỗ trợ giao thức xác thực mạnh và kênh giao tiếp được mã hóa giữa các thực thể được quản trị. Năm 2002, phiên bản này được chuyển từ bản thảo sang thành chuẩn, bao gồm các RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418, và RFC 2576. Vì SNMPv3 là chuẩn mới được công bố, do vậy chỉ có một số hãng lớn như Cisco mới hỗ trợ SNMPv3. Tuy nhiên với nhu cầu ngày càng cao của bảo mật trong quản trị mạng, sẽ có thêm ngày càng nhiều các hãng hỗ trợ SNMPv3 trong các sản phẩm của mình.

Trong kiến trúc của SNMP có hai loại thực thể là manager và agent. Manager là Server chạy một phần mềm có khả năng điều khiển các công việc quản trị cho một mạng. Manager thường được gọi là trạm quản trị - Network Management Station (NMS). Trong một mạng, trạm quản trị chịu trách nhiệm thăm dò (polling) và nhận các trap từ agent. Thăm dò là hành động truy vấn một agent (router, switch, Server Unix...) yêu cầu một số thông tin. Các thông tin này được trạm quản trị lưu trữ, phân tích và hiển thị. Trap cho phép agent thông báo cho trạm quản trị nếu có điều gì đó vượt khỏi phạm vi cho phép xảy ra. Khi nhận được trap, tùy theo thông tin mà trap cung cấp, trạm quản trị sẽ thực hiện một số thao tác đã được cấu hình từ trước. Chẳng hạn,

nếu đường T1 kết nối ra Internet có sự cố, ngay lập tức router gửi trap cho trạm quản trị, khi đó trạm quản trị có thể thực hiện hành động như thông báo lại cho người quản trị.

Thực thể thứ hai là agent, là một phần mềm nhỏ chạy trên thiết bị được quản trị [SnmpFAQ]. Nó có thể là một chương trình độc lập như một tiến trình daemon trong Unix, có thể là thành phần tích hợp bên trong hệ điều hành như IOS của router Cisco hay là hệ điều hành cấp thấp điều khiển UPS. Agent cung cấp thông tin về rất nhiều hoạt động của thiết bị. Ví dụ, agent trong router có thể theo dõi trạng thái up/down của các interface. Trạm quản trị có thể truy vấn trạng thái của các interface này và thức hiện các hành động tương ứng nếu interface down. Hoặc là nếu agent được cấu hình để có khả năng nhận biết một số sự kiện xấu, agent có thể gửi trap đến trạm quản trị, nơi mà các tác vụ tương ứng sẽ được thực hiện. Một vài thiết bị. Hình dưới minh họa mối quan hệ giữa trạm quản trị và agent.



Hình 1: Mối quan hệ giữa manager và agent

(Nguồn: https://www.keil.com/support/man/docs/rlarm/rlarm_tn_using_snmp.htm)

Chú ý là trap và thăm dò có thể xảy ra đồng thời. Không có hạn chế gì về thời điểm trạm quản trị có thể thăm dò agent và thời điểm agent gửi trap.

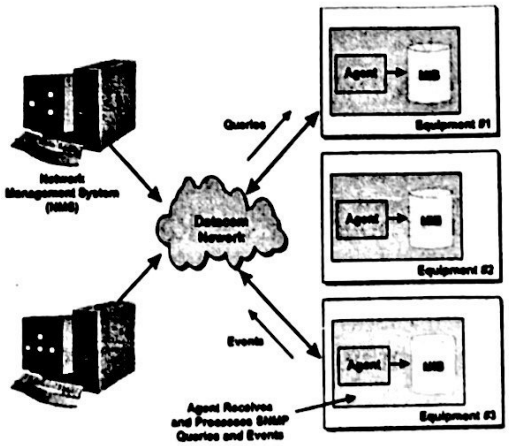
Mô hình SNMP của một hệ thống quản trị mạng bao gồm bốn thành phần trọng yếu (các thành phần này được mô tả ở hình 2):

- Trạm quản trị;
- Thực thể bị quản trị (node hay Network Element - NE);
- Cơ sở thông tin quản trị;
- Giao thức quản trị.

Việc quản trị mạng được thực hiện bởi các trạm máy tính quản trị. Các máy tính này sử dụng các phần mềm quản trị có nhiệm vụ quản lý một phần hoặc toàn bộ cấu hình của mạng theo yêu cầu của các ứng dụng quản trị hoặc các nhà quản trị mạng. Các phần mềm này có thể có giao diện đồ học cho phép các nhà quản trị theo dõi trạng thái của mạng và thực hiện các thao tác cần thiết khi có yêu cầu.

Các "điểm" quản trị (NE) có thể là các trạm làm việc, các thiết bị định tuyến, cầu hoặc chuyển mạch hoặc là bất kỳ một thiết bị nào có khả năng trao đổi dữ liệu về trạng thái của mình với thế giới bên ngoài. Để có thể thực hiện được các chức năng "bị quản lý", các NE phải có được các tính năng cơ bản của một SNMP agent, thực chất đó là một modul phần mềm có chức năng lưu trữ và cập nhật các thông tin quản trị của thiết bị cũng như có khả năng gửi các thông tin đó đến cho trạm quản trị khi được yêu cầu. Cấu trúc của các thông tin được xác định bởi thành phần Cơ sở thông tin quản trị (Management Information Base - MIB).

Mỗi một hệ thống trên mạng duy trì một MIB phản ánh các trạng thái của các tài nguyên cần quản trị trong hệ thống đó.



Hình 2: Các thành phần cơ bản của SNMP

(Nguồn: https://www.sciencedirect.com/topics/computer-science/information-technology-architecture)

Việc trao đổi dữ liệu giữa Manager và Agent được thực hiện trên giao thức SNMP [ietf]. Giao thức này cho phép các thực thể quản trị gửi các đến Agent các truy vấn về trạng thái các tài nguyên (còn gọi là các đối tượng). Các đối tượng này được định nghĩa trong MIB của các agent và có thể được thay đổi khi có yêu cầu. SNMP cung cấp ba tác vụ cơ bản như sau:

• Get: Trạm quản lý yêu cầu nhận giá trị của một hoặc nhiều đối tượng quản lý (MO) từ trạm bị quản lý;

• Set: Trạm quản lý yêu cầu thay đổi giá trị của một hoặc nhiều đối tượng quản lý (MO) tại trạm bị quản lý;

• Trap: Trạm bị quản lý gửi thông tin về trạng thái của một đối tượng quản lý khi có một biến cố đã được định nghĩa trước xảy ra.

Theo quy định của giao thức SNMP, Get bao gồm 2 tác vụ GetRequest và GetNextRequest, trong đó:

• GetRequest: lấy giá trị của một hoặc nhiều biến.

• GetNextRequest: lấy giá trị của biến kế tiếp.

Từ phiên bản SNMP v2, có thêm một tuỳ chọn nữa được đưa vào, đó là GetBulkRequest. Câu lệnh này được sử dụng chính để lấy một lượng lớn dữ liệu dạng ma trận.

Bên cạnh đó, SNMP còn định nghĩa các tác vụ khác như:

• GetResponse: trả về giá trị của một hoặc nhiều biến sau khi phát lệnh GetRequest hoặc GetNextRequest, hoặc SetRequest.

• InformRequest: Cho phép các trạm quản trị gửi thông tin dạng trap đến các trạm quản lý khác (từ SNMP v2).

Trong mạng TCP/IP, SNMP là một giao thức hoạt động ở tầng ứng dụng và sử dụng giao thức UDP. Do đó, SNMP là một giao thức phi kết nối, tức là giữa manager và agent không có sự duy trì kết nối trong suốt quá trình trao đổi dữ liệu.

KẾT LUẬN

Với giao thức SNMP thì việc quản trị mạng IP sẽ trở nên dễ dàng, nhanh chóng trong hệ thống thư viện số. Điều đó mới giúp các thư viện số trở thành Trung tâm Tri thức số hoạt động liên tục, xử lý nhiều giao dịch điện tử hơn, tiết kiệm nhiều chi phí và thời gian, đảm bảo tính chính xác và bảo mật tối đa cho cơ sở dữ liệu.

Ngày nay, việc sử dụng công nghệ để khai thác dữ liệu là điều không thể thiếu đối với người sử dụng thư viện, thế hệ thống thư viện số cần giúp họ khai thác dữ liệu và trích xuất ấn phẩm thông tin từ cơ sở dữ liệu lớn và mạng lưới rộng lớn không gian thông tin trong thư viện số.

Đổi mới công nghệ để khai thác dữ liệu là tiền đề cơ bản của tồn tại và phát triển thông tin. Chúng ta nên tăng cường trao đổi liên thư viện, để lượng tài liệu luôn được phát triển và cập nhập mới mẻ. Khi công nghệ tiến bộ và yêu cầu thay đổi, ứng dụng khai thác dữ liệu trong quản lý thư viện sẽ được chú ý nhiều hơn. Nó sẽ thúc đẩy sự phát triển nhanh hơn của thủ thư và tạo ra lợi ích xã hội tốt.

TÀI LIỆU THAM KHẢO

1. Bretthauer, David (2002), *Open Source Software: A History*. ITAL: Information Technology and Libraries. 21(1), 3-11. Retrieved January 21, 2008, http://www.ala.org/ala/lita/litapublications/ital/2101bretthauer.cfm.
2. Neill Wilkison, John Wiley & Sons (2002), *Next Generation Network Services: Technology and Strategies.*
3. Jean-Chrisostome Bolot, Characterizing The End-To-End Behavior Of *The Internet: Measurements, Analysis, And Applications*, http://citeseer.ist.psu.edu.
4. Ram Jadageesan, *Packet Loss Model*, Cisco System Inc, TR-41.3.3/99.