BÁO CÁO ĐỒ ÁN MÔN HỌC
QUẢN LÝ HỆ THỐNG MẠNG

Đề tài: **Tìm hiểu giao thức SNMP và phần mềm quản lý hệ thống mạng CiscoWorks LAN Management Solution.**

Giáo viên : Lê Tự Thanh
Lớp : MM02A – Nhóm 4
Sinh viên thực hiện

- **Trần Hữu Đạt**
- **Khương văn Phúc**
- **Phan Văn Ty**

LỜI NÓI ĐẦU

Với sự phát triển các máy trạm, các máy chủ và mạng LAN đã làm thay đổi mạng máy tính liên tục. Mặc khác với sự phát triển mạnh mẻ của các hệ thống và thiết bị, phần mềm của các nhà sản xuất khác nhau. Mặt khác do sự mua bán các hệ thống và thiết bị, phần mềm của các nhà sản xuất khác nhau. Do vậy các nhà sản xuất thiết bị hoặc phần mềm phải cung cấp phần mềm giao tiếp với thiết bị để có thể cấu hình và quản lý chúng. Và như vậy, mỗi một nhà sản xuất ít nhất là phải có một phần mềm quản lý riêng với nguyên tắc hoạt động riêng cho sản phẩm của mình. Điều này gây ra nhiều bất tiện. Do vậy, người ta xây dựng các giao thức quản lý thiết bị chung cho tất cả các nhà sản xuất. Trong các giao thức đó, thì giao thức đợc biết đến nhiều nhất là giao thức SNMP (Simple Network Management Protocol). Các thiết bị dù đơn giản hay phức tạp đều chứa phần mềm SNMP dùng để tham gia vào việc quản lý mạng.

Hiện nay, các đơn vị nghiên cứu phát triển trong lĩnh vực viễn thông trong nớc nói chung và CDiT nói riêng đã có nhiều sản phẩm đợc sử dụng trên mạng lới. Tuy nhiên việc quản lý các sản phẩm này vẫn cha đợc thực hiện theo tiêu chuẩn quốc tế nh các sản phẩm nhập hay chuyển giao từ nớc ngoài. Trên thế giới việc nghiên cứu và ứng dụng thủ tục SNMP trong việc quản lý các hệ thống và thiết bị viễn thông đã làm từ lâu, và việc ứng dụng SNMP vào quản lý là mặc định. Đứng trớc cơ hội hội nhập quốc tế, thì việc áp dụng một giao thức tiêu chuẩn quốc tế vào quản lý sản phẩm là cần thiết vì nó thống nhất đợc giao diện quản lý trên mạng, tạo điều kiện thuận lợi cho việc cung cấp giao diện quản lý chuẩn khi phát triển các hệ thống và thiết bị viễn thông trong nớc.

Trong phạm vi của một đồ án môn học, nhóm xin trình bày về các phần cơ bản của giao thức SNMP và phần mềm giám sát hệ thống mạng CiscoWorks LAN Management Solution.

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN VỀ QUẢN LÝ HỆ THỐNG MẠNG VỚI GIAO THỨC SNMP 1
1.1. Giới thiệu chung về quản lý hệ thống mạng....1
1.2. Tổng quan về giao thức SNMP....1
1.2.1. Hai phương thức giám sát Poll và Alert....1
1.2.1.1. Phương thức Poll....2
1.2.1.2. Phương thức Alert....2
1.2.1.3. So sánh phương thức Poll và Alert....2
1.2.2. Giới thiệu giao thức SNMP....3
1.2.3. Các thành phần chính của giao thức SNMP....4
1.2.3.1. ObjectID:....5
1.2.3.2. Object access:....6
1.2.3.3. Management Information Base:....6
1.2.3.4. Các thực thể của hệ thống quản lý mạng....7
1.2.3.5. Quan điểm quản lý Manager – Agent thực thể....8
1.3. Các phương thức của SNMP....8
1.3.1. GetRequest....8
1.3.2. SetRequest....8
1.3.3. GetResponse....9
1.3.4. Trap....9
1.4. Các đối tượng trong giao thức SNMP....10
1.5. Cấu trúc và đặc điểm của thông tin quản lý (SMI)....11
1.6. SNMPv2....11
1.6.1. Cấu trúc bản tin SNMPv2....11
1.6.2. Cơ sở thông tin quản lí MIB trong SNMPv2....12
1.6.3. Nguyên tắc hoạt động của SNMP....13
1.6.3.1. Truyền một bản tin SNMPv2....13
1.6.3.2. Nhận một bản tin SNMPv2....14
1.6.3.3. Các trạng thái thích ứng cho SNMPv2....14
1.7. SNMPv3....14
1.7.1. Các đặc điểm mới của SNMP v3....14
1.7.2. Hỗ trợ bảo mật và xác thực trong SNMPv3....15
CHƯƠNG 2: CÁC YÊU CẦU CỦA QUẢN LÝ HỆ THỐNG MẠNG....16
2.1. Các yêu cầu quản lý hệ thống mạng....16
2.2. Kiến trúc quản lý hệ thống mạng....16
2.2.1. Kiến trúc quản lý mạng....16
2.2.2. Cơ chế quản lý mạng....17
CHƯƠNG 3: TRIỂN KHAI PHẦN MỀM QUẢN LÝ HỆ THỐNG MẠNG CISCOWORKS LAN MANAGEMENT SOLUTION....17
3.1. Giới thiệu....17
3.2. Triển khai phần mềm....18
3.2.1. Mô hình hệ thống triển khai thực nghiệm....18
3.2.2. Cấu hình hệ thống yêu cầu....19
3.2.3. Cài đặt phần mềm....19
3.2.4. Giao diện sử dụng vào các tính năng cơ bản....21

Tổng Kết 28
Tài liệu tham khảo 28

CHƯƠNG 1: TỔNG QUAN VỀ QUẢN LÝ HỆ THỐNG MẠNG VỚI GIAO THỨC SNMP

1.1. Giới thiệu chung về quản lý hệ thống mạng

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

Nhiệm vụ của quản lý mạng rất rõ ràng về mặt nguyên tắc chung, nhưng các bài toán quản lý cụ thể lại có độ phức tạp rất lớn. Điều này xuất phát từ tính đa dạng của các hệ thống thiết bị và các đặc tính quản lý của các loại thiết bị, và xa hơn nữa là chiến lược quản lý phải phù hợp với kiến trúc mạng và đáp ứng yêu cầu của người sử dụng. Một loạt các thiết bị điển hình cần được quản lý gồm: Máy tính cá nhân, máy trạm, server, máy vi tính cỡ nhỏ, máy vi tính cỡ lớn, các thiết bị đầu cuối, thiết bị đo kiểm, máy điện thoại, tổng đài điện thoại nội bộ, các thiết bị truyền hình, máy quay, modem, bộ ghép kênh, bộ chuyển đổi giao thức, CSU/DSU, bộ ghép kênh thống kê, bộ ghép và giải gói, thiết bị tương thích ISDN, card NIC, các bộ mã hoá và giải mã tín hiệu, thiết bị nén dữ liệu, các gateway, các bộ xử lý front-end, các đường trung kế, DSC/DAC, các bộ lặp, bộ tái tạo tín hiệu, các thiết bị chuyển mạch, các bridge, router và switch, tất cả mới chỉ là một phần của danh sách các thiết bị sẽ phải được quản lý.

Toàn cảnh của bức tranh quản lý phải bao gồm quản lý các tài nguyên mạng cũng như các tài nguyên dịch vụ, người sử dụng, các ứng dụng hệ thống, các cơ sở dữ liệu khác nhau trong các loại môi trường ứng dụng. Về mặt kĩ thuật, tất cả thông tin trên được thu thập, trao đổi và được kết hợp với hoạt động quản lý mạng dưới dạng các số liệu quản lý bởi các kĩ thuật tương tự như các kĩ thuật sử dụng trong mạng truyền số liệu. Tuy nhiên sự khác nhau căn bản giữa truyền thông số liệu và trao đổi thông tin quản lý là việc trao đổi thông tin quản lý đòi hỏi các trường dữ liệu chuyên biệt, các giao thức truyền thông cũng như các mô hình thông tin chuyên biệt, các kỹ năng chuyên biệt để có thể thiết kế, vận hành hệ thống quản lý cũng như biên dịch các thông tin quản lý về báo lỗi, hiện trạng hệ thống, cấu hình và độ bảo mật.

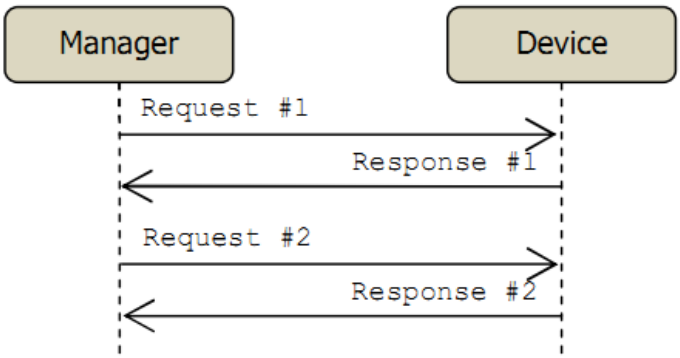
1.2. Tổng quan về giao thức SNMP

1.2.1. Hai phương thức giám sát Poll và Alert

Hai phương thức giám sát "Poll" và "Alert", đây là 2 phương thức cơ bản của các kỹ thuật giám sát hệ thống, nhiều phần mềm và giao thức được xây dựng dựa trên 2 phương thức này, trong đó có SNMP. Việc hiểu rõ hoạt động của Poll & Alert và ưu nhược điểm của chúng sẽ giúp chúng ta dễ dàng tìm hiểu nguyên tắc hoạt động của các giao thức hay phần mềm giám sát khác.

1.2.1.1. Phương thức Poll

Nguyên tắc hoạt động: Trung tâm giám sát (manager) sẽ thường xuyên hỏi thông tin của thiết bị cần giám sát (device). Nếu Manager không hỏi thì Device không trả lời, nếu Manager hỏi thì Device phải trả lời. Bằng cách hỏi thường xuyên, Manager sẽ luôn cập nhật được thông tin mới nhất từ Device.

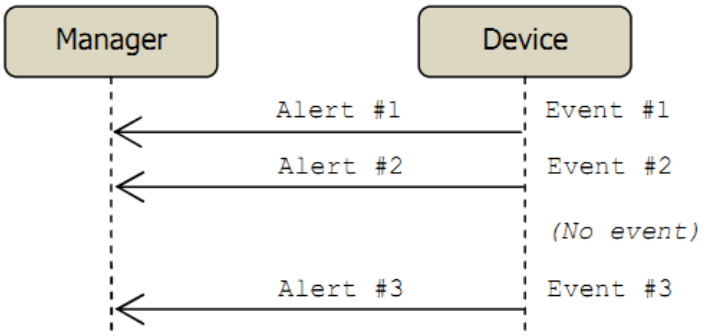


Hình minh họa cơ chế Poll

1.2.1.2. Phương thức Alert

Nguyên tắc hoạt động : Mỗi khi trong Device xảy ra một sự kiện (event) nào đó thì Device sẽ tự động gửi thông báo cho Manager, gọi là Alert. Manager không hỏi thông tin định kỳ từ Device.

Device chỉ gửi những thông báo mang tính sự kiện chứ không gửi những thông tin thường xuyên thay đổi, nó cũng sẽ không gửi Alert nếu chẳng có sự kiện gì xảy ra. Chẳng hạn khi một port down/up thì Device sẽ gửi cảnh báo, còn tổng số byte truyền qua port đó sẽ không được Device gửi đi vì đó là thông tin thường xuyên thay đổi. Muốn lấy những thông tin thường xuyên thay đổi thì Manager phải chủ động đi hỏi Device, tức là phải thực hiện phương thức Poll.



Hình minh họa cơ chế Alert

1.2.1.3. So sánh phương thức Poll và Alert

Hai phương thức Poll và Alert là hoàn toàn khác nhau về cơ chế. Một ứng dụng giám sát có thể sử dụng Poll hoặc Alert, hoặc cả hai, tùy vào yêu cầu cụ thể trong thực tế.

Bảng sau so sánh những điểm khác biệt của 2 phương thức :

Ký hiệu so sánh

Thuận lợi
Bất lợi

POLL	ALERT
Có thể chủ động lấy những thông tin cần thiết từ các đối tượng mình quan tâm, không cần lấy những thông tin không cần thiết từ những nguồn không quan tâm.	Tất cả những event xảy ra đều được gửi về Manager. Manager phải có cơ chế lọc những event cần thiết, hoặc Device phải thiết lập được cơ chế chỉ gửi những event cần thiết.
Có thể lập bảng trạng thái tất cả các thông tin của Device sau khi poll qua một lượt các thông tin đó. VD Device có một port down và Manager được khởi động sau đó, thì Manager sẽ biết được port đang down sau khi poll qua một lượt tất cả các port.	Nếu không có event gì xảy ra thì Manager không biết được trạng thái của Device. VD Device có một port down và Manager được khởi động sau đó, thì Manager sẽ không thể biết được port đang down.
Trong trường hợp đường truyền giữa Manager và Device xảy ra gián đoạn và Device có sự thay đổi, thì Manager sẽ không thể cập nhật. Tuy nhiên khi đường truyền thông suốt trở lại thì Manager sẽ cập nhật được thông tin mới nhất do nó luôn luôn poll định kỳ.	Khi đường truyền gián đoạn và Device có sự thay đổi thì nó vẫn gửi Alert cho Manager, nhưng Alert này sẽ không thể đến được Manager. Sau đó mặc dù đường truyền có thông suốt trở lại thì Manager vẫn không thể biết được những gì đã xảy ra.
Chỉ cần cài đặt tại Manager để trỏ đến tất cả các Device. Có thể dễ dàng thay đổi một Manager khác.	Phải cài đặt tại từng Device để trỏ đến Manager. Khi thay đổi Manager thì phải cài đặt lại trên tất cả Device để trỏ về Manager mới.
Nếu tần suất poll thấp, thời gian chờ giữa 2 chu kỳ poll (polling interval) dài sẽ làm Manager chậm cập nhật các thay đổi của Device. Nghĩa là nếu thông tin Device đã thay đổi nhưng vẫn chưa đến lượt poll kế tiếp thì Manager vẫn giữ những thông tin cũ.	Ngay khi có sự kiện xảy ra thì Device sẽ gửi Alert đến Manager, do đó Manager luôn luôn có thông tin mới nhất tức thời.
Có thể bỏ sót các sự kiện : khi Device có thay đổi, sau đó thay đổi trở lại như ban đầu trước khi đến lượt poll kế tiếp thì Manager sẽ không phát hiện được.	Manager sẽ được thông báo mỗi khi có sự kiện xảy ra ở Device, do đó Manager không bỏ sót bất kỳ sự kiện nào.

1.2.2. Giới thiệu giao thức SNMP

SNMP là "giao thức quản lý mạng đơn giản", như vậy thế nào là giao thức quản lý mạng đơn giản.

Giao thức là một tập hợp các thủ tục mà các bên tham gia cần tuân theo để có thể giao tiếp được với nhau. Trong lĩnh vực thông tin, một giao thức quy định cấu trúc, định dạng (format) của dòng dữ liệu trao đổi với nhau và quy định trình tự, thủ tục để trao đổi dòng dữ liệu đó. Nếu một bên tham gia gửi dữ liệu không đúng định dạng hoặc không theo trình tự thì các bên khác sẽ không hiểu hoặc từ chối trao đổi thông tin. SNMP là một giao thức, do đó nó có những quy định riêng mà các thành phần trong mạng phải tuân theo.

Một thiết bị hiểu được và hoạt động tuân theo giao thức SNMP được gọi là "có hỗ trợ SNMP" (SNMP supported) hoặc "tương thích SNMP" (SNMP compartible). SNMP dùng để quản lý, nghĩa là có thể theo dõi, có thể lấy thông tin, có thể được thông báo, và có thể tác động để hệ thống hoạt động như ý muốn. VD một số khả năng của phần mềm SNMP :

- ✓ Theo dõi tốc độ đường truyền của một router, biết được tổng số byte đã truyền/nhận.
- ✓ Lấy thông tin máy chủ đang có bao nhiêu ổ cứng, mỗi ổ cứng còn trống bao nhiêu.

- ✓ Tự động nhận cảnh báo khi switch có một port bị down.
- ✓ Điều khiển tắt (shutdown) các port trên switch.

SNMP dùng để quản lý mạng, nghĩa là nó được thiết kế để chạy trên nền TCP/IP và quản lý các thiết bị có nối mạng TCP/IP. Các thiết bị mạng không nhất thiết phải là máy tính mà có thể là switch, router, firewall, adsl gateway, và cả một số phần mềm cho phép quản trị bằng SNMP.

SNMP là giao thức đơn giản, do nó được thiết kế đơn giản trong cấu trúc bản tin và thủ tục hoạt động, và còn đơn giản trong bảo mật (ngoại trừ SNMP version 3). Sử dụng phần mềm SNMP, người quản trị mạng có thể quản lý, giám sát tập trung từ xa toàn mạng của mình.

Ưu điểm của thiết kế SNMP

SNMP được thiết kế để đơn giản hóa quá trình quản lý các thành phần trong mạng. Nhờ đó các phần mềm SNMP có thể được phát triển nhanh và tốn ít chi phí .

SNMP được thiết kế để có thể mở rộng các chức năng quản lý, giám sát. Không có giới hạn rằng SNMP có thể quản lý được cái gì. Khi có một thiết bị mới với các thuộc tính, tính năng mới thì người ta có thể thiết kế "custom" SNMP để phục vụ cho riêng mình (trong chương 3 tác giả sẽ trình bày file cấu trúc dữ liệu của SNMP).

SNMP được thiết kế để có thể hoạt động độc lập với các kiến trúc và cơ chế của các thiết bị hỗ trợ SNMP. Các thiết bị khác nhau có hoạt động khác nhau nhưng đáp ứng SNMP là giống nhau.

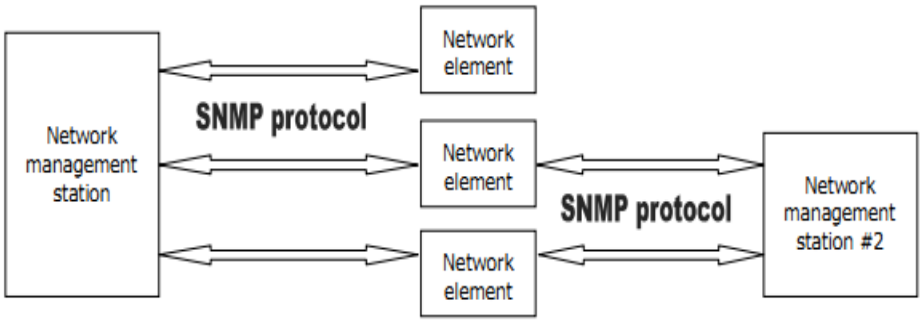
Các phiên bản của SNMP

SNMP có 4 phiên bản : SNMPv1, SNMPv2c, SNMPv2u và SNMPv3. Các phiên bản này khác nhau một chút ở định dạng bản tin và phương thức hoạt động. Hiện tại SNMPv1 là phổ biến nhất do có nhiều thiết bị tương thích nhất và có nhiều phần mềm hỗ trợ nhất. Trong khi đó chỉ có một số thiết bị và phần mềm hỗ trợ *SNMPv3*.

1.2.3. Các thành phần chính của giao thức SNMP

Theo RFC1157, kiến trúc của SNMP bao gồm 2 thành phần : các trạm quản lý mạng (network management station) và các thành tố mạng (network element).

Network management station thường là một máy tính chạy phần mềm quản lý SNMP (SNMP management application), dùng để giám sát và điều khiển tập trung các network element.



Network element là các thiết bị, máy tính, hoặc phần mềm tương thích SNMP và được

quản lý bởi network management station. Như vậy element bao gồm device, host và aplication.

Một management station có thể quản lý nhiều element, một element cũng có thể được quản lý bởi nhiều management station. Vậy nếu một element được quản lý bởi 2 station thì điều gì sẽ xảy ra ? Nếu station lấy thông tin từ element thì cả 2 station sẽ có thông tin giống nhau. Nếu 2 station tác động đến cùng một element thì element sẽ đáp ứng cả 2 tác động theo thứ tự cái nào đến trước.

Ngoài ra còn có khái niệm *SNMP agent*. SNMP agent là một tiến trình (process) chạy trên network element, có nhiệm vụ cung cấp thông tin của element cho station, nhờ đó station có thể quản lý được element. Chính xác hơn là application chạy trên station và agent chạy trên element mới là 2 tiến trình SNMP trực tiếp liên hệ với nhau.

1.2.3.1. ObjectID:

Một thiết bị hỗ trợ SNMP có thể cung cấp nhiều thông tin khác nhau, mỗi thông tin đó gọi là một *object*. Ví dụ :

- ✓ Máy tính có thể cung cấp các thông tin : tổng số ổ cứng, tổng số port nối mạng, tổng số byte đã truyền/nhận, tên máy tính, tên các process đang chạy, ….
- ✓ Router có thể cung cấp các thông tin : tổng số card, tổng số port, tổng số byte đã truyền/nhận, tên router, tình trạng các port của router, ….

Mỗi object có một tên gọi và một mã số để nhận dạng object đó, mã số gọi là *Object ID* (OID). Ví dụ :

Tên thiết bị được gọi là sysName, OID là 1.3.6.1.2.1.1.5 **4**.

- ✓ Tổng số port giao tiếp (interface) được gọi là ifNumber, OID là 1.3.6.1.2.1.2.1.
- ✓ Địa chỉ Mac Address của một port được gọi là ifPhysAddress, OID là 1.3.6.1.2.1.2.2.1.6.
- ✓ Số byte đã nhận trên một port được gọi là ifInOctets, OID là 1.3.6.1.2.1.2.2.1.10.

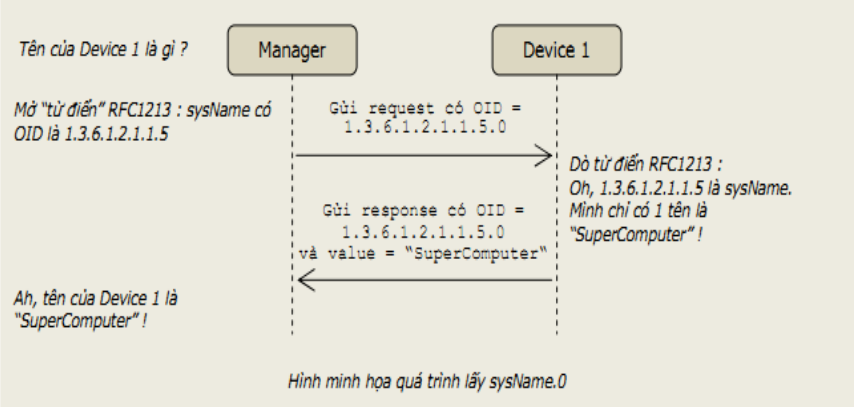
Bạn hãy khoan thắc mắc ý nghĩa của từng chữ số trong OID, chúng sẽ được giải thích trong phần sau. Một object chỉ có một OID, chẳng hạn tên của thiết bị là một object. Tuy nhiên nếu một thiết bị lại có nhiều tên thì làm thế nào để phân biệt ? Lúc này người ta dùng thêm 1 chỉ số gọi là “scalar instance index” (cũng có thể gọi là “sub-id”) đặt ngay sau OID.

Ở hầu hết các thiết bị, các object có thể có nhiều giá trị thì thường được viết dưới dạng có sub-id. Ví dụ: một thiết bị dù chỉ có 1 tên thì nó vẫn phải có OID là sysName.0 hay 1.3.6.1.2.1.1.5.0. Bạn cần nhớ quy tắc này để ứng dụng trong lập trình phần mềm SNMP manager.

Sub-id không nhất thiết phải liên tục hay bắt đầu từ 0. VD một thiết bị có 2 mac address thì có thể chúng được gọi là ifPhysAddress.23 và ifPhysAddress.125645.

OID của các object phổ biến có thể được chuẩn hóa, OID của các object do bạn tạo ra thì bạn phải tự mô tả chúng. Để lấy một thông tin có OID đã chuẩn hóa thì SNMP application phải gửi một bản tin SNMP có chứa OID của object đó cho SNMP agent, SNMP agent khi nhận được thì nó phải trả lời bằng thông tin ứng với OID đó.

VD : Muốn lấy tên của một PC chạy Windows, tên của một PC chạy Linux hoặc tên của một router thì SNMP application chỉ cần gửi bản tin có chứa OID là 1.3.6.1.2.1.1.5.0. Khi SNMP agent chạy trên PC Windows, PC Linux hay router nhận được bản tin có chứa OID 1.3.6.1.2.1.1.5.0, agent lập tức hiểu rằng đây là bản tin hỏi sysName.0, và agent sẽ trả lời bằng tên của hệ thống. Nếu SNMP agent nhận được một OID mà nó không hiểu (không hỗ trợ) thì nó sẽ không trả lời.



Hình minh họa quá trình lấy sysName.0

Một trong các ưu điểm của SNMP là có được thiết kế để chạy độc lập với các thiết bị khác nhau. Chính nhờ việc chuẩn hóa OID mà ta có thể dùng một SNMP application để lấy thông tin các loại device của các hãng khác nhau.

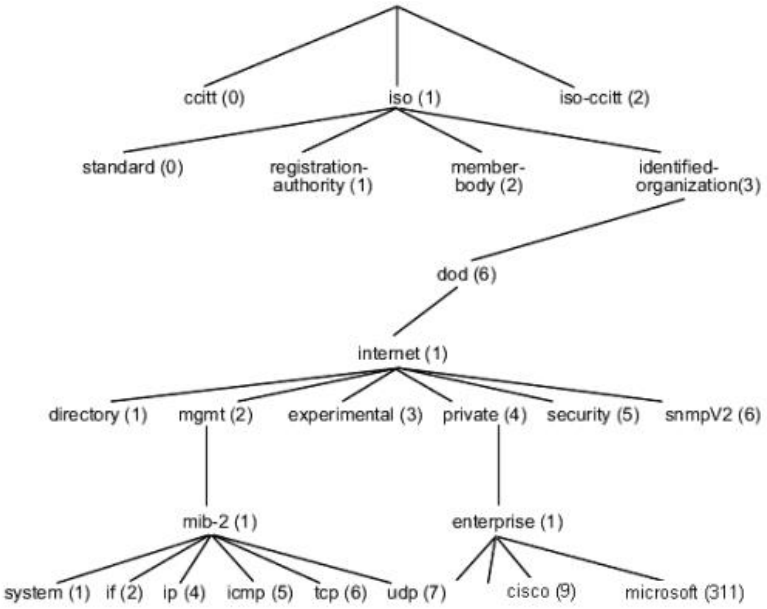
1.2.3.2. Object access:

Mỗi object có quyền truy cập là READ_ONLY hoặc READ_WRITE. Mọi object đều có thể đọc được nhưng chỉ những object có quyền READ_WRITE mới có thể thay đổi được giá trị. VD : Tên của một thiết bị (sysName) là READ_WRITE, ta có thể thay đổi tên của thiết bị thông qua giao thức SNMP. Tổng số port của thiết bị (ifNumber) là READ_ONLY, dĩ nhiên ta không thể thay đổi số port của nó.

1.2.3.3. Management Information Base:

MIB (cơ sở thông tin quản lý) là một cấu trúc dữ liệu gồm các đối tượng được quản lý (managed object), được dùng cho việc quản lý các thiết bị chạy trên nền TCP/IP. MIB là kiến trúc chung mà các giao thức quản lý trên TCP/IP nên tuân theo, trong đó có SNMP. MIB được thể hiện thành 1 file (MIB file), và có thể biểu diễn thành 1 cây (MIB tree). MIB có thể được chuẩn hóa hoặc tự tạo.

Hình sau minh họa MIB tree:



Một node trong cây là một object, có thể được gọi bằng tên hoặc id.

Các objectID trong MIB được sắp xếp thứ tự nhưng không phải là liên tục, khi biết một OID thì không chắc chắn có thể xác định được OID tiếp theo trong MIB. VD trong chuẩn mib-2 thì object ifSpecific và object atIfIndex nằm kề nhau nhưng OID lần lượt là 1.3.6.1.2.1.2.2.1.22 và 1.3.6.1.2.1.3.1.1.1
Muốn hiểu được một OID nào đó thì bạn cần có file MIB mô tả OID đó. Một MIB file không nhất thiết phải chứa toàn bộ cây ở trên mà có thể chỉ chứa mô tả cho một nhánh con. Bất cứ nhánh con nào và tất cả lá của nó đều có thể gọi là một mib.

Một manager có thể quản lý được một device chỉ khi ứng dụng SNMP manager và ứng dụng SNMP agent cùng hỗ trợ một MIB. Các ứng dụng này cũng có thể hỗ trợ cùng lúc nhiều MIB.

Trong chương này chúng ta chỉ đề cập đến khái niệm MIB ngắn gọn như trên. Chương 3 sẽ mô tả chi tiết cấu trúc của file MIB.

1.2.3.4. Các thực thể của hệ thống quản lý mạng

Ban đầu, hệ thống quản lý mạng được xây dựng dựa trên mô hình khá đơn giản. Quản lý được định nghĩa là sự tương tác qua lại giữa hai thực thể: thực thể quản lý và thực thể bị quản lý. Thực thể quản lý đặc trưng bởi hệ thống quản lý, nền tảng quản lý (flatform) và ứng dụng quản lý.

Agent cũng có thể là Agent quản lý hoặc Agent bị quản lý. Manager chính là thực thể quản lý, trong khi đó Agent làm thực thể ẩn dưới sự tương tác giữa Manager và các nguồn tài nguyên bị quản lý thực sự.

Mô hình Manager – Agent rất thôn dụng, dùng để mô tả thực thể quản lý và thực thể bị quản lý ở lớp cao. Đây cũng chính là lý do mà các mô hình được tạo ra tự nhiên cho mục đích quản lý đều gần với mô hình Manager – Agent. Tuy nhiên trong thực tế mô hình này phức tạp hơn nhiều.

Có một số mô hình khác cũng dùng cho việc trao đổi thông tin quản lý như mô hình Client – Server hay mô hình Application – Object server. Nhưng mô hình này, về

bản chất dùng để xây dựng các ứng dụng phân bố hoặc các môi trường đối tượng phân bố.

1.2.3.5. Quan điểm quản lý Manager – Agent thực thể

Các quan điểm về quản lý cho rằng chức năng quan trọng nhất trong quản lý là quan hệ giữa thực thể quản lý và thực thể bị quản lý. Điều này dựa trên mô hình phản hồi. Manager sẽ yêu cầu từ Agent các thông tin quản lý đặc trưng và thực thể bị quản lý , thông qua Agent, sẽ được quản lý lại bằng thông tin chứa đầy đủ các yêu cầu. Nếu thông tin yêu cầu phản hồi được sử dụng liên tục để tìm kiếm mỗi Agent và các đối tượng bị quản lý tương ứng thì cơ chế này gọi là polling và lần đầu tiên được ứng dụng để quản lý trong môi trường internet dựa trên giao thức quản lý mạng đơn giản SNMP.

1.3. Các phương thức của SNMP

Giao thức SNMPv1 có 5 phương thức hoạt động, tương ứng với 5 loại bản tin như sau :

Bản tin/phương thức	Mô tả tác dụng
GetRequest	Manager gửi GetRequest cho agent để yêu cầu agent cung cấp thông tin nào đó dựa vào ObjectID (trong GetRequest có chứa OID)
GetNextRequest	Manager gửi GetNextRequest có chứa một ObjectID cho agent để yêu cầu cung cấp thông tin nằm kế tiếp ObjectID đó trong MIB.
SetRequest	Manager gửi SetRequest cho agent để đặt giá trị cho đối tượng của agent dựa vào ObjectID.
GetResponse	Agent gửi GetResponse cho Manager để trả lời khi nhận được GetRequest/GetNextRequest
Trap	Agent tự động gửi Trap cho Manager khi có một sự kiện xảy ra đối với một object nào đó trong agent.

Mỗi bản tin đều có chứa OID để cho biết object mang trong nó là gì. OID trong GetRequest cho biết nó muốn lấy thông tin của object nào. OID trong GetResponse cho biết nó mang giá trị của object nào. OID trong SetRequest chỉ ra nó muốn thiết lập giá trị cho object nào. OID trong Trap chỉ ra nó thông báo sự kiện xảy ra đối với object nào.

1.3.1. GetRequest

Bản tin GetRequest được manager gửi đến agent để lấy một thông tin nào đó. Trong GetRequest có chứa OID của object muốn lấy. VD : Muốn lấy thông tin tên của Device1 thì manager gửi bản tin GetRequest OID=1.3.6.1.2.1.1.5 đến Device1, tiến trình SNMP agent trên Device1 sẽ nhận được bản tin và tạo bản tin trả lời.

Trong một bản tin GetRequest có thể chứa nhiều OID, nghĩa là dùng một GetRequest có thể lấy về cùng lúc nhiều thông tin.

1.3.2. SetRequest

Bản tin SetRequest được manager gửi cho agent để thiết lập giá trị cho một object nào đó. Ví dụ :

- Có thể đặt lại tên của một máy tính hay router bằng phần mềm SNMP manager, bằng cách gửi bản tin SetRequest có OID là 1.3.6.1.2.1.1.5.0 (sysName.0) và có giá trị là tên mới cần đặt.

- Có thể shutdown một port trên switch bằng phần mềm SNMP manager, bằng cách gửi bản tin có OID là 1.3.6.1.2.1.2.2.1.7 (ifAdminStatus) và có giá trị là 2^7.

Chỉ những object có quyền READ_WRITE mới có thể thay đổi được giá trị.

1.3.3. GetResponse

Mỗi khi SNMP agent nhận được các bản tin GetRequest, GetNextRequest hay SetRequest thì nó sẽ gửi lại bản tin GetResponse để trả lời. Trong bản tin GetResponse có chứa OID của object được request và giá trị của object đó.

1.3.4. Trap

Bản tin Trap được agent tự động gửi cho manager mỗi khi có sự kiện xảy ra bên trong agent, các sự kiện này không phải là các hoạt động thường xuyên của agent mà là các sự kiện mang tính biến cố. Ví dụ : Khi có một port down, khi có một người dùng login không thành công, hoặc khi thiết bị khởi động lại, agent sẽ gửi trap cho manager.

Tuy nhiên không phải mọi biến cố đều được agent gửi trap, cũng không phải mọi agent đều gửi trap khi xảy ra cùng một biến cố. Việc agent gửi hay không gửi trap cho biến cố nào là do hãng sản xuất device/agent quy định.

Phương thức trap là độc lập với các phương thức request/response. SNMP request/response dùng để quản lý còn SNMP trap dùng để cảnh báo. Nguồn gửi trap gọi là *Trap Sender* và nơi nhận trap gọi là *Trap Receiver*. Một trap sender có thể được cấu hình để gửi trap đến nhiều trap receiver cùng lúc.

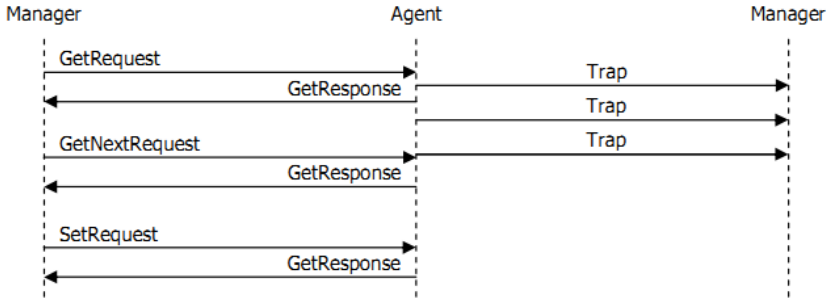
Có 2 loại trap : trap phổ biến (generic trap) và trap đặc thù (specific trap). Generic trap được quy định trong các chuẩn SNMP, còn specific trap do người dùng tự định nghĩa (người dùng ở đây là hãng sản xuất SNMP device). Loại trap là một số nguyên chứa trong bản tin trap, dựa vào đó mà phía nhận trap biết bản tin trap có nghĩa gì.

Theo SNMPv1, generic trap có 7 loại sau : coldStart(0), warmStart(1), linkDown(2), linkUp(3), authenticationFailure(4), egpNeighborloss(5), enterpriseSpecific(6). Giá trị trong ngoặc là mã số của các loại trap. Ý nghĩa của các bản tin generic-trap như sau :

- ColdStart : thông báo rằng thiết bị gửi bản tin này đang khởi động lại (reinitialize) và cấu hình của nó có thể bị thay đổi sau khi khởi động.
- WarmStart : thông báo rằng thiết bị gửi bản tin này đang khởi động lại và giữ nguyên cấu hình cũ.
- LinkDown : thông báo rằng thiết bị gửi bản tin này phát hiện được một trong những kết nối truyền thông (communication link) của nó gặp lỗi. Trong bản tin trap có tham số chỉ ra ifIndex của kết nối bị lỗi.
- LinkUp : thông báo rằng thiết bị gửi bản tin này phát hiện được một trong những kết nối truyền thông của nó đã khôi phục trở lại. Trong bản tin trap có tham số chỉ ra ifIndex của kết nối được khôi phục.
- AuthenticationFailure : thông báo rằng thiết bị gửi bản tin này đã nhận được một bản tin không được chứng thực thành công (bản tin bị chứng thực không thành công có thể thuộc nhiều giao thức khác nhau như telnet, ssh, snmp, ftp, …). Thông thường trap loại này xảy ra là do user đăng nhập không thành công vào thiết bị.

- EgpNeighborloss : thông báo rằng một trong số những "EGPneighbor" của thiết bị gửi trap đã bị coi là down và quan hệ đối tác (peer relationship) giữa 2 bên không còn được duy trì.
- EnterpriseSpecific : thông báo rằng bản tin trap này không thuộc các kiểu generic như trên mà nó là một loại bản tin do người dùng tự định nghĩa. Người dùng có thể tự định nghĩa thêm các loại trap để làm phong phú thêm khả năng cảnh báo của thiết bị như : boardFailed, configChanged, powerLoss, cpuTooHigh, v.v….

Người dùng tự quy định ý nghĩa và giá trị của các specific trap này, và dĩ nhiên chỉ những trap receiver và trap sender hỗ trợ cùng một MIB mới có thể hiểu ý nghĩa của specific trap. Do đó nếu bạn dùng một phần mềm trap receiver bất kỳ để nhận trap của các trap sender bất kỳ, bạn có thể đọc và hiểu các generic trap khi chúng xảy ra; nhưng bạn sẽ không hiểu ý nghĩa các specific trap khi chúng hiện lên màn hình vì bản tin trap chỉ chứa những con số.



Hình minh họa các phương thức của SNMPv1

Đối với các phương thức Get/Set/Response thì SNMP Agent lắng nghe ở port UDP 161, còn phương thức trap thì SNMP Trap Receiver lắng nghe ở port UDP 162.

1.4. Các đối tượng trong giao thức SNMP

SNMP gồm hai đối tượng chính: người quản lý và người phục vụ (Agent). Agent bao gồm cả một phần của phần mềm trong máy. SNMP Agent tồn tại ở tất cả các phần của thiết bị , tuy nhiên thiết lập Agent không cho phép làm bất cứ gì cho đến khi hỏi người quản lý. Đây là một chương trình riêng lẻ, người quản trị chạy chính máy của mình để hỏi những câu hỏi đến máy Agent để thu thập thông tin.

Thiết lập thông tin được gọi là MIB (Management Information Base) cơ sở quản lý thông tin. Hầu hết mỗi Agent đều có những MIB nhỏ cho phép người quản trị xem những gói tin nhập xuất của hệ thống. Ngoài MIB cơ bản này, mỗi Agent hỗ trợ những MIB khác nhau chứa đựng thông tin về mục đích đặc biệt của nó.

Một giao tiếp (community) SNMP là mối quan hệ logic giữa người phục vụ SNMP và một hoặc nhiều người quản lý. Một community gồm có tên và tất tất cả những thành viên trong community có cùng một quyền truy cập như nhau. Thao tác TRAP gửi những thông tin đến trạm quản lý (Management Station) khi một đối tượng được thay đổi (cho thấy rằng việc thay đổi quan trọng đến việc phải gởi những thông báo)

Mặc định chuỗi community cung cấp kiểm tra hay đọc những khả năng thì thường xuyên được biết đến mặc định sự điều khiển hay viết những chuỗi community thì thường xuyên được giấu kín. SNMP khai thác những thuận lợi của những chuỗi community mặc định để cho phép người tấn công thu thập thông tin về những thiết bị sử dụng những chuỗ community chung, hay người tấn công có thể thay đổi cấu hình hệ thống sử dụng những chuỗi community kín đáo.

1.5. Cấu trúc và đặc điểm của thông tin quản lý (SMI)

SMI (Structure Management Information) định nghĩa một cơ cấu tổ chức chung cho thông tin quản lý. SMI nhận dạng các kiểu dữ liệu trong MIB và chỉ rõ cách thức miêu tả và đặt tên các tài nguyên trong MIB. SIM duy trì tính đơn giản và khả năng mở rộng trong MIB, vì thế MIB chỉ lưu trữ những loại dữ liệu đơn giản. SMI không cung cấp cách tạo hoặc truy xuất các cấu trúc dữ liệu phức tạp. Các MIB sẽ chứa các loại dữ liệu do nhà cung cấp tạo ra.

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

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

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

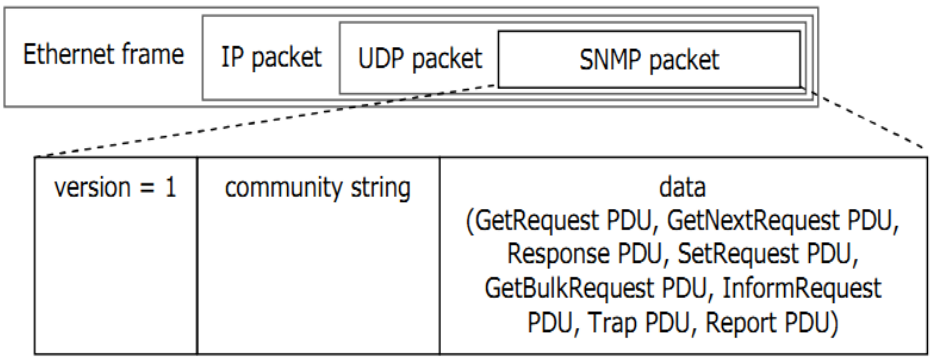
- ✓ Object: Tên đối tượng
- ✓ Systax: Cú pháp cho loại đối tượng.
- ✓ Definition : Các định nghĩa.
- ✓ Truy cập (Access): Có thể là chỉ đọc, đọc – ghi, không thể truy cập.
- ✓ Trạng thái (Status): Có thể cưỡng chế, tùy chọn hay không còn hiệu lực.

1.6. SNMPv2

SNMPv2 tích hợp khả năng liên điều hành từ manager tới manager và hai đơn vị dữ liệu giao thức mới. Khả năng liên kết điều hành manager-manager cho phép SNMP hỗ trợ quản lí mạng phân tán trong một trạm và gửi báo cáo tới một trạm khác. Để hỗ trợ tương tác tốt nhất, SNMPv2 thêm các nhóm cảnh báo và sự kiện vào trong cơ sở thông tin quản lí MIB. Nhóm cảnh báo cho phép đặt ngưỡng thiết lập cho các bản tin cảnh báo. Nhóm sự kiện được đưa ra khi thông tin Trap xác định các giá trị phần tử MIB.

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

1.6.1. Cấu trúc bản tin SNMPv2



Hình: Cấu trúc bản tin SNMPv2

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

+ Trường phiên bản (Version) thể hiện phiên bản của giao thức SNMPv2.

+ Trường Community là một chuỗi password xác nhận cho cả tiến trình lấy và thay đổi dữ liệu. SNMP PDU chứa kiểu điều hành (get, set), yêu cầu đáp ứng (cùng số thứ tự với bản tin gửi đi) - cho phép người điều hành gửi đồng thời nhiều bản tin. Biến ghép gồm các thiết bị được đặc tả trong RFC 2358 và chứa cả giá trị đặt tới đối tượng.

Trường đơn vị dữ liệu giao thức (PDU) gồm có các trường con: Kiểu đơn vị dữ liệu giao thức, nhận dạng các yêu cầu (Request ID), trạng thái lỗi, chỉ số lỗi, các giá trị và đối tượng.

Các kiểu đơn vị dữ liệu giao thức PDU thể hiện các bản tin sử dụng trong SNMPv2 gồm có: GetRequest,GetNextRequest, SetRequest, GetResponse, Trap, GetBulkReques, InformRequest .

1.6.2. Cơ sở thông tin quản lí MIB trong SNMPv2

IB trong SNMPv2 định nghĩa các đối tượng mô tả tác động của một phần tử NMPv2. MIB này gồm 3 nhóm:

- ✓ Nhóm hệ thống (System group): là một mở rộng của nhóm system trong MIB-II gốc, bao gồm một nhóm các đối tượng cho phép một Agent SNMPv2 mô tả các đối tượng tài nguyên của nó. Các đối tượng mới trong phần mở rộng có tên bắt đầu bằng sysOR, chúng liên quan đến tài nguyên hệ thống và được sử dụng bởi một Agent SNMPv2 để mô tả các đối tượng tài nguyên mà việc điều khiển chúng tuỳ thuộc vào cấu hình động bởi một bộ phận quản lí.
- ✓ Nhóm SNMP (SNMP group): một cải tiến của nhóm SNMP trong MIB-II gốc, bao gồm các đối tượng cung cấp các công cụ cơ bản cho hoạt động giao thức. Nó có thêm một số đối tượng mới và loại bỏ một số đối tượng ban đầu. Nhóm SNMP chứa một vài thông tin lưu lượng cơ bản liên quan đến toán tử SNMPv2 và chỉ có một trong các đối tượng là bộ đếm chỉ đọc 32-bit.
- ✓ Nhóm các đối tượng MIB (MIB objects group): một tập hợp các đối tượng liên quan đến các SNMPv2-Trap PDU và cho phép một vài phần tử SNMPv2 cùng hoạt động, thực hiện như trạm quản trị, phối hợp việc sử dụng của chúng trong toán tử Set của SNMPv2.

Phần đầu của nhóm này là một nhóm con, snmpTrap, bao gồm hai đối tượng liên quan đến Trap:

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

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

Đối tượng snmpSet được sử dụng theo cách sau: Khi một manager muốn đặt một hay nhiều giá trị đối tượng trong một Agent, đầu tiên nó nhận giá trị của đối tượng snmpSet. Sau đó nó gửi SetRequest PDU có danh sách biến liên kết bao gồm cả đối tượng snmpSet với giá trị đã nhận được của nó. Nếu nhiều manager gửi các setRequestPDU sử dụng cùng một giá trị của snmpSet, bản tin đến Agent trước sẽ được thực hiện (giả sử không có lỗi), kết quả là làm tăng snmpSet; các toán tử set còn lại sẽ bị lỗi vì không phù hợp với giá trị snmpSet. Hơn nữa, nếu một manager muốn gửi một chuỗi các toán tử set và đảm bảo rằng chúng được thực hiện theo một trật tự nhất định thì đối tượng snmpSet phải được gộp vào trong mỗi toán tử.

1.6.3. Nguyên tắc hoạt động của SNMP

1.6.3.1. Truyền một bản tin SNMPv2

Qui tắc gửi và nhận bản tin của Manager và Agent được thể hiện trong bảng sau:

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

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

- ✓ Sử dụng ASN.1 để mô tả một PDU.

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

1.6.3.2. Nhận một bản tin SNMPv2

1.6.3.3. Các trạng thái thích ứng cho SNMPv2

1.7. SNMPv3

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

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

1.7.1. Các đặc điểm mới của SNMP v3

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

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

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

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

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

1.7.2. Hỗ trợ bảo mật và xác thực trong SNMPv3

Một trong những mục tiêu chính – nếu không coi là một mục đích chính chính – khi phát triển SNMPv3 đó là thêm đặc tính bảo mật cho quản lí SNMP. Xác thực và bảo vệ thông tin, cũng như xác thực và điều khiển truy cập, đã được nêu rõ ở trên. Cấu trúc SNMPv3 cho phép sử dụng linh hoạt bất cứ một giao thức nào cho xác thực và bảo vệ thông tin. Dù sao, nhóm IETF SNMPv3 đã đưa ra mô hình bảo mật người dùng. Chúng ta sẽ tìm hiểu thêm về các khía cạnh chung về bảo mật kết hợp với các kiểu của các mối đe doạ bảo mật, mô hình bảo mật, định dạng dữ liệu bản tin để điều tiết các tham số bảo mật và sử dụng cũng như quản lí của các khoá trong phần này.

Các mối đe doạ bảo mật.

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

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

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

Mô hình bảo mật

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

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

CHƯƠNG 2: CÁC YÊU CẦU CỦA QUẢN LÝ HỆ THỐNG MẠNG

2.1. Các yêu cầu quản lý hệ thống mạng

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

- ✓ Chức năng giám sát có nhiệm vụ thu thập liên tục các thông tin về trạng thái của các tài nguyên được quản lý sau đó chuyển các thông tin này dưới dạng các sự kiện và đưa ra các cảnh báo khi các tham số của tài nguyên mạng được quản lý vượt quá ngưỡng cho phép.
- ✓ Chức năng quản lý có nhiệm vụ thực hiện các yêu cầu của người quản lý hoặc các ứng dụng quản lý nhằm thay đổi trạng thái hay cấu hình của một tài nguyên được quản lý nào đó.
- ✓ Chức năng đưa ra báo cáo có nhiệm vụ chuyển đổi và hiển thị các báo cáo dưới dạng mà người quản lí có thể đọc, đánh giá hoặc tìm kiếm, tra cứu thông tin được báo cáo.

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

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

2.2. Kiến trúc quản lý hệ thống mạng

2.2.1.Kiến trúc quản lý mạng

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

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

- ✓ Quản lý phần tử mạng: Quản lý từng thiết bị đơn trong mạng, ví dụ bộ định tuyến, chuyển mạch, Hub.

Quản lý mạng có thể chia thành hai chức năng cơ sở: truyền tải thông tin quản lý qua hệ thống và quản lý các phần tử thông tin quản lý mạng. Các chức năng này gồm các nhiệm vụ khác nhau như: Giám sát, cấu hình, sửa lỗi và lập kế hoạch được thực hiện bởi nhà quản trị hoặc nhân viên quản lý mạng.

2.2.2. Cơ chế quản lý mạng

Cơ chế quản lý mạng bao gồm cả các giao thức quản lý mạng, các giao thức quản lý mạng cung cấp các cơ chế thu thập, thay đổi và truyền các dữ liệu quản lý mạng qua mạng.

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

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

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

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

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

- ✓ Các câu lệnh SET của SNMP
- ✓ Truy nhập qua telnet và giao diện dòng lệnh
- ✓ Truy nhập qua HTTP
- ✓ Truy nhập qua kiến trúc CORBA
- ✓ Sử dụng FTP/TFTP để lấy file cấu hình

CHƯƠNG 3: TRIỂN KHAI PHẦN MỀM QUẢN LÝ HỆ THỐNG MẠNG CISCOWORKS LAN MANAGEMENT SOLUTION

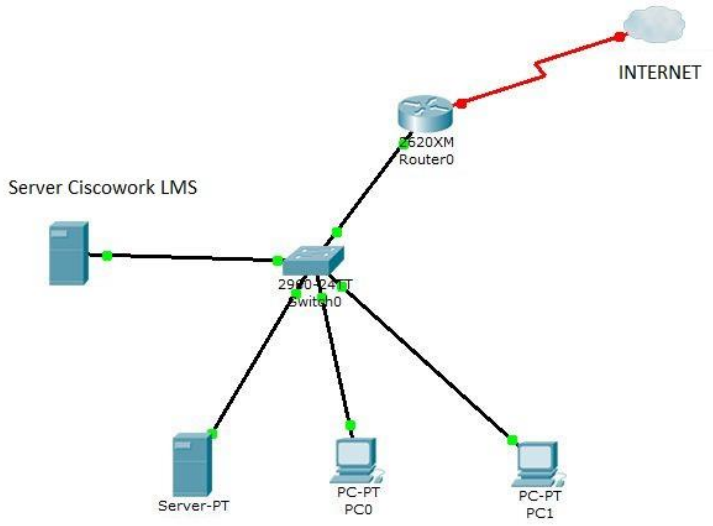
3.1. Giới thiệu

Với các hệ thống mạng lớn, việc quản trị các thiết bị mạng bao gồm Router, Switch và Access Point là rất quan trọng. Đặc biệt là với các hệ thống với số lượng thiết bị lớn và thời gian gián đoạn mạng cho phép ngắn. Thông qua việc quản trị này, người quản trị có thể thay đổi cấu hình các thiết bị mạng cũng như thuận tiện trong

việc sửa lỗi một cách nhanh nhất có thể. Với các yêu cầu này, Cisco có cung cấp bộ giải pháp quản trị mạng dành cho các thiết bị như Routers, Switches và Access points.
Chi tiết các thông số kỹ thuật:
LMS là một phần của giải pháp quản trị mạng CiscoWorks, cung cấp các công cụ cài đặt, quản trị, giám sát, phát hiện lỗi, và khắc phục sự cố có thể xảy ra trong mạng. Các công cụ này có thể áp dụng cho hầu hết các thiết bị trong mạng, bao gồm Switch, Router, PIX Firewall và kể cả thiết bị mới chạy phần mềm Cisco CallManager.
Bộ phần mềm LMS được viết trên các giao thức chuẩn của Internet và thêm các chức năng mở rộng cho các thiết bị và phần mềm của Cisco, tạo nên một công cụ mạnh mẽ giúp nhà quản trị mạng có thể quản lý mạng nội bộ của mình một cách hiệu quả. LMS có giao diện web nên nhà quản trị có thể dễ dàng xem các sơ đồ mạng, xem các cấu hình, và thông tin về tình trạng của các thiết bị từ bất kỳ một vị trí nào trong mạng thông qua trình duyệt web.
LMS được thiết kế linh hoạt, có thể cài đặt riêng hoặc dùng chung với các phần mềm quản trị mạng khác của HP, Sun… giúp cho nhà quản trị có nhiều lựa chọn phù hợp với kinh nghiệm của mình.
Bộ phần mềm CiscoWorks LAN Management Solution bao gồm các thành phần sau:
Campus Manager (CM) – là phần mềm quản lý các thiết bị switch của Cisco qua giao diện web, cung cấp thông tin về các thiết bị ở lớp 2, mô hình kết nối chi tiết, cấu hình VLAN, ATM LANE, quản lý các thiết bị của người dùng, điện thoại IP…
Device Fault Manager (DFM) – Phần mềm giám sát hoạt động và kiểm tra lỗi của các thiết bị mạng Cisco hoạt động ở thời gian thực, thông báo lỗi qua các thông báo lỗi, qua email, hoặc kết hợp với các thông báo của các chương trình khác.
Resource Manager Essentials (RME) – Giúp quản lý danh sách các thiết bị mạng, cấu hình phần cứng, phần mềm, các sự cố xảy ra… Sử dụng phần mềm này chủ yếu nhằm mục đích thông kê, lập báo cáo, lưu hồ sơ về mạng.
eGenius Real-Time Monitor (RTM) – Đây là phần mềm mới được đưa vào bộ CWLMS, hoạt động dựa vào giao thức RMON nhằm quản lý, giám sát hoạt động và khắc phục sự cố của mạng. Các kết quả phân tích, báo cáo đều được đưa lên màn hình web trực quan với đầy đủ thông tin.
CiscoView (CV) – Đây là phần mềm phổ biến nhất của Cisco dùng để truy cập xem thông tin trạng thái và cài đặt cấu hình của thiết bị mạng.

Với tập hợp các phần mềm trên, giải pháp LMS cung cấp giám sát từ mọi góc cạnh trong hoạt động của mạng LAN, từ những gì đã xảy ra cho đến hiện tại nhằm phát hiện, đề phòng và khắc phục sự cố mạng có thể xảy ra, giảm thời gian gián đoạn mạng xuống mức thấp nhất.. Do tập trng vào quản lý, giám sát các hoạt động của các thiết bị mạng, bộ phần mềm LSM giúp nhà quản trị mạng luôn yên tâm về thời gian hoạt động của mạng nội bộ.

3.2. Triển khai phần mềm
3.2.1.Mô hình hệ thống triển khai thực nghiệm
Ciscowork LMS là một phần mềm mạnh, hỗ trợ các hệ thống mạng lớn, phức tạp, nhiều thiết bị khác nhau như: Switch, router, server, PC, IP Phone…..
Ở đây nhóm xin đưa ra một mô hình nhỏ để triển khai thực nghiệm bao gồm các thiết bị như switch, router, server, PC như hình dưới.



Hình: Mô hình hệ thống.

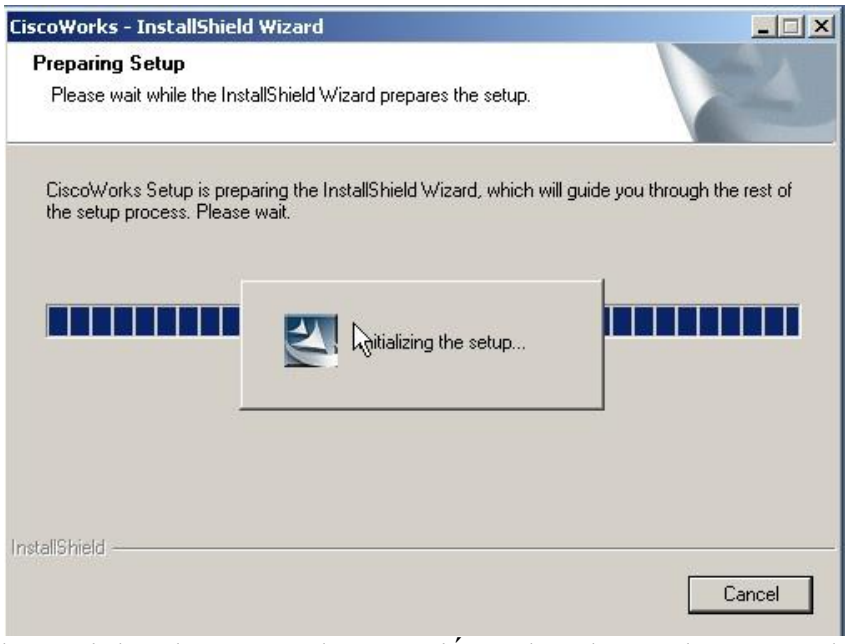
3.2.2. Cấu hình hệ thống yêu cầu

Part Number (SKU)	Solaris (Memory and Hardware Recommendations)	Microsoft Windows (Memory and Hardware Recommendations)
CWLMS-4.0-SBE-K9[2] **CWLMS-4.0-100-K9**	Not supported	1 CPU with dual core or 2 CPU with single core 4 GB RAM and 8 GB swap space, 60 GB free disk space, 32 or 64 bit OS
CWLMS-4.0-300-K9	1 CPU with dual core or 2 CPU with single core 4 GB RAM and 8 GB swap space, 60 GB free disk space, 32/64 dual stack OS	1 CPU with dual core or 2 CPU with single core 4 GB RAM and 8 GB swap space, 60 GB free disk space, 32 or 64 bit OS
CWLMS-4.0-750-K9	2 CPUs with dual core or 4 CPU with single core 8 GB RAM and 16 GB swap space, 60 GB free disk space, 32/64 dual stack OS	2 CPUs with dual core or 4 CPU with single core, 8 GB RAM and 16 GB swap space, 60 GB free disk space, 32 or 64 bit OS
CWLMS-4.0-1.5K-K9	2 CPUs with dual core or 4 CPU with single core 8 GB RAM and 16 GB swap space, 60 GB free disk space, 64 bit OS	2 CPUs with dual core or 4 CPU with single core, 8 GB RAM and 16 GB swap space, 60 GB free disk space, 64 bit OS
CWLMS-4.0-2.5K-K9	2 CPUs with quad core or 4 CPU with dual core 16 GB RAM and 32 GB swap space, 60 GB free disk space, 64 bit OS	2 CPUs with quad core or 4 CPU with dual core,16 GB RAM and 32 GB swap space, 60 GB free disk space, 64-bit OS
CWLMS-4.0-5K-K9 **CWLMS-4.0-10K-K9**[3]	2 CPUs with 8 core or 4 CPU with quad core 16 GB RAM and 32 GB swap space, 120 GB free disk space, 64 bit OS	2 CPUs with 8 core or 4 CPU with quad core 16 GB RAM and 32 GB swap space, 120 GB free disk space, 64 bit OS
Processor support	• UltraSPARC IIIi processor • UltraSPARC IV processor • UltraSPARC IV+ processor • UltraSPARC T1 processor • UltraSPARC T2 processor • UltraSPARC T2+ processor • SPARC64 VI processor • Sparc64 VII processor Note: minimum processor speed must be 1.35 Ghz or higher	Intel processors • Intel Xeon processor • Intel Core Duo processor T2600 - T2300 • Intel Itanium Processor (32 bit OS only, 1.7Ghz or higher CPU) • Intel-VT processors (VMware Optimized hardware) • Intel Xeon processor 5400 series • Intel Xeon processor 5300 series • Intel Xeon processor 7300 series • Intel Xeon processor 5500 series • Intel Xeon processor 5600 series AMD processors • Dual-Core AMD Opteron Processor • AMD Opteron Processor • AMD Athlon 64 FX Processor • AMD Athlon 64 X2 Dual-Core • AMD -V Note: minimum processor speed must be 2.33 Ghz or higher

3.2.3. Cài đặt phần mềm

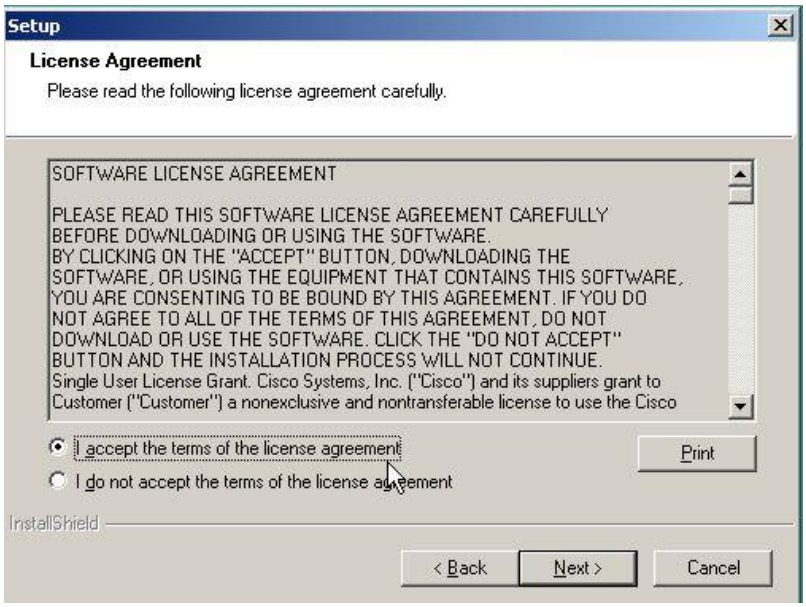
Cài đặt CiscoWorks LAN Management Solution 3.2 cũng giống như cài đặt những phần mềm khác. Hoàn toàn bằng giao diện, rất dễ dàng cho việc cài đặt dù cho người mới tiếp xúc lần đầu cũng không mấy khó khăn trong việc sử dụng.

Chương trình chỉ chạy trên các phiên bản hệ điều hành mạng như Windows 2K3 hoặc Windows 2K8. Ở đây nhóm triển khai thực nghiệm trên môi trường Windows 2K3 phiên bản R2.

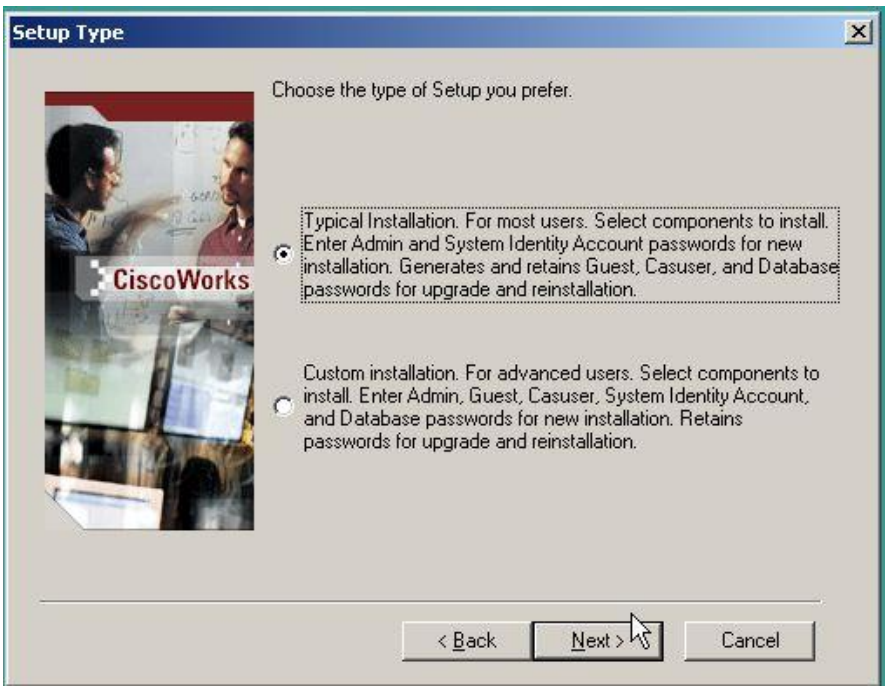


Quá trình khởi chạy cài đặt chương trình cũng giống như những chương trình bình thường khác ta thường cài đặt.

Xuất hiện bảng thông báo ta nhấn NEXT để tiếp tục công việc cài đặt



Yêu cầu chấp nhận các điều khoản giữa nhà phát triển và người sử dụng phần mềm của hãng cung cấp. Ta nhấn vào "*I accept the term of the license agreement*" và nhấn NEXT để tiếp tục công việc cài đặt.



Yêu cầu lựa chọn cài đặt theo cấu hình mặc định của nhà sản xuất phần mềm hoặc là cài theo tùy chỉnh của người sử dụng. Ta lựa chọn một trong 2 phương thức cài đặt mà ta cho là phù hợp. Sau đó tiếp tục nhấn NEXT.

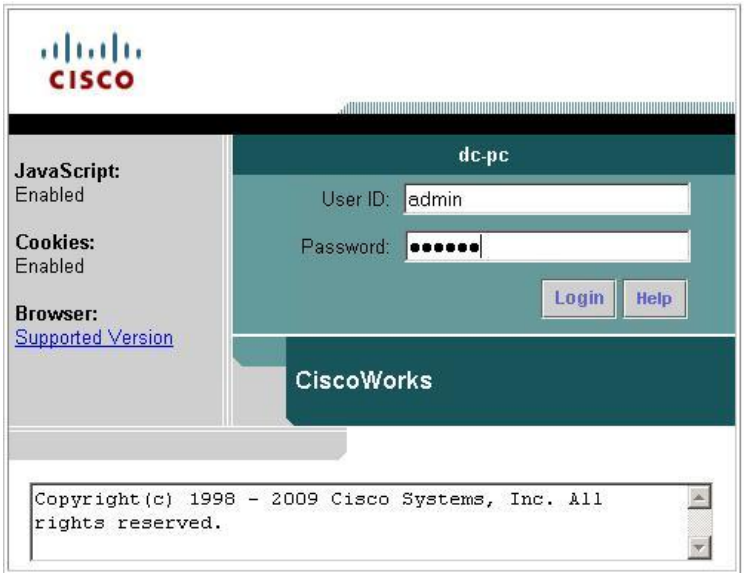
Sau một vài lần lặp lại các bước tương tự là ta đã cài đặt xong phần mềm.

3.2.4. Giao diện sử dụng vào các tính năng cơ bản

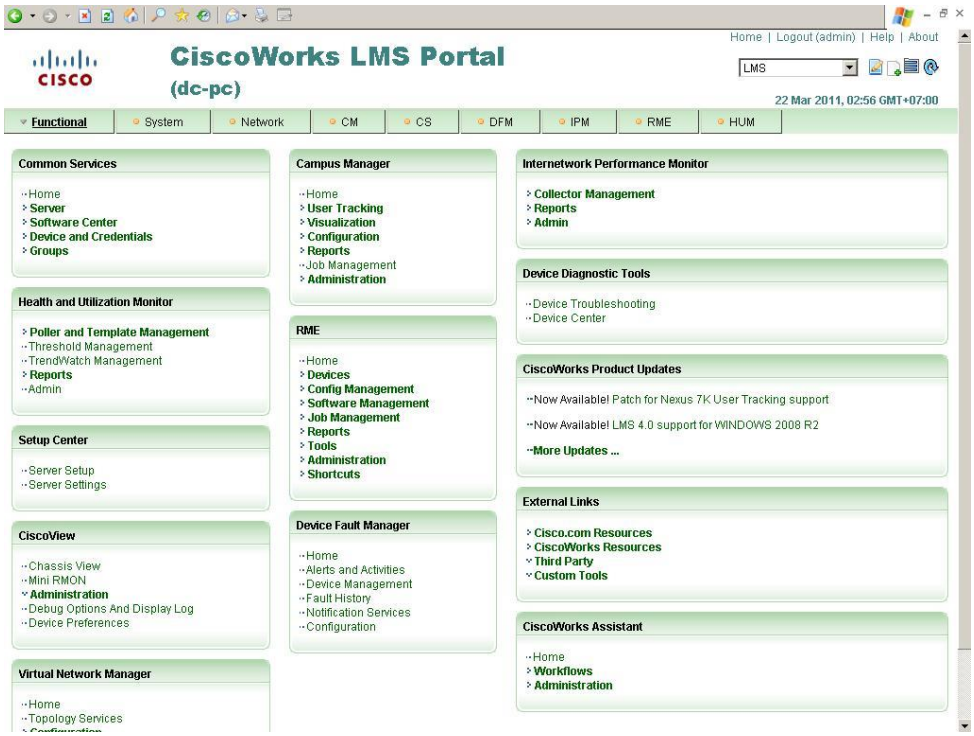
Sau khi cài đặt thành công ta kích hoạt chương trình. Chương trình giám sát mạng ***ciscoworks lan management solution*** là một chương trình có giao diện chạy hoàn toàn

trên ứng dụng web, sử dụng giao thức HTTP hoặc HTTPS tùy theo yêu cầu công việc mà ta có thể tùy chọn. Nếu lựa chọn HTTP thì chương trình sẽ hoạt động nhanh nhưng kém bảo mật, ngược lại HTTPS lại cho ta tính bảo mật cao nhưng lại làm cho hệ thống bị chậm đi.

Ta đăng nhập vào chương trình bằng User và Password đã điền vào trước lúc cài đặt để login vào chương trình.



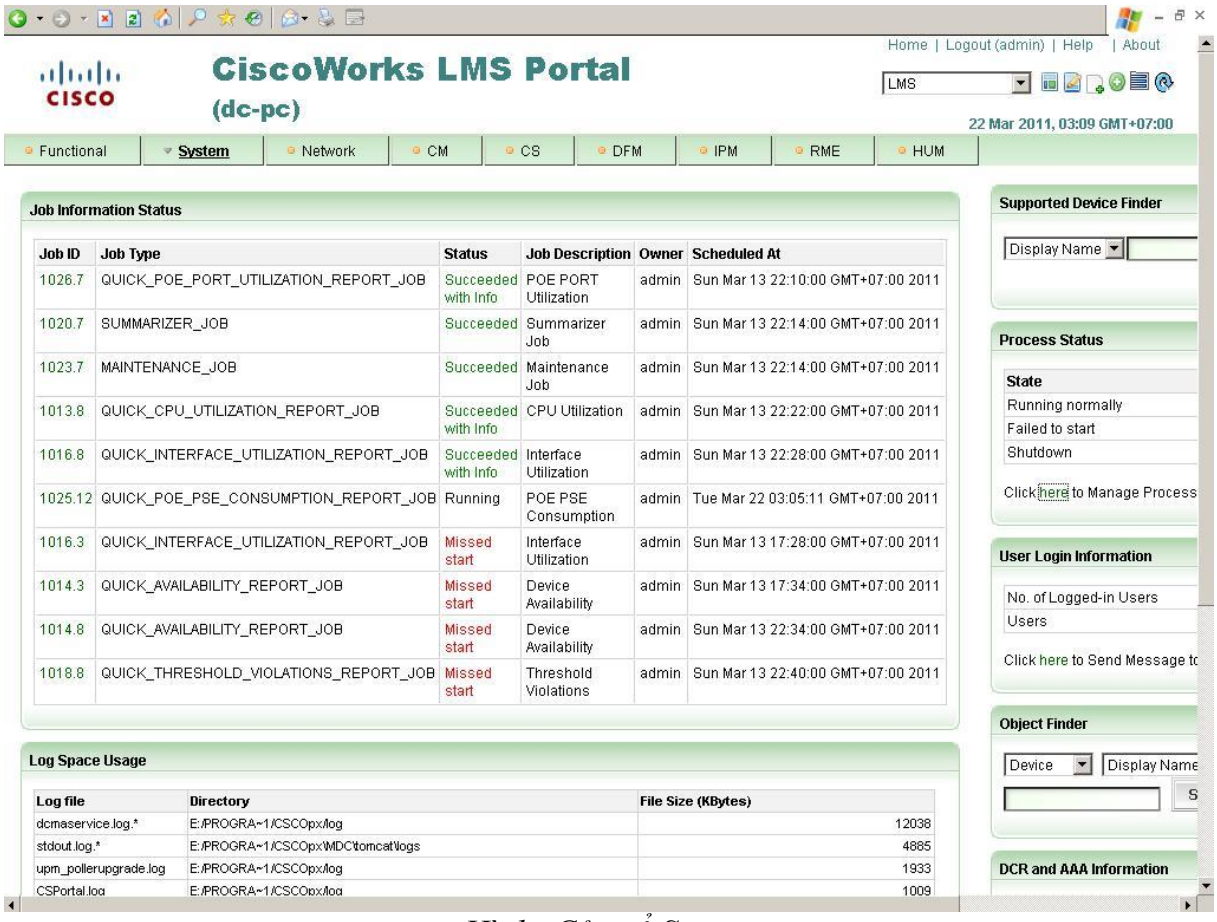
Sau khi đăng nhập thành công chương trình sẽ đưa cho chúng ta một giao diện gồm các tính năng để điều khiển, xem xét, quản lý….



Hình: Giao diện chính của chương trình.

Giao diện chính của chương trình là tổng thể các điều khiển nằm trong tab ***Functional*** bao gồm các tính năng như:

- ✓ Common service: cho ta biết về tình trạng server, trung tâm phần mền, các thiết bị…
- ✓ Setup Centrer: Nơi ta cấu hình cho toàn bộ chương trình như tạo user, thêm, sửa thông tin, xóa các thiết bị, các kết nối…
- ✓ Campus Manager: là trung tâm điều khiển, hiển thị các user đang làm việc, xem thông báo, cấu hình….
- ✓ Cisco View : Nơi chúng ta có thể xem xét tổng quan các thiết bị, dùng Mini Rmon để sửa lỗi cho các thiết bị, sự cố mạng…
- ✓ Ngoài ra còn có các Report để giúp diễn giải những hướng dẫn cho người dùng bằng các Clip ngắn giúp người dùng dễ dàng sử dụng.

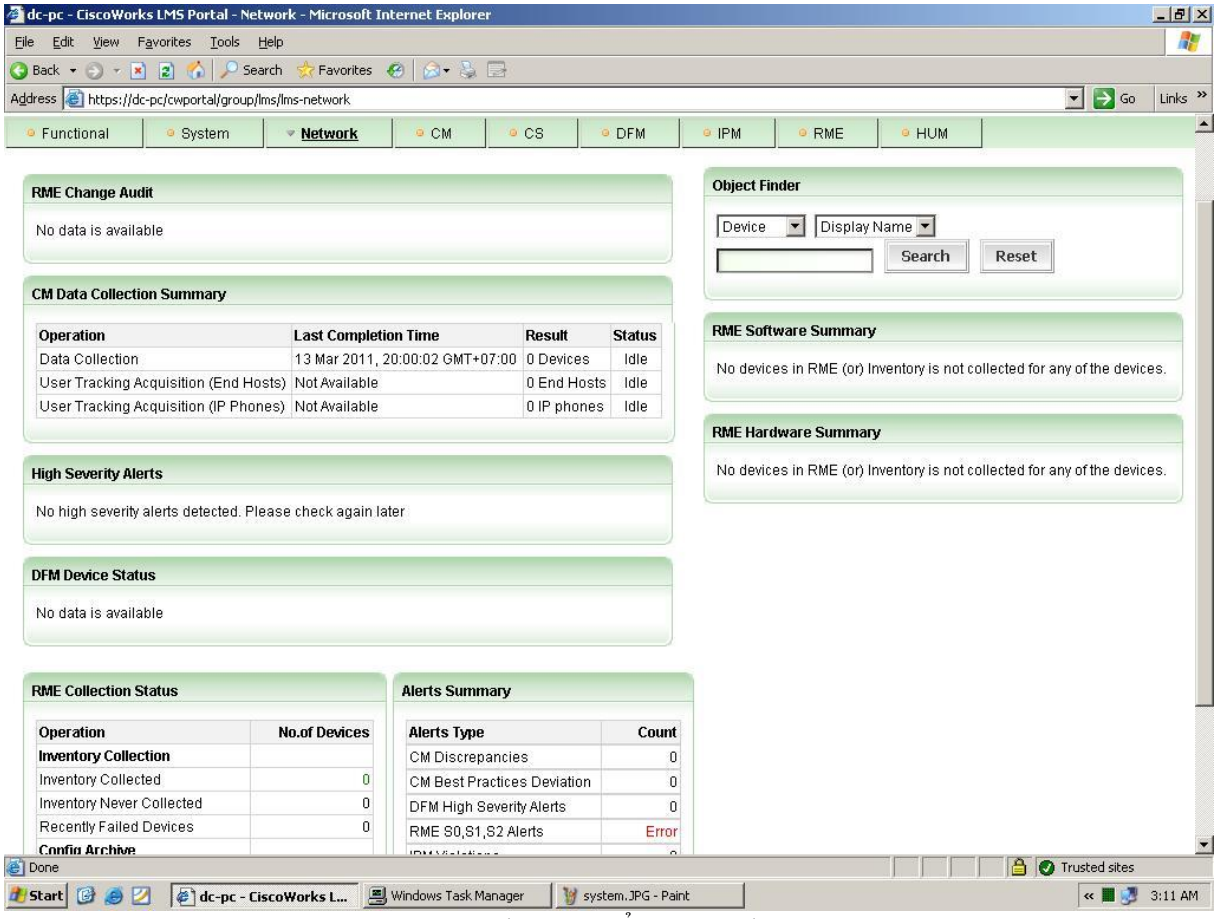


Hình: Cửa sổ System

Cửa sổ System để cho ta biết về các công việc nào đang hoạt động, công việc nào đang bị ngưng, công việc nào đã hoàn thành hay chưa.

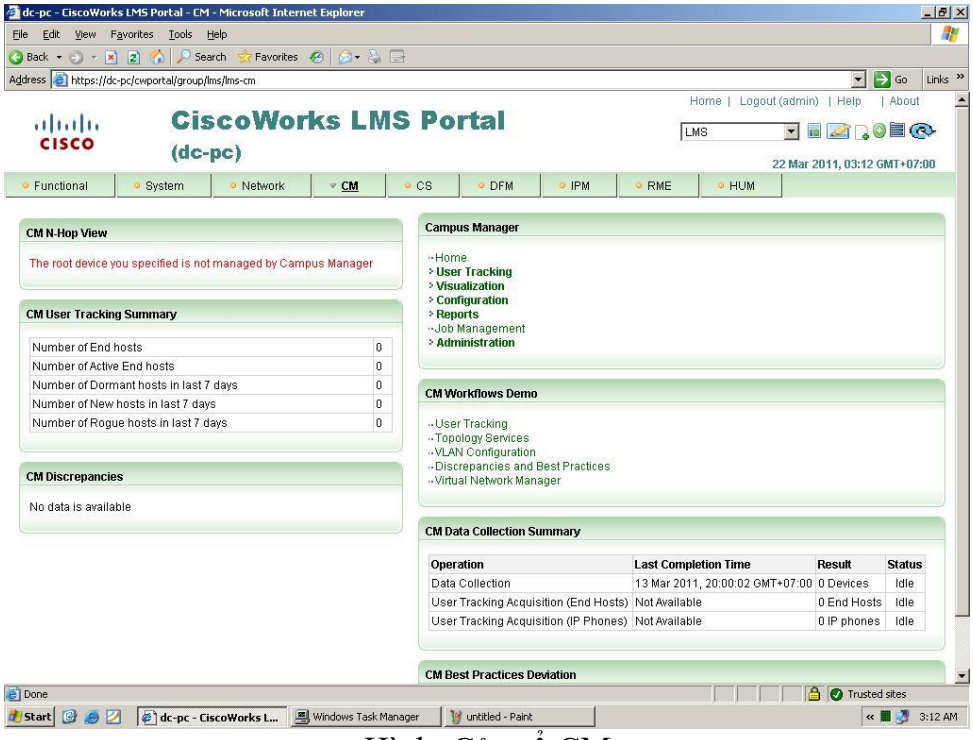
Trong phần Log space Usage còn cho ta biết tình trạng các file log ghi lại các sự kiện của hệ thống.

Ngoài ra chương trình còn hỗ trợ chức năng tìm kiếm để xem các công việc, thiết bị, công hoạt động…



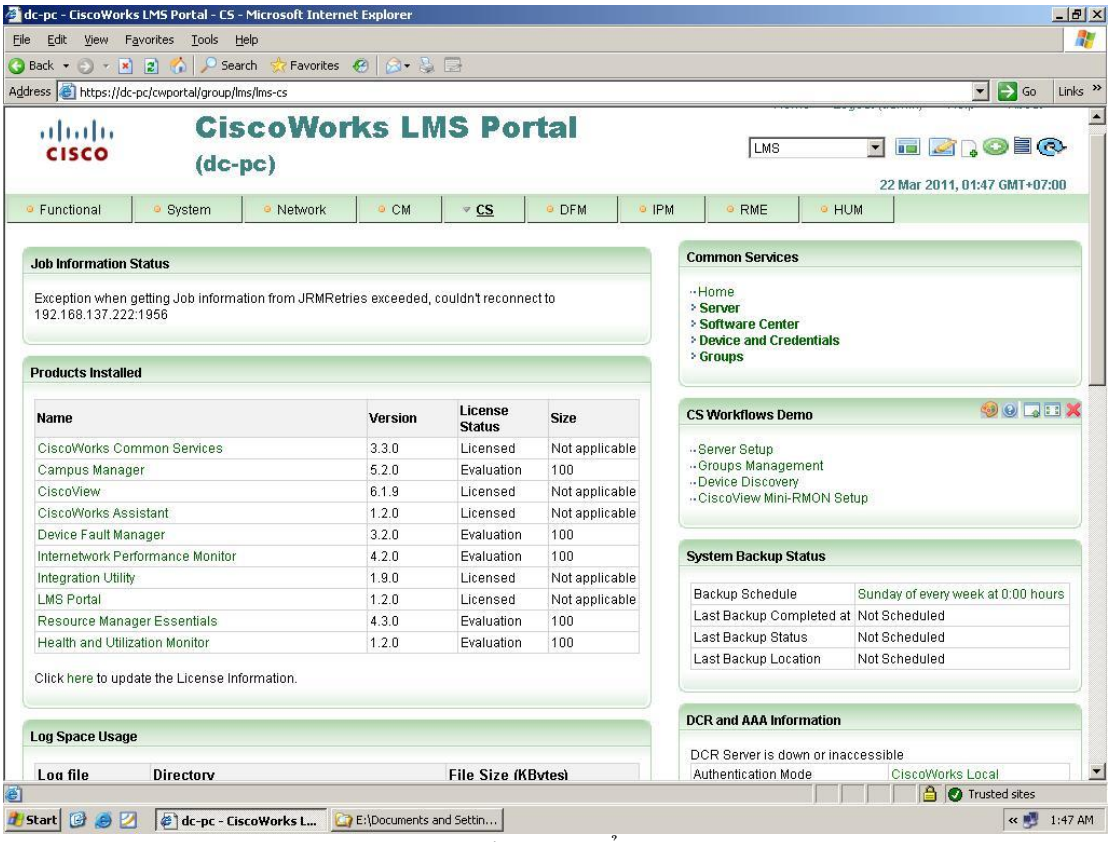
Hình: Cửa sổ Network

Cửa sổ Network cho ta thấy các thông tin về hệ thống mạng đang hoạt động bao gồm các thiết bị đang hoạt động, tình trạng của thiết bị mạng, các tác tử liên quan…



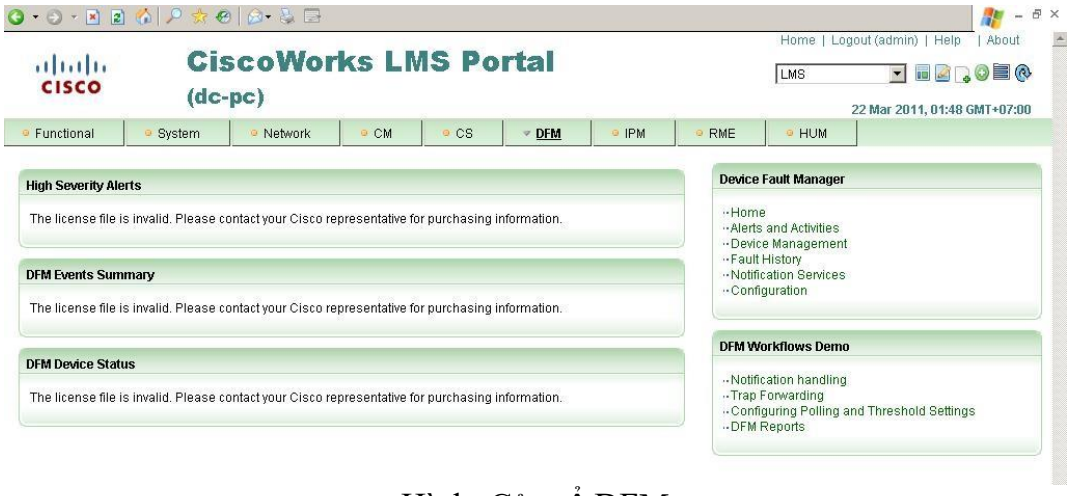
Hình: Cửa sổ CM

Campus Manager (CM) – là phần mềm quản lý các thiết bị switch của Cisco qua giao diện web, cung cấp thông tin về các thiết bị ở lớp 2, mô hình kết nối chi tiết, cấu hình VLAN, ATM LANE, quản lý các thiết bị của người dùng, điện thoại IP…



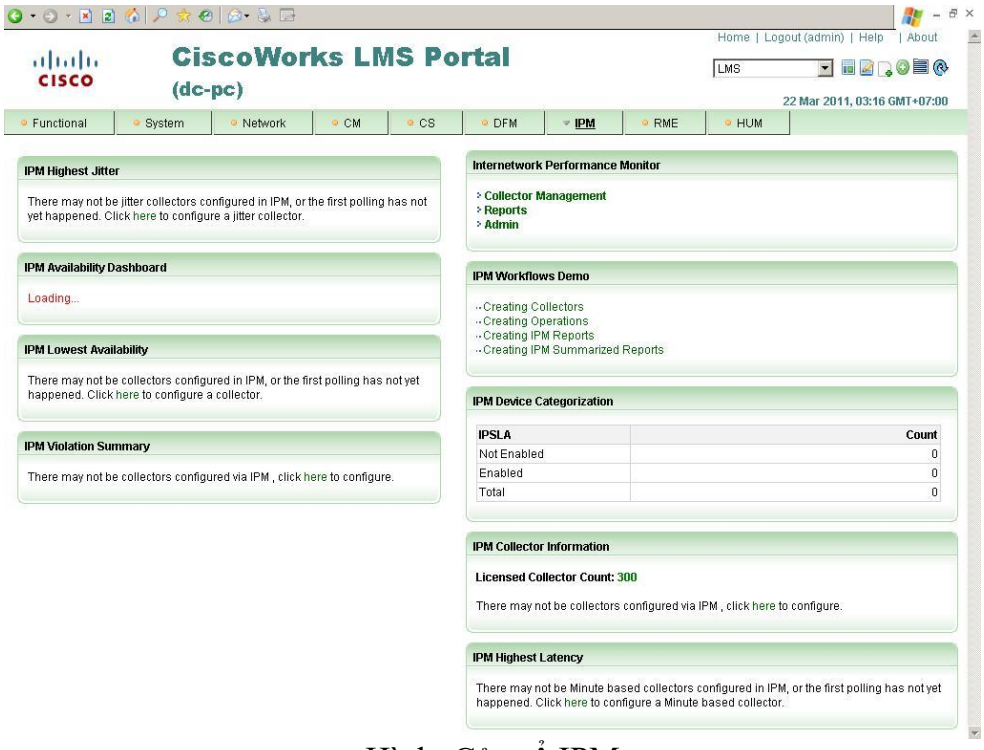
Hình: Cửa sổ CS

CS là cửa sổ hiển thị các dịch vụ được cài đặt và chạy trên hệ thống mạng, các chế độ Backup của hệ thống và tình trạng hoạt động của các ứng dụng ở các cửa sổ khác.



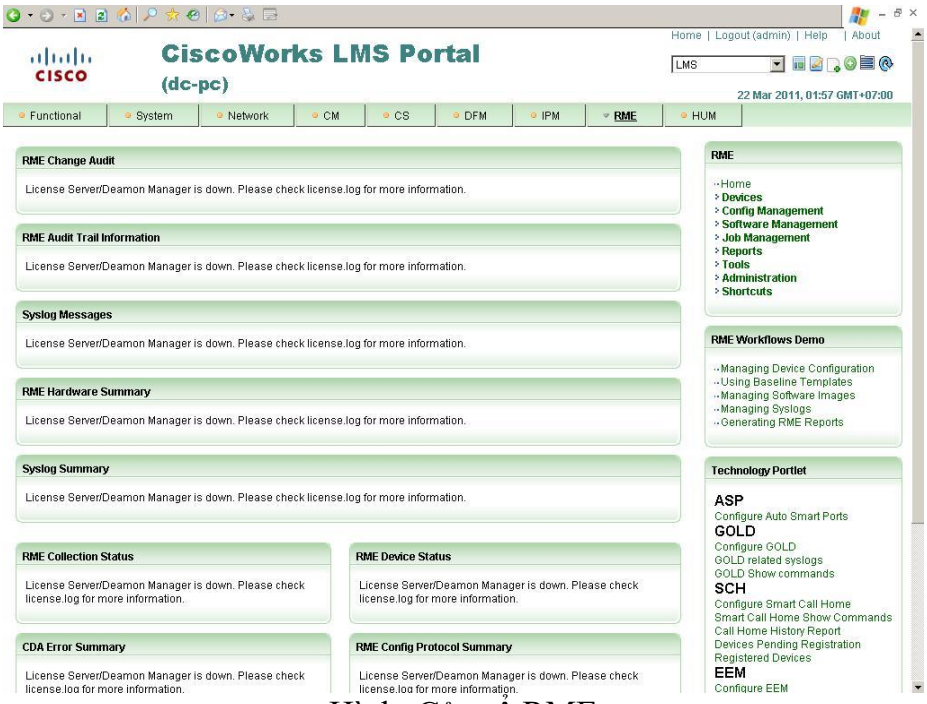
Hình: Cửa sổ DFM

DFM là phần mềm giám sát hoạt động và kiểm tra lỗi của các thiết bị mạng Cisco hoạt động ở thời gian thực, thông báo lỗi qua các thông báo lỗi, qua email, hoặc kết hợp với các thông báo của các chương trình khác.



Hình: Cửa sổ IPM

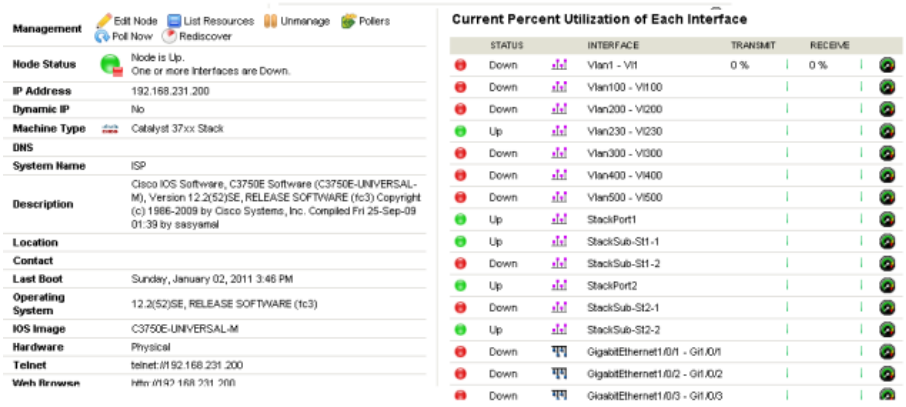
IPM cung cấp cho chúng ta các thông tin về các hoạt động qua lại giữa các mạng khác nhau trong hệ thống mà chúng ta quản lý.



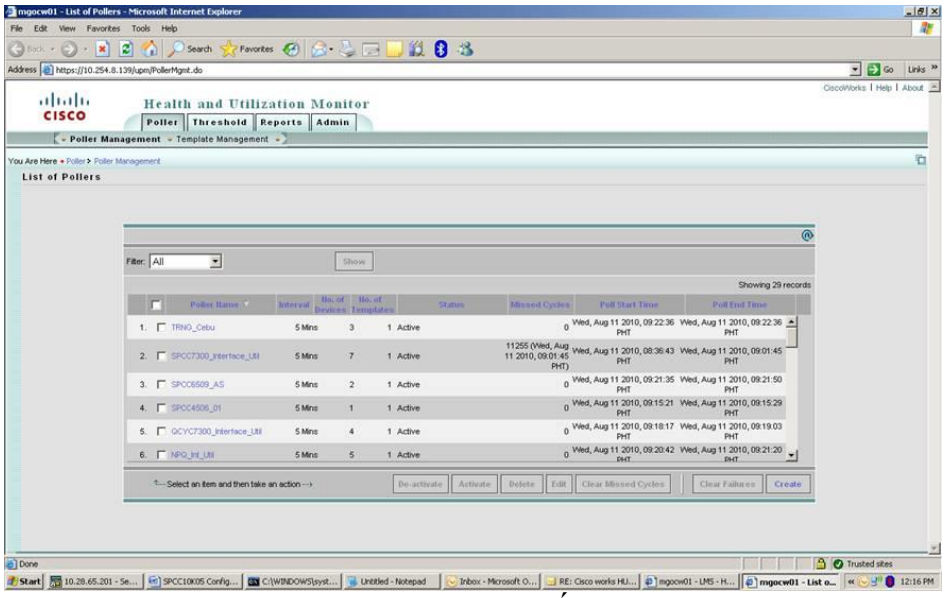
Hình: Cửa sổ RME

Resource Manager Essentials (RME) – Giúp quản lý danh sách các thiết bị mạng, cấu hình phần cứng, phần mềm, các sự cố xảy ra… Sử dụng phần mềm này chủ yếu nhằm mục đích thông kê, lập báo cáo, lưu hồ sơ về mạng.

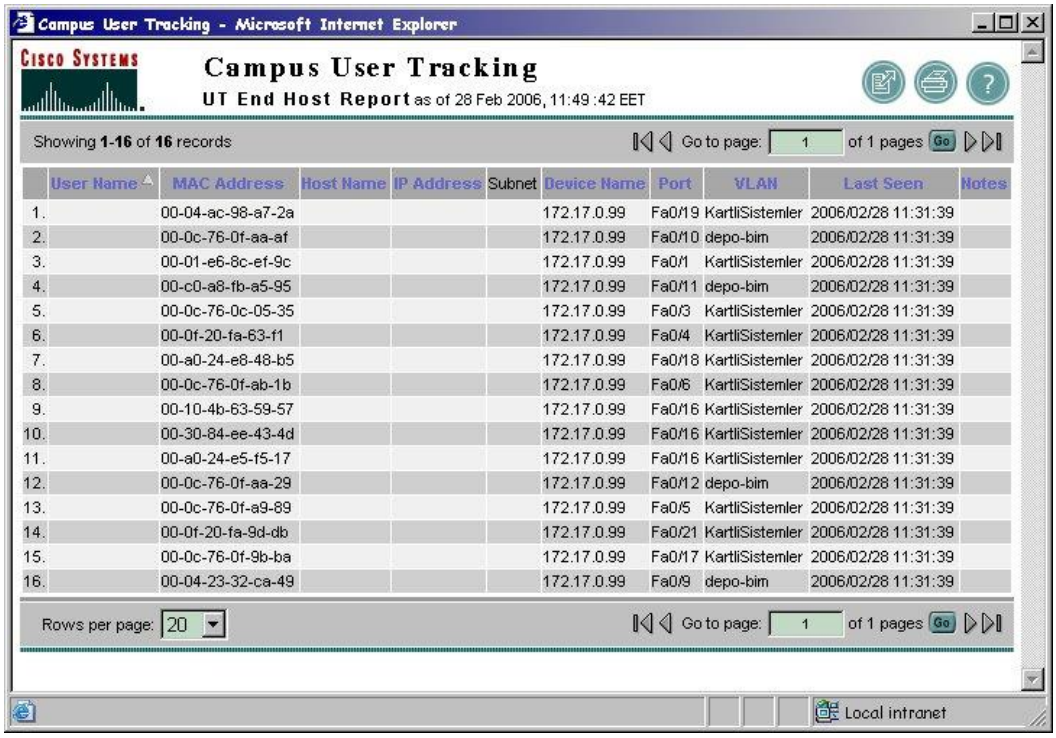
Ngoài ra phần mền còn cung cấp các thống kê như "sức khỏe" của hệ thống, tình trạng thiết bị, hệ thống mạng…



Hình: Thông tin về thiết bị trong mạng



Hình: Tình trạng của các thiết bị trong mạng



Hình: Hiện trạng của các port

Tổng Kết

Qua đồ án này giúp cho sinh viên có kỹ năng làm việc theo nhóm. Cũng cố các kiến thức đã học trong bộ môn quản lý hệ thống mạng, giúp cho sinh viên có thêm kinh nghiệm khi ra trường không bị gặp khó khăn khi tiếp xúc với các công nghệ mới. Nhưng đây chỉ là một đồ án môn học nên quá trình tìm hiểu, lượng kiến thức còn ít, còn nhiều hạn chế trong cách trình bày…

Về phần nhóm, nhóm đã rất cố gắng cùng nhau chia sẻ công việc, tìm kiếm, trao đổi tài liệu để có một đồ án tốt nhất có thể. Song do lượng kiến thức còn ít và kinh nghiệm còn thiếu nên cũng sẽ khó tránh khỏi những sai sót trong công việc. Phần mềm ***ciscoworks lan management solution*** là một phần mềm lớn, đòi hỏi cấu hình máy chủ khá cao, có bản quyền sử dụng… Mặc dù đã được phép dùng thử nhưng lại bị hạn chế nhiều tính năng cộng với máy cấu hình không đủ mạnh đã làm cho nhóm gặp nhiều khó khăn trong việc triển khai mô hình trên thực tế.

Tài liệu tham khảo

SNMP toàn tập – Diệp Thành Nguyên.
Giải pháp an ninh trong kiến trúc quản trị mạng SNMP – Trần Duy Minh.
http://nhatnghe.com
http://hvaonline.net
http://net-snmp.sourceforge.net