TRƯỜNG CĐ CNTT HỮU NGHỊ VIỆT HÀN

KHOA KHOA HỌC MÁY TÍNH

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 Orion Netflow Traffic Analyzer

Giáo viên: Thạc sĩ Đặng Quang Hiển

Lớp : MM03A – Nhóm 1

Sinh viên thực hiện :

- Lê Long Bảo
- Trần Ngọc Khải

Đà Nẵng, tháng 3 năm 2012

LỜI MỞ ĐẦU

Ngày nay với các doanh nghiệp có hệ thống mạng lớn, quy mô, thì việc quản lý hệ thống này trở nên cấp thiết hơn, với các yêu cầu về người quản trị như xem xét, hiểu được lúc nào hệ thống bị tắt nghẽn, quan sát được băng thông mạng đang thay đổi như thế nào. Nắm bắt được trạng thái của hệ thống mạng để đảm bảo hệ thống mạng được hoạt động xuyên suốt… Với môn học "Quản lý hệ thống mạng" là môn học cung cấp cho sinh viên các kiến thức về giám sát và quản lý mạng , giúp sinh viên có cái nhìn tổng quan, cách thức hoạt động, cũng như cung cấp các công cụ cần thiết để quản lý hệ thống mạng.

Với mục đích đó, nhóm 1 lớp MM03A đã lựa chọn đề tài "Tìm hiểu giao thức SNMP và phần mềm quản lý hệ thống mạng Orion Netflow Traffic Analyzer" để làm đồ án môn học. Nội dung đồ án gồm 3 chương:

- ✓ Chương 1: Tổng quan về quản lý mạng với giao thức SNMP. Mục đích của chương này là cung cấp cho chúng ta các khái niệm cơ bản nhất về giao thức quản lý mạng đơn giản SNMP.
- ✓ Chương 2: Tổng quan về phần mềm giám sát và quản trị mạng Solarwind Orion Netflow Traffic Analyzer. Trong chương này sẽ giới thiệu chung về phần mềm cũng như các bước cài đặt phần mềm.
- ✓ Chương 3: Tính năng chính của phần mềm Orion Netflow Traffic Analyzer. Chương này sẽ đi vào phần giới thiệu các tính năng cơ bản của phần mềm Orion NTA

Trong quá trình làm đồ án chắc chắn không tránh khỏi thiếu sót. Mong các thầy cô và các bạn đóng góp ý kiến để đồ án được hoàn thiện hơn. Xin chân thành cảm ơn!

Đà nẵng, tháng 3 năm 2012.

Nhóm 1 – MM03A

MỤC LỤC

DANH MỤC KÝ HIỆU VÀ TỪ VIẾT TẮT

Ký hiệu	Ý nghĩa
SNMP	Simple Network Management Protocol
IETF	Internet Engineering Task Force
MIB	Management Information Base
OID	Object ID
RMON	Remote Network Monitoring
SGMP	Simple Gateway Management Protocol
PDU	Protocol Data Unit
NTA	Network Traffic Analyzer
NPM	Network Performer Monitor

DANH MỤC HÌNH VẼ

CHƯƠNG 1: TỔNG QUAN VỀ QUẢN LÝ 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 hóa 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 đặt 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 hóa và giải mã tín hiệu, thiết bị nén dữ liệu, các gateway, các bộ xử lý front-end, các đường trung kết, DSC/DAC, các bộ lặp, bộ tái tạo tín hiệu, các thiết bị chuyển mạch, các bridge, router và switch, tất cả mới chỉ là một phần của danh sách các thiết bị sẽ phải được quản lý.

Toàn cảnh của bức tranh quản lý phải bao gồm quản lý các tài nguyên mạng cũng như các tài nguyên dịch vụ, người sử dụng, các ứng dụng hệ thống, các cơ sở dữ liệu khác nhau trong các loại môi trường ứng dụng. Về mặt kỹ thuật, tất cả thông tin trên được thu thập, trao đổi và được kết hợp với hoạt động quản lý mạng lưới dưới dạng các số liệu

quản lý bởi các kỹ thuật tương tự như các kỹ thuật sử dụng trong mạng truyền số liệu. Tuy nhiên sự khác nhau căn bản giữa truyền thông số liệu và trao đôi thông tin quản lý là việc trao đôi 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.

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

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

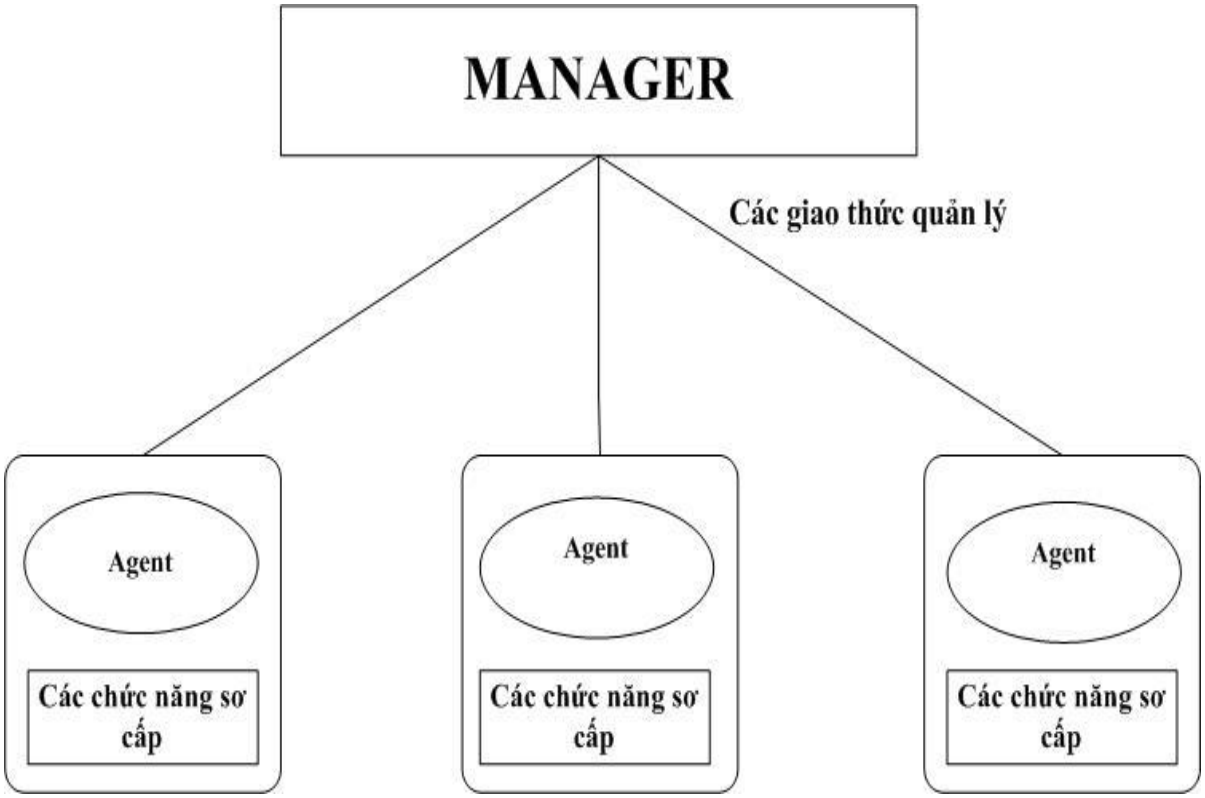
Chức năng quản lý: có nhiệm vụ thực hiện các yêu cầu của người quản lý hoặc các ứng dụng quản lý nhằm thay đổi trạng thái hay cấu hình của một tài nguyên được quản lý nào đó.

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

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

Hiện nay có hai phương pháp quản lý mạng được sử dụng khá phổ biến là quản lý mạng tập trung và quản lý mạng phân cấp.

Đối với hình thức quản lý mạng tập trung: Chỉ có một thiết bị quản lý thu nhận các thông tin và điều khiển toàn bộ các thực thể mạng. Các chức năng quản lý được thực hiện bởi manager, khả năng của hệ thống phụ thuộc rất lớn vào mức độ thông minh của manager. Kiến trúc này thường được sử dụng rất nhiều và có trung tâm quản trị mạng. So với các chức năng thuộc manager chức năng Agent thường rất đơn giản, thông tin trao đổi từ manager tới các agent thông qua các giao thức thông tin quản lý như giao thức SNMP. Tuy nhiên hệ thống quản lý tập trung rất khó mở rộng vì mức độ phức tạp của hệ thống tăng.

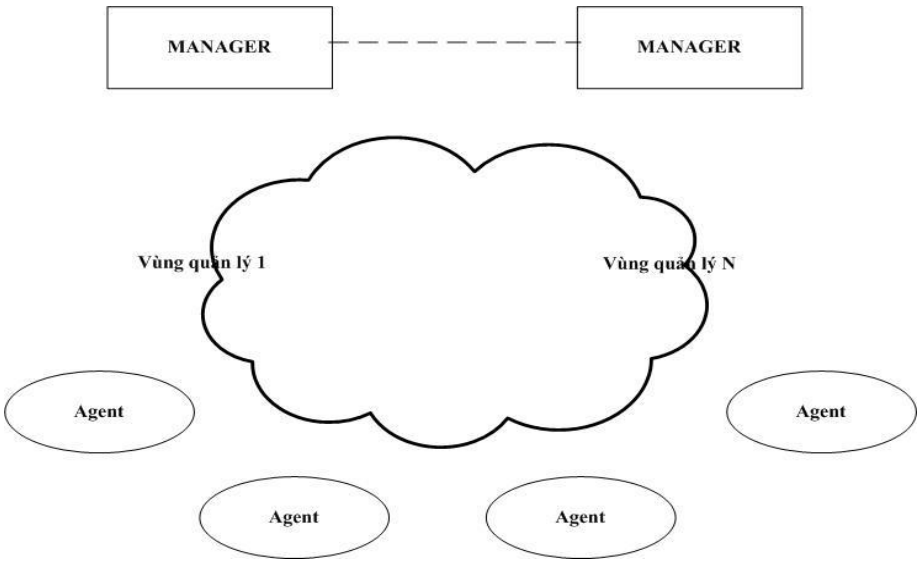


Hình 1.1: Mô hình quản lí tập trung

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

Nhược điểm: Lỗi hệ thống quản lý chính sẽ gây tác hại tới toàn bộ mạng. Tăng độ phức tạp khi có thêm các phân tử mới vào mạng.

Đối với phương thức quản lý phân cấp: Hệ thống được chia thành các vùng tùy theo nhiệm vụ quản lý tạo ra hệ thống phân cấp quản lý. Trung tâm xử lý đặt tại gốc của cây phân cấp, các hệ thống phân tán được đặt tại nhánh cây.



Hình 1.2: Mô hình quản lí phân tán

Ưu điểm: Có khả năng mở rộng hệ thống quản lý nhanh.

Nhược điểm: Danh sách thiết bị quản lý phải được xác định và cấu hình trước

1.2. TỔNG QUAN VỀ GIAO THỨC SNMP

1.2.1. Giới thiệu giao thức SNMP

Các bài toán được đặt ra để quản lý một hệ thống mạng bao gồm: Giám sát tài nguyên máy chủ, giám sát lưu lượng trên các port của switch - router, và bài toán cuối cùng là hệ thống tự động cảnh báo sự cố tức thời.

Với các bài toán trên thì giao thức SNMP ra đời nhằm giúp người quản trị quản lý tốt hệ thống của mình, giúp họ biết được tài nguyên đang được sử dụng , lưu lượng ra vào trên các cổng là bao nhiêu, và thông báo các sự cố kịp thời.

Với bài toán giám sát tài nguyên máy chủ, yêu cầu được đặt ra là nếu bạn có hàng ngàn máy chủ chạy các hệ điều hành khác nhau, vậy làm thế nào bạn có thể giám sát tài

nguyên của tất cả máy chủ hàng ngày, hàng giờ để kịp thời phát hiện các máy chủ đang quá tải. Giám sát tài nguyên máy chủ là theo dõi tỷ lệ chiếm dụng CPU, dung lượng còn lại của ổ cứng, tỷ lệ sử dụng bộ nhớ RAM,...Ứng dụng SNMP giúp người quản trị giám sát được máy chủ, nó sẽ lấy được thông tin từ nhiều HĐH khác nhau.

Với bài toán giám sát lưu lượng trên các port của switch, yêu cầu được đặt ra là làm thế nào giám sát lưu lượng đang truyền qua tất cả các port của thiết bị suốt 24/24, kịp thời phát hiện các port sắp quá tải. Ứng dụng SNMP giúp bạn giám sát lưu lượng, nó sẽ lấy được thông tin lưu lượng đang truyền qua các thiết bị.

Với bài toán hệ thống tự động cảnh báo sự cố tức thời, yêu cầu được đặt ra là nếu một port nào đó mất tín hiệu, hoặc có ai đó vừa đăng nhập vào hệ thống nhưng khai báo sai thông tin username và password và hệ thống tự động khởi động lại, vậy làm thế nào người quản trị biết được sự kiện đó đang xảy ra, để giải quyết vấn đề này, ứng dụng thu thập sự kiện (event) và cảnh báo (warning) bằng SNMP, nó sẽ nhận cảnh báo từ tất cả các thiết bị và hiện nó lên màn hình hoặc gửi email cho người quản trị.

1.2.1.1. Khái niệm giao thức SNMP

Cốt lõi của SNMP là một tập hợp đơn giản các hoạt động giúp nhà quản trị mạng có thể quản lý, thay đổi trạng thái của mạng. Ví dụ chúng ta có thể dùng SNMP để tắt một interface nào đó trên router của mình, theo dõi hoạt động của card Ethernet, hoặc kiểm soát nhiệt độ trên switch và cảnh báo khi nhiệt độ quá cao.

SNMP thường được tích hợp vào trong router, nhưng khác với SGMP (Simple Gateway Management Protocol) được dùng chủ yếu cho các router Internet, SNMP có thể dùng để quản lý các hệ thống Unix, Window, máy in, nguồn điện … Nói chung, tất cả các thiết bị có thể chạy phần mềm cho phép lấy được thông tin SNMP đều có thể quản lý được. Không chi các thiết bị vật lý mới quản lý được mà cả những phần mềm như web server, database.

Một hướng khác của quản lý hệ thống mạng là theo dõi hoạt động mạng, có nghĩa là theo dõi toàn bộ một mạng, trái với theo dõi router, host, hay các thiết bị riêng lẻ. RMON (Remote Network Monitoring) có thể giúp ta hiểu làm sao một mạng có thể tự hoạt động, làm sao các thiết bị riêng lẽ trong một mạng có thể hoạt động đồng bộ trong mạng đó.

1.2.1.2. Ưu và nhược điểm của 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. Khi có một thiết bị mới với các thuộc tính, tính năng mới thì người ta có thể thiết kế tùy chọn SNMP để phục vụ cho riêng mình. 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 hoạt động dựa trên giao thức SNMP là giống nhau.

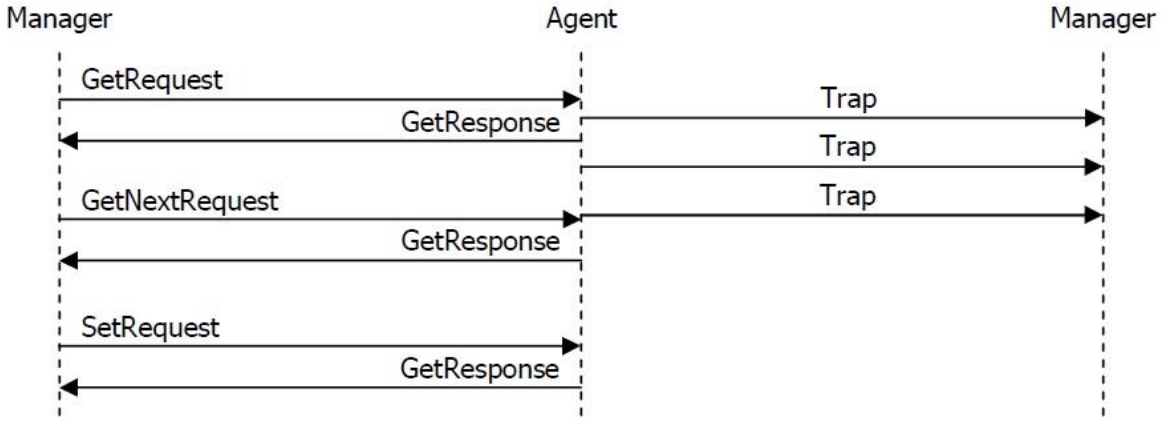
1.2.1.3. Các phiên bản của SNMP

IETF (Internet Engineering Task Force) là tổ chức đã đưa ra chuẩn SNMP thông qua các RFC. Hiện tại SNMP có 3 phiên bản: SNMPv1, SNMPv2, SNMPv3. Các phiên bản này khác nhau một chút ở định dạng bản tin và phương thức hoạt động. Hiện nay SNMPv1 là phổ biến nhất do có nhiều thiết bị tương thích nhất và có nhiều phần mềm hỗ trợ nhất.

Phiên bản SNMPv1: Phiên bản đầu tiên của SNMP, bao gồm 5 phương thức Get Request, Get Next Request, Set Request, Get Response, Trap

- *Get Request* : Bản tin GetRequest được manager gửi đến agent để lấy một thông tin nào đó. Trong Get Request có chứa ID của object muốn lấy. Ví dụ: muốn lấy thông tin tên Device 1 thì manager gửi bản tin Get Request ID = 1.3.6.1.2.1.1.5 đến Device 1, tiến trình SNMP trên Agent sẽ nhận được bản tin và tạo bản tin trả lời. Trong một bản tin Get Request có thể chứa nhiều Object ID, nghĩa là dùng một Get Request có thể lấy về cùng lúc nhiều thông tin.
- *Get Next Request:* Bản tin GetNextRequest cũng dùng để lấy thông tin và cũng có chứa OID, tuy nhiên nó dùng để lấy thông tin của object nằm kế tiếp object được chỉ ra trong bản tin. Chúng ta đã biết khi đọc qua những phần trên: một MIB bao gồm nhiều OID được sắp xếp thứ tự nhưng không liên tục, nếu biết một OID thì không xác định được OID kế tiếp. Do đó ta cần GetNextRequest để lấy về giá trị của OID kế tiếp. Nếu thực hiện GetNextRequest liên tục thì ta sẽ lấy được toàn bộ thông tin của agent.

- *Set Request:* 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.
- *Get Response:* 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.
- *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.



Hình 1.3. Các phương thức trong SNMPv1

Phiên bản 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. 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. 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.

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

Nhóm hệ thống (System group): là một mở rộng của nhóm system trong MIB-II gốc, bao gồm một nhóm các đối tượng cho phép một Agent SNMPv2 mô tả các đối tượng tài nguyên của nó.

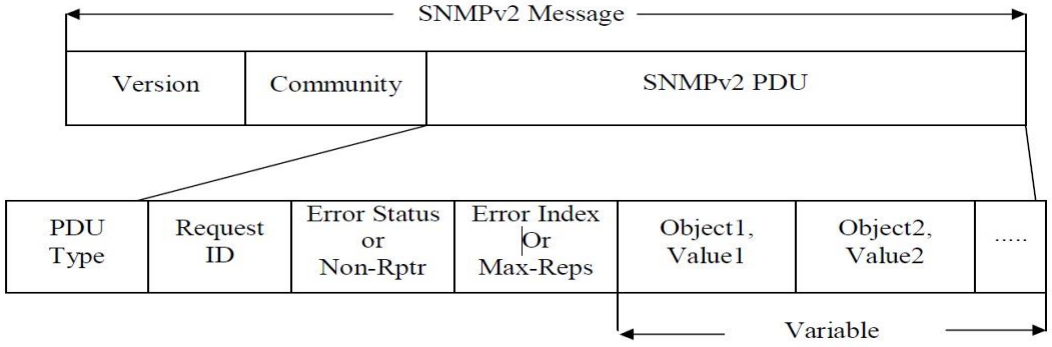
Nhóm SNMP (SNMP group): một cải tiến của nhóm SNMP trong MIB-II gốc, bao gồm các đối tượng cung cấp các công cụ cơ bản cho hoạt động giao thức.

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

Nhóm hệ thống: nhóm system định nghĩa trong SNMPv2 giống trong MIB-II và bổ sung một vài đối tượng mới.

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

Nhóm đối tượng MIB: Nhóm các đối tượng MIB chứa các đối tượng thích hợp thêm vào việc điều khiển các đối tượng MIB.



Hình 1.4: Cấu trúc bản tin SNMPv2

1.2.2. Hai phương thức giám sát Poll và Alert

1.2.2.1. 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 nhập được thông tin mới nhất từ device.

Ví dụ: Người quản lý cần theo dõi khi nào thợ làm xong việc. Anh ta cứ thường xuyên hỏi người thợ "Anh đã làm xong chưa", và người thợ sẽ trả lời "Xong" hoặc "Chưa".

1.2.2.2. 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.

Ví dụ: Người quản lý cần theo dõi tình hình làm việc của thợ, anh ta yêu cầu người thợ thông báo cho mình khi có vấn đề gì đó xảy ra. Người thợ sẽ thông báo các sự kiện đại loại như "Tiến độ đã hoàn thành 50%", "Mất điện lúc 10h", "Có điện lúc 11h", "Có tai nạn xảy ra".

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 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.

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:

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 mình không quan tâm.	✶ Tất cả những event xảy ra đều được gửi về Manager. Manager phải có cơ chế lọc nhưng 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. Ví dụ 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. Ví dụ device có một port down và Manager được khởi động sau đó thì Manager sẽ không 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 nhập. Tuy nhiên khi đường truyền thông suốt trở lại thì Manager sẽ cập nhập được thông tin mới nhất do nó luôn poll định kỳ.	✶ Khi đường truyền xảy ra 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 từng device để trỏ đến Manager. Khi thay đổi Manager thì phải cài đặt lại trên tất cả device.
✶ Nếu tần suất Poll thấp, thời gian chờ	✓ Ngay khi có sự kiện xảy ra thì device

	giữa 2 chu kỳ poll dài sẽ làm Manager chậm cập nhập 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.		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.

Poll hay Alert:

Hai phương thức Poll và Alert có điểm thuận lợi và bất lợi ngược nhau, do đó nhiều trường hợp ta nên sử dụng kết hợp cả Poll lẫn Alert để đạt được hiệu quả kết hợp của cả hai.

Các ví dụ ứng dụng cơ chế Poll & Alert :

- Giao thức Syslog : mỗi khi có sự kiện xảy ra thì thiết bị sẽ gửi bản tin syslog đến Syslog Server.
- Phần mềm NetworkView, giám sát tình trạng các server bằng cách ping liên tục.
- Giao thức STP, phát hiện loop trong mạng bằng cách gửi nhận các gói BPDU và gửi bản tin Topology change mỗi khi phát hiện thay đổi.
- Trong quản lý người ta luôn thực hiện song song chế độ kiểm tra và báo cáo, thường xuyên kiểm tra để phát hiện vấn đề và báo cáo ngay khi xảy ra vấn đề.

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. Object ID

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 :

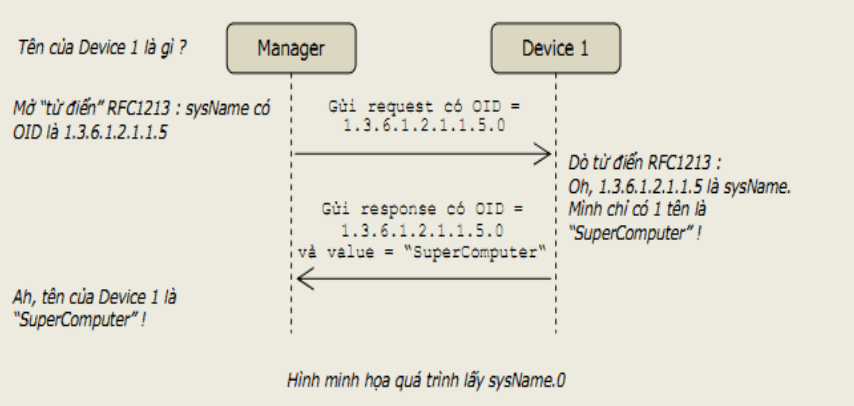
- ✓ Tổng số port giao tiếp (interface) được gọi là ifNumber, OID là 1.3.6.1.2.1.2.1.
- ✓ Tên thiết bị được gọi là sysName, OID là 1.3.6.1.2.1.1.5.
- ✓ Địa chỉ Mac Address của một port được gọi là ifPhysAddress, OID là 1.3.6.1.2.1.2.2.1.6.
- ✓ Số byte đã nhận trên một port được gọi là ifInOctets, OID 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 1.5. Minh họa quá trình lấy sysName

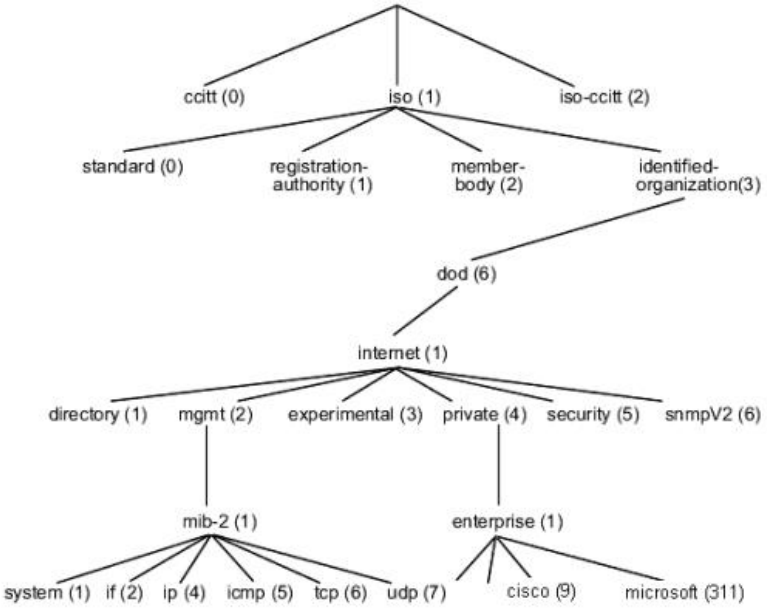
1.2.3.2. Object access

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 1.6. Minh họa MID 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.

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 thông 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. Mối quan hệ giữa Manager – Agent

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.

CHƯƠNG 2: TỔNG QUAN VỀ PHẦN MỀM GIÁM SÁT VÀ QUẢN TRỊ MẠNG SOLARWINDS ORION NTA

2.1. Giới thiệu về Solarwinds

Solarwinds là bộ công cụ hỗ trợ đắc lực cho nhà quản trị nhằm phân tích, giám sát cũng như các công cụ quản lý việc thực thi trên hệ thống mạng. Phần lớn các công cụ trong solarwinds đều sử dụng giao thức SNMP để truyền thông. Solarwinds bao gồm 32 công cụ được chia làm 6 phần lớn.

- ✓ Network Discovery Tools
- ✓ Ping Diagnostic Tools
- ✓ Tools for Cisco Routers
- ✓ IP Address Management Tools
- ✓ Fault & Performance Monitoring Tools
- ✓ Miscellaneous Tools

Các chức năng quản trị của Solarwinds.

1. Performance management: Quản lý việc thực thi của hệ thống.
   - ➢ Độ tin cậy.
   - ➢ Thời gian truyền
   - ➢ Tính hiệu quả
   - ➢ Công cụ sử dụng: Network performance monitor.
2. Configuration management: Quản lý các thông số cấu hình của hệ thống.
   - ➢ Install (Cài đặt)
   - ➢ Update (Cập nhật)
   - ➢ Extension (Mở rộng)
   - ➢ Công cụ sử dụng: Network performance monitor, DNS Analyser và DNS/Whois Resover.
3. Fault management: Quản lý lỗi cho hệ thống mạng.
   - ➢ Preactive: Khắc phục khi có sự cố xảy ra.
   - ➢ Proactive: Tác động đến hệ thống trước khi hệ thống xảy ra lỗi (điều này dựa vào kinh nghiệm của người quản trị mạng)

- Công cụ sử dụng: Network performance monitor.

4. Security management: Quản lý bảo mật hệ thống mạng.
   - Packer Filter: Lọc gói dữ liệu
   - Access Control: Điều khiển truy cập.
   - Tài nguyên mạng.
   - Service:
     - Xác thực ai muốn dùng tài nguyên
     - Giới hạn quyền cho tất cả người dùng sử dụng tài nguyên.
     - Bất kỳ dữ liệu lưu trữ nào cũng được cấp quyền.
     - Tính toàn vẹn dữ liệu trên đường truyền.
     - Tính không chối cãi của việc chia sẽ.
   - Công cụ sủ dụng:
     - Port Scanner: Xác định trên Agent có những dịch vụ nào đang chạy thông qua số hiệu cổng của dịch vụ.
     - SNMP Brute Force Attack: Công cụ quét community của Agent.
5. Accounting management: Quản lý tài khoản người dùng.
   - Xác thực.
   - Cấp quyền.
   - Giám sát quyền hạn trên Agent.
   - Công cụ sử dụng: IP Network Browser.

2.2. Cài đặt và cấu hình Solarwind Orion Netflow Traffic Analyzer

2.3.1. Giới thiệu về Orion NTA

Orion NTA là phần mềm cung cấp cho người dùng khả năng theo dõi tài nguyên mạng một cách nhanh chóng và dễ dàng.

Orion NTA cung cấp các tính năng giúp cho người dùng có thể theo dõi và kích hoạt thiết bị mạng của họ và tự động bổ sung các nguồn NetFlow.

Vì sao phải dùng Orion NTA:

- Cải thiện tính năng và hiệu suất

Với Orion NTA, người dùng có thể nhanh chóng phát hiện, chẩn đoán, và giải quyết sự cố mạng.

- Giúp phân tích được hiệu suất mạng

Orion NTA làm nổi bật xu hướng lưu lượng truy cập mạng, cho phép người dùng có thể dễ dàng dự đoán được băng thông ở các khu vực gặp tắt nghẽn

- Tối ưu hóa mạng lưới cấp phát tài nguyên

Thông tin được cung cấp bởi Orion NTA cho phép người dùng xác định được các khu vực đang bị giới hạn hoặc gặp sự cố về kết nối mạng. Sau đó, người dùng có thể chuyển hướng lưu lượng truy cập hiện tại sang các khu vực có băng thông tốt hơn.

- Các tài nguyên được liên kết

Bởi vì Orion NTA được xây dựng dựa trên Orion NPM, người dùng có thể đánh giá được các nhu cầu của mạng doanh nghiệp trong một cái nhìn tổng thể và các chi tiết chức năng cụ thể của giao diện và nút mạng.

- Tăng cường bảo mật

Orion NTA cung cấp cho người dùng khả năng một cách nhanh chóng và chính xác kiểm tra lưu lượng mạng và sau đó xác định và đưa ra mô hình những biểu hiện bất thường và có thể phát hiện virus, bot, hoặc các phần mềm gián điệp.

Người dùng có thể chuyển đổi giữa các chương trình để có được một sơ đồ hoàn chính việc sử dụng, hiệu suất, và nhu cầu của mạng. Tất cả mọi thứ người dùng cần theo dõi lưu lượng sẽ được hiển thị trong Orion NPM và Orion NTA.

- **Cài đặt và cấu hình**

Yêu cầu cần thiết trước khi cài đặt.

a. Yêu cầu về phần cứng máy chủ.

Yêu cầu	Quản lý từ 100 đến 500 đối tượng	500< đối tượng < 2000	Lớn hơn 2000 đối tượng
Tốc độ xử lý CPU	2.0 GHz	2.4 GHz	3.0 GHz
	Ghi chú: Dùng bộ xử lý kép (Dual processor)		
Dung lượng vật lý tối thiểu	2 GB	5GB	20GB
	Ghi chú: cần ít nhất 1GB dung lượng trống để cài đặt Orio NPM và pải cài đặt vào cùng ổ hệ thống nơi đang lưu trữ hệ		

	điều hành		
Bộ nhớ chính	3GB	4GB	4GB

Bảng **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.1. Yêu cầu phần cứng máy chủ trước khi cài đặt Solawinds

b. Yêu cầu về phần mềm.

Phần mềm	Yêu cầu
Opera System	- Windows Server 2003 hoặc 2008, với IIS ở chế độ 32-bit.IIS phải được cài đặt. Nên quản trị cục bộ để đảm bảo đầy đủ chức năng của công cụ Orion NPM - Lưu ý: SolarWinds khuyên người dùng không nên cài đặt Orion NPM trong môi trường Windows XP, Windows Vista hoặc Windows 7.
Máy chủ WEB	-Microsoft IIS phiên bản 6.0 và cao hơn, ở chế độ 32-bit.
.NET Framework	- Phiên bản 3.5 trở lên.
Dịch vụ Trap SNMP	- Các thành phần, công cụ giám sát và quản lý hệ điều hành Windown
Trình duyệt web	- Internet Explorer phiên bản 6.0 trở lên hoặc Firefox phiên bản 3.0 trở lên.

Bảng 2.2. Yêu cầu phần mềm trước khi cài đặt Solawinds

c. Yêu cầu về cơ sở dữ liệu.

Yêu cầu	Quản lý từ 100 đến 500 đối tượng	500< đối tượng < 2000	Lớn hơn 2000 đối tượng
SQL Server	- SQL Server 2005 SP1 Express, Standard, or Enterprise. - SQL Server 2008 Express, Standard, or Enterprise.		

Tốc độ xử lý CPU	2GHz	2.4GHz	3GHz
Dung lượng đĩa cứng	2GB	5GB	20GB
Bộ nhớ chính	2GB	3GB	4GB

Bảng **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.2. Yêu cầu về CSDL

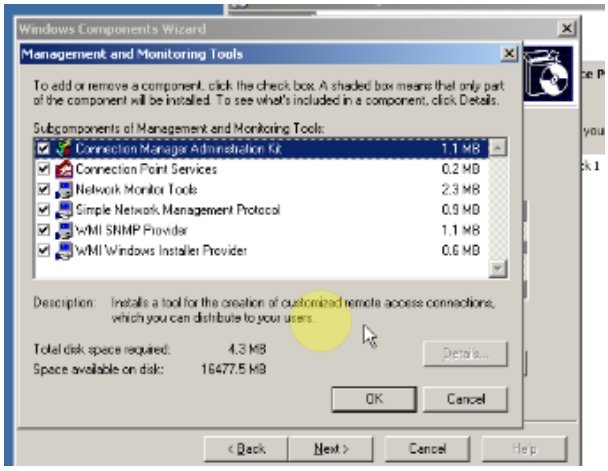
Cài đặt.

➢ Một số lưu ý:

- Trước khi cài đặt Orion NTA ta phải cài Solarwind Orion NPM
- Trước khi cài NPM phải cài .Net Framwork phiên bản 3.5 trở lên trước.
- Cài đặt IIS trước khi bạn cài NPM, mà chủ yếu là World Wide Web Service (www), Simple Network Management Protocol (SNMP) và WMI SNMP Provider.
- Khi cài đặt, tốt nhất nên cài vào ổ đĩa hệ thống, tức là ổ đĩa logic lưu file cài đặt NPM và hệ điều hành là một.
- Nên tắt phần hỗ trợ IPv6 đối với các hệ điều hành Windows Server 2008, Windows Vista, or Windows 7 trước khi cài đặt.

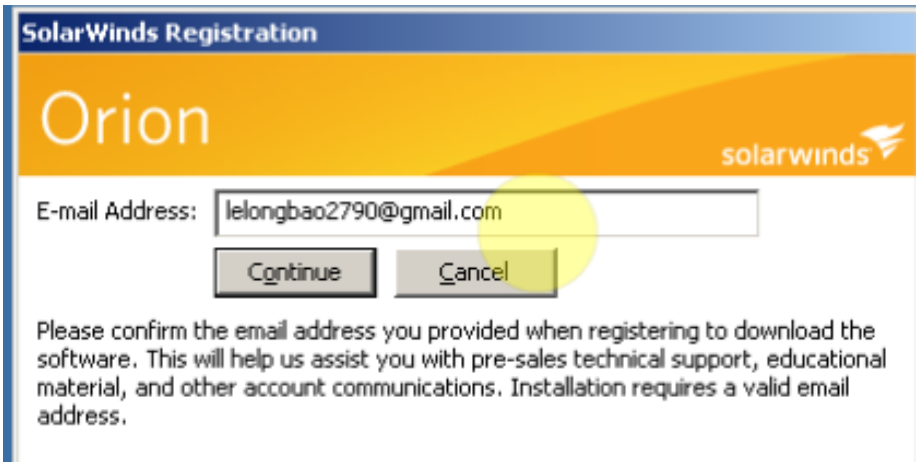
➢ ***Quá trình cài đặt Orion NPM***

Vào Start/ Control Panel/ Add or Remove Program/ Windows Component



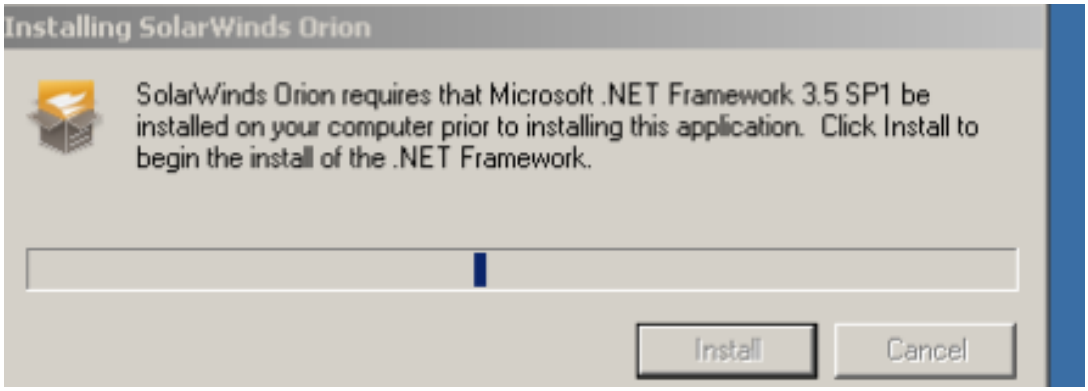
Hình 2.1. Cài đặt dịch vụ SNMP lên máy chủ

Điền email của bạn vào bấm Continue

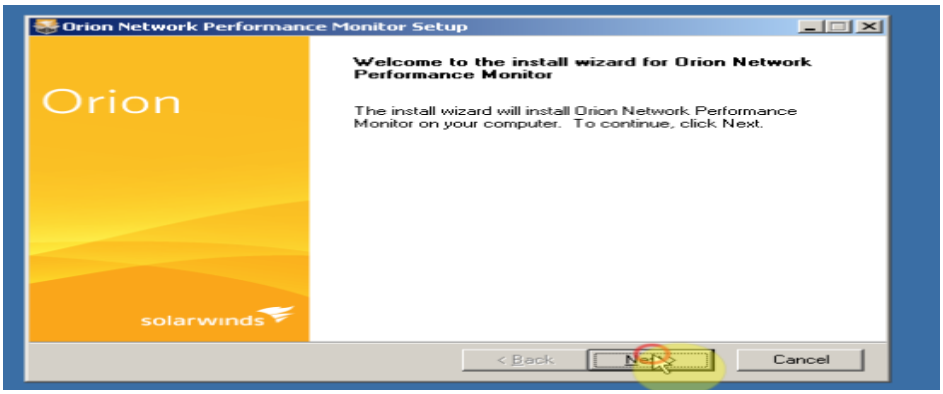


Hình 2.2. Nhập thông tin email để đăng ký

Chương trình yêu cầu cài đặt .NET Framwork trước khi cài đặt phần mềm

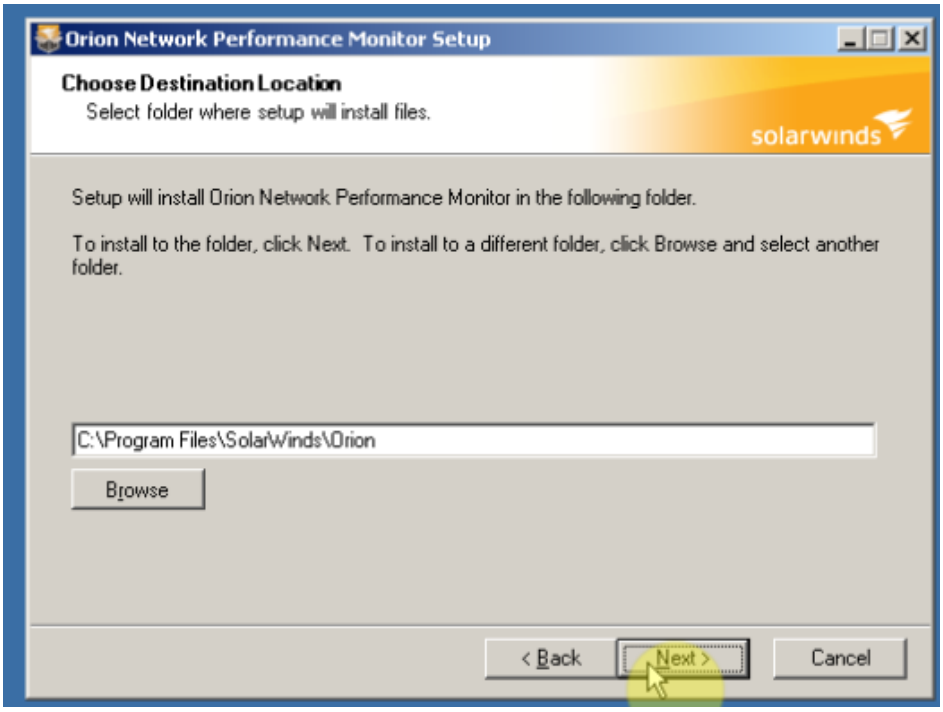


Hình 2.3. Chương trình cài .NET Framework 3.5

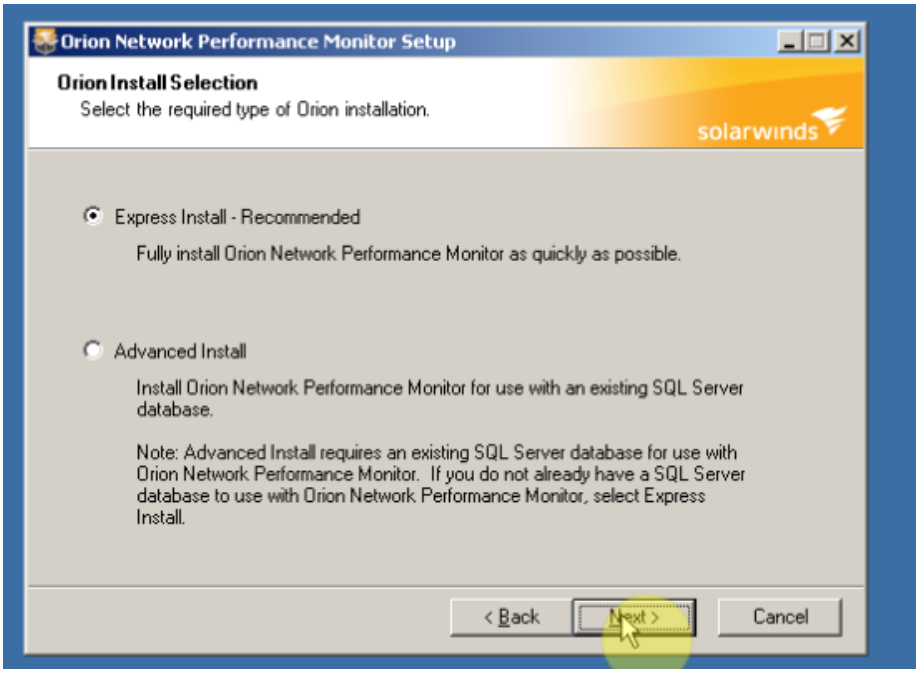


Hình 2.4. Chương trình Orion bắt đầu cài đặt

Hình 2.5. Bảng yêu cầu chấp nhận điều khoản phần mềm

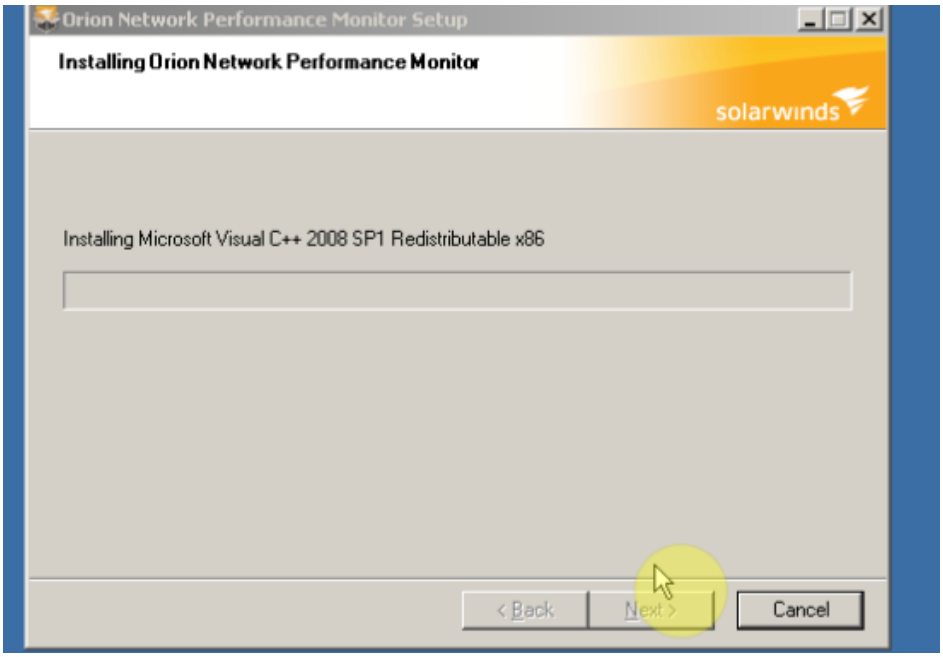


Hình 2.6. Chọn nơi cài đặt phần mềm

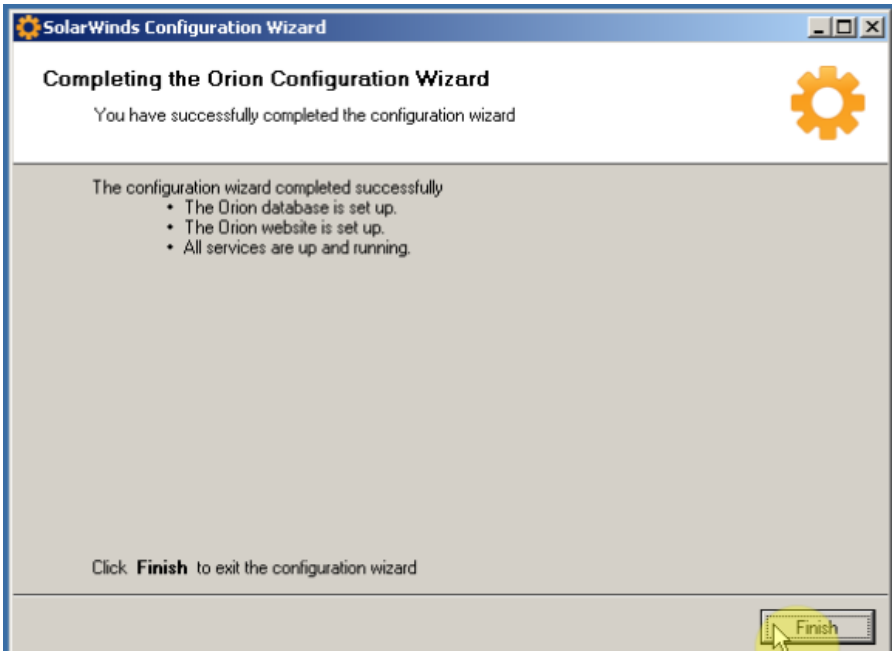


Hình 2.7. Tùy chọn cài đặt

+ Express Install: Cài đặt khi không có SQL Server database sử dụng cùng với NPM.
+ Advanced Install: Cài đặt NPM sử dụng SQL database đang hiện hành



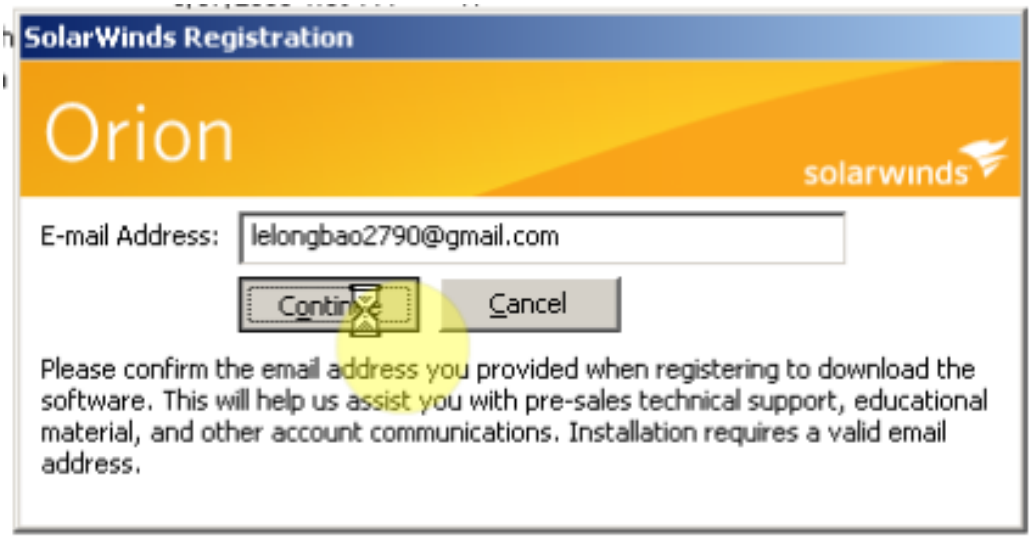
Hình 2.8. Quá trình cài đặt các gói cấu hình



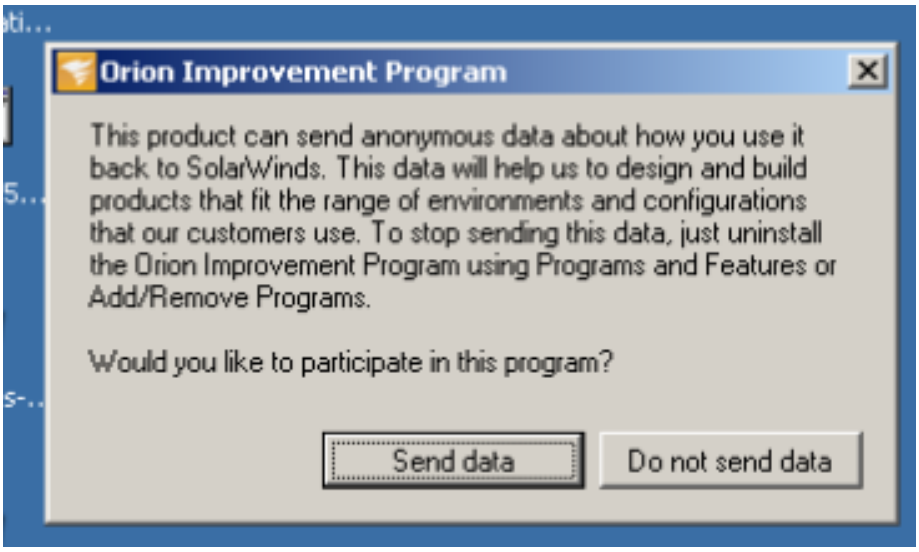
Hình 2.9. Quá trình cài đặt NPM thành công

- ***Quá trình cài đặt Orion NTA***

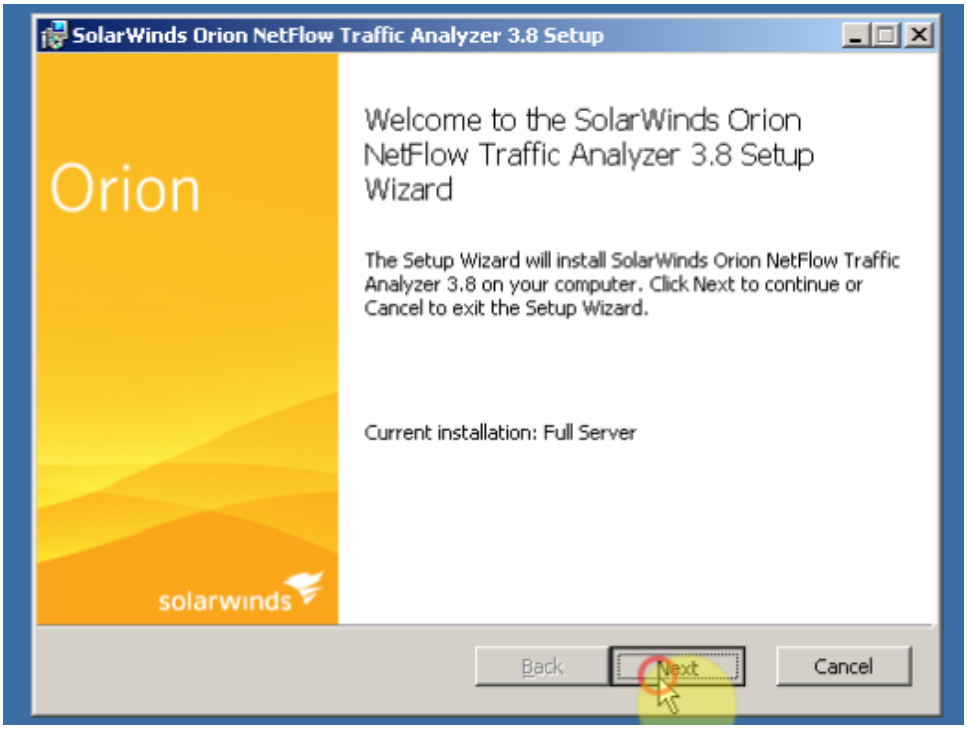
Điền email của bạn vào, bấm Continue



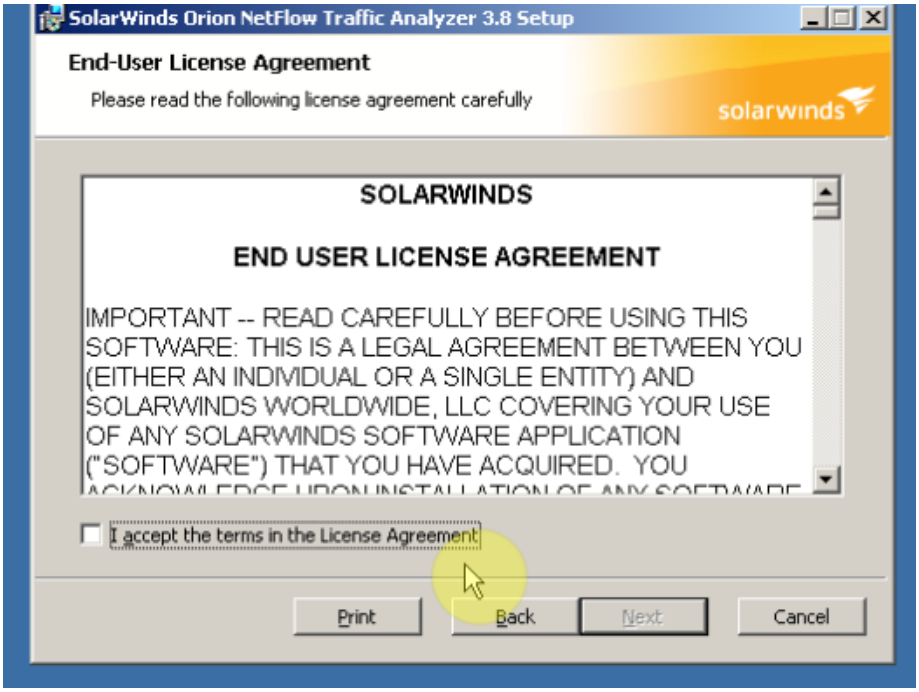
Hình 2.10. Nhập thông tin email đăng ký



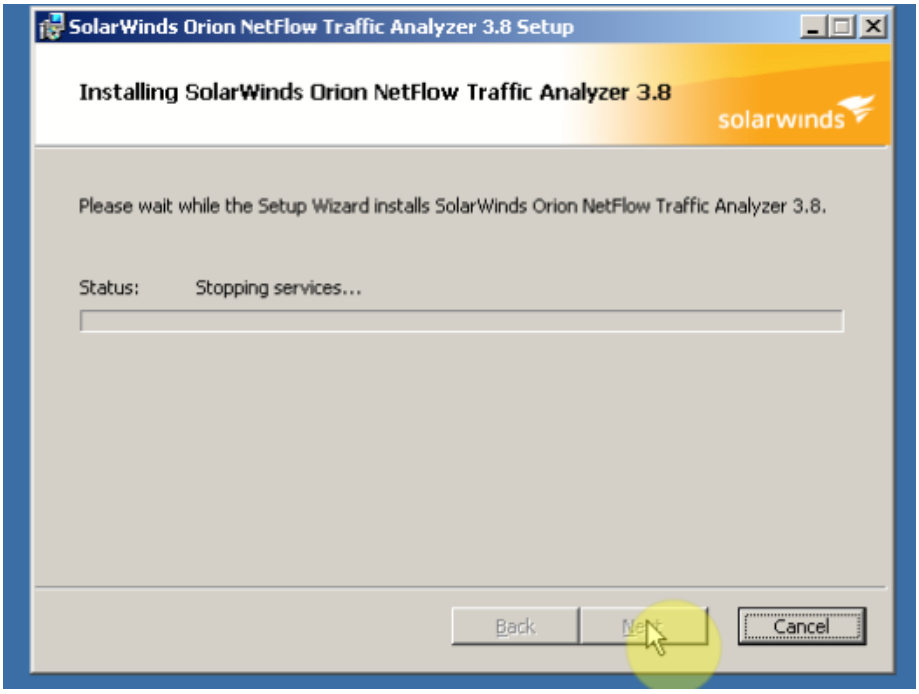
Hình 2.11. Bảng thông báo về việc gửi dữ liệu cập nhập



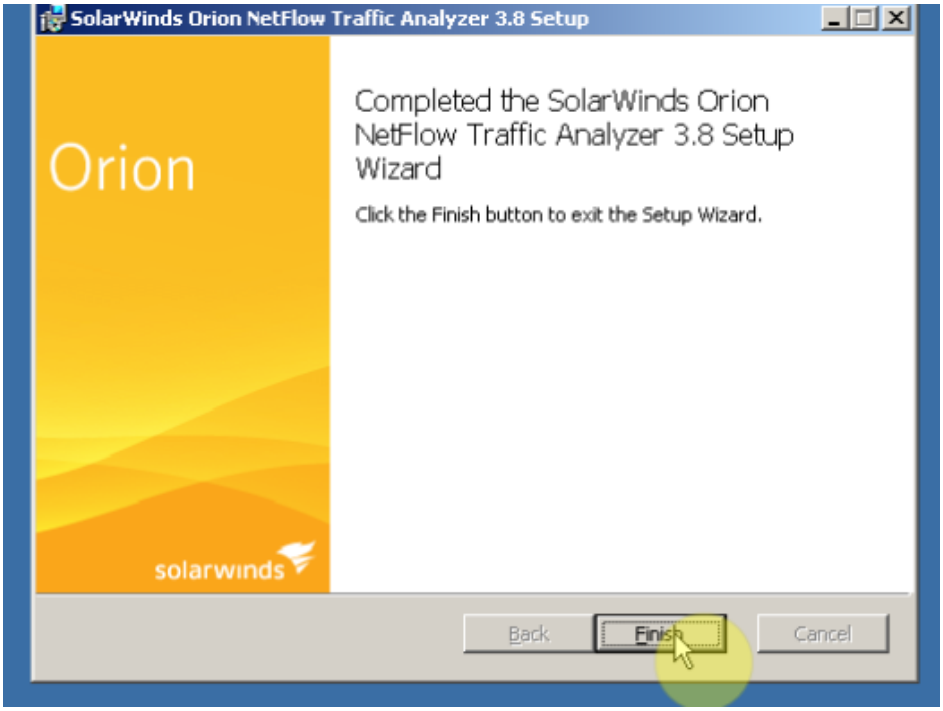
Hình 2.12. Bảng cài đặt của chương trình



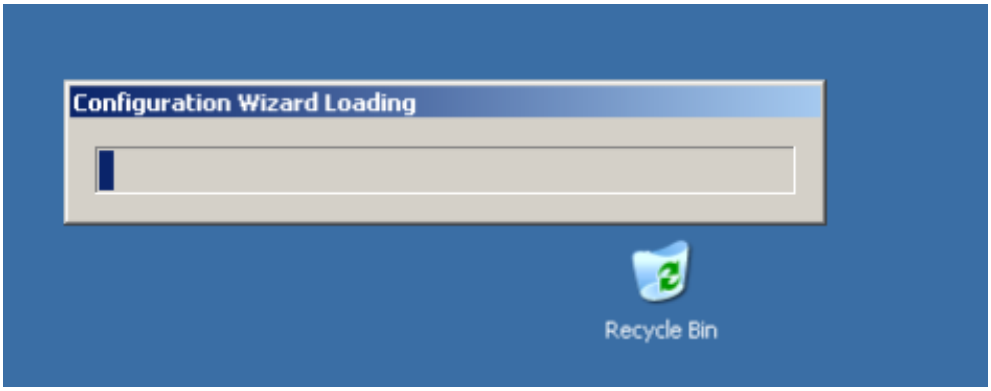
Hình 2.13. Bảng thông báo về các điều khoản của phần mềm



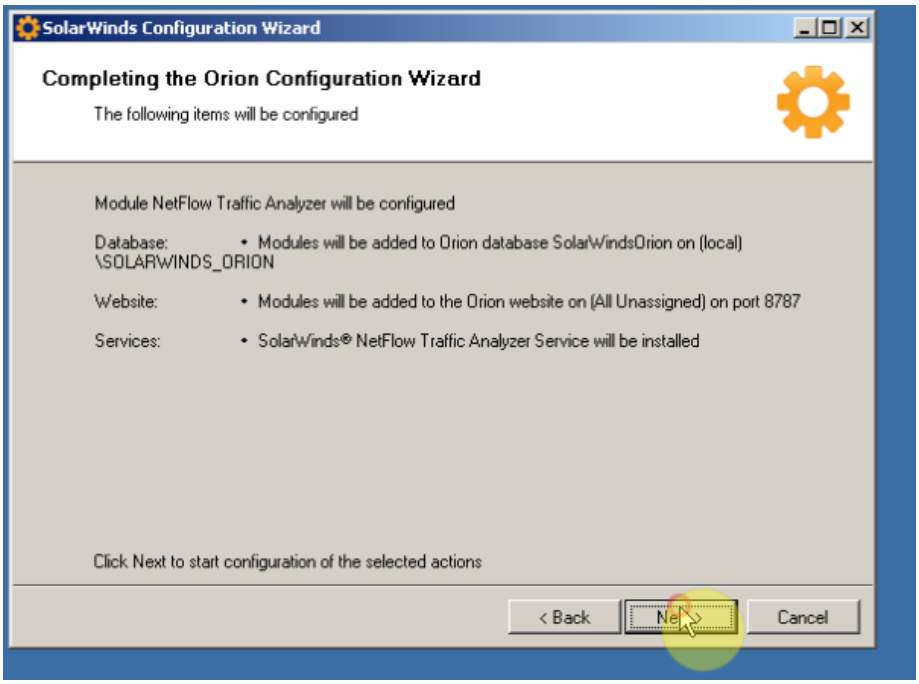
Hình 2.14. Chương trình bắt đầu cài đặt



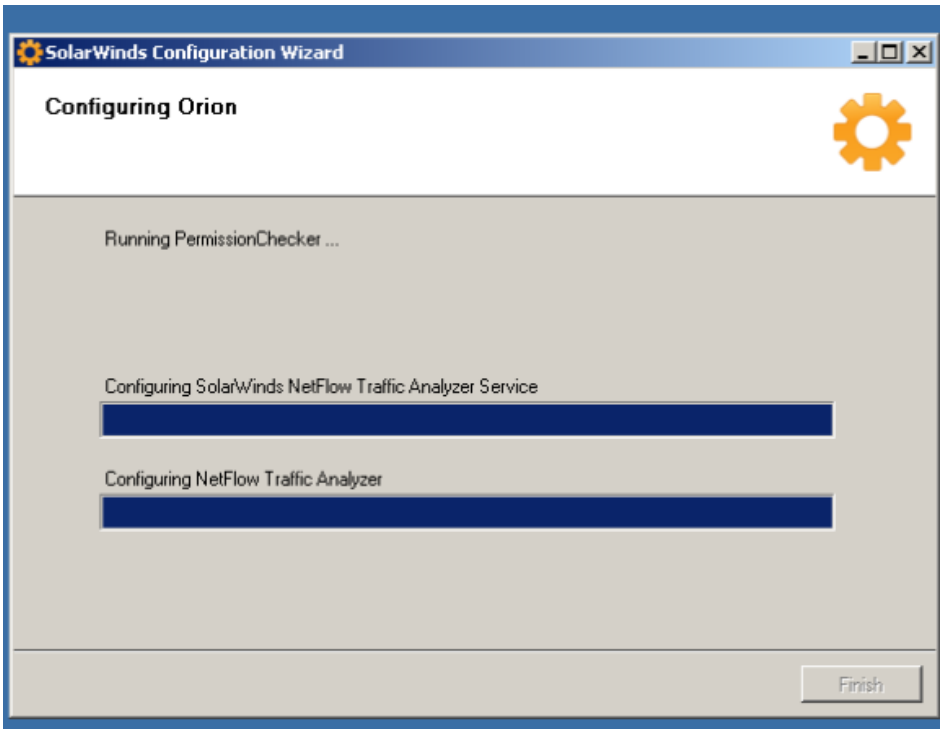
Hình 2.15. Quá trình cài đặt Orion NTA thành công



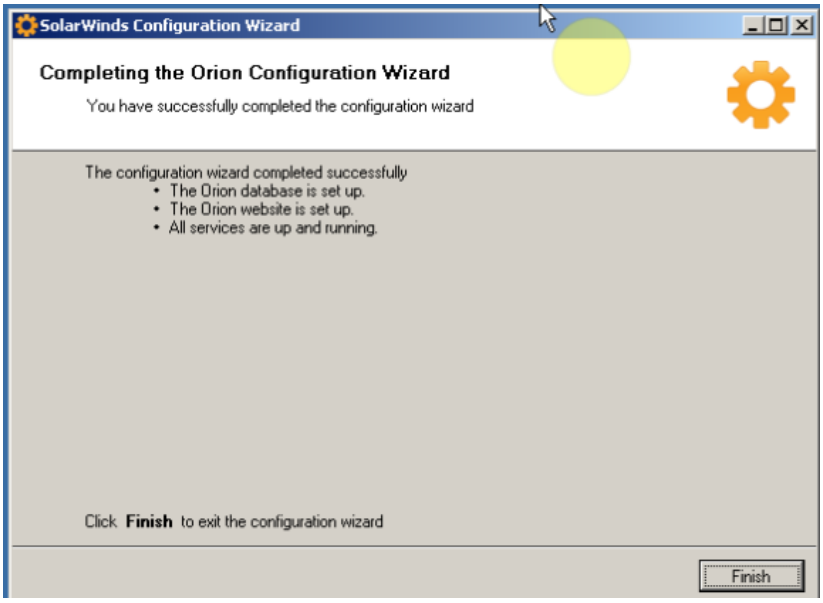
Hình 2.16. Chương trình tự động cấu hình



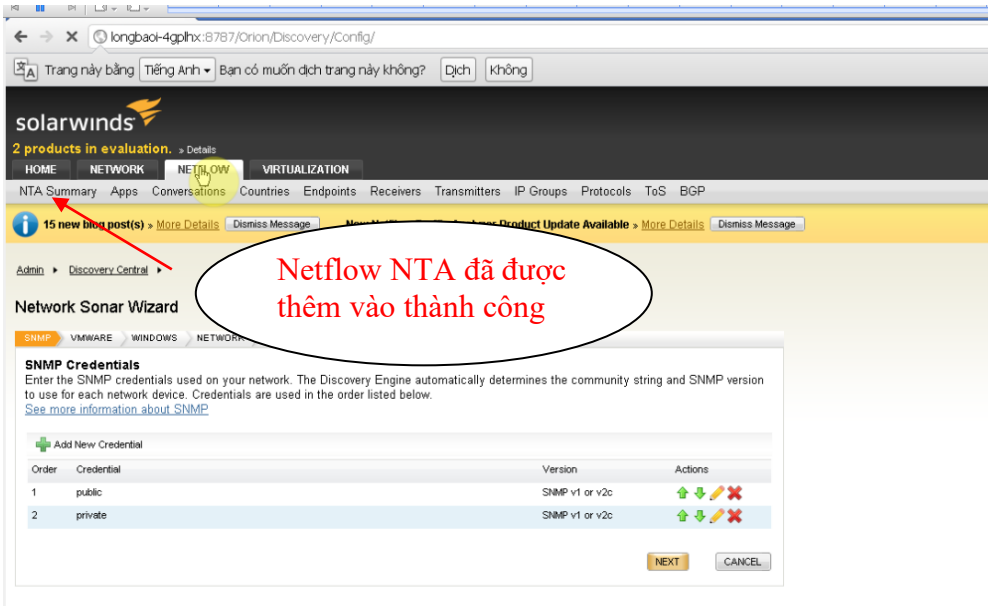
Hình 2.17. Chương trình sẽ cấu hình 3 thành phần quan trọng



Hình 2.18. Quá trình cấu hình diễn ra



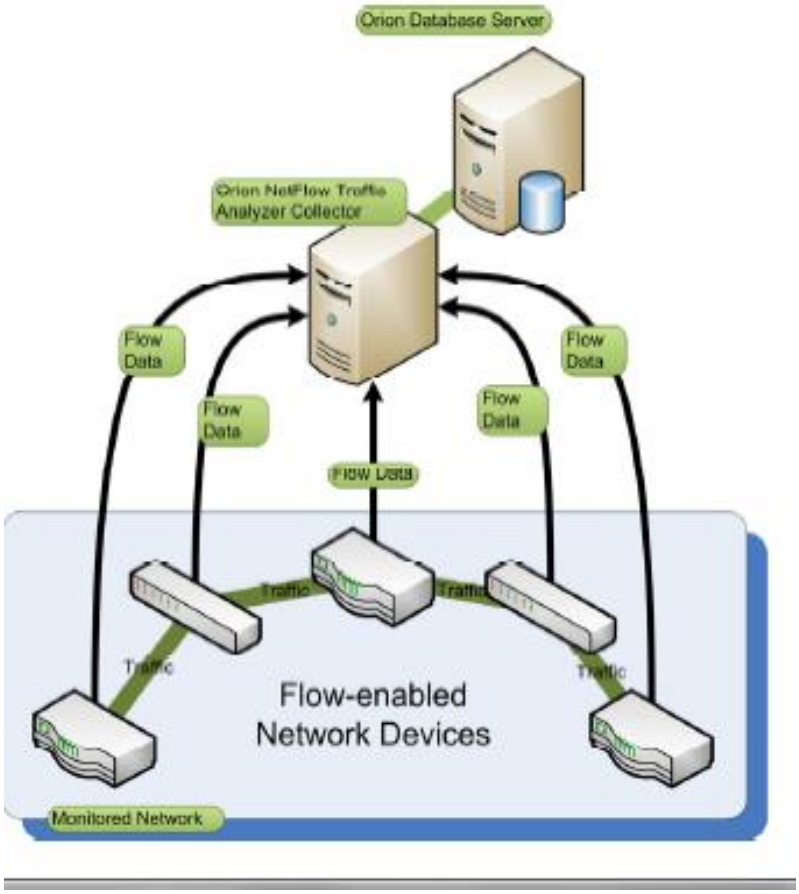
Hình 2.19. Cấu hình Orion NTA thành công



Hình 2.20. Trang chính của Solarwind sau khi cài đặt thành công

CHƯƠNG 3: TÍNH NĂNG CHÍNH TRONG SOLARWINDS ORION NETFLOW TRAFFIC ANALYZER

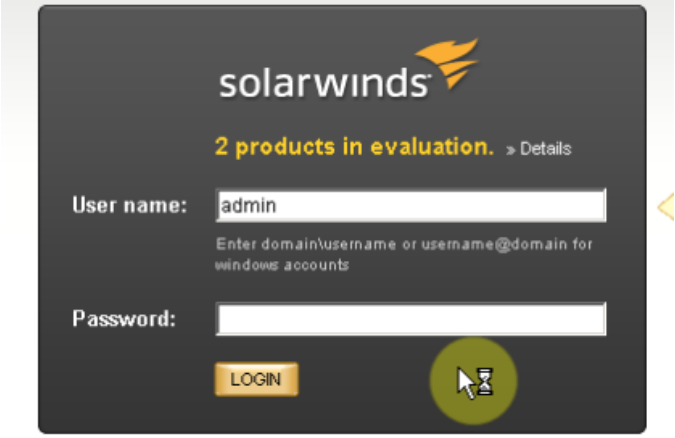
3.1. Orion NTA làm việc như thế nào



Hình 3.1. Cách thức phần mềm làm việc

Các thiết bị đầu cuối sẽ được kích hoạt luồng thông tin, giúp cung cấp các địa chỉ IP, cũng như băng thông mạng. Orion NTA sẽ thu thập các luồng dữ liệu này, sau đó tổng hợp, phân tích, và thể hiện chi tiết về miền mạng trên phần mềm Orion NPM, bằng cách này chúng ta sẽ dễ dàng biết được về miền mạng của mình thông qua sơ đồ, các báo cáo về băng thông từ miền mạng của bạn. Bản báo cáo này sẽ giúp chúng ta quan sát được băng thông, lưu lượng đang diễn ra trong miền mạng.

3.2. Sử dụng chương trình

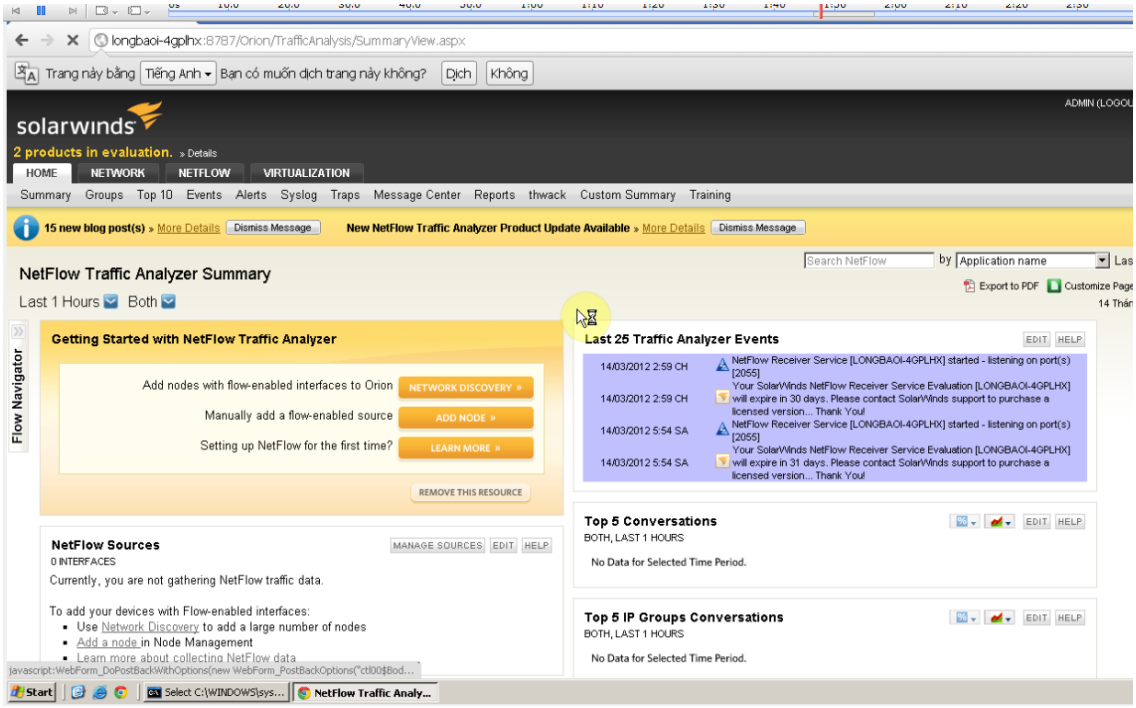


Hình 3.2. Giao diện đăng nhập

Nhập username và password mặc định để vào giao diện chính của chương trình

Dùng username: admin và password trống để đăng nhập chương trình

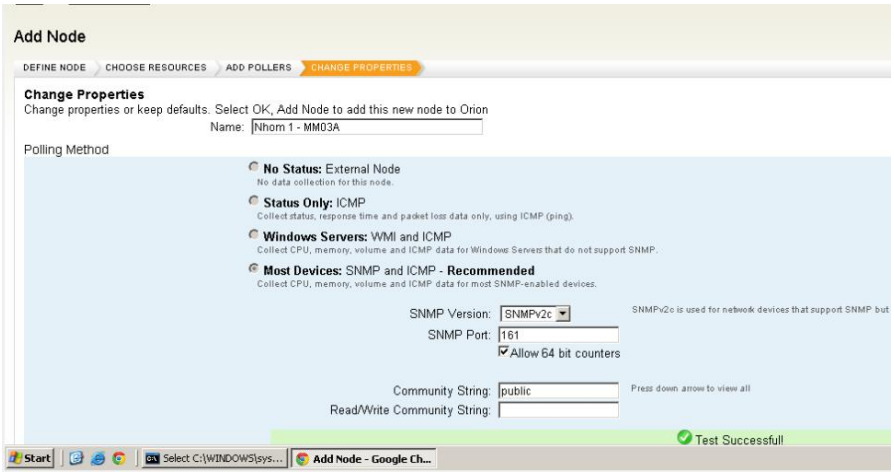
3.3. Giao diện chính của chương trình



Hình 3.3. Hiển thị các thông tin chung của hệ thống mạng

- Bao gồm các tab
  - Home: Hiện thị tổng thể về thông tin chung của mạng

- Network: Hiển thị thông tin về các node mạng, các thông báo mới nhất.
- Netflow: Hiển thị các sự kiện như port nào down, up, máy nào đang mở, lưu lượng băng thông mạng, hệ thống hoạt động như thế nào…



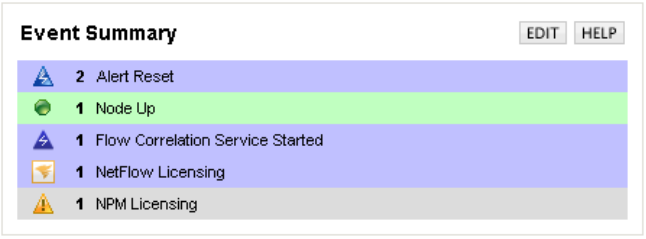
Hình 3.4. Add các node mạng

Giới Thiệu Giao Diện Home:

Summary

Ở tab này ta có cái nhìn tổng quan về các sự kiện của hệ thống.

➢ Có thể biết tổng cộng các loại sự kiện ở "Event Summary"

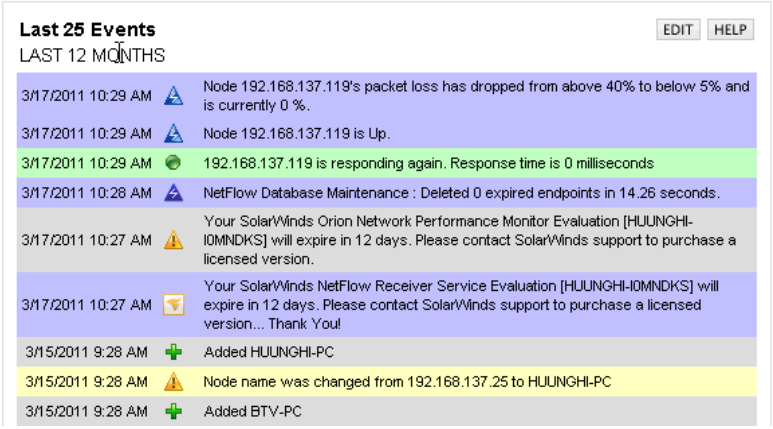


Hình **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.5 Tính năng thống kê sự kiện

➢ Có thể tìm kiếm node ở "Search Nodes"

Hình **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.6. Tính năng tìm kiếm

➢ Có bảng xếp hạng 25 sự kiện sau cùng.

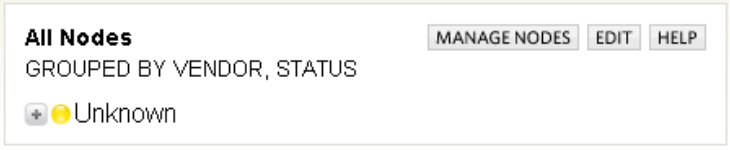


Hình **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.7. Xếp hạng và thống kê các sự kiện của hệ thống

➢ Có thể có cái nhìn tổng quan hệ thống mạng với "Map" – sơ đồ mạng.

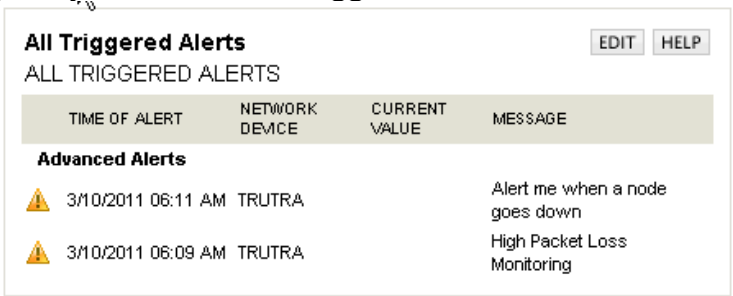
Hình **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.8. Sơ đồ nhìn tổng quan của mạng

➢ Có thể quản lý Nodes với "All Nodes"



Hình **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.9. Hệ thống quản lý node

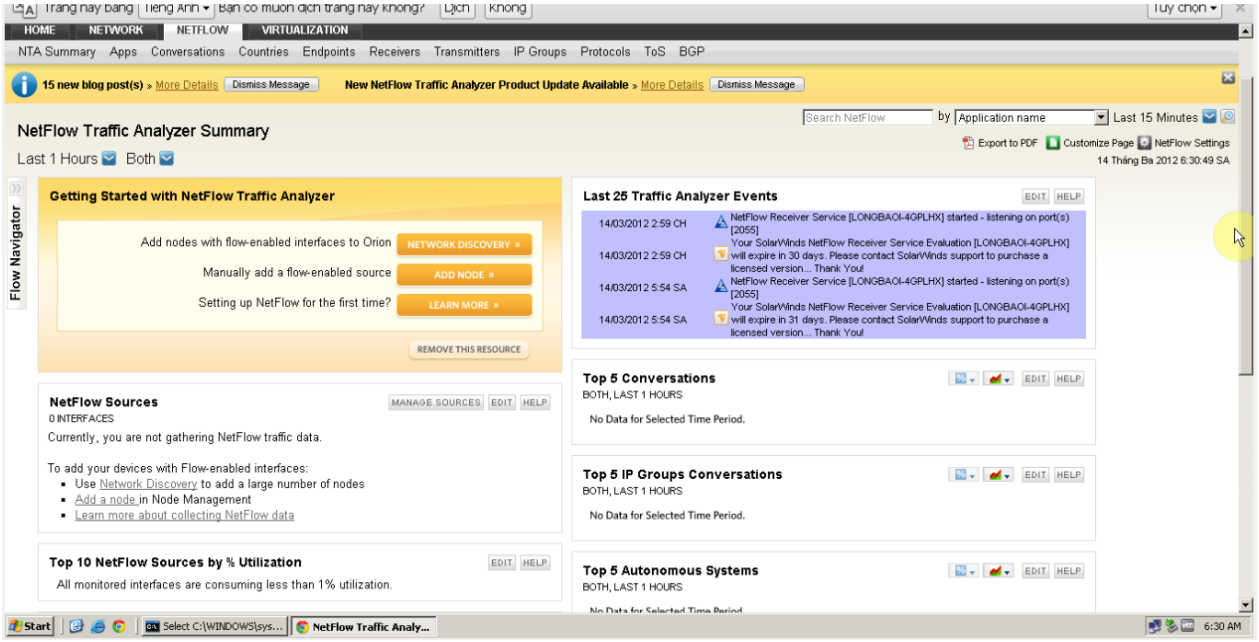
➢ Có thể quản lý alert với "All Triggered Alerts"



Hình **Lỗi! Không có văn bản nào có kiểu đã chỉ định trong tài liệu.**.10. Quản lý triggered Alerts

3.5. Giới thiệu về mục NetFlow

3.6.1. NTA Sumary



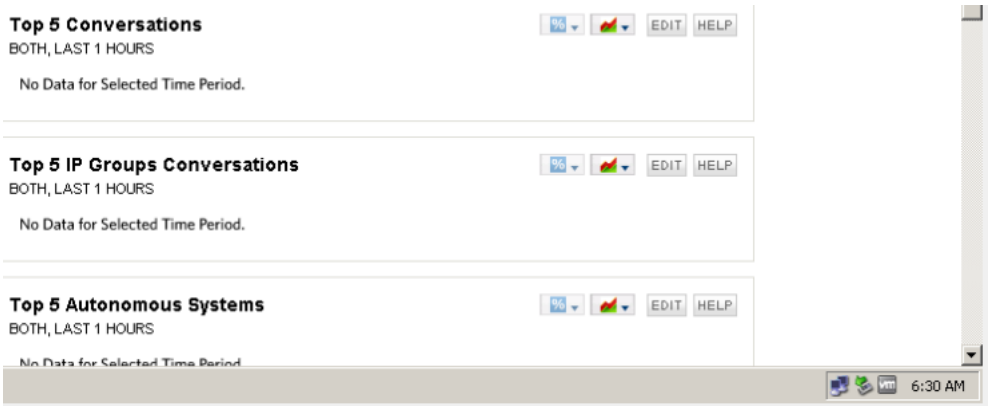
Hình 3.11. Bảng thông tin chung về Netflow

Ở tab này sẽ cho chúng ta biết về lưu lượng băng thông của hệ thống

- Có thể biết các sự kiện gì đang xảy ra, port nào down, port nào đang lắng nghe…

Hình 3.12. Thông tin sự kiện

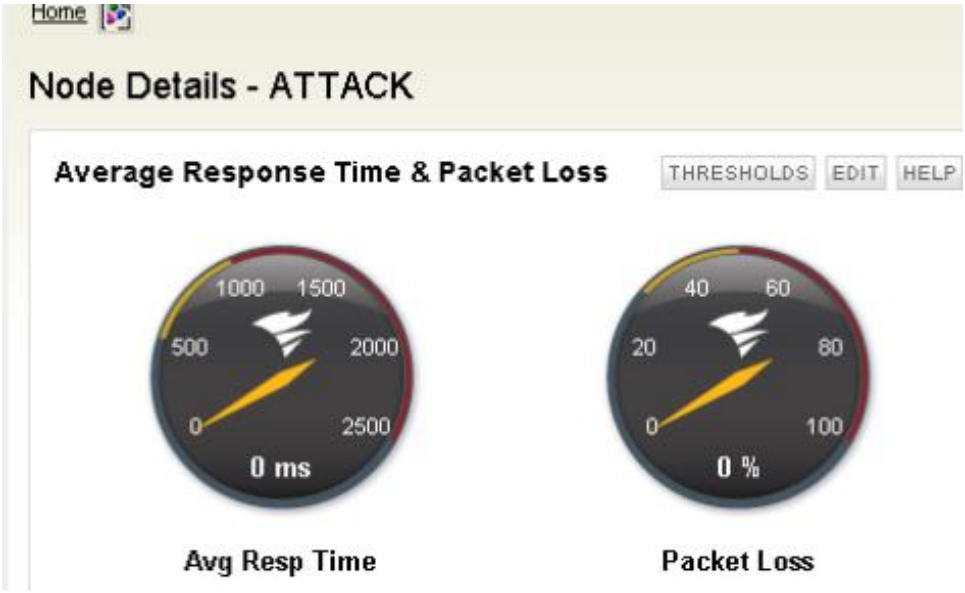
- Có thể biết được hệ thống hoạt động như thế nào



Hình 3.13. Hiển thị về top các thông tin hệ thống

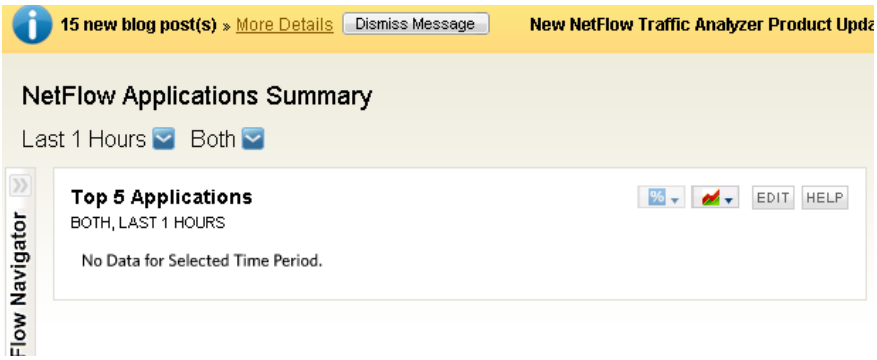
- Top 5 Conversations: Mục này chứa các thông tin về việc trao đổi dữ liệu thông tin vào ra.
- Top 5 IP Autonomous Systems: Mục này chứa các thông tin về hệ thống.

➢ Các lưu lượng gói tin bị mất



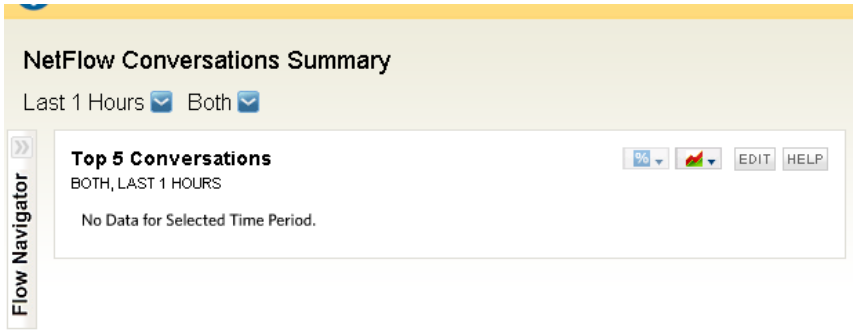
Hình 3.14. Phần trăm lưu lượng, gói tin bị mất.

➢ Các ứng dụng nào đang được chạy trên máy chủ hoặc máy trạm



Hình 3.15. Các ứng dụng nào đang được chạy

- Các cuộc hội thoại trao đổi nào đang diễn ra



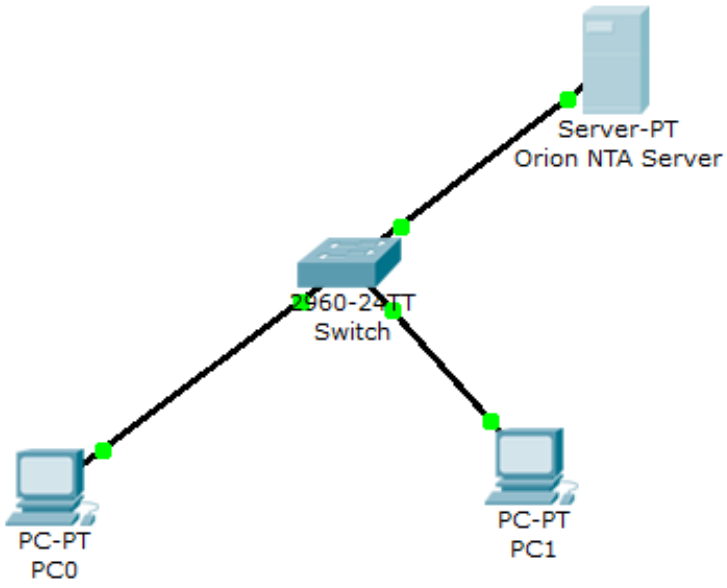
Hình 3.16. Top 5 các cuộc hội thoại trao đổi dữ liệu

- Các giao thức nào được sử dụng

Hình 3.17. Top 5 các giao thức

3.6. Thực hành giám sát mạng với phần mềm Orion NTA

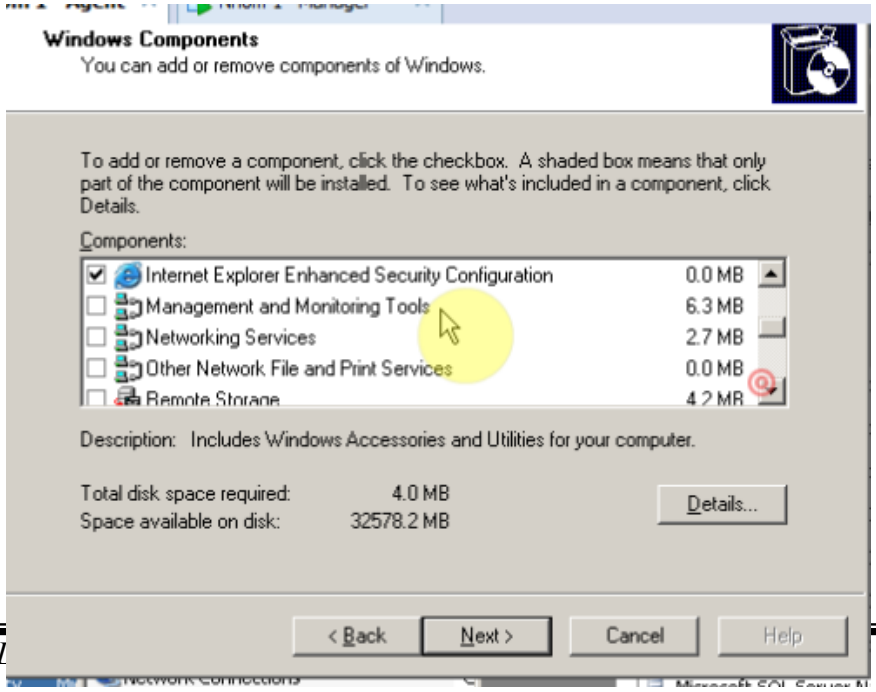
3.6.1. Mô hình giả lập



Hình 3.18. Mô hình giả lập quản lý mạng

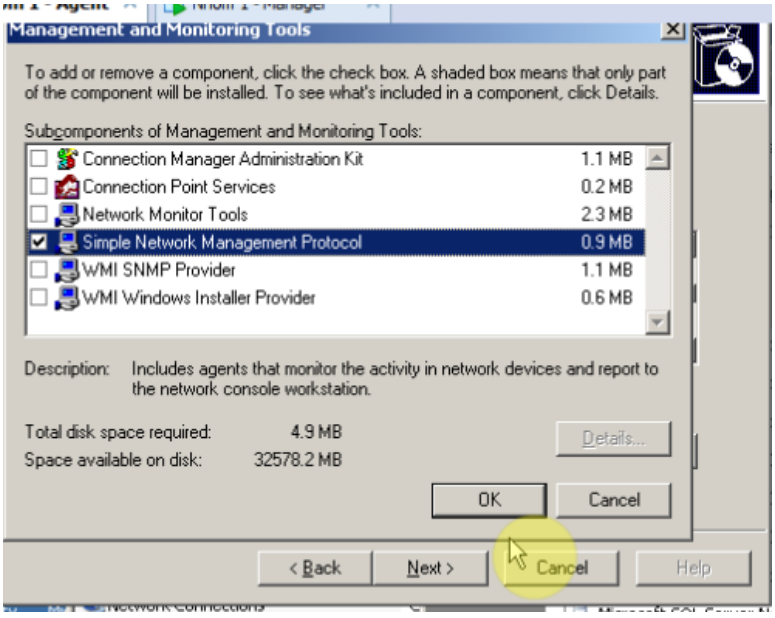
Để thực hiện giám sát với mô hình giả lập như trên, giao thức SNMP phải được kích hoạt trên các thiết bị mạng và thực hiện cài đặt phần mềm Solarwinds NPM và Orion NTA trên Server Manager chạy hệ điều hành Windows server 2003.

3.6.2. Cài đặt và cấu hình SNMP Agent trên PC



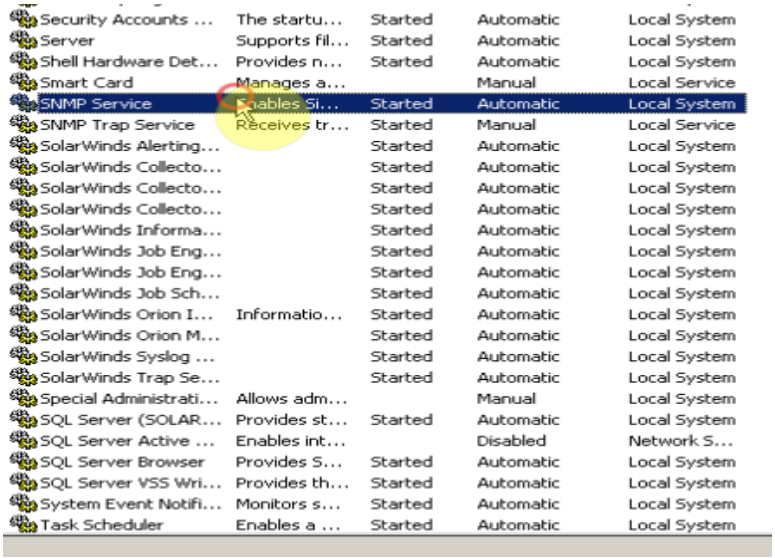
Hình 3.19. Cài đặt dịch vụ SNMP lên các máy chủ và PC

Để cài đặt thêm các dịch vụ : Start/Control Panel/ Add or Remove Program/ Add or Remove Windows Component/ Manage and Monitor Tool/ Simple Network Management Protocol.



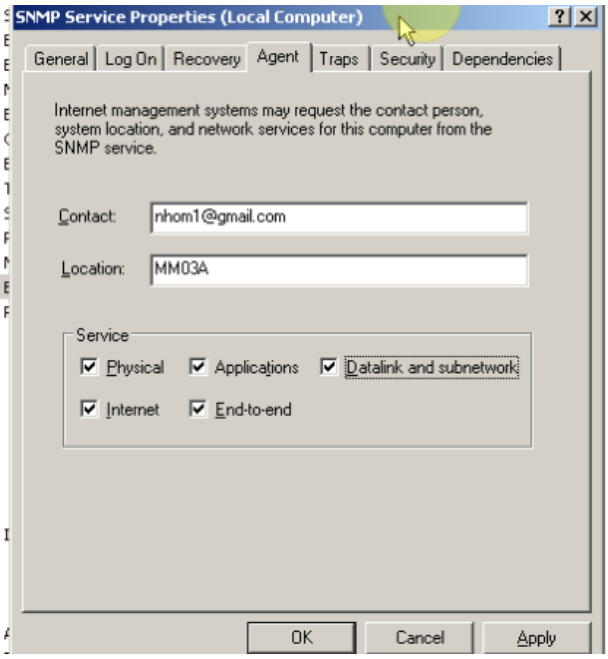
Hình 3.20. Chọn Simple Network Management Protocol

Sau khi chọn xong bấm OK để tiến hành cài đặt dịch vụ SNMP lên máy chủ và các máy PC.



Hình 3.21. Dịch vụ SNMP sau khi cài đặt thành công

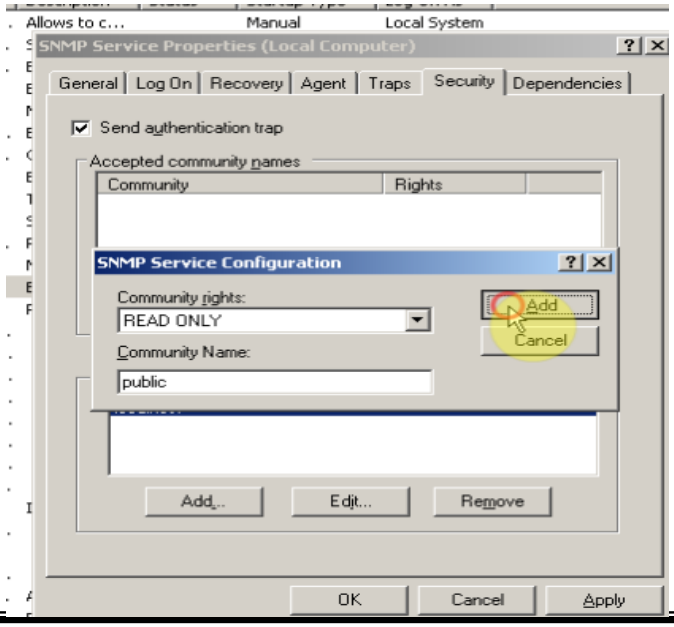
Để cấu hình dịch vụ SNMP, chuột phải vào My Computer/Manage/Service. Sau đó chuột phải vào dịch vụ SNMP Service/Properties. Chọn Tab Agent.



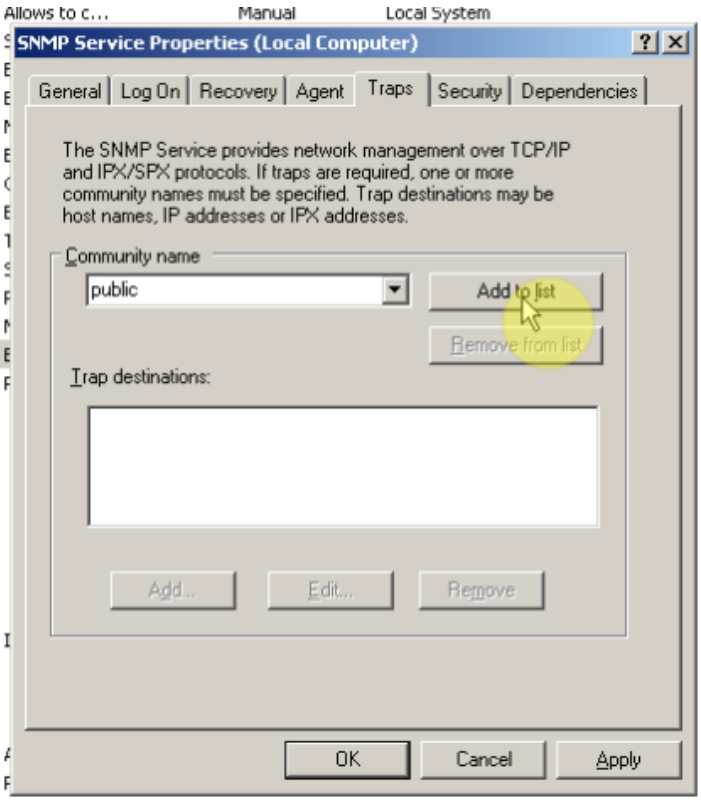
Hình 3.22. Cấu hình Agent SNMP

Để Máy chủ quan sát và thấy được máy trạm thì cần thiết lập Community Name với tên bất kỳ hoặc là public.

Chọn Tab Sercurity/ Add.

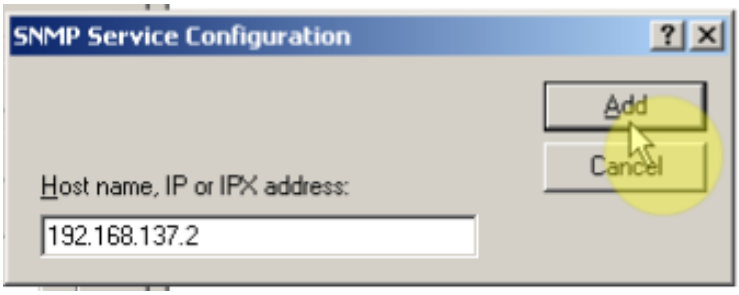


Hình 3.23. Add Community Name



Hình 3.24. Cấu hình Trap

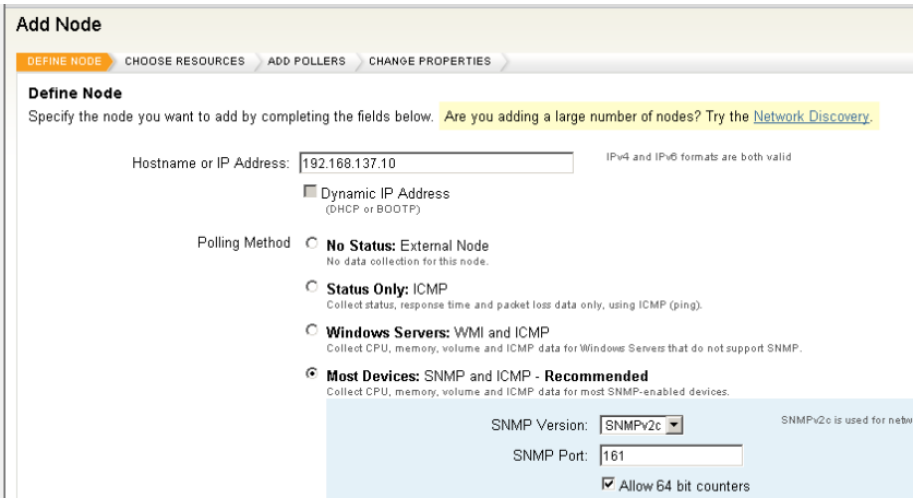
Chọn Tab Trap và add community là public.



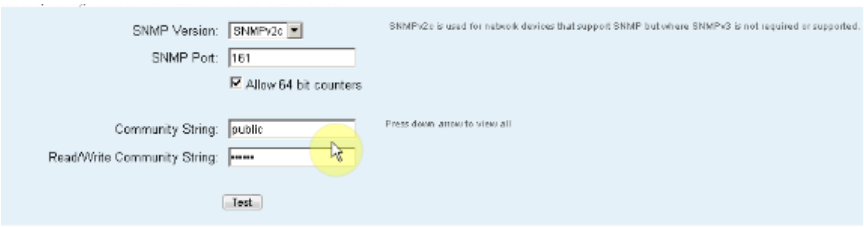
Hình 3.25. Nhập IP máy cần quan sát

3.6.3. Thực hiện việc add các node mạng

Nhập IP miền mạng cần quét, để tiến hành quét các máy trong miền mạng cần quan sát, để thu thập và lấy thông tin

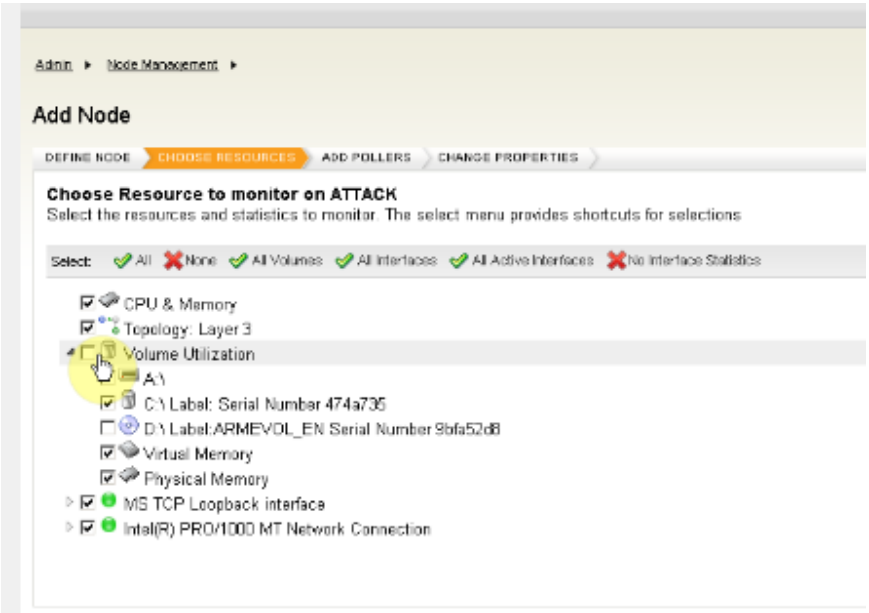


Hình 3.26. Add các node mạng



Hình 3.27. Nhập community string được khai báo ở trên vào

3.6.4. Quan sát thông tin về PC

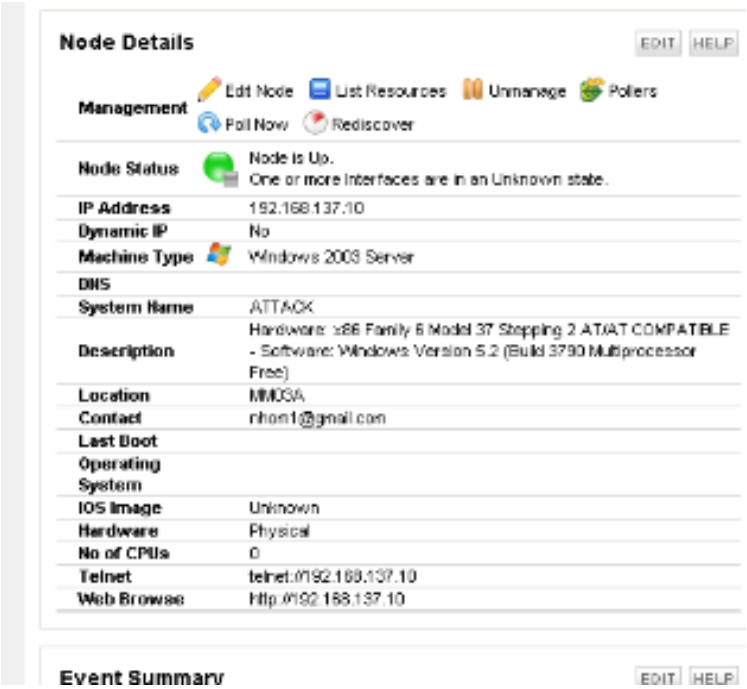


Hình 3.28. Thông tin máy PC cần quét

➢ Sau khi cấu hình và add các node thành công thì các thông tin của máy PC sẽ hiện lên như:

- CPU & Memory
- Dung lượng từng phân vùng và tên của mỗi phân vùng
- Thông tin về Cardmang

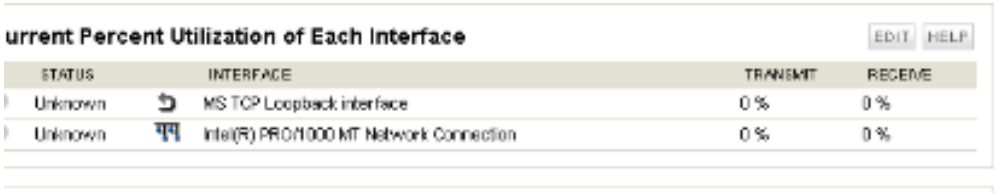
➢ Thông tin chi tiết được thể hiện như sau



Hình 3.29. Chi tiết về node

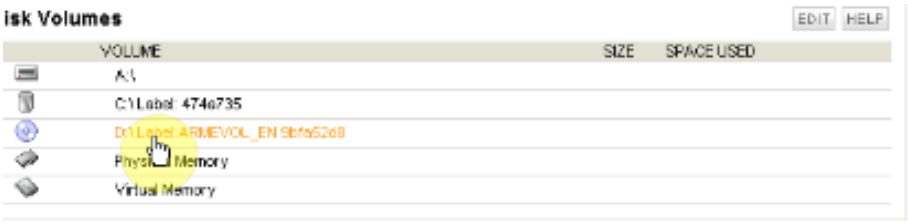
- Node Status: Up. Chứng tỏ node này đang được bật
- IP Address: IP của máy cần quan sát chính là Server
- Hệ điều hành: Windows 2003 Server
- Tên máy: Attack
- Description: Phần mô tả chi tiết thông tin của hệ thống.
- Location: Thông tin vị trí .

Ngoài ra còn một số chi tiết khác như



Hình 3.30. Lưu lượng vào ra của card mạng

➢ Tại mục này sẽ cho biết, lưu lượng đang chuyển vào hay ra của card mạng là bao nhiêu phần trăm, từ đó cho chúng ta biết hiệu suất của mạng như thế nào.



Hình 3.31. Thông tin về ổ đĩa của máy

➢ Các thông tin như tên ổ đĩa, kích thước và số dung lượng được dùng, được thể hiện

KẾT LUẬN

- **Kết quả đạt được**
  - **Về lý thuyết:**

Nhóm đã tìm hiểu được tổng quan về giao thức giám sát mạng SNMP, các phương thức giám sát mạng. Ưu nhược điểm trong thiết kế của SNMP.

Tìm hiểu lý thuyết về phần mềm quản trị mạng Orion Netflow Traffic Analyzer

  - **Về thực hành**

Triển khai hệ thống giám sát và quản trị mạng với Orion Netflow Traffic Analyzer trên mô hình giả lập, thực hiện một số tiện ích giám sát và quản trị mạng cơ bản.

- **Hạn chế**

Vì thời gian có hạn nên chưa tìm hiểu hết các tính năng của bộ phần mềm. Chưa đi sâu vào giao thức SNMP.

Đồ án chưa mang tính thực tế cao. Hệ thống mạng ứng dụng phần mềm Orion NTA không triển khai thực tế nên chưa phát hiện được các lỗi cũng như các vấn đề phát sinh.

- **Hướng mở**

Triển khai phần mềm giám sát và quản lý mạng Orion NTA trong môi trường thực tế nếu có điều kiện. Tiếp tục tìm hiểu bộ phần mềm Solarwind một cách triện để hơn nữa.

TÀI LIỆU THAM KHẢO

- **Sách, giáo trình, đồ án**

[1]. *AdministratorGuide-Orion Common Components* – Tài liệu tham khảo từ nhà sản xuất.

[2]. *AdministratorGuide-OrionNPM* - tài liệu tham khảo từ nhà sản xuất.

[3]. *EvaluationGuide-OrionNPM* - tài liệu tham khảo từ nhà sản xuất.

[4]. *QuickStartGuide-OrionNPM* - tài liệu tham khảo từ nhà sản xuất.

[5]. Báo Cáo Triển Khai Solawind trong mô hình thực tế - Nguyễn Tiến Lực – Học Viện Bưu Chính Viễn Thông.

- **Internet**

http://solarwinds.com/support/