Chương 2

Quản lý mạng với SNMP

- Ứng dụng quản lý mạng với SNMP
- Cách thức khai báo SNMP manager và SNMP agent
- Giám sát router ADSL bằng SNMP
- Giám sát máy chủ Windows & Linux bằng SNMP
- Giám sát switch bằng SNMP

1. Ứng dụng quản lý mạng với SNMP

Trong chương này tác giả sẽ giới thiệu các ứng dụng quản lý thiết bị mạng bằng SNMP và làm thế nào để triển khai chúng vào thực tế. Các phần mềm được giới thiệu đều dễ tìm và các ví dụ thì đơn giản nhưng thực tế để mọi độc giả đều có thể thực hiện được.

Các bạn sẽ thực hiện những bài sau :

+ Giám sát lưu lượng và cảnh báo của ADSL router (modem internet adsl) bằng phần mềm SNMP Traffic Monitor và SNMP Trap Receiver. Loại ADSL router được lấy làm ví dụ là loại Dlink DSL-520T.

+ Giám sát tài nguyên và cảnh báo của máy chủ Windows và Linux bằng phần mềm Solarwinds. Các bạn đang công tác ở vị trí quản trị mạng máy chủ tại các doanh nghiệp có thể thực hiện bài này trên hệ thống mà các bạn đang quản lý.

+ Giám sát lưu lượng và cảnh báo của một switch Cisco Catalyst 2950 bằng phần mềm PRTG. Các bạn đang công tác ở vị trí quản trị mạng phần cứng có thể thực hiện bài này vì switch C2950 là loại phổ biến.

Thay vì chỉ giới thiệu một phần mềm thương mại có đầy đủ chức năng như Solarwinds thì tác giả sẽ giới thiệu nhiều phần mềm nhằm giúp người đọc dễ dàng tìm kiếm, và quan trọng hơn là làm quen cách cấu hình những phần mềm khác nhau từ đơn giản đến phức tạp.

2. Cách thức khai báo SNMP manager và SNMP agent

Nhiều bạn cài đặt các phần mềm giám sát về chạy nhưng không thu được thông tin gì cả, là vì các bạn chưa thực hiện các khai báo cấu hình đầy đủ. Để thực hiện giám sát một thiết bị (agent) bằng phần mềm giám sát (manager), các bạn phải cấu hình SNMP manager và SNMP agent đúng cách.

Các manager và agent có giao diện hay câu lệnh cấu hình khác nhau, nhưng chúng đều có các thông số chung cần cài đặt. Bạn phải cấu hình 2 phần cho SNMP Get/Set và SNMP Trap. Như đã trình bày trong chương 1, Get/Set dùng để lấy/thiết lập thông tin còn trap dùng để cảnh báo. Bạn hãy ghi nhớ các bước cấu hình được trình bày dưới đây, nó sẽ giúp bạn cấu hình đúng các manager và agent khác nhau, giúp bạn nhanh chóng phát hiện ra các thiếu sót.

Cấu hình Get/Set trên SNMP agent

+ Bật tính năng SNMP agent trên thiết bị cần giám sát : các thiết bị hỗ trợ SNMP có thể không mặc định bật tính năng này, bạn phải bật nó lên để tiến trình agent hoạt động.

+ Khai báo community-string và quyền truy cập tương ứng : bạn phải khai báo các community string và chỉ ra community nào có quyền gì (read, write, set).

+ Khai báo phiên bản SNMP : chỉ định agent sẽ hoạt động bằng phiên bản SNMP nào (v1, v2, v3). Nếu agent không cho phép khai báo version thì agent này có thể chỉ hỗ trợ SNMPv1.

+ Khai báo SNMP ACL : ACL cho phép chỉ những dãy IP nào đó mới được giám sát agent.

+ Khai báo Location, Contact, HostName : đây là các tham số phụ, không quan trọng.

Cấu hình trên SNMP manager

+ Khai báo IP của thiết bị cần giám sát.

+ Khai báo community-string : community string được khai báo trên manager phải giống như đã khai báo trên agent.

+ Khai báo phiên bản SNMP : phiên bản mà manager sử dụng để giám sát phải giống với phiên bản đã khai báo trên agent.

+ Chu kỳ lấy mẫu : do SNMP Get/Set sử dụng phương thức poll nên bạn cần khai báo chu kỳ lấy thông tin của manger.

Cấu hình Trap trên SNMP agent

+ Bật tính năng trap sender.

+ Khai báo địa chỉ IP của trap receiver.

+ Khai báo community-string của bản tin trap.

+ Khai báo version của SNMP trap.

Cấu hình Trap trên SNMP Trap Receiver

+ Bật tính năng trap receiver.

+ Khai báo dãy địa chỉ IP của sender mà trap receiver sẽ nhận, những IP nằm ngoài dãy này thì trap receiver sẽ không nhận trap. Tính năng này là tùy chọn, có thể nhiều trap receiver không hỗ trợ.

+ Khai báo bộ lọc kiểu trap : đây là danh sách các kiểu trap sẽ được hiện ra trên màn hình của trap receiver. Tính năng này cũng là tùy chọn.

Cấu hình SNMPv3

+ Đối với SNMPv3 các bạn sẽ phải cấu hình thêm các thông số : engineId, user, authentiation-type, authen-password, encryption algorithm, encryption key. Trong chương này chúng ta không khảo sát cách thực hiện với SNMPv3, chúng ta sẽ có một chương riêng về version 3.

3. Giám sát router ADSL

Cấu hình tính năng SNMP agent cho ADSL Router Dlink DSL-520T

Kết nối máy tính của bạn vào một ADSL Router DLink DSL-520T. Login vào trang web của modem, chuyển qua tab [Advanced], chọn nút [SNMP] để vào trang cấu hình SNMP Management. Nhấn chọn checkbox [Enabled SNMP Agent], các mục [Name], [Location] và [Contact] là tùy chọn. Trong phần [Community] nhập community string là "public", quyền ReadOnly.

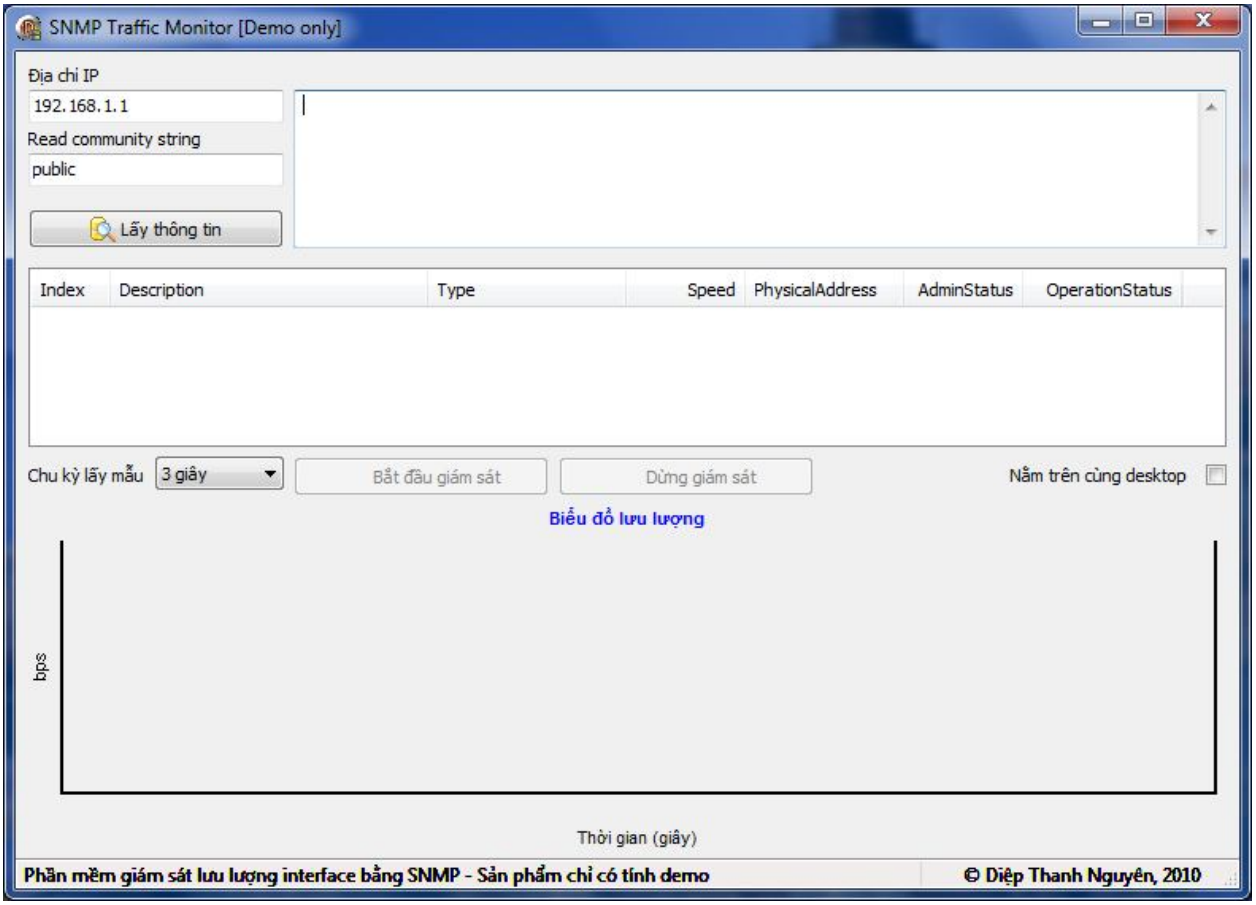
Tiếp theo là cấu hình Trap. Nhập IP máy tính của bạn vào [Destination IP], nhập community cho bản tin trap vào [Trap Community] và chọn version của trap là SNMPv1. Cuối cùng nhấn nút Apply.

Giám sát lưu lượng bằng phần mềm SNMP Traffic Monitor

SNMP Traffic Monitor là phần mềm được tác giả viết để demo cho quyển tài liệu này, dùng để giám sát lưu lượng của interface bằng SNMP. Mục đích của phần mềm này không phải là để dùng trong thực tế mà là để hỗ trợ cho các bạn mới tìm hiểu SNMP một công cụ đơn giản nhất để thực tập khi cấu hình SNMP cho thiết bị. Phần mềm và source code có thể download tại trang chủ của quyển tài liệu này. Trong chương 5, tác giả sẽ trình bày cách viết phần mềm này.

Phần mềm này giúp người mới làm quen với SNMP có thể sử dụng nhanh chóng. Thực tế trong doanh nghiệp các bạn nên dùng những phần mềm chuyên nghiệp hơn như PRTG, Solarwinds.

Sau khi cài đặt và khởi động, phần mềm có giao diện như sau :



Cách sử dụng phần mềm để giám sát :

+ Nhập địa chỉ IP của thiết bị cần giám sát vào ô “Địa chỉ IP”

+ Nhập read-community vào ô “Read community string”, giá trị mặc định là “public”.

+ Nhấn nút “Lấy thông tin”, phần mềm sẽ lấy về các thông tin của thiết bị, tổng số interface (port) đang có và thông tin của từng interface.

+ Chọn một interface cần giám sát trong danh sách interface.

+ Chọn chu kỳ lấy mẫu.

+ Nhấn nút “Bắt đầu giám sát”, biểu đồ lưu lượng sẽ được vẽ ra bên dưới, đường màu GREEN là input, BLUE là ouput.

Ví dụ giám sát ADSL Router DLink DSL-520T :

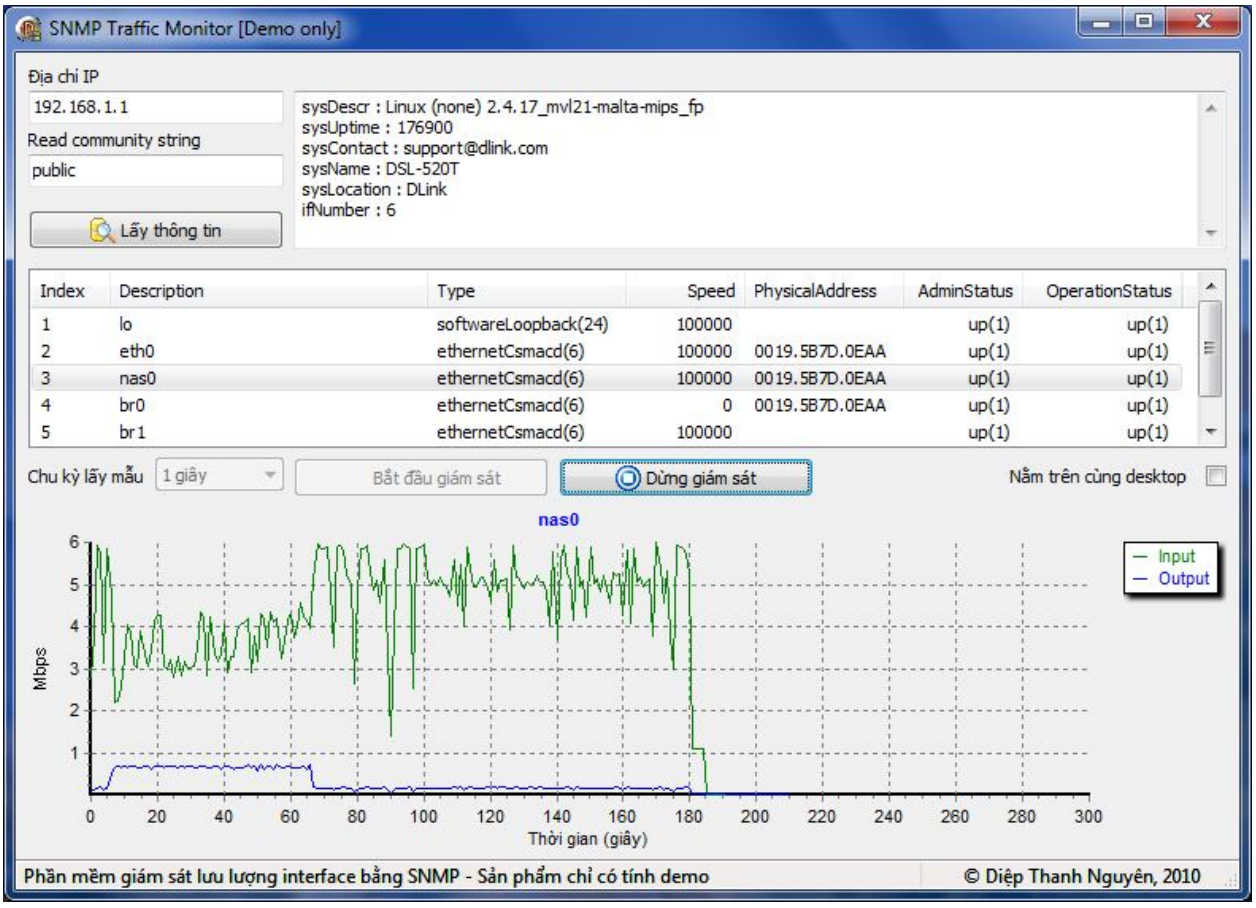
+ Nhập IP router là 192.168.1.1

+ Sau khi nhấn “Lấy thông tin” thì sẽ xuất hiện nhiều interface. Đối với thiết bị Dlink DSL-520T được chọn làm minh họa thì nó chỉ có 1 interface ethernet tên là “eth0” (modem 1 port), còn nếu bạn dùng modem 4 port thì nó sẽ có 4 interface ethernet. Nếu bạn chọn giám sát interface ethernet thì phần mềm sẽ theo dõi lưu lượng của port đó, còn nếu bạn chọn giám sát interface “nas0” thì phần mềm sẽ giám sát lưu lượng của port adsl (port đấu nối với nhà cung cấp), tức là giám sát toàn bộ lưu lượng ra vào modem.

+ Chọn chu kỳ là 1 giây.

+ Chọn interface “nas0” và nhất “Bắt đầu giám sát”, lưu lượng sẽ được vẽ ra.

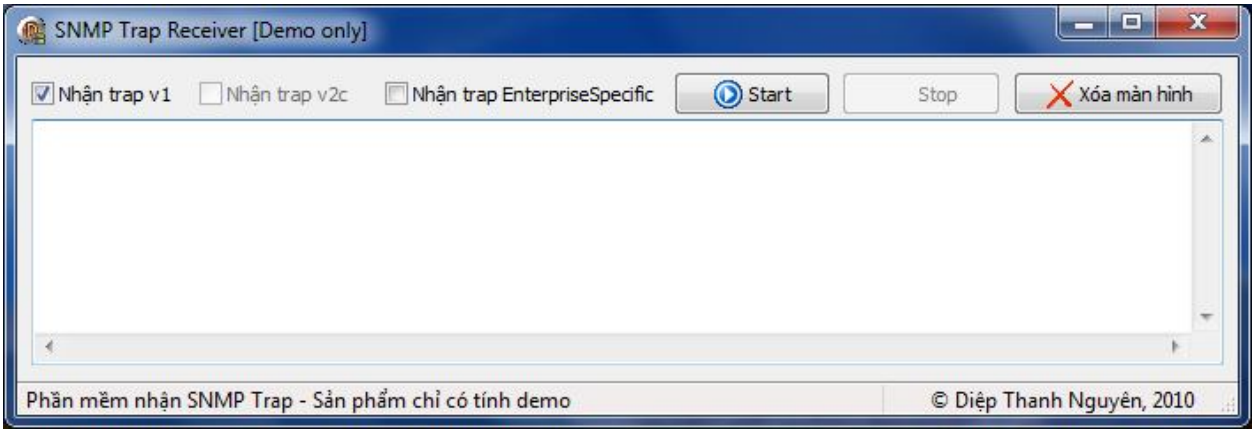
Chú ý : phần mềm sử dụng SNMPv1, nếu thiết bị của bạn hỗ trợ nhiều version thì bạn phải cấu hình SNMP agent cho phép dùng v1.



Nhận trap bằng phần mềm SNMP Trap Receiver

SNMP Trap Receiver là phần mềm nhận trap SNMPv1 do tác giả viết demo cho quyển tài liệu này. Mục đích của nó cũng không phải là để dùng trong thực tế mà là để các bạn mới làm quen có được công cụ đơn giản nhất để đọc trap của thiết bị.

Sau khi cài đặt và khởi động thì giao diện của phần mềm như sau :

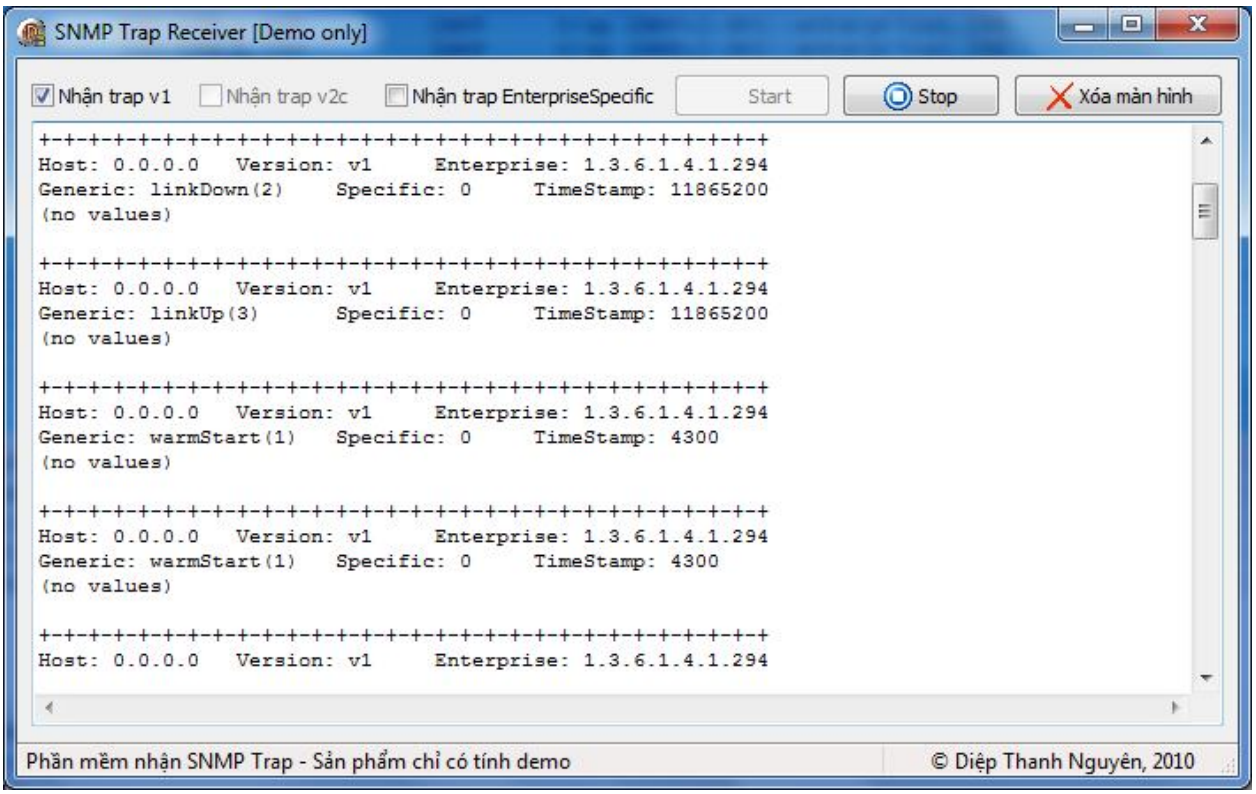


SNMP Trap Receiver sẽ tự động nhận trap ở port UDP 162. Các bản tin trap được gửi đến máy tính chạy SNMP Trap Receiver sẽ được hiện lên màn hình. Chú ý rằng bạn chỉ có thể đọc được dễ dàng các bản tin trap thuộc loại generic vì chúng đã được mô tả trong chuẩn, còn trap loại specific thì vẫn hiện lên màn hình nhưng bạn sẽ không hiểu được nếu không có tài liệu mô tả của hãng.

Sau khi bật SNMP Trap Receiver, bạn rút dây cáp adsl ra khỏi router DSL-520T thì router sẽ gửi trap linkDown đến máy tính của bạn (chú ý rút dây adsl chứ không phải dây cáp mạng). Sau đó bạn cắm lại cáp adsl thì router sẽ gửi trap linkUp.

Hình dưới là trap nhận được từ con DSL-520T, bạn sẽ nhìn thấy Source IP là 0.0.0.0. Điều này là do trong bản tin trap của router DSL-520T gửi có trường agent-address = 0.0.0.0. Đây là IP chứa trong bản tin trap chứ không phải source IP chứa trong bản tin IP.

Bạn hãy tắt router và bật lại, một lúc sau bạn sẽ nhận được trap warmStart báo hiệu thiết bị vừa khởi động lại. Sau đó các trap linkUp sẽ xuất hiện do sau khi khởi động thì các port sẽ chuyển sang trạng thái up.



Nếu bạn nhận chọn "Nhận trap enterpriseSpecific" thì phần mềm sẽ hiện ra các trap không chuẩn (do các hãng tự định nghĩa) và bạn cần có tài liệu mô tả mới có thể hiểu được. VD hình dưới là trap của một switch Cisco 2950, nó gửi trap thông báo rằng OID x có giá trị là x; bạn cần đọc file mib của C2950 mới hiểu được x là object nào và y có nghĩa là gì.

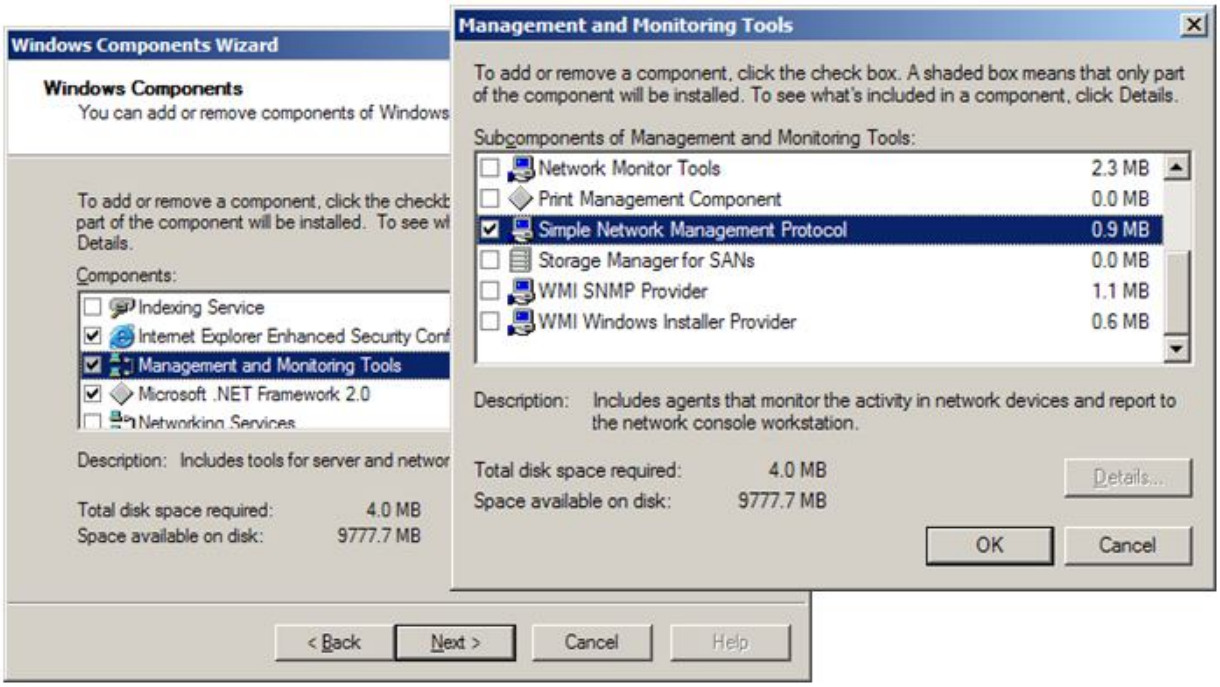
4. Giám sát máy chủ bằng SNMP

Trong phần này bạn sẽ thực hiện giám sát máy chủ Windows Server 2003 và CentOS 5.x bằng phần mềm Solarwinds [1].

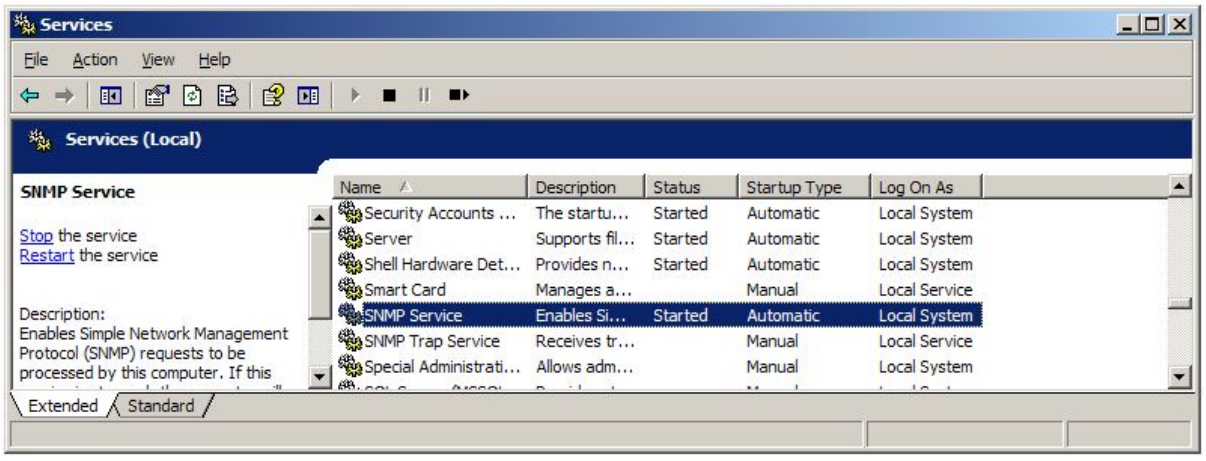
Cấu hình SNMP agent trên hệ điều hành Windows [2]

Tính năng SNMP trên HĐH Windows phải được cài đặt và cấu hình trước khi bạn có thể giám sát nó bằng một phần mềm SNMP manager. SNMP Service trên Windows là một SNMP agent, nó sẽ đáp ứng các request của phần mềm giám sát, giúp phần mềm giám sát lấy được các thông tin từ một máy chủ Windows.

Để cài đặt dịch vụ SNMP, vào [Add/remove Windows components], chọn [Management and Monitoring Tools], click nút [Details]. Trong hộp thoại [Management and Monitoring Tools], chọn [Simple Network Management Protocol], nhấn OK để cài đặt dịch vụ SNMP.



Kiểm tra lại service SNMP phải đang hoạt động.



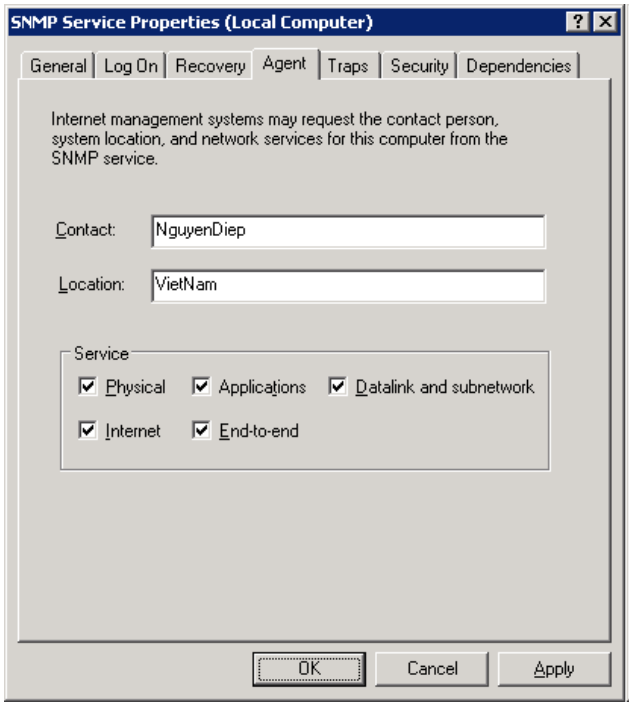
[1] Trang chủ của Solarwinds : http://www.solarwinds.com

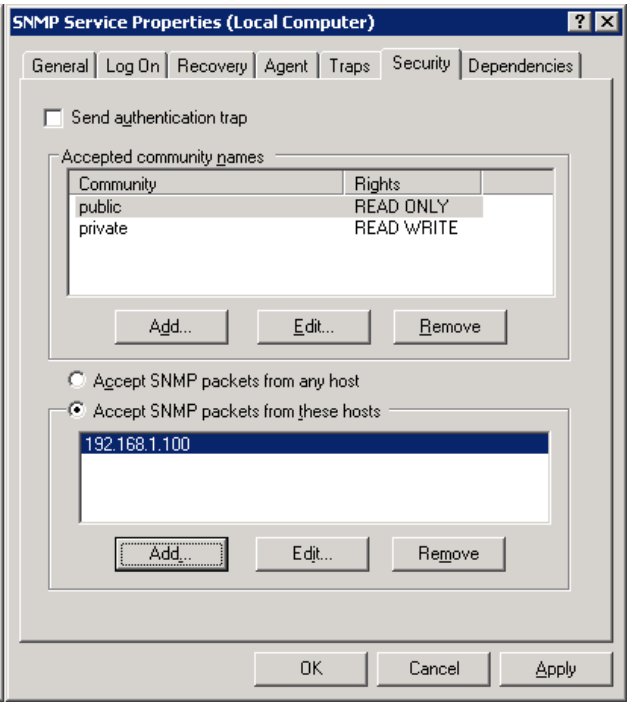
[2] Tài liệu chính thức của Microsoft tại http://support.microsoft.com/kb/324263

Double click lên SNMP Service để vào [SNMP Service Propertites].

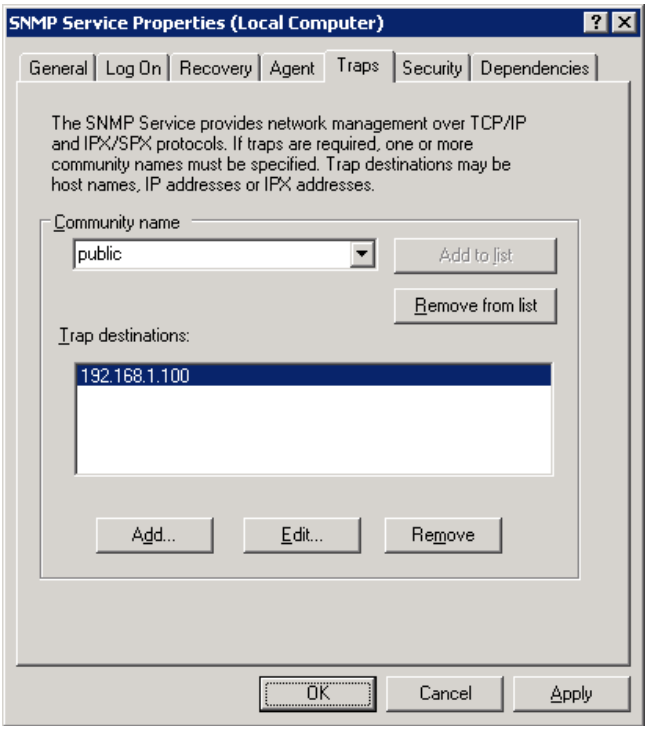
Chuyển qua tab [Security]. Groupbox [Accepted community names] là nơi bạn tạo các community, bạn hãy thêm một read-community string là "public". Danh sách "Accept SNMP packets from these hosts" là nơi bạn đặt SNMP ACL, chỉ cho phép một số SNMP manager nào đó quản lý.

Chuyển qua tab [Agent]. Chọn tất cả các Service có sẵn (nhất là Physical).





Cuối cùng là cấu hình Trap, chuyển qua tab [Traps], nhập vào community name của bản tin trap và nơi nhận trap.



Cấu hình SNMP agent trên hệ điều hành Linux

Trên CentOS, để bật dịch vụ snmp agent thì bạn cần cài đặt package net-snmp, để thực hiện được các phương thức snmp bằng dòng lệnh thì bạn cần cài đặt package net-snmp-utils. Phần này hướng dẫn cách cấu hình snmp agent trên CentOS, còn cách sử dụng net-snmp-utils thì sẽ được trình bày trong chương 3.

Đầu tiên bạn nên kiểm tra xem các package đã được cài đặt hay chưa, trong hình dưới là kết quả khi package đã được cài đặt.

```
[root@localhost ~]# yum list installed net-snmp net-snmp-utils
...
Installed Packages
net-snmp.i386                 1:5.3.2.2-7.el5_4.2                installed
net-snmp-utils.i386           1:5.3.2.2-7.el5_4.2                installed
```

Nếu package chưa được cài đặt, bạn có thể tự động download và cài đặt các package bằng lệnh "yum install" (máy chủ phải có kết nối internet).

```
[root@localhost ~]# yum install net-snmp, net-snmp-utils
Loading "installonlyn" plugin
Setting up Install Process
Setting up repositories
Reading repository metadata in from local files
Parsing package install arguments
Resolving Dependencies
...
Installed: net-snmp-utils.i386 1:5.3.2.2-7.el5_4.2
Dependency Installed: net-snmp.i386 1:5.3.2.2-7.el5_4.2
Dependency Updated: net-snmp-libs.i386 1:5.3.2.2-7.el5_4.2
Complete!
```

Sau khi cài đặt bạn nên khởi động snmpd (snmp agent) để đảm bảo bản cài đặt là tốt

```
[root@localhost ~]# service snmpd start
Starting snmpd:                                            [  OK  ]
```

Cấu hình của snmpd nằm trong file /etc/snmp/snmp.conf. Cách cấu hình snmp agent được hướng dẫn ngay trong file này, bao gồm các bước như sau :

+ Bước 1 : Khai báo community-string và ánh xạ nó vào một secutiryName nào đó.

+ Bước 2 : Khai báo version snmp tương ứng với securityName đó, ánh xạ vào một groupName.

+ Bước 3 : Tạo các view, cho phép bao gồm (include) hoặc không gồm (exclude) một nhánh con nào đó trong mib.

+ Bước 4 : Tạo một truy cập bằng cách gán một view cho một groupName.

```
# First, map the community name "public" into a "security name"
#         sec.name         source      community
com2sec   ConfigUser       default     public

# Second, map the security name into a group name:
#       groupName     securityModel   securityName
group   ConfigGroup   v1              ConfigUser
group   ConfigGroup   v2c             ConfigUser

# Third, create a view for us to let the group have rights to:
#       name           incl/excl    subtree              mask(optional)
view    systemview     included     .1.3.6.1.2.1.1
view    systemview     included     .1.3.6.1.2.1.25.1.1

# Finally, grant the group read-only access to the systemview view.
#      group        context sec.model sec.level prefix read       write notif
access ConfigGroup  ""      any       noauth    exact  systemview none  none
```

+ Mặc định sau khi cài đặt thì snmp agent trên máy chủ CentOS chỉ cho phép 2 view hạn chế là :

. iso.org.dod.internet.mgmt.mib-2.system (1.3.6.1.2.1.1) [3]

. iso.org.dod.internet.mgmt.mib-2.host.hrSystem.hrSystemUptime (1.3.6.1.2.1.25.1.1) [4]

+ Các view này chỉ chứa thông tin dạng "tên tuổi" của agent, không cho phép view các OID chứa các thông tin khác như thống kê lưu lượng card mạng, dung lượng ổ cứng. Để các chương trình SNMP manager có thể lấy được các thông tin khác bạn cần sửa 2 dòng view thành như sau :

```
#       name            incl/excl     subtree          mask(optional)
view    systemview      included      .1.3.6.1.2.1
view    systemview      included      .1.3.6.1.2.1.25
```

Sau đó bạn khởi động lại snmpd để các thay đổi có hiệu lực

```
[root@localhost ~]# service snmpd restart
Stopping snmpd:                                            [  OK  ]
Starting snmpd:                                            [  OK  ]
```

Mục đích của việc thay đổi này là đặt lại OID của view. Ban đầu server chỉ cho phép view từ 1.3.6.1.2.1.1 (iso.org.dod.internet.mgmt.mib-2.system) trở xuống, nhánh này không chứa nhánh iso.org.dod.internet.mgmt.mib-2.if (1.3.6.1.2.1.2) chứa các thông tin về interface (card mạng) do đó manager sẽ không thể lấy các thông tin thống kê tốc độ card mạng; sau khi sửa lại thành 1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2) thì view sẽ bắt đầu từ nhánh mib-2, tức là bao gồm mib-2.if, và manager sẽ lấy được các thông tin thống kê. Tương tự ta cũng đặt lại dòng thứ 2 thành 1.3.6.1.2.1.25 (iso.org.dod.internet.mgmt.mib-2.host) để cho phép view tất cả các object từ host trở xuống, bao gồm các thông tin về Storage, Device, Software. Bạn hãy để ý dòng 1 bao trùm dòng 2, như vậy bạn có thể xóa dòng 2 đi cũng được.

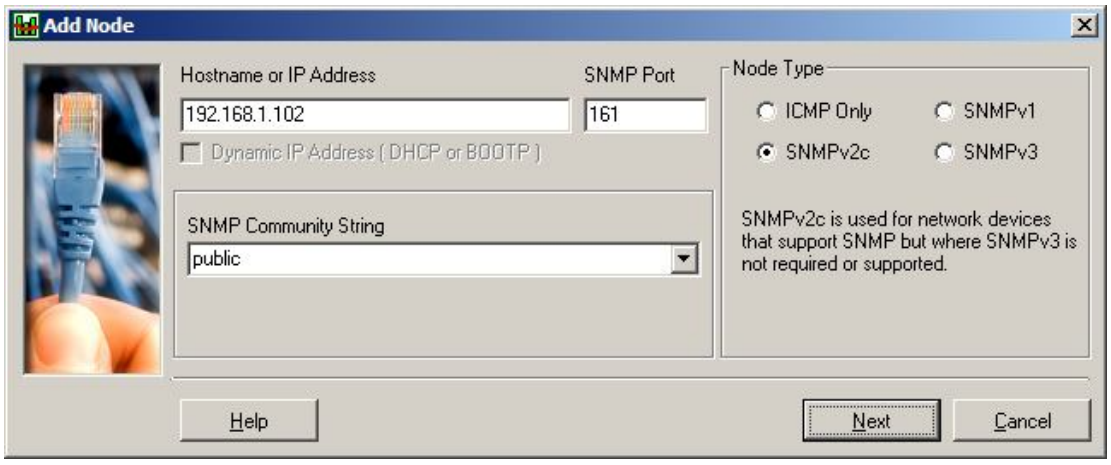
Cuối cùng là đặt chế độ tự chạy snmpd khi máy khởi động

```
[root@localhost ~]# chkconfig snmpd on
```

Giám sát máy chủ bằng phần mềm Solarwinds

Bạn hãy cài đặt Solarwinds để giám sát các máy chủ (cách cài đặt không được trình bày ở đây). Sau khi cài đặt, bạn dùng chương trình Orion System Manager của bộ Solarwinds để add thêm các server cần giám sát.

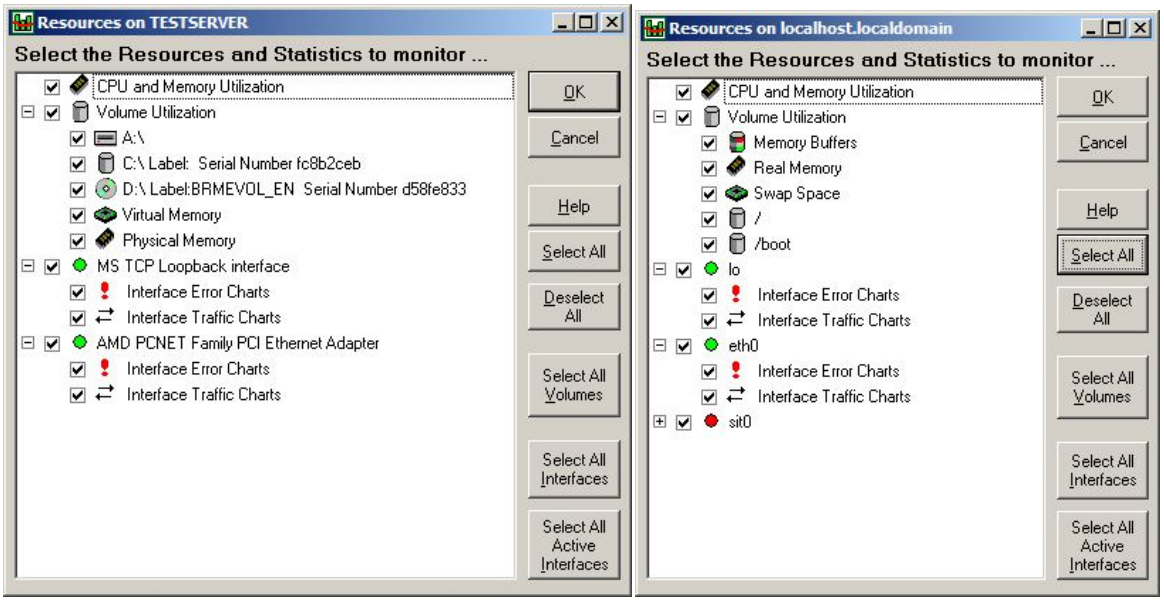
Trên giao diện của Orion System Manager, nhấn nút Add để hiện hộp thoại Add Device. Nhập IP của server vào [Hostname or IP Address], chọn [SNMP Community String] là "public" do trước đây bạn đã cấu hình server có read-community là public, chọn [Node Type] là SNMPv1 hay SNMPv2c đều được, sau đó nhấn nút [Next].



[3] RFC1213 – MIB for network management : http://www.ietf.org/rfc/rfc1213.txt

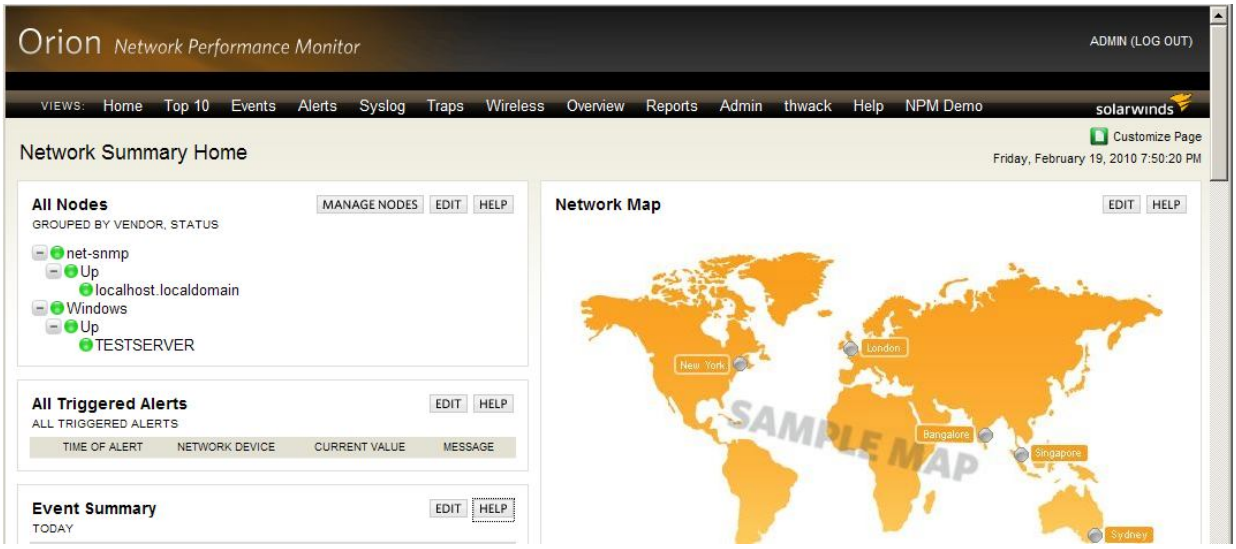
[4] RFC2790 – Host resources MIB : http://www.ietf.org/rfc/rfc2790.txt

Solarwinds sẽ tiến hành scan các tài nguyên trên máy chủ và hiện danh sách cho bạn chọn. Bạn hãy chọn giám sát những thứ mong muốn và nhấn OK.

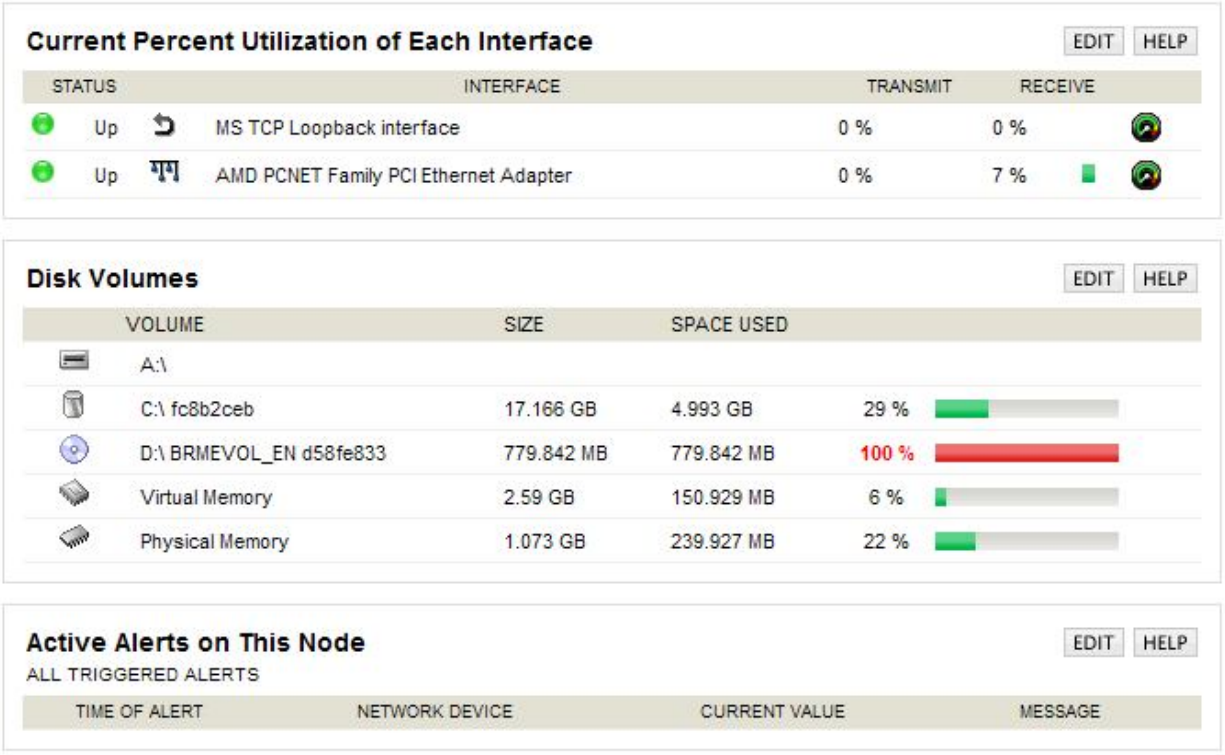


Minh họa resource trên server Win2003 *Minh họa resource trên server CentOS 5*

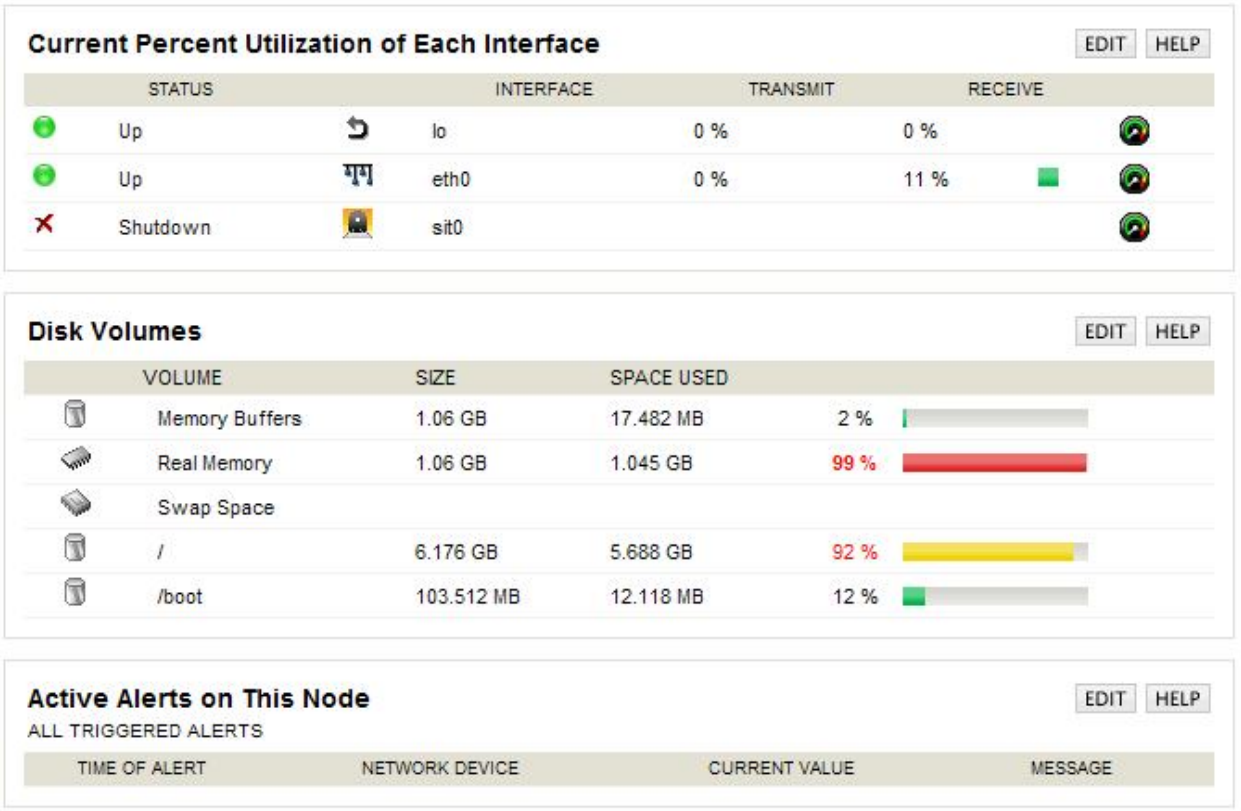
Để xem kết quả giám sát, bạn đăng nhập vào trang web quản trị Solarwinds, bạn sẽ thấy các server vừa add. Solarwinds nhận diện được các agent là Windows và net-snmp.



Click vào server Windows 2003 cần giám sát bạn sẽ thấy Solarwinds hiển thị thông tin trạng thái bao gồm tốc độ của các card mạng, tình trạng chiếm dụng bộ nhớ và đĩa.



Click vào server CentOS bạn cũng có thể thấy các thông tin tương tự.



Click vào từng card mạng hay partition đang được giám sát bạn sẽ thấy nhiều biểu đồ khác. Tuy nhiên tài liệu này không phải là tài liệu hướng dẫn sử dụng phần mềm nên chúng ta sẽ dừng ở đây.

5. Giám sát switch bằng SNMP

Trong phần này bạn sẽ tham khảo cách giám sát một switch C2950 bằng một phần mềm giám sát phổ biến khác là PRTG. Tài liệu đầy đủ về cài đặt, cấu hình và vận hành PRTG có thể tìm thấy trên trang chủ của sản phẩm [5].

Cấu hình SNMP trên switch Cisco C2950

Không phải mọi switch đều có thể giám sát được qua SNMP. Đó phải là switch hỗ trợ SNMP, các switch bình thường như switch ở phòng net thường không hỗ trợ SNMP. Cách cấu hình SNMP agent trên C2950 theo trình tự chung như phần trên đã trình bày.

```
C2950#configure terminal
C2950(config)#snmp-server enable
C2950(config)#snmp-server enable traps
C2950(config)#snmp-server community public ro
C2950(config)#snmp-server community private rw
C2950(config)#snmp-server host 192.168.1.100 version 1 public
```

Sau khi cấu hình xong thì ta show lại toàn bộ cấu hình SMP để đảm bảo agent đã được cài đặt đầy đủ.

```
C2950#show snmp
Chassis: FOC0833X23A
Contact:
Location:
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
1 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    1 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 192.168.1.100.162, 0/10, 1 sent, 0 dropped.
SNMP agent enabled
```

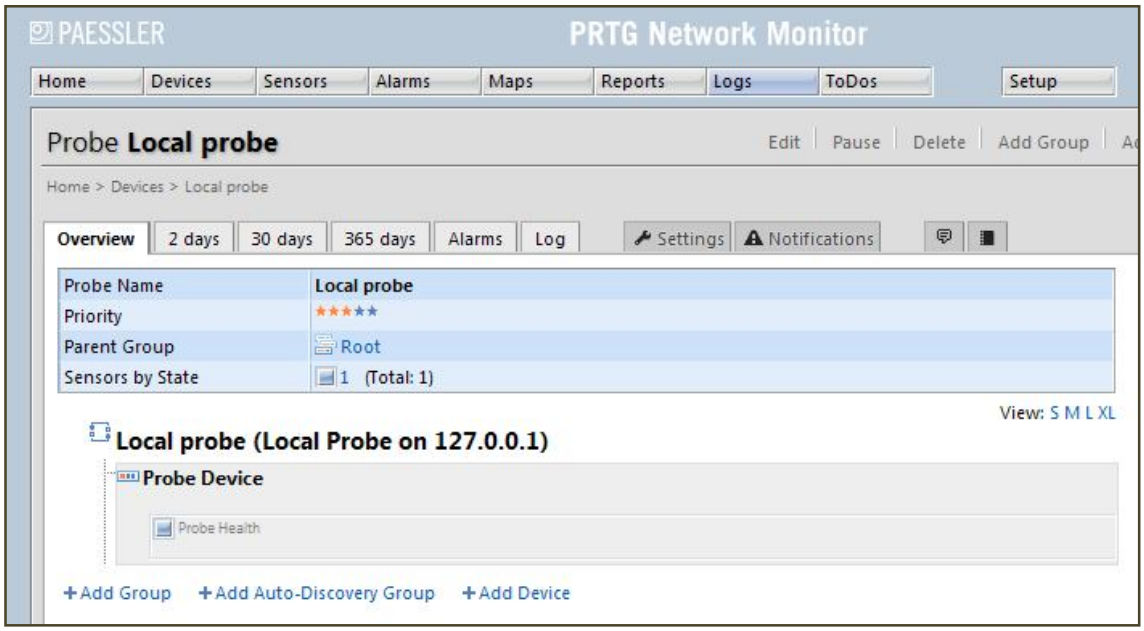
Giám sát switch bằng phần mềm PRTG

Giám sát máy chủ khác với giám sát lưu lượng của switch hay router. Giám sát lưu lượng là theo dõi tốc độ, lưu lượng truyền nhận trên các cổng của thiết bị, còn giám sát máy chủ ngoài lưu lượng cổng mạng còn có các thông số CPU, RAM, diskfree.

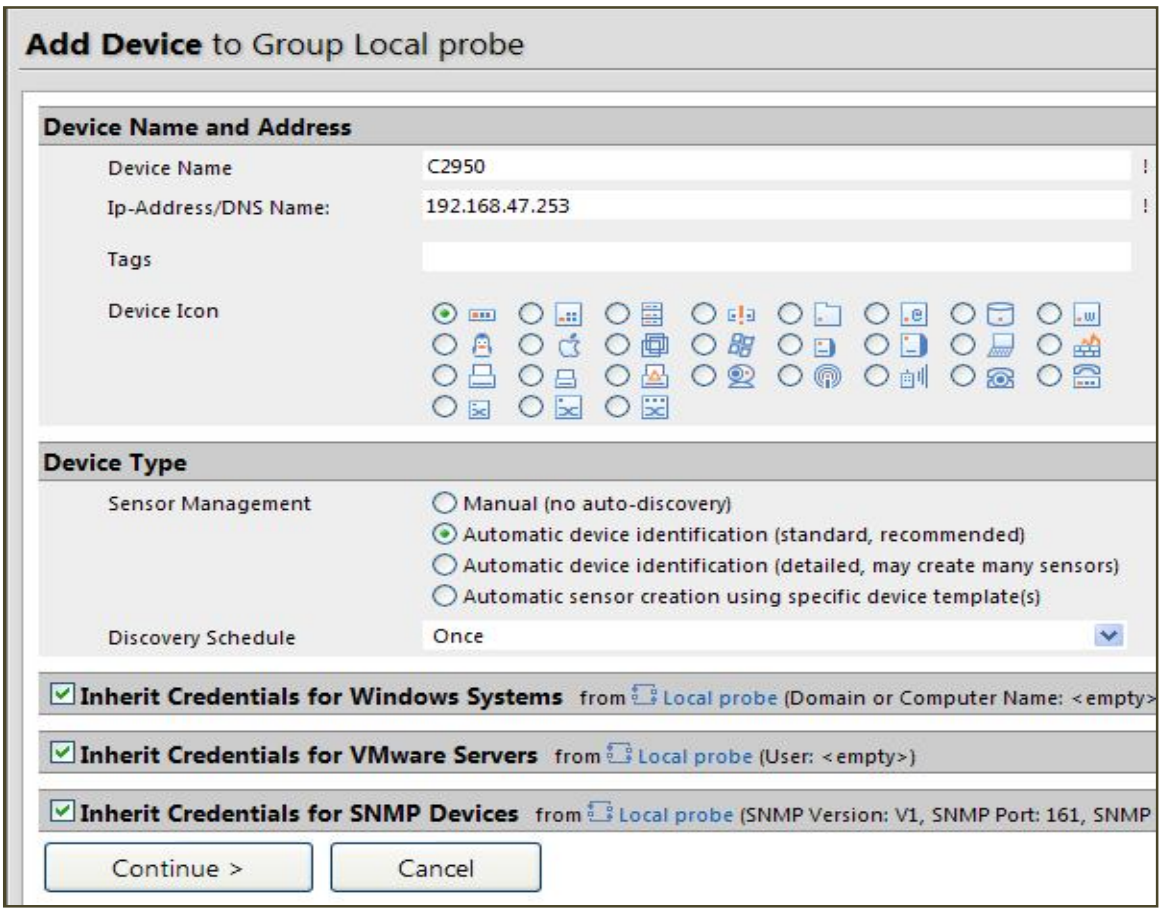
PRTG là phần mềm có thể giám sát các thiết bị mạng phần cứng và các server. Cách cài đặt và hướng dẫn sử dụng đầy đủ có thể tìm thấy trên trang chủ của PRTG hoặc trong rất nhiều tài liệu khác trên internet. Trong tài liệu này tác giả chỉ hướng dẫn một số bước tối thiểu để bạn có thể giám sát được một server.

Sau khi cài đặt PRTG Network Monitor, ta vào phần mềm qua giao diện web, đăng nhập bằng account và password mặc định “prtgadmin”, chuyển qua tab [Devices] và nhấn link [+Add Device].

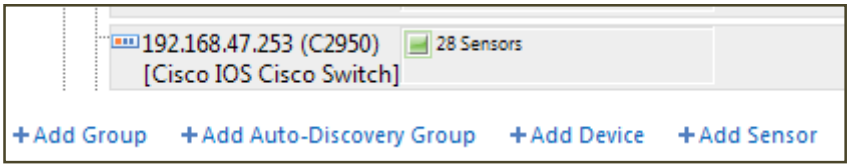
[5] Trang chủ PRTG : http://www.paessler.com/prtg



Nhập tên của máy chủ cần giám sát vào [Device Name], nhập IP của máy chủ vào [Ip-Address/DNS Name], chọn "Automatic device identification (standard, recommended)" để PRTG tự động dò tìm thiết bị SNMP đang được tạo là gì. Nhấn nút Continue, PRTG sẽ bắt đầu tiến trình dò tìm.



Sau đó các tài nguyên có thể giám sát được sẽ hiện ra màn hình.



Ở hình trên ta thấy PRTG phát hiện được 28 object có thể giám sát. Click vào tên thiết bị để mở ra màn hình giám sát, liệt kê danh sách các port FastEthernet của switch và băng thông đang sử dụng.

Pos	Sensor	Status	Message	Graph	Priority
1.	CPU Load 1	Up	OK	CPU Load 1 %	★★★★★
2.	(001) FastEthernet0/1	Up	OK	Sum 0 kbit/s	★★★★★
3.	(002) FastEthernet0/2	Up	OK	Sum 0 kbit/s	★★★★★
4.	(003) FastEthernet0/3	Up	OK	Sum 26 kbit/s	★★★★★
5.	(004) FastEthernet0/4	Up	OK	Sum 0 kbit/s	★★★★★
6.	(005) FastEthernet0/5	Up	OK	Sum 0 kbit/s	★★★★★
7.	(006) FastEthernet0/6	Up	OK	Sum 291,402 kbit/s	★★★★★
8.	(007) FastEthernet0/7	Up	OK	Sum 0 kbit/s	★★★★★
9.	(008) FastEthernet0/8	Up	OK	Sum 57,567 kbit/s	★★★★★
10.	(009) FastEthernet0/9	Up	OK	Sum 0 kbit/s	★★★★★
11.	(010) FastEthernet0/10	Up	OK	Sum 446,124 kbit/s	★★★★★

Như bạn đã biết, SNMP manager chỉ lấy được những thông tin mà SNMP agent cung cấp, do đó không phải tất cả mọi thứ trên máy chủ đều hiện ra trên PRTG để giám sát. Nhiều bạn khi chưa hiểu cơ chế của SNMP đã cho rằng PRTG không giám sát được một cái gì đó trên máy chủ là do nhược điểm của PRTG và mong muốn tìm kiếm một công cụ khác hay hơn. Thực chất nếu agent trên thiết bị không hỗ trợ thông tin thì mọi phần mềm giám sát đều không thể lấy thông tin đó.

Tóm tắt

+ Khai báo trên SNMP Agent gồm : enabled, read/write community string, snmp version, access list.

+ Khai báo trên SNMP manager gồm : host cần giám sát, read/write community string, snmp version, chu kỳ poll.

+ Khai báo trên Trap Sender gồm : enabled, IP của thiết bị nhận trap, trap-community string, snmp version.

+ Để giám sát được máy chủ Windows cần : cài đặt SNMP service, đặt read/write community string, đặt danh sách các host được phép gửi snmp request.

+ Để giám sát được máy chủ Linux cần : cài đặt một dịch vụ SNMP như net-snmp, kiểm tra lại các khai báo trong file /etc/snmp/snmp.conf, mở các view cần thiết, đặt snmpd ở chế độ tự khởi động.

+ Để giám sát được một switch cần : khai báo snmp agent đầy đủ các bước trên switch.

+ PRTG và Solarwinds là các phần mềm giám sát SNMP mạnh mẽ, Solarwinds thích hợp với mạng lớn hơn.