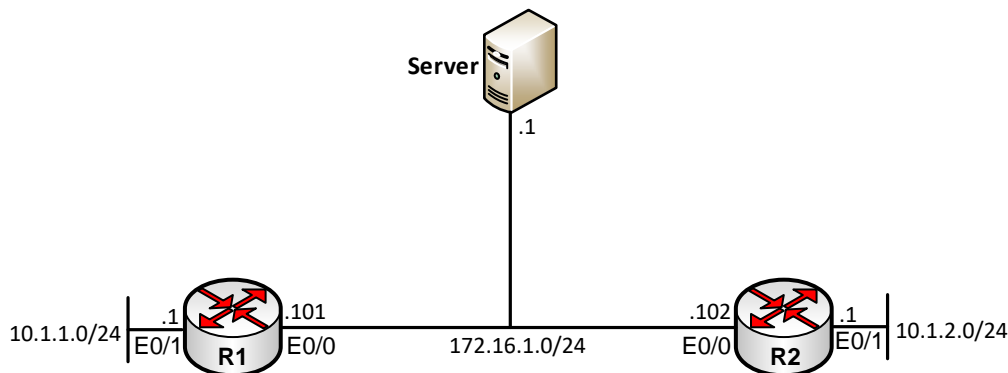


Lab 10 – Syslog, NTP, SNMP

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm 2 router và một PC đóng vai trò như một monitor server, được kết nối với nhau như được chỉ ra trên hình 1.
- Trong bài lab này, các bạn học viên sẽ thực hiện cấu hình một số tính năng về quản lý mạng trên router Cisco. Thông qua cấu hình các tính năng này và quan sát kết quả hiển thị trên các tool đi kèm, các bạn học viên sẽ ôn tập và nắm vững hơn các vấn đề liên quan đến các giao thức phục vụ quản lý mạng như Syslog, SNMP, NTP.

Thực hiện:

1. Cấu hình Syslog (1):

- Cấu hình các router để các thông điệp syslog về Server theo yêu cầu như sau:
 - Router R1 gửi mọi thông điệp syslog từ level 7 trở lên đến management server.
 - Router R2 chỉ gửi các thông điệp syslog từ level 5 trở lên đến management server.
- Trên Server cài phần mềm giả lập syslog server Kiwi syslog để kiểm tra cấu hình vừa thực hiện.

Cấu hình:

Trên R1:

```
R1(config)#logging 172.16.1.1
R1(config)#logging trap debugging
```

Trên R2:

```
R2(config)#logging 172.16.1.1
R2(config)#logging trap notifications
```

Ghi chú:

Syslog là một công cụ không thể thiếu trong hoạt động quản lý mạng. Syslog cho phép một thiết bị phát đi các báo cáo về các hoạt động đang diễn ra trên thiết bị cũng như các cảnh báo lỗi hoặc sự cố đang xảy ra. Các thông điệp báo cáo hay cảnh báo này có thể được lưu trữ nội bộ trên bản thân thiết bị hoặc có thể được gửi đến một server quản lý tập trung nào đó. Thông điệp syslog cũng có thể được gửi qua kết nối console để hiển thị trên màn hình console hoặc được gửi qua các kết nối telnet/SSH để hiển thị lên màn hình truy nhập từ xa của người quản trị.

Một thông điệp syslog sẽ đưa ra hai thông tin về vấn đề được cảnh báo:

1. *Chỉ rõ thông điệp phát ra để thực hiện cảnh báo về vấn đề gì (ta gọi là Facility).*
Ví dụ: IP (các vấn đề liên quan đến hoạt động của giao thức IP trên thiết bị), OSPF (các vấn đề liên quan đến hoạt động của giao thức OSPF trên thiết bị), Link (những vấn đề liên quan đến một đường link nào đó của thiết bị), v.v...

2. *Cho biết mức độ nghiêm trọng của thông điệp (ta gọi là Level).*

Có tổng cộng 8 level cho một thông điệp syslog gồm:

- Emergency (level 0).
- Alert (level 1).
- Critical (level 2).
- Error (level 3).
- Warning (level 4).
- Notice (level 5).
- Informational (level 6).
- Debugging (level 7).

Theo đó, chỉ số level càng thấp, mức độ nghiêm trọng càng tăng (level 0 là nghiêm trọng nhất và level 7 là ít nghiêm trọng nhất).

Thông điệp syslog có thể được hiển thị dưới nhiều định dạng khác nhau tùy vào các dòng sản phẩm của các hãng khác nhau. Ở đây, chúng ta cùng xét định dạng thông điệp syslog trên các thiết bị của Cisco:

```
%Facility-Level-Mnemonic: Message - text
```

Ví dụ:

```
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
```

Một thông điệp log của thiết bị Cisco sẽ được mở đầu bằng ký tự “%” và có cấu trúc gồm các phần như sau:

- **Facility:** Một đoạn text gồm các ký tự được viết hoa để chỉ ra vấn đề đang được phát syslog cảnh báo. Vấn đề này có thể là về phần cứng, phần mềm, các tiến trình, v.v... Trong ví dụ trên, phần Facility của thông điệp log chỉ ra rằng thông điệp này đang phát cảnh báo về trạng thái đường link (“LINK”).
- **Level:** Chính là level của thông điệp syslog, nằm trong 8 level từ 0 đến 7 đã trình bày ở trên, cho biết mức độ nghiêm trọng của cảnh báo được phát ra. Trong ví dụ ở trên, level của thông điệp log là level 3 (có tên gọi là Error).

- **Mnemonic:** Là một đoạn text đặc thù gồm các kí tự viết hoa dùng để định danh duy nhất cho sự kiện cụ thể của vấn đề được cảnh báo. Trong ví dụ ở trên, mnemonic của thông điệp là “UPDOWN” cho biết đây là thông điệp cảnh báo về tình trạng up/down của đường link.
- **Message – text:** Một đoạn text mô tả cụ thể vấn đề đang xảy ra, cung cấp thông tin chi tiết về sự kiện được phát thông điệp syslog. Trong ví dụ trên, thông điệp chỉ ra rất rõ ràng là cổng F0/0 mới chuyển trạng thái lên thành UP: “Interface FastEthernet0/0, changed state to up”.

Một thông điệp syslog của Cisco có thể có độ dài lên đến 80 kí tự theo sau dấu “%”.

Thông thường, để phục vụ mục đích quản lý, các thông điệp syslog đều được đính kèm với thời gian xảy ra sự kiện:

```
Mar 1 00:38:40.267: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
```

Ta có thể bật/tắt chế độ hiển thị thời gian phát syslog bằng lệnh:

```
R(config)#[no] service timestamps
```

Mặc định, trên các thiết bị Cisco, các thông điệp syslog được gửi ra cổng console để hiển thị trên màn hình cấu hình. Ta có thể tắt chế độ này bằng cách sử dụng lệnh:

```
R(config)#no logging console
```

Khi được gửi đi đến các server ở xa, các thông điệp syslog được đóng gói vào các UDP segment sử dụng port 514. Để cấu hình thiết bị gửi các thông điệp syslog về một server nào đó, chúng ta sử dụng lệnh:

```
R(config)#logging địa_chỉ_của_syslog_server
```

Mặc định, tất cả các thông điệp syslog phát ra trên thiết bị từ level 6 (Informational) trở lên level 0 đều được thiết bị đẩy về server. Để có thể giới hạn lại các level syslog mà ta muốn đẩy về server, chúng ta sử dụng thêm câu lệnh:

```
R(config)#logging trap N
```

Khi đó, mọi thông điệp syslog từ level N trở về level 0 đều sẽ được đẩy về syslog server.

Kiểm tra:

Ta giả lập một syslog server trên host 172.16.1.1 bằng cách cài đặt phần mềm Kiwi Syslog của hãng Solarwind trên host này. Phần mềm này có thể download miễn phí từ link: <https://www.solarwinds.com/products/freetools/free-kiwi-syslog-server.aspx>

Việc cài đặt phần mềm có thể được tiến hành hoàn toàn bình thường. Chỉ có một lưu ý nhỏ trong quá trình cài đặt là nếu chúng ta sử dụng host với hệ điều hành Window dùng cho PC cá nhân, ta sẽ chọn cài Kiwi như một ứng dụng chứ không chọn cài như một dịch vụ khi được hỏi trong cửa sổ cài đặt (hình 2):



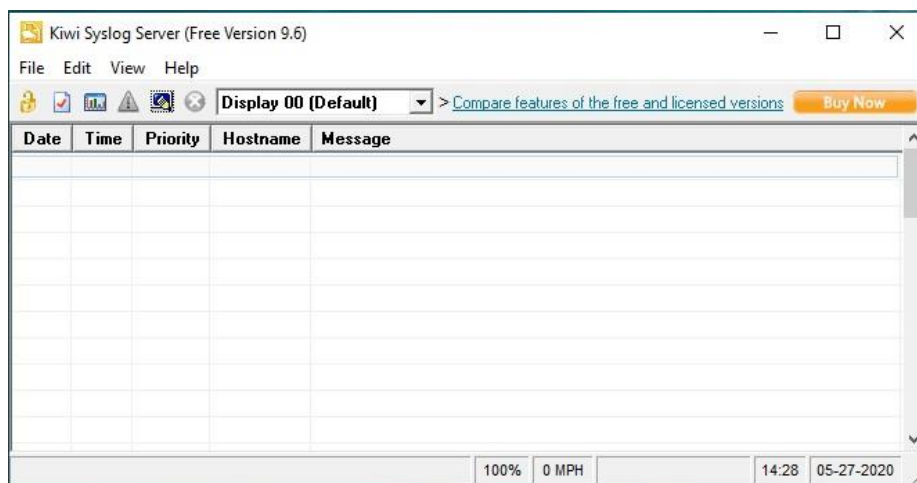
Hình 2 – Tùy chọn cài đặt cho phần mềm Kiwi.

Sau khi cài đặt xong, chương trình sẽ có biểu tượng như sau trên desktop (hình 3):



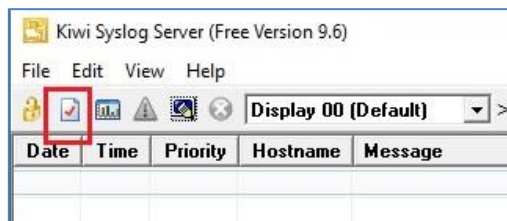
Hình 3 – Biểu tượng của chương trình Kiwi.

Và giao diện của chương trình (hình 4):



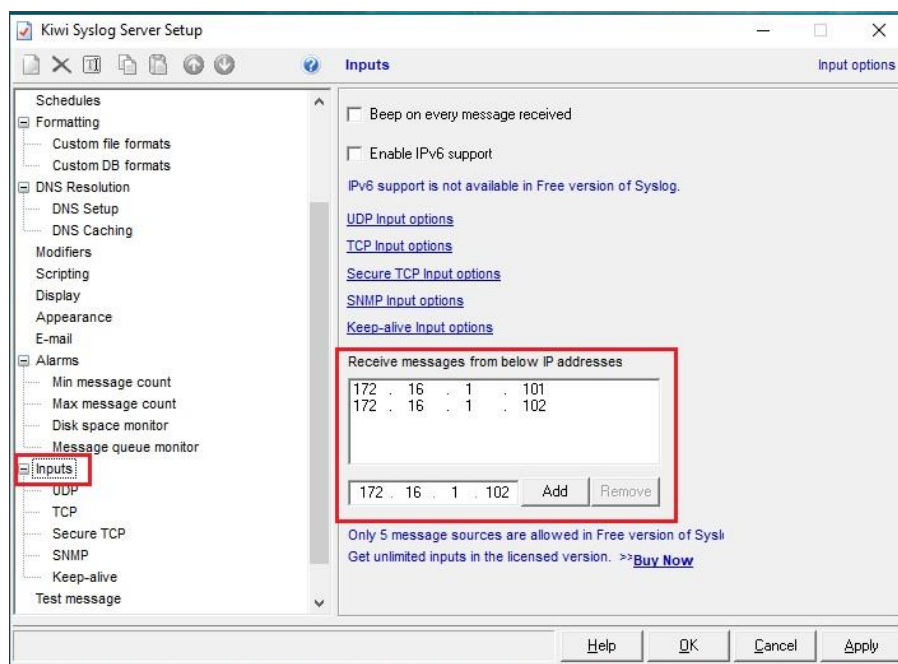
Hình 4 – Giao diện của chương trình.

Bản Free Kiwi của Solarwind chỉ hỗ trợ tiếp nhận các thông điệp syslog từ tối đa 5 nguồn phát và ta phải chỉ rõ các nguồn này. Để chỉ ra các nguồn phát syslog (là các router R1 và R2), chúng ta nhấn vào biểu tượng “Setup” của chương trình (hình 5):



Hình 5 – Chọn “Setup”.

Trong cửa sổ cấu hình mục “Setup”, ta click chuột vào mục “Inputs” ở ô bên trái rồi tiến hành nhập địa chỉ của các router vào ô “Receive messages from below IP addresses” ở ô bên phải (hình 6):



Hình 6 – Cửa sổ của mục “Setup”.

Các địa chỉ được ta chọn vào ô địa chỉ nguồn phát syslog gồm: 172.16.1.101 (R1), 172.16.1.102 (R2). Sau khi nhập các địa chỉ, ta nhấn “Apply” rồi “OK” để kết thúc hoạt động setup.

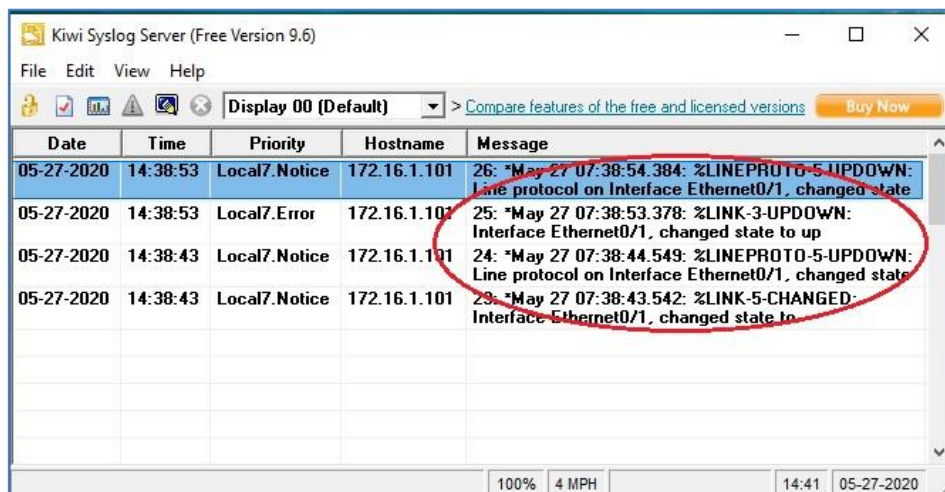
Tiếp theo, ta kiểm tra rằng các thông điệp syslog do các router phát ra sẽ được gửi đến syslog server vừa thiết lập.

Ta tạo một vài thông điệp log trên R1:

```
R1(config)#interface e0/1
R1(config-if)#shutdown
R1(config-if)#
*May 27 07:38:43.542: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to
administratively down
*May 27 07:38:44.549: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*May 27 07:38:53.378: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
```

```
*May 27 07:38:54.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to up
R1(config-if)#exit
```

Các thông điệp syslog này đã được đẩy đến server (hình 7):



Hình 7 – Các thông điệp syslog của R1 nhận được trên server.

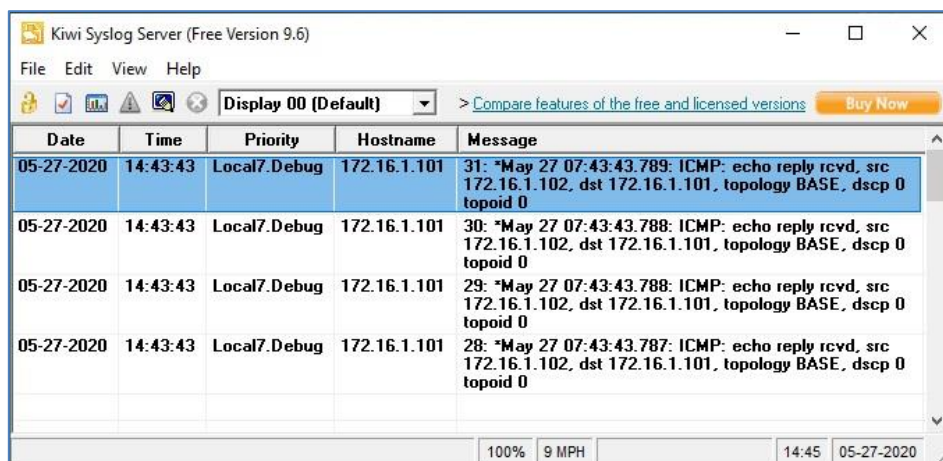
Ta thực hiện debug trên R1 để kiểm tra rằng kết quả debug trên R1 cũng được xuất đến server:

```
R1#debug ip icmp
ICMP packet debugging is on

R1#ping 172.16.1.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.102, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R1#
*May 27 07:43:43.787: ICMP: echo reply rcvd, src 172.16.1.102, dst 172.16.1.101, topology
BASE, dscp 0 topoid 0
*May 27 07:43:43.788: ICMP: echo reply rcvd, src 172.16.1.102, dst 172.16.1.101, topology
BASE, dscp 0 topoid 0
*May 27 07:43:43.788: ICMP: echo reply rcvd, src 172.16.1.102, dst 172.16.1.101, topology
BASE, dscp 0 topoid 0
*May 27 07:43:43.789: ICMP: echo reply rcvd, src 172.16.1.102, dst 172.16.1.101, topology
BASE, dscp 0 topoid 0
```

Kết quả debug trên R1 cũng đã xuất hiện đầy đủ trên thống kê của server syslog (hình 8):



Hình 8 – Kết quả debug trên R1 đã được xuất đến server.

Sau khi kiểm tra xong, ta nên tắt debug đã bật trên R1:

```
R1#undebug all
All possible debugging has been turned off
```

Ta có thể thực hiện kiểm tra tương tự với R2.

Như vậy, đến đây, chúng ta đã thực hiện xong cấu hình để các router R1 và R2 gửi kết quả log về một server quản lý tập trung.

2. Cấu hình Syslog (2):

Hiệu chỉnh lại cấu hình syslog đã thực hiện trên các router theo yêu cầu sau:

- R1 thực hiện chuyển qua sử dụng TCP port 5001 để gửi thông điệp syslog đến server syslog.
- R2 vẫn sử dụng UDP để gửi các thông điệp syslog đến server nhưng đổi lại destination port thành 5000.

Cấu hình:

Trên R1:

```
R1(config)#no logging 172.16.1.1
R1(config)#logging host 172.16.1.1 transport tcp port 5001
```

Trên R2:

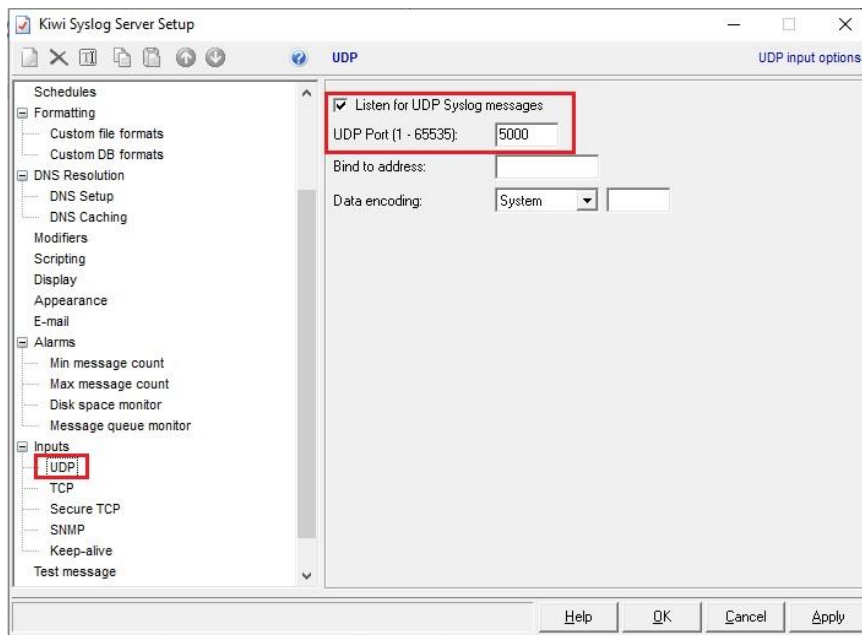
```
R2(config)#no logging 172.16.1.1
R2(config)#logging host 172.16.1.1 transport udp port 5000
```

Ta có thể thay đổi phương thức truyền tải cho các thông điệp syslog thay cho phương thức mặc định là sử dụng UDP port 514. Ta có thể sử dụng TCP để truyền tải hoặc có thể vẫn sử dụng UDP nhưng thay đổi port tiếp nhận trên server. Cấu hình cụ thể trên các thiết bị phát syslog đã được trình bày cụ thể ở trên.

Kiểm tra:

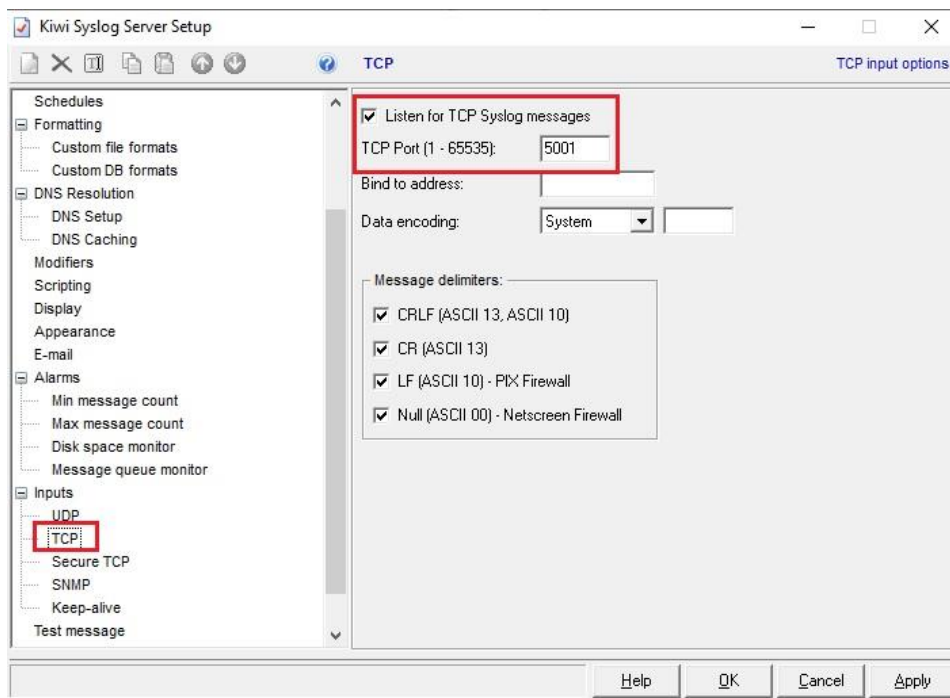
Ta thay đổi lại phương thức tiếp nhận syslog trên server: với UDP, đổi thành port 5001 và bật thêm việc tiếp nhận syslog trên kết nối TCP với destination port là 5000.

Để chuyển đổi với UDP, ở ô bên trái, ta vào lại mục “Inputs”, chọn “UDP”; ở ô bên phải, ta đổi port thành 5000 (hình 9):



Hình 9 – Chỉnh sửa port UDP.

Ta chọn mục “TCP” ở ô bên trái; thực hiện bật việc tiếp nhận syslog trên kết nối TCP bằng cách đánh dấu vào mục “Listen for TCP Syslog messages” ở ô bên phải và đổi port tiếp nhận thành 5001 (hình 10):



Hình 10 – Bật việc tiếp nhận syslog trên kết nối TCP port 5001.

Sau khi thiết lập xong, chúng ta nhấn phím “Apply” rồi “OK” để hoàn tất việc cấu hình.

Thực hiện tạo một vài thông điệp syslog trên R1 và kiểm tra rằng các thông điệp này đã được gửi đến server:

```
R1(config)#interface e0/1
R1(config-if)#shutdown
R1(config-if)#
*May 27 08:01:51.707: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to
administratively down
*May 27 08:01:52.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to down
R1(config-if)#
*May 27 08:01:52.789: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.16.1.1 port 5001
started - reconnection
R1(config-if)#no shutdown
R1(config-if)#
*May 27 08:02:01.008: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*May 27 08:02:02.018: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to up
```

Kết quả tiếp nhận syslog trên server (hình 11):

Date	Time	Priority	Hostname	Message
05-27-2020	15:02:00	Local7.Notic	172.16.1.101	40: *May 27 08:02:02.018: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
05-27-2020	15:02:00	Local7.Error	172.16.1.101	39: *May 27 08:02:01.008: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
05-27-2020	15:01:53	Local7.Info	172.16.1.101	38: *May 27 08:01:52.789: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.16.1.1 port 5001 started - reconnection
05-27-2020	15:01:51	Local7.Notic	172.16.1.101	37: *May 27 08:01:52.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
05-27-2020	15:01:51	Local7.Notic	172.16.1.101	36: *May 27 08:01:51.707: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down

Hình 11 – Các thông điệp syslog từ R1.

Ta thấy syslog server đã tiếp nhận các thông điệp syslog từ R1 bằng phương thức truyền tải mới.

Ta có thể kiểm tra tương tự với router R2.

3. Cấu hình NTP:

- Cấu hình để R1 đóng vai trò là nguồn đồng bộ thời gian thực cho hệ thống mạng. R1 sẽ sử dụng stratum cấp độ 5.
- Cấu hình để router R2 đồng bộ thời gian thực trên đồng hồ của mình theo thời gian của R1.

Cấu hình:

```
R1(config)#ntp master 5
R2(config)#ntp server 172.16.1.101
```

Ghi chú:

Một trong những yêu cầu quan trọng của quản lý mạng là đồng bộ thời gian trên đồng hồ hệ thống giữa các thiết bị trong hệ thống mạng. Các thiết bị trên hệ thống cần phải sử dụng đồng hồ có thời gian được đồng bộ với nhau. Để thực hiện được điều này, chúng ta có thể cấu hình các thiết bị chạy giao thức chuyên dùng để đồng bộ thời gian thực: NTP – Network Time Protocol.

Sự phân phối thông tin về thời gian với NTP được thực hiện theo mô hình một cây phân phối không vòng lặp. Ở gốc của cây phân phối là một server kết nối trực tiếp đến một đồng hồ nguồn có độ chính xác rất cao, ví dụ như đồng hồ nguyên tử, đồng hồ vệ tinh GPS,... Server kết nối trực tiếp đến nguồn chính xác này được gọi là server stratum 1 – cấp độ có độ chính xác cao nhất trong thang bậc của NTP. Một số thiết bị khác sẽ đóng vai trò NTP client lấy đồng bộ từ server stratum 1 này và có cấp độ là stratum 2. Các thiết bị khác có thể trở thành NTP client lấy tín hiệu đồng bộ từ các thiết bị stratum 2, và có cấp độ là stratum 3, v.v...

Cứ như vậy, các thiết bị NTP client nhận tín hiệu đồng bộ từ thiết bị stratum N sẽ có cấp độ là stratum N+1. Đến lượt nó, các thiết bị stratum N+1 lại trở thành NTP server cho các client stratum N+2,... Để đảm bảo cơ chế phân cấp và chống loop trong việc đồng bộ thời gian, một thiết bị có stratum N sẽ không bao giờ đồng bộ theo thiết bị có stratum N+1, việc đồng bộ chỉ xảy ra giữa một thiết bị có số hiệu stratum cao hơn theo thiết bị có số hiệu stratum thấp hơn.

Một thiết bị có thể được cấu hình chỉ định nhiều server để nó đồng bộ theo. Trong trường hợp này, thiết bị sẽ chỉ chọn một nguồn đồng bộ duy nhất là nguồn gần nó nhất về mặt định tuyến và có độ lệch về thời gian đồng bộ so với nó là ít nhất; các nguồn đồng bộ khác sẽ được sử dụng cho mục đích dự phòng. Câu lệnh khai báo NTP server để router đồng bộ theo:

```
R(config)#ntp server Địa_chi_IP_của_NTP_server [prefer]
```

Tùy chọn “prefer” được sử dụng trong trường hợp ta cấu hình nhiều NTP server trên router và chỉ định một server nào đó làm NTP server chính mà ta muốn đồng bộ và các server còn lại chỉ để dự phòng.

Ta có thể cấu hình cấp độ stratum cho một router đang đóng vai trò NTP server:

```
R(config)#ntp master Giá_trị_stratum
```

Ngoài ra, để phục vụ mục đích quản lý, ta nên cố định source IP của các gói tin NTP. Để thực hiện điều này, chúng ta sử dụng lệnh:

```
R(config)#ntp source Interface_trên_router
```

Lúc này, router sẽ sử dụng IP trên cổng được chỉ định để làm source cho mọi gói tin NTP.

Một điều lưu ý là tuy đã cấu hình đúng đắn trên mọi thiết bị nhưng các client có thể phải mất khá nhiều thời gian mới đồng bộ với server của mình, đặc biệt là khi thời gian trên đồng hồ của client và server có độ chênh lệch lớn. Để giảm thiểu thời gian chờ đồng bộ, ta nên chỉnh tay đồng hồ trên các thiết bị về càng gần nhau càng tốt và để giao thức NTP chỉ làm thao tác chỉnh tinh việc đồng bộ giữa các thiết bị mà thôi.

NTP chạy trên nền UDP sử dụng port 123.

4. Cấu hình SNMP (1):

- Cấu hình router R1 cho phép NMS 172.16.1.1 đọc thông tin SNMP sử dụng community string là “CISCORO” và cho phép NMS này được phép sửa đổi thông tin SNMP sử dụng community string là “CISCORW”.
- Cấu hình trên R1 các object Location và Contact theo yêu cầu như sau:
 - Location: WAREN Training Center
 - Contact: www.waren.vn
- Các bạn học viên sử dụng phần mềm “HiliSoft MIB Browser” thực hiện các thao tác sau:
 - Truy xuất các object Location và Contact đã thiết lập trên R1 trước đó.
 - Truy xuất các object mô tả về các interface của router R1.

Cấu hình trên R1:

Bật SNMP trên R1 và khai báo các community string như yêu cầu:

```
R1(config)#snmp-server community CISCORO ro
R1(config)#snmp-server community CISCORW rw
```

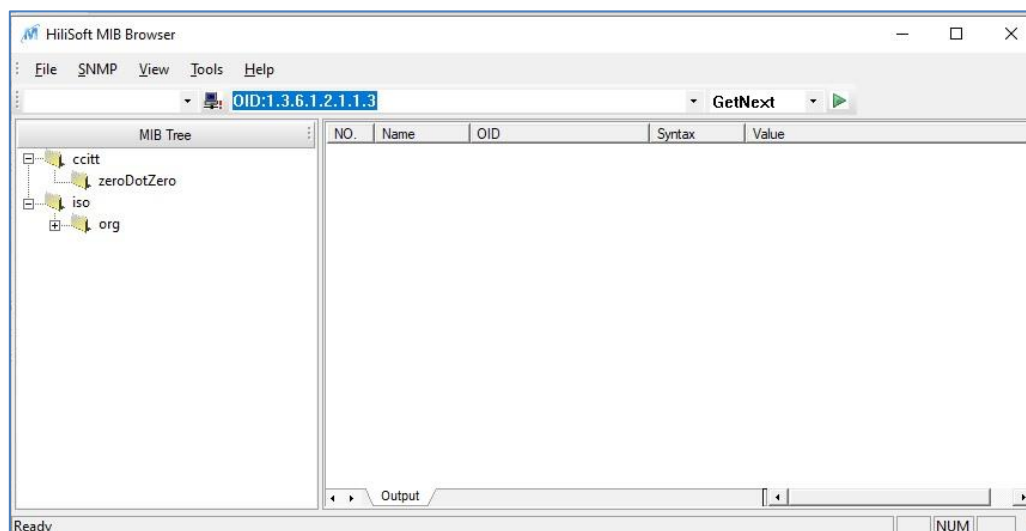
Thiết lập giá trị cho các object Location và Contact trên R1:

```
R1(config)#snmp-server location WAREN Training Center
R1(config)#snmp-server contact www.waren.vn
```

Sử dụng phần mềm truy xuất các object trên R1:

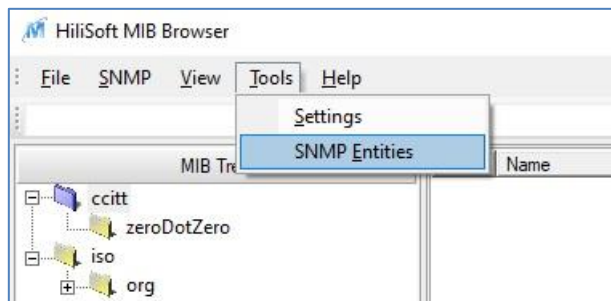
“HiliSoft MIB Browser” là một phần mềm miễn phí gọn nhẹ cho phép truy xuất các SNMP object trên một thiết bị có hỗ trợ SNMP. Phần mềm này cho phép chúng ta thực hiện các tác vụ SNMP như GET, GET NEXT, GET BULK, SET và WALK đến hệ thống object SNMP của thiết bị. Thông qua việc thử nghiệm các hoạt động này, chúng ta sẽ hình dung rõ hơn về hoạt động của SNMP.

Giao diện của phần mềm HiliSoft MIB Browser (hình 12):



Hình 12 – Giao diện phần mềm Hilisoft MIB Browser.

Trước hết, ta cấu hình trên phần mềm để nó thực hiện giám sát router R1. Để thực hiện điều này, ta vào menu “Tools”, chọn “SNMP Entities” (hình 13):



Hình 13 – Chọn menu khai báo thiết bị sẽ giám sát.

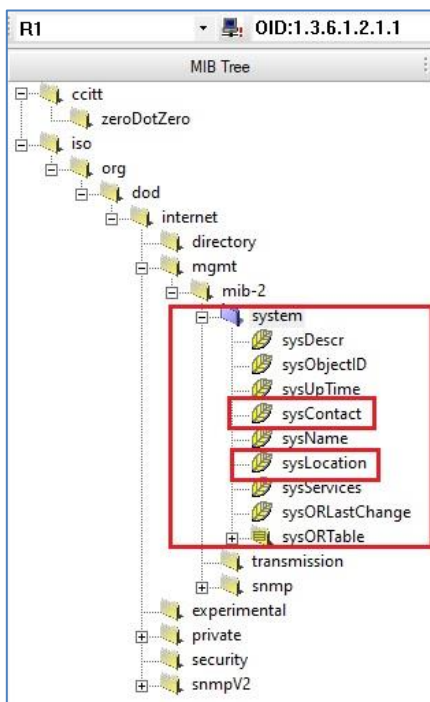
Cửa sổ giao diện hiện ra (hình 14):

 A screenshot of the 'SNMP Entities' configuration window. The 'Entity R1' is selected in the dropdown. The 'Name' field is 'R1' and the 'Address' is '172.16.1.101'. The 'Port' is '161' and 'Trapd Port' is '162'. Under the 'SNMP' section, 'SNMP V2c' is selected. The 'Time Out' is '500' ms, 'Retries' is '3', 'Non Reps' is '0', and 'Max Reps' is '10'. Under the 'SNMP V1/V2c' section, 'Read Community' is 'CISCORO' and 'Write Community' is 'CISCORW'. The 'SNMPv3' section is collapsed. At the bottom are 'Save', 'OK', and 'Cancel' buttons.

Hình 14 – Khai báo thiết bị sẽ giám sát.

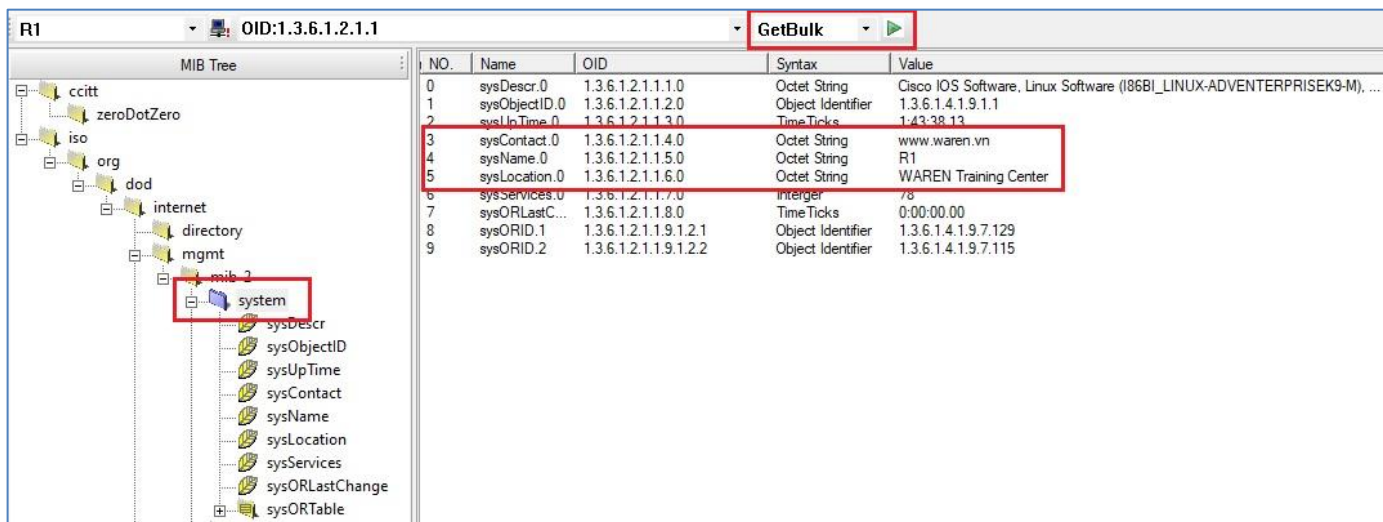
Trong cửa sổ này, ta khai báo các tham số như hình 14, sau đó nhấn “Save” rồi “OK” để hoàn tất khai báo.

Các object Location và Contact của thiết bị R1 nằm trên nhánh con “system” của nhánh “mib-2” (hình 15):



Hình 15 – Nhánh con “system” của “mib – 2”.

Trong ô lựa chọn tác vụ, ta chọn “GetBulk” để đọc toàn bộ các object của nhánh “system” (hình 16):



Hình 16 – Các object của nhánh “system”.

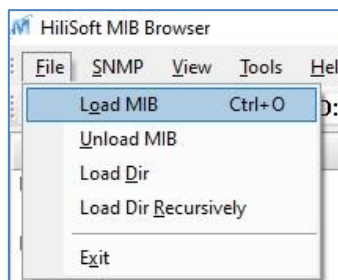
Từ kết quả thu được, ta thấy các object Contact và Location trên R1 đã được thiết lập đúng theo yêu cầu.

Bên cạnh việc thu thập tất cả các object của một nhánh bằng hành động “GetBulk”, chúng ta cũng có thể chọn cụ thể từng object và truy xuất bằng hành động “Get” hoặc “GetNext”.

Chúng ta tiếp tục sử dụng công cụ này để truy xuất các object mô tả về các interface của R1. Các object này nằm trong nhánh con “interfaces” của “mib – 2”. Tuy nhiên, hiện nay phần mềm chưa có file MIB mô tả

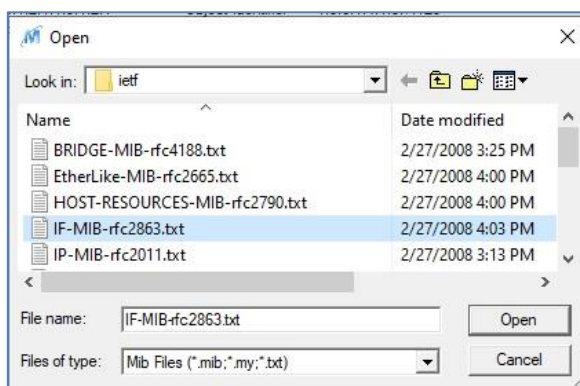
nhánh này trong cơ sở dữ liệu của nó nên khi quan sát sơ đồ cây ở hình 15, ta thấy nhánh “mib – 2” vẫn chưa có nhánh con “interfaces”. Do đó, trước hết, ta thực hiện load file MIB mô tả nhánh con này.

Ta chọn menu “File” và tiếp theo là “Load MIB” (hình 17):



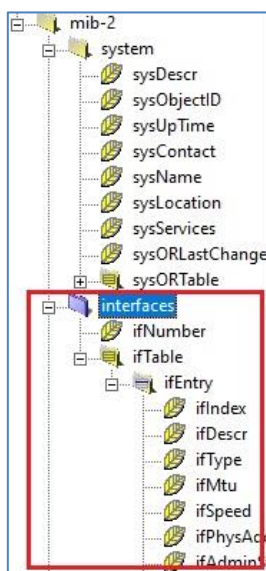
Hình 17 – Menu load file MIB.

Trong cửa sổ hiện ra tiếp theo, ta chọn file MIB cần load là “IF-MIB-rfc2863” (hình 18):



Hình 18 – Load file IF-MIB.

Lúc này, nhánh con “interfaces” đã xuất hiện trong sơ đồ cây tổ chức object của phần mềm (hình 19):



Hình 19 – Nhánh con “interfaces”.

Ta thực hiện truy xuất một vài object của nhánh này, ví dụ object “ifDescr”, object này chứa một chuỗi ký tự mô tả về interface tương ứng. Vì trên router có nhiều interface nên ta sử dụng hành động “GetBulk” để lấy được đầy đủ các sub – object của object này (hình 20):

NO.	Name	OID	Syntax	Value
0	ifDescr.1	1.3.6.1.2.1.2.2.1.2.1	Octet String	Ethernet0/0
1	ifDescr.2	1.3.6.1.2.1.2.2.1.2.2	Octet String	Ethernet0/1
2	ifDescr.3	1.3.6.1.2.1.2.2.1.2.3	Octet String	Ethernet0/2
3	ifDescr.4	1.3.6.1.2.1.2.2.1.2.4	Octet String	Ethernet0/3
4	ifDescr.5	1.3.6.1.2.1.2.2.1.2.5	Octet String	VoIP-Null0
5	ifDescr.6	1.3.6.1.2.1.2.2.1.2.6	Octet String	Null0
6	ifType.1	1.3.6.1.2.1.2.2.1.3.1	Integer	6
7	ifType.2	1.3.6.1.2.1.2.2.1.3.2	Integer	6
8	ifType.3	1.3.6.1.2.1.2.2.1.3.3	Integer	6
9	ifType.4	1.3.6.1.2.1.2.2.1.3.4	Integer	6

Hình 20 – Các giá trị của object “ifDescr”.

Ta có thể kiểm tra tương ứng trên router R1:

```
R1#show snmp mib ifmib ifindex
```

```
Ethernet0/1: Ifindex = 2
Ethernet0/3: Ifindex = 4
VoIP-Null0: Ifindex = 5
Ethernet0/0: Ifindex = 1
Null0: Ifindex = 6
Ethernet0/2: Ifindex = 3
```

Object “ifAdminStatus” mô tả trạng thái hoạt động của một interface bằng một biến kiểu “integer”; trong đó: 1 – interface up, 2 – interface down, 3 – testing. Ta thử truy xuất object này (hình 21):

NO.	Name	OID	Syntax	Value
0	ifAdminStatus.1	1.3.6.1.2.1.2.2.1.7.1	Integer	1
1	ifAdminStatus.2	1.3.6.1.2.1.2.2.1.7.2	Integer	1
2	ifAdminStatus.3	1.3.6.1.2.1.2.2.1.7.3	Integer	2
3	ifAdminStatus.4	1.3.6.1.2.1.2.2.1.7.4	Integer	2
4	ifAdminStatus.5	1.3.6.1.2.1.2.2.1.7.5	Integer	1
5	ifAdminStatus.6	1.3.6.1.2.1.2.2.1.7.6	Integer	1
6	ifOperStatus.1	1.3.6.1.2.1.2.2.1.8.1	Integer	1
7	ifOperStatus.2	1.3.6.1.2.1.2.2.1.8.2	Integer	1
8	ifOperStatus.3	1.3.6.1.2.1.2.2.1.8.3	Integer	2
9	ifOperStatus.4	1.3.6.1.2.1.2.2.1.8.4	Integer	2

Hình 21 – Các giá trị của object ifAdminStatus.

Từ kết quả thu được ta biết được trạng thái của các cổng hiện tại trên router, ví dụ, cổng E0/0 đang bật (ifAdminStatus.1 = 1), cổng E0/2 đang down (ifAdminStatus.3 = 2). Các giá trị index tương ứng của các interface có thể tham chiếu thông qua kết quả show ở trên hoặc trên kết quả thu được trên hình 20.

Ta thử thông qua SNMP để thay đổi trạng thái của cổng, lúc này ta sử dụng hành động “Set” để thay đổi giá trị của object “ifAdminStatus.index” tương ứng với cổng. Ví dụ, ta sẽ shutdown cổng E0/1 của R1 (hình 22):

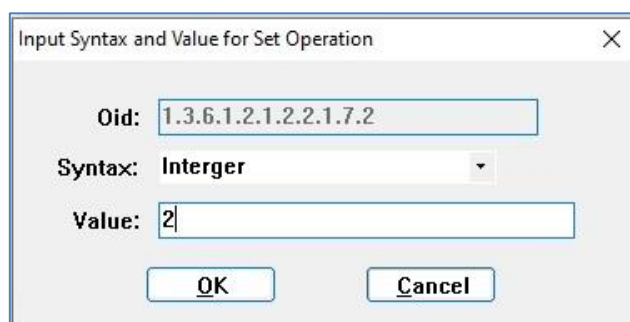


Hình 22 – Set giá trị cho object.

Trong ô “OID”, ta sử dụng giá trị “1.3.6.1.2.1.2.2.1.7.2”, trong đó, “2” chính là index của cổng E0/1. Tiếp theo ta chọn hành động “Set” (hình 22).

Trong cửa sổ khai báo giá trị hiện ra sau đó, ta nhập các thông số mới cho object (hình 23):

- Syntax: Integer.
- Value: 2.



Hình 23 – Nhập các thông số cho object.

Sau khi nhập xong ta nhấn “OK” để hoàn tất quá trình.

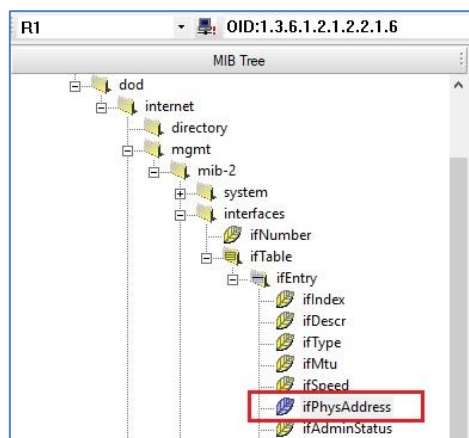
Lúc này cổng E0/1 của R1 đã được shutdown, các thông điệp syslog được phát ra thông báo về điều này:

```
May 27 14:59:22.239: %SYS-5-CONFIG I: Configured from 172.16.1.1 by snmp
May 27 14:59:24.238: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
May 27 14:59:25.249: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down

R1#show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Ethernet0/0              172.16.1.101   YES NVRAM    up              up
Ethernet0/1              10.1.1.1       YES NVRAM    administratively down down
Ethernet0/2              unassigned     YES NVRAM    administratively down down
Ethernet0/3              unassigned     YES NVRAM    administratively down down
```

Tiếp theo, ta sẽ thử thu thập các thông số cơ bản của một cổng Ethernet trên router R1, ví dụ: địa chỉ MAC, giá trị MTU, địa chỉ IP trên cổng E0/0.

Địa chỉ MAC của cổng sẽ được lưu trong object “ifPhysAddress” thuộc nhánh con “interfaces” của nhánh “mib – 2” (hình 24):



Hình 24 - Vị trí của object “ifPhysAddress”.

Tương tự như các object đã khảo sát trước đó, vì router có nhiều interface nên ta sẽ thực hiện hành động “GetBulk” với object này để thu thập được thông số tương ứng trên tất cả các interface (hình 25). Nhắc lại rằng, khi một object phải mô tả nhiều đối tượng, nó sẽ được chia thành các sub – object cho từng đối tượng với định dạng của ID sẽ là “tên_object.index”, với “index” chính là chỉ số định danh cho từng đối tượng.

NO.	Name	OID	Syntax	Value
0	#PhysAddress.1	1.3.6.1.2.1.2.2.1.6.1	Octet String	AA BB CC 00 10 00
1	#PhysAddress.2	1.3.6.1.2.1.2.2.1.6.2	Octet String	AA BB CC 00 10 10
2	#PhysAddress.3	1.3.6.1.2.1.2.2.1.6.3	Octet String	AA BB CC 00 10 20
3	#PhysAddress.4	1.3.6.1.2.1.2.2.1.6.4	Octet String	AA BB CC 00 10 30
4	#PhysAddress.5	1.3.6.1.2.1.2.2.1.6.5	Octet String0
5	#PhysAddress.6	1.3.6.1.2.1.2.2.1.6.6	Octet String	
6	#AdminStatus.1	1.3.6.1.2.1.2.2.1.7.1	Integer	1
7	#AdminStatus.2	1.3.6.1.2.1.2.2.1.7.2	Integer	1
8	#AdminStatus.3	1.3.6.1.2.1.2.2.1.7.3	Integer	2
9	#AdminStatus.4	1.3.6.1.2.1.2.2.1.7.4	Integer	2

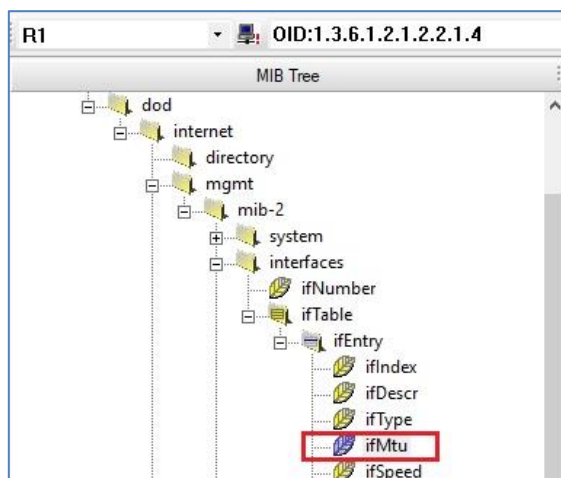
Hình 25 – Địa chỉ MAC của các interface.

Căn cứ vào các giá trị index tương ứng với các interface mà ta đã biết được ở các thao tác đã thực hiện trước đó, ta xác định được địa chỉ MAC của cổng E0/0 được lưu trên trên sub – object “ifPhysAddress.1”. Địa chỉ này là “AABB.CC00.1000”. Có thể kiểm tra lại điều này trên R1:

```
R1#show interfaces e0/0 | inc bia
```

```
Hardware is AmdP2, address is aabb.cc00.1000 (bia aabb.cc00.1000)
```

Tiếp theo, ta xác định giá trị MTU của cổng E0/0. Giá trị này được lưu trong object “ifMTU” của nhánh “interfaces” thuộc “mib – 2” (hình 26):



Hình 26 – Vị trí của object “ifMTU”.

Tương tự như trên, ta thực hiện “GetBulk” để thu thập thông số MTU trên các interface (hình 27):

NO.	Name	OID	Syntax	Value
0	ifMtu.1	1.3.6.1.2.1.2.2.1.4.1	Integer	1500
1	ifMtu.2	1.3.6.1.2.1.2.2.1.4.2	Integer	1500
2	ifMtu.3	1.3.6.1.2.1.2.2.1.4.3	Integer	1500
3	ifMtu.4	1.3.6.1.2.1.2.2.1.4.4	Integer	1500
4	ifMtu.5	1.3.6.1.2.1.2.2.1.4.5	Integer	1500
5	ifMtu.6	1.3.6.1.2.1.2.2.1.4.6	Integer	1500
6	ifSpeed.1	1.3.6.1.2.1.2.2.1.5.1	Gauge32	10000000
7	ifSpeed.2	1.3.6.1.2.1.2.2.1.5.2	Gauge32	10000000
8	ifSpeed.3	1.3.6.1.2.1.2.2.1.5.3	Gauge32	10000000
9	ifSpeed.4	1.3.6.1.2.1.2.2.1.5.4	Gauge32	10000000

Hình 27 – Giá trị MTU của các interface.

Tương tự như đã thực hiện ở trên, ta xác định được giá trị MTU của cổng E0/0 trên R1 là 1500 byte (ifMTU.1 = 1500). Ta có thể kiểm chứng lại điều này trên R1:

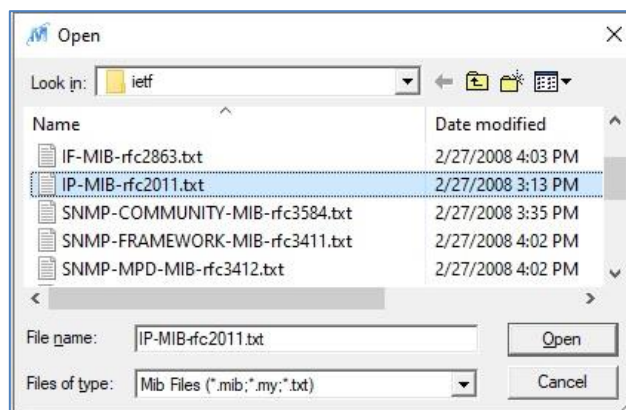
```
R1#show interfaces e0/0 | inc MTU
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
```

Cuối cùng, ta thực hiện truy xuất tiếp địa chỉ IP của cổng E0/0.

Trong nhánh con “interfaces” không chứa các object liên quan đến IP trên các cổng. Để có thể lấy được thông tin IP trên các cổng theo yêu cầu đặt ra, ta cần truy xuất đến các object thuộc về một nhánh khác chuyên về địa chỉ IP; tuy nhiên, hiện nay trong cây MIB của phần mềm đang không có nhánh con cần thiết này, do đó, trước hết, ta cần phải load file MIB cho các object về địa chỉ IP.

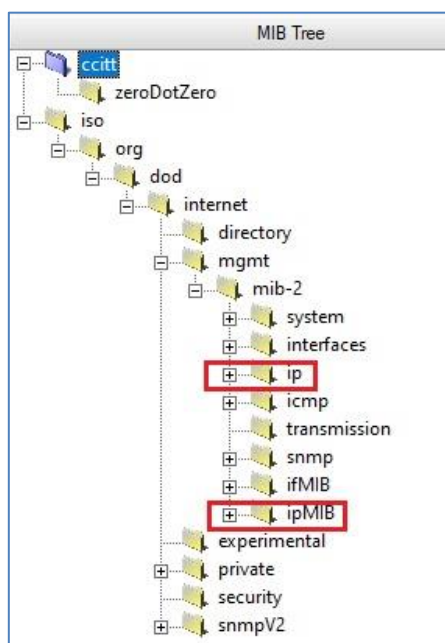
Giống như đã thực hiện ở trên, ta lại đi vào menu “File” và chọn “Load MIB” (xem hình 17 ở trên).

Trong cửa sổ “Open” hiện ra sau đó, ta chọn file “IP-MIB-rfc2011.txt” trong thư mục “ietf” của chương trình (hình 28):



Hình 28 – Chọn load file “IP-MIB-rfc2011”.

Sau khi ta nhấn “Open”, một số nhánh mới liên quan đến thông tin IP xuất hiện trong cây MIB của phần mềm (hình 29):

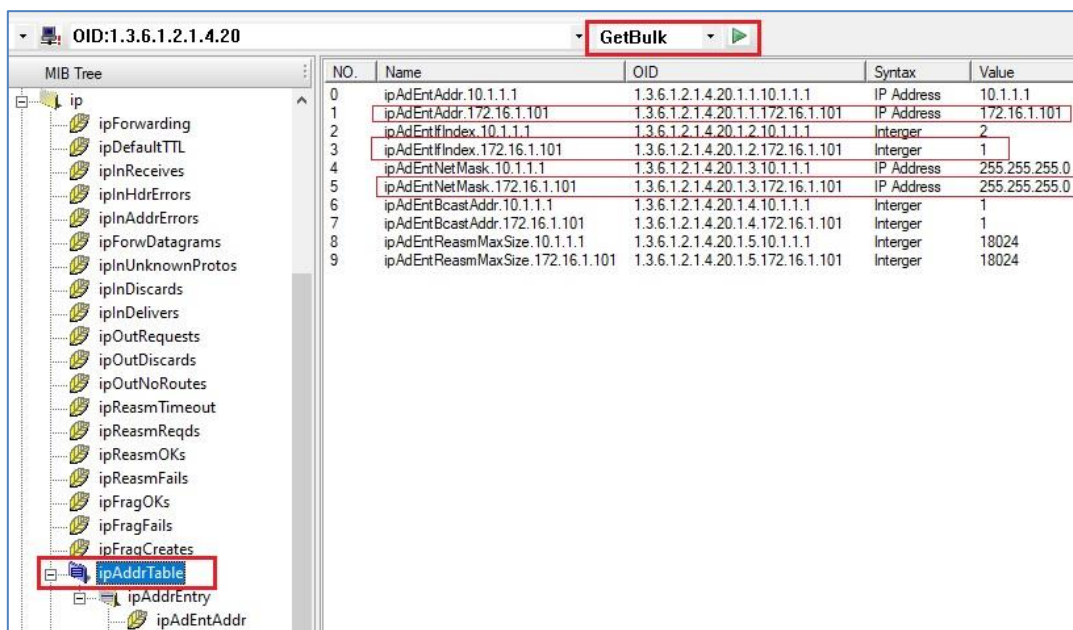


Hình 29 – Các nhánh về IP.

Trong nhánh con “ip”, ta chọn object “ipAddrTable” và thực hiện hành động “GetBulk” với object này. Trong kết quả nhận được, ta thấy có nhiều thông số liên quan đến cấu hình IP hiện có trên các cổng của router R1 (hình 30). Từ kết quả này, ta có thể xác định được địa chỉ IP trên cổng E0/0 của router R1 là 172.16.1.101/24. Lưu ý rằng, index của cổng E0/0 trong object “ipAdEntIfIndex” trùng với index của cổng này trong các object của nhánh “interfaces”.

Ta kiểm tra địa chỉ IP của cổng E0/0 để đối chiếu với kết quả nhận được từ truy xuất MIB:

```
R1#show ip interface e0/0
Ethernet0/0 is up, line protocol is up
  Internet address is 172.16.1.101/24
(...)
```

NO.	Name	OID	Syntax	Value
0	ipAdEntAddr.10.1.1.1	1.3.6.1.2.1.4.20.1.1.10.1.1.1	IP Address	10.1.1.1
1	ipAdEntAddr.172.16.1.101	1.3.6.1.2.1.4.20.1.1.172.16.1.101	IP Address	172.16.1.101
2	ipAdEntIndex.10.1.1.1	1.3.6.1.2.1.4.20.1.2.10.1.1.1	Integer	2
3	ipAdEntIndex.172.16.1.101	1.3.6.1.2.1.4.20.1.2.172.16.1.101	Integer	1
4	ipAdEntNetMask.10.1.1.1	1.3.6.1.2.1.4.20.1.3.10.1.1.1	IP Address	255.255.255.0
5	ipAdEntNetMask.172.16.1.101	1.3.6.1.2.1.4.20.1.3.172.16.1.101	IP Address	255.255.255.0
6	ipAdEntBcastAddr.10.1.1.1	1.3.6.1.2.1.4.20.1.4.10.1.1.1	Integer	1
7	ipAdEntBcastAddr.172.16.1.101	1.3.6.1.2.1.4.20.1.4.172.16.1.101	Integer	1
8	ipAdEntReasmMaxSize.10.1.1.1	1.3.6.1.2.1.4.20.1.5.10.1.1.1	Integer	18024
9	ipAdEntReasmMaxSize.172.16.1.101	1.3.6.1.2.1.4.20.1.5.172.16.1.101	Integer	18024

Hình 30 – Thông tin IP trên cổng E0/0 của R1.

Đến đây, ta đã hoàn tất khảo sát việc truy xuất một số object SNMP trên router R1 thông qua công cụ Hilisoft MIB Browser.

5. Cấu hình SNMP (2):

- Trên R2 thực hiện cấu hình một view tên là “ALL” cho phép hiển thị mọi object SNMP trên thiết bị.
- Trên router R2 thực hiện cấu hình SNMPv3 theo yêu cầu sau:
 - Tạo group có tên là “SNMPv3”, với security level là “priv” (thực hiện đầy đủ xác thực và mã hóa các gói tin SNMP). Cấu hình các read – view, write – view và notify – view của group tham chiếu đến view “ALL” đã tạo ở trên.
 - Tạo user với username là “NMS” thuộc group “SNMPv3” mới tạo ở trên. Phương thức xác thực là MD5, mã hóa là DES – 56; sử dụng key “CISCO1” cho xác thực và mã hóa.

Cấu hình:

Trên R2:

```
R2(config)#snmp-server view ALL iso included
R2(config)#snmp-server group SNMPv3 v3 priv read ALL write ALL notify ALL
R2(config)#snmp-server user NMS SNMPv3 v3 auth md5 CISCO1 priv des CISCO1
```

Ghi chú:

Việc bảo mật với SNMPv1 và SNMPv2/2c được thực hiện rất sơ sài, chỉ thông qua một community – string ở dạng clear text. SNMPv3 khắc phục nhược điểm này bằng cách thực hiện các cơ chế xác thực và mã hóa an toàn cho tất cả các gói tin SNMP được trao đổi. Có 3 mức độ security cho SNMPv3 (security level):

- *NoAuthNoPriv*: Không xác thực, không mã hóa.
- *AuthNoPriv*: Xác thực nhưng không mã hóa. Việc xác thực được thực hiện bằng cách sử dụng các phương thức xác thực HMAC – MD5 và HMAC – SHA.

- *AuthPriv*: Xác thực và mã hóa. Xác thực được thực hiện giống như trên. Mã hóa được thực hiện bằng kỹ thuật mã hóa DES, 3DES hay AES với key mã hóa được cấu hình tĩnh trên cả NMS lẫn Agent.

Mô hình hoạt động của SNMPv3 trên router/switch Cisco được tổ chức như sau:

- Trong truy vấn SNMP, Agent (router/switch) sẽ đóng vai trò như một SNMP server và NMS đóng vai trò như một client truy vấn thông tin trên server này. Do đó, trên Agent router/switch, mỗi NMS sẽ được xem như một user.
- Các user, đến lượt chúng, lại được tổ chức vào thành từng group. Với mỗi group, ta sẽ quy định cụ thể là group này được truy vấn những thành phần nào của hệ thống object trên Agent và phải thực hiện mức độ bảo mật nào trong 3 mức độ bảo mật của SNMPv3 đã nói ở trên.
- Với cách thức tổ chức vừa nêu, ta sẽ thực hiện các bước cấu hình như sau:
 - Đầu tiên, khai báo các view. View là một profile tham chiếu đến một phần nào đó của hệ thống file MIB lưu trên router/switch.
 - Tiếp theo, ta khai báo các group. Mỗi group sẽ được tham chiếu đến một view nào đó đã khai báo ở trên, group tham chiếu đến view nào thì các user của group sẽ chỉ được truy vấn các object nằm trong bộ phận của hệ thống file MIB mà view ấy trỏ tới. Bên cạnh đó, ta cũng khai báo rõ group phải thực hiện các mức độ bảo mật nào của SNMPv3.
 - Cuối cùng, ta khai báo các user cho các NMS (NMS là user). Mỗi user sẽ được đặc trưng bởi username, group mà nó thuộc về. Khi khai báo user, ta cũng sẽ phải chỉ ra phương pháp mã hóa, xác thực và các key cụ thể mà user này phải sử dụng cho hoạt động xác thực/mã hóa.

Ta đi vào từng bước cấu hình cụ thể:

Cấu hình view

Để cấu hình một view trên router, chúng ta sử dụng lệnh:

```
R(config)#snmp-server view Tên_view Nhánh_cây_MIB_muốn_tham_chiếu {included|excluded}
```

Trong câu lab này, vì ta muốn định nghĩa view cho phép truy vấn đến mọi object của mọi MIB, ta sẽ cấu hình view này tham chiếu đến nhánh “iso”, nhánh này của cây MIB chứa mọi tham số SNMP cho các thiết bị mạng mà ta có thể truy vấn:

```
R(config)#snmp-server view ALL iso included
```

Ta đặt tên view vừa cấu hình là “ALL”. Từ khóa “included” của câu lệnh cho phép tham chiếu đến toàn bộ nhánh “iso”. Ngược lại, nếu ta sử dụng từ khóa “excluded”, ta được tham chiếu đến toàn bộ cây MIB, ngoại trừ nhánh được đề cập.

Cấu hình group

Tiếp theo, ta thực hiện cấu hình group trên các router. Câu lệnh cấu hình group:

```
R(config)#snmp-server group Tên_group Security_model Security_level [read read_view] [write write_view] [notify notify_view]
```

Các thông số mà ta có thể chỉ định cho một group gồm:

- **Các view mà group sẽ tham chiếu:** Có 3 loại view: read – view, write – view và notify – view.
 - *Read – view:* quy định quyền đọc của NMS đối với khu vực nào của cây MIB.
 - *Write – view:* quy định quyền ghi/sửa của NMS đối với khu vực nào của cây MIB.
 - *Notify – view:* quy định quyền phát trap của Agent đối với các object thuộc khu vực nào của cây MIB.
 - Mặc định, nếu ta không khai báo read – view, mọi object đều có thể được đọc bởi NMS; nhưng ngược lại, nếu ta không khai báo write – view và notify – view, mọi object đều không thể ghi/sửa bởi NMS và không thể phát trap bởi Agent.
- **Security model và security level:**
 - Có 3 security model có thể được áp dụng cho một group: SNMPv1 (từ khóa “v1”), SNMPv2c (từ khóa “v2c”) và SNMPv3 (từ khóa “v3”).
 - Có 3 security level có thể được áp dụng cho một group: noAuthnoPriv (từ khóa “noauth”), AuthnoPriv (từ khóa “auth”) và AuthPriv (từ khóa “priv”).
 - Nếu ta sử dụng model v1 hoặc v2c, security level chọn được chỉ có thể là noAuthnoPriv. Nếu ta sử dụng model v3, security level chọn được có thể là bất kỳ level nào trong 3 level đã nêu. Trong trường hợp ta sử dụng security level noAuthnoPriv (trong cả 3 model), username của user sẽ được sử dụng như community string để xác thực NMS muốn truy vấn lên thiết bị.

Cấu hình khai báo user

Cuối cùng, sau khi cấu hình xong các group, ta khai báo các user và gán chúng vào các group:

```
R(config)#snmp-server user user_name group_name security_model security_level [auth {md5|sha} Authentication_key] [priv {des|3des|aes} Encryption_key]
```

Như định dạng của câu lệnh đã chỉ ra, mỗi user sẽ được định danh bởi một username (“username”) và được gán vào một group đã xây dựng trước đó (“group_name”). Cũng trong câu lệnh khai báo user, ta cũng nêu lại các security model và security level (*security_model security_level*) mà ta sẽ áp dụng cho user.

Với xác thực (**auth**), ta chỉ rõ phương pháp xác thực sẽ sử dụng là MD5 (**md5**) hay SHA – 1 (**sha**), đồng thời cũng khai báo key được sử dụng cho hoạt động xác thực này (*Authentication_key*). Tương tự, với mã hóa (**priv**), ta cũng phải chỉ rõ phương pháp mã hóa DES – 56 (**des**), 3DES (**3des**) hay AES (**aes**) và key sử dụng cho hoạt động mã hóa (*Encryption_key*). Ở phía NMS, chúng ta cũng phải khai báo lại chính xác các key xác thực và mã hóa đã cấu hình trên Agent để NMS có thể truy vấn được thông tin trên Agent.

Kiểm tra:

Trên phần mềm, tương tự như với R1, ta vào menu “Tools” và chọn “SNMP Entities” để khai báo thiết bị cần giám sát R2. Trong cửa sổ khai báo, ta nhập các thông số cho R2 (hình 31):

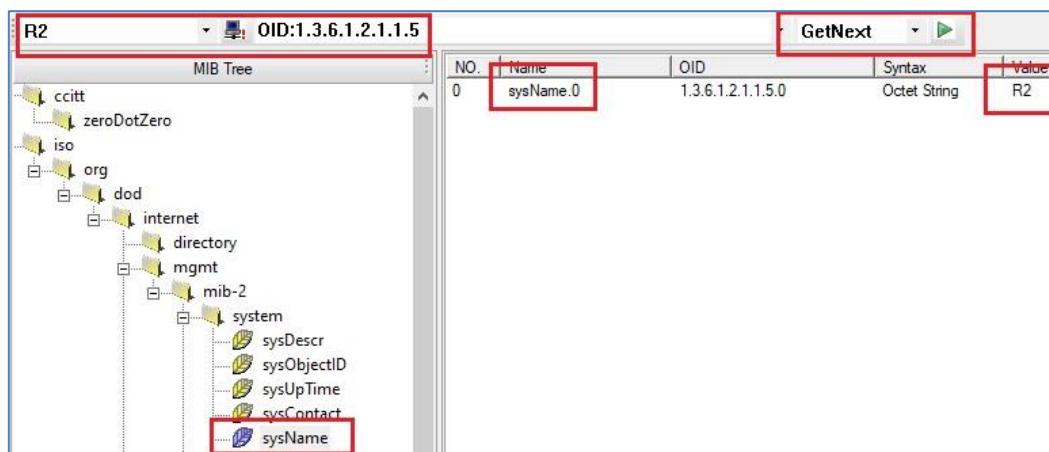
Hình 31 – Khai báo cho R2.

Trong đó:

- Ta chọn version là SNMPv3.
- Security Name: chính là username “NMS”.
- Trong ô “Security Level”, ta chọn “Auth, Priv” (vừa xác thực, vừa mã hóa).
- Trong các ô “Auth Protocol” và “Priv Protocol”, ta chọn các phương thức là MD5 và DES như yêu cầu và nhập các key tương ứng đã khai báo (ở đây là “CISCO1”).

Sau khi khai báo, ta nhấn “OK” để hoàn tất quá trình.

Đến đây, ta đã có thể truy xuất các object của R2 bằng SNMPv3 (hình 32):



Hình 32 – Truy xuất bằng SNMPv3 đến các object của R2.

Đến đây, ta đã hoàn thành cấu hình và kiểm tra SNMPv3 cho thiết bị R2.

6. Cấu hình SNMP (3):

- Cấu hình để router R1 phát trap gửi về Trap Receiver đặt trên server 172.16.1.1. Hoạt động phát Trap trên R1 sẽ được thực hiện khi một interface bất kỳ của router chuyển trạng thái giữa up và down.
- Các bạn học viên sử dụng phần mềm “iReasoning MIB Browser” để kiểm tra hoạt động Trap này.

Cấu hình Trap trên R1:

Trên R1, ta thực hiện cấu hình phát trap cho các sự kiện link up/down và đẩy về server 172.16.1.1 như sau:

```
R1(config)#snmp-server enable traps snmp linkup linkdown
R1(config)#snmp-server host 172.16.1.1 version 2c CISCOTRAP
```

Kiểm tra hoạt động Trap:

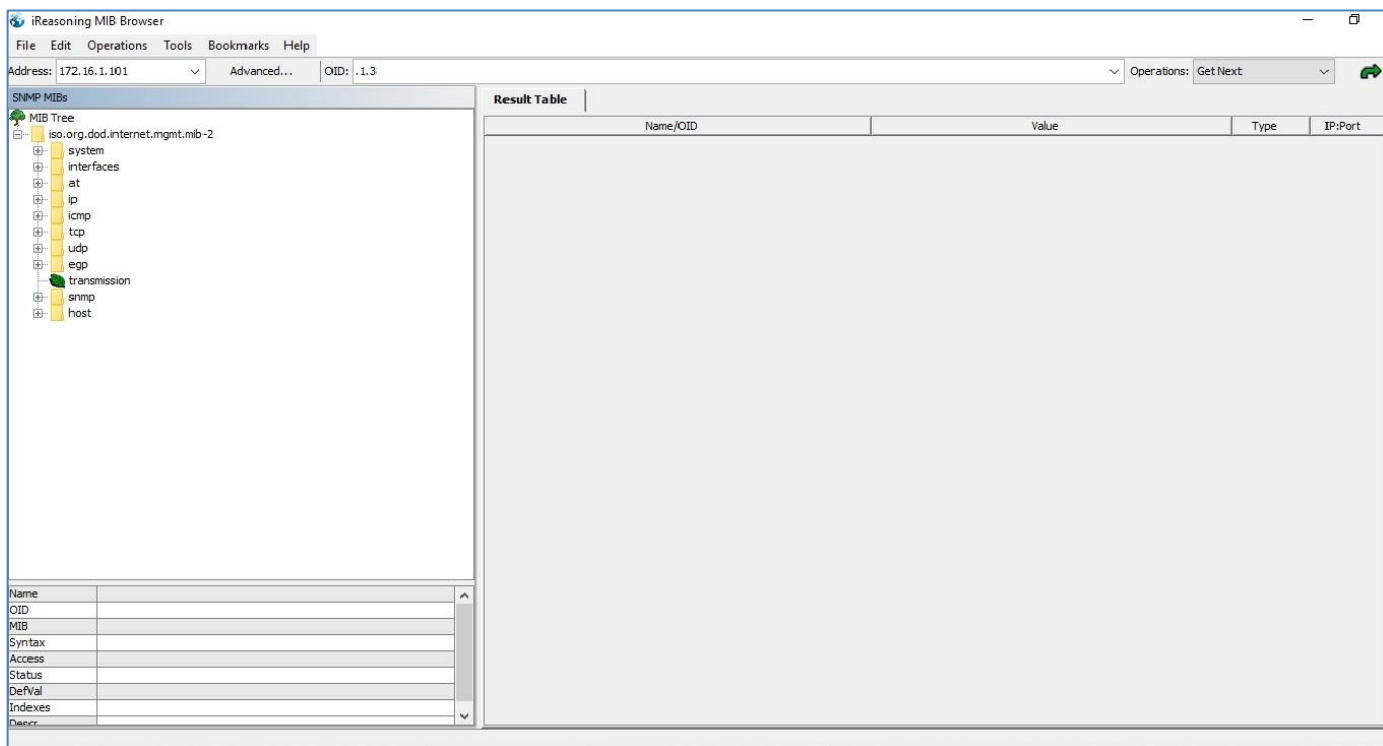
Phần mềm “iReasoning MIB Browser”, bản miễn phí, cho phép chúng ta có thể truy xuất được các object SNMP trên cây MIB của thiết bị với SNMP v1 và v2c (giống như đã thực hiện ở các bước trên với phần mềm “MIB Browser”), đồng thời cũng cho phép chúng ta tiếp nhận và phân tích các Trap gửi đến từ thiết bị (tính năng này không có trong “MIB Browser” ở trên). “iReasoning MIB Browser” sẽ được giảng viên chia sẻ với các bạn học viên trong bộ tài nguyên học tập của khóa học, hoặc các bạn có thể trực tiếp download về từ đường link: <https://www.ireasoning.com/download.shtml>

Sau khi tải về máy, các bạn thực hiện cài đặt giống như các phần mềm thông thường trên Windows. Trên hình 33 là biểu tượng của chương trình khi được cài đặt trên máy:



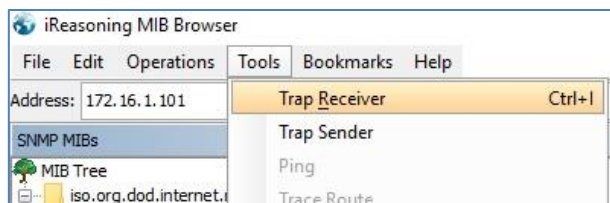
Hình 33 – Biểu tượng của chương trình iReasoning Browser.

Giao diện của chương trình (hình 34):



Hình 34 – Giao diện của chương trình “iReasoning Browser”.

Để bắt trap của R1 gửi đến Server, chúng ta bật tính năng Trap Receiver trên phần mềm bằng cách vào mục “Tools” trên menu của phần mềm và chọn “Trap Receiver” (hình 35):



Hình 35 – “Trap Receiver” trong “Tools”.

Sau khi chọn xong, trong ô lớn bên phải của cửa sổ giao diện sẽ hiện ra thêm một bảng “Trap Receiver” nằm ngay cạnh bảng “Result Table” (hình 36):



Hình 36 – Cửa sổ “Trap Receiver”.

Tiếp theo, ta thực hiện tạo Trap trên R1 và xác nhận rằng các Trap này đều được tiếp nhận đầy đủ trên phần mềm vừa cài đặt.

Trên R1, ta thực hiện bật debug và shutdown cổng E0/1 để tạo và quan sát thông tin về hoạt động gửi Trap:

```
R1#debug snmp packets
SNMP packet debugging is on

R1(config)#interface e0/1
R1(config-if)#shutdown
R1(config-if)#
Jun  1 03:26:34.471: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to
administratively down
Jun  1 03:26:35.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to down
Jun  1 03:26:35.475: SNMP: Queuing packet to 172.16.1.1
Jun  1 03:26:35.475: SNMP: V2 Trap, reqid 5, errstat 0, erridx 0
sysUpTime.0 = 256005
snmpTrapOID.0 = snmpTraps.3
ifIndex.2 = 2
ifDescr.2 = Ethernet0/1
ifType.2 = 6
lifEntry.20.2 = administratively down
R1(config-if)#
Jun  1 03:26:35.735: SNMP: Packet sent via UDP to 172.16.1.1
```

Trap Receiver trên Server đã nhận được Trap này và hiển thị thông tin chi tiết trên giao diện (hình 37):

Result Table			
Trap Receiver			
Operations Tools			
<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>			
Description	Source	Time	Severity
.1.3.6.1.6.3.1.1.5.3	172.16.1.101	2020-06-01 10:26:36	
<div> <div>Source:</div> <div>172.16.1.101</div> <div>Timestamp:</div> <div>42 minutes 40 seconds</div> <div>SNMP Version:</div> <div>2</div> </div>			
<div> <div>Trap OID:</div> <div>.1.3.6.1.6.3.1.1.5.3</div> <div>Community:</div> <div>CISCOTRAP</div> </div>			
Variable Bindings:			
<div> <div>Name:</div> <div>.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0</div> <div>Value:</div> <div>[TimeTicks] 42 minutes 40 seconds (256005)</div> </div>			
<div> <div>Name:</div> <div>snmpTrapOID</div> <div>Value:</div> <div>[OID] .1.3.6.1.6.3.1.1.5.3</div> </div>			
<div> <div>Name:</div> <div>.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.2</div> <div>Value:</div> <div>[Integer] 2</div> </div>			
<div> <div>Name:</div> <div>.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.2</div> <div>Value:</div> <div>[OctetString] Ethernet0/1</div> </div>			
<div> <div>Name:</div> <div>.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType.2</div> <div>Value:</div> <div>[Integer] ethernetCsmacd (6)</div> </div>			
<div> <div>Name:</div> <div>.1.3.6.1.4.1.9.2.2.1.1.20.2</div> <div>Value:</div> <div>[OctetString] administratively down</div> </div>			
Description:			

Hình 37 – Trap “LinkDown” nhận được từ R1.

Các bạn học viên có thể click vào dòng thông tin trên ô “Description” và hiệu chỉnh kích thước của các cửa sổ trên giao diện một cách phù hợp để quan sát được đầy đủ các thông tin chi tiết về Trap.

Tiếp theo, ta có thể no shutdown lại cổng E0/1 của R1 để nhận được Trap “LinkUp” từ router:


```
R1(config)#interface e0/1
R1(config-if)#no shutdown
R1(config-if)#
Jun  1 04:06:14.081: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
Jun  1 04:06:15.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to up
Jun  1 04:06:15.093: SNMP: Queuing packet to 172.16.1.1
Jun  1 04:06:15.093: SNMP: V2 Trap, reqid 6, errstat 0, erridx 0
sysUpTime.0 = 493967
snmpTrapOID.0 = snmpTraps.4
ifIndex.2 = 2
ifDescr.2 = Ethernet0/1
ifType.2 = 6
lifEntry.20.2 = up
R1(config-if)#
Jun  1 04:06:15.353: SNMP: Packet sent via UDP to 172.16.1.1
```

Tương tự như trên, ta nhận được Trap “LinkUp” trên Trap Receiver (hình 38):

Result Table			
Trap Receiver x			
Operations Tools			
Description	Source	Time	Severity
.1.3.6.1.6.3.1.1.5.4	172.16.1.101	2020-06-01 11:06:16	
.1.3.6.1.6.3.1.1.5.3	172.16.1.101	2020-06-01 10:26:36	
Source: 172.16.1.101 Timestamp: 42 minutes 40 seconds SNMP Version: 2 Trap OID: .1.3.6.1.6.3.1.1.5.3 Community: CISCOTRAP Variable Bindings:			
Name: .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 Value: [TimeTicks] 42 minutes 40 seconds (256005)			
Name: snmpTrapOID Value: [OID] .1.3.6.1.6.3.1.1.5.3			
Name: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.2 Value: [Integer] 2			
Name: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.2 Value: [OctetString] Ethernet0/1			
Name: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType.2 Value: [Integer] ethernetCsmacd (6)			
Name: .1.3.6.1.4.1.9.2.2.1.1.20.2 Value: [OctetString] administratively down			
Description:			

Hình 38 – Trap “LinkUp” nhận được từ R1.

Đến đây, chúng ta đã hoàn tất kiểm tra hoạt động Trap của SNMP trên router R1.

7. Cấu hình SNNP (4):

- Cấu hình hiệu chỉnh router R1 để router này chỉ cho phép NMS có địa chỉ 172.16.1.1 truy vấn thông tin SNMP của mình.
- Mọi truy vấn đến từ các NMS khác đều bị từ chối, đồng thời một bản tin syslog sẽ được phát ra để thông báo về sự vi phạm này.

Cấu hình:

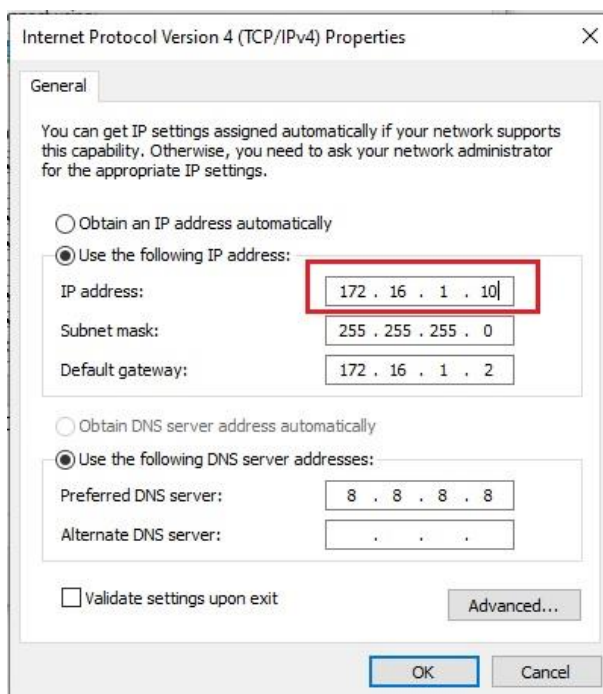
```
R1(config)#access-list 1 permit 172.16.1.1
R1(config)#access-list 1 deny any log
R1(config)#snmp-server community CISCORO RO 1
R1(config)#snmp-server community CISCORW RW 1
```

Ghi chú:

Trên router ta có thể cấu hình để giới hạn lại các NMS được phép truy vấn SNMP đến router. Điều này được thực hiện bằng cách sử dụng thêm access – list kèm theo khai báo community: chỉ những NMS có địa chỉ IP được permit trong ACL mới được quyền truy vấn SNMP đến thiết bị. Trong cấu hình ở trên, do yêu cầu đặt ra là mọi sự vi phạm đều phải được thông báo syslog, dòng mặc định “deny any” của access – list 1 sử dụng thêm tùy chọn “log”; với tùy chọn này, cứ mỗi khi hành động deny diễn ra, hệ thống sẽ phát ra một thông báo syslog cảnh báo đến người quản trị (hành động deny diễn ra khi có một sự vi phạm – NMS với địa chỉ không hợp lệ truy vấn đến router).

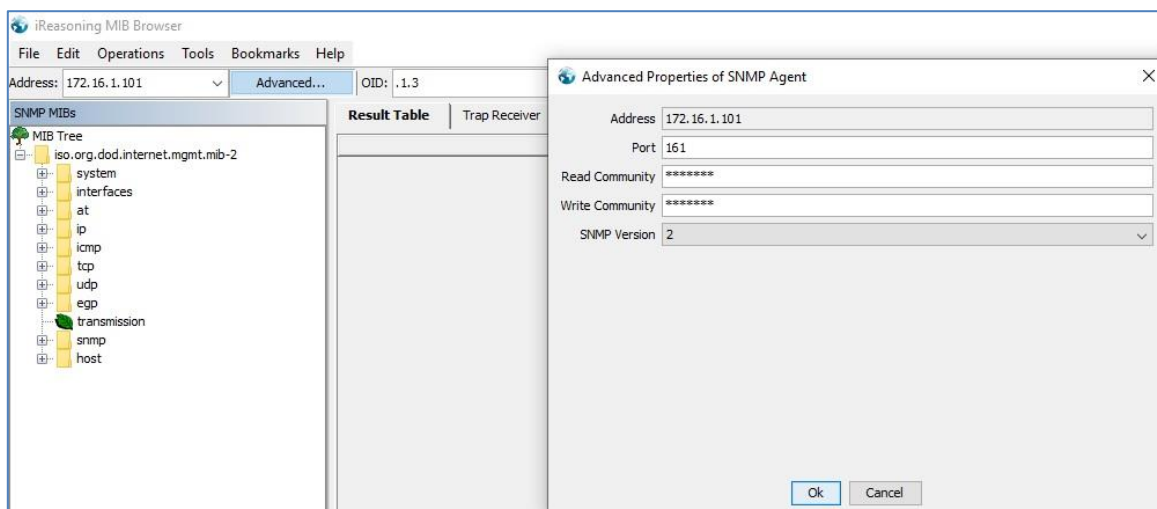
Kiểm tra:

Ta thực hiện thay đổi địa chỉ của server NMS thành một địa chỉ khác (hình 39):



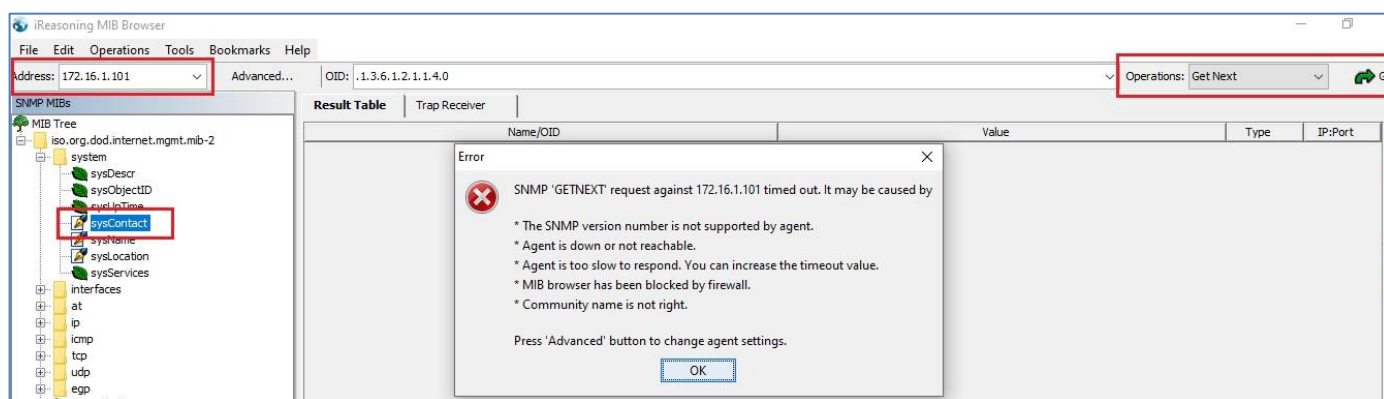
Hình 39 – Thay đổi địa chỉ của NMS.

Tiếp theo, từ phần mềm “iReasoning MIB Browser”, ta thiết lập một SNMP session đến router R1 sử dụng địa chỉ mới này (hình 40):



Hình 40 – Thiết lập SNMP session đến router R1.

Ta thực hiện truy vấn SNMP đến một object bất kỳ của R1, ví dụ “sysContact”, tuy nhiên, lần này truy vấn không thành công (hình 41):



Hình 41 – Truy vấn SNMP đến R1 không thành công.

Trên R1 phát ra một thông điệp Syslog cảnh báo về điều này:

```
R1#
Jun  1 04:43:20.574: %SEC-6-IPACCESSLOGNP: list 1 denied 0 172.16.1.10 -> 0.0.0.0, 1
packet
R1#show access-list
Standard IP access list 1
 10 permit 172.16.1.1
 20 deny any log (1 match)
```

Như vậy, tính năng bảo mật giới hạn các NMS truy nhập SNMP đã hoạt động đúng theo yêu cầu.