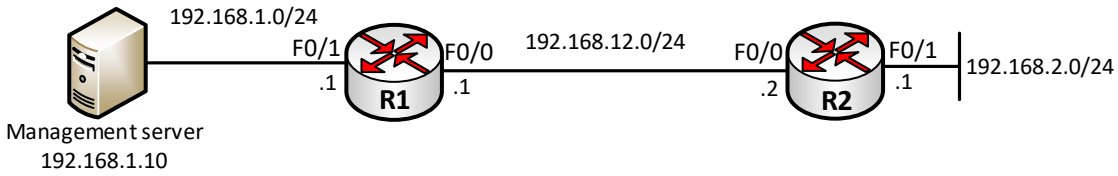
Lab – SNMP, Syslog, NTP

Sơ đồ:



Hình 1 – Sơ đồ bài Lab

Yêu cầu:

1. Cấu hình ban đầu

- Đặt địa chỉ IP trên các interface của các Router theo quy hoạch IP được chỉ ra trên hình 1.
- Cấu hình định tuyến RIPv2 đảm bảo mọi địa chỉ trên sơ đồ hình 1 thấy nhau.

Cấu hình:

Trên R1:

```
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0

R1(config)#interface f0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.12.0
```

Trên R2:

```
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.12.2 255.255.255.0

R2(config)#interface f0/1
R2(config-if)#no keepalive
R2(config-if)#ip address 192.168.2.1 255.255.255.0

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.12.0
```

Ghi chú:

Trong môi trường Lab, có thể để trống các cổng F0/1 của Router R2 không cần đấu nối đi đâu mà cổng vẫn "up/up" bằng cách sử dụng thêm lệnh "`no keep-alive`" trên cổng này.

2. Cấu hình syslog (1)

- Cấu hình Router R1 gửi mọi thông điệp syslog từ level 7 trở lên đến management Server.
- Cấu hình Router R2 gửi mọi thông điệp syslog từ level 5 trở lên đến management Server.

Cấu hình:

Trên R1:

```
R1(config)#logging 192.168.1.10
R1(config)#logging trap debugging
```

Trên R2:

```
R2(config)#logging 192.168.1.10
R2(config)#logging trap notifications
```

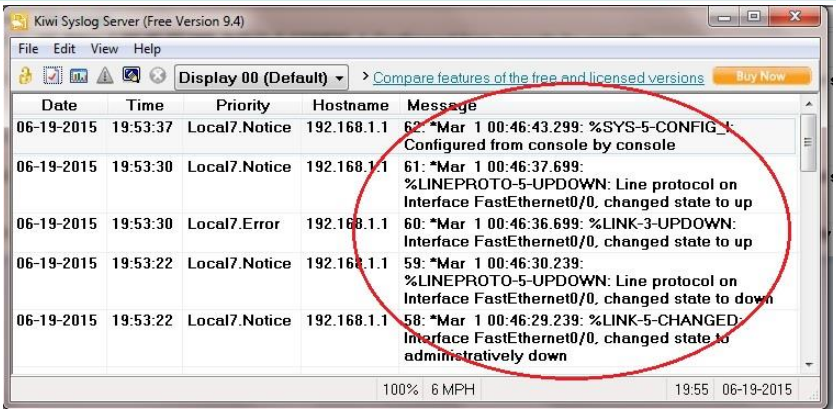
Kiểm tra:

Có thể cài chương trình Kiwi Syslog trên Server 192.168.1.10 để kiểm tra.

Thực hiện tạo một vài thông điệp log trên R1:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*Mar    1  00:46:29.239:  %LINK-5-CHANGED:  Interface  FastEthernet0/0,  changed
state to administratively down
*Mar    1  00:46:30.239:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*Mar    1  00:46:36.699:  %LINK-3-UPDOWN:  Interface  FastEthernet0/0,  changed
state to up
*Mar    1  00:46:37.699:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#exit
R1#
*Mar  1 00:46:43.299: %SYS-5-CONFIG_I: Configured from console by console
```

Các thông điệp syslog này đã được đẩy đến Server (hình 2):

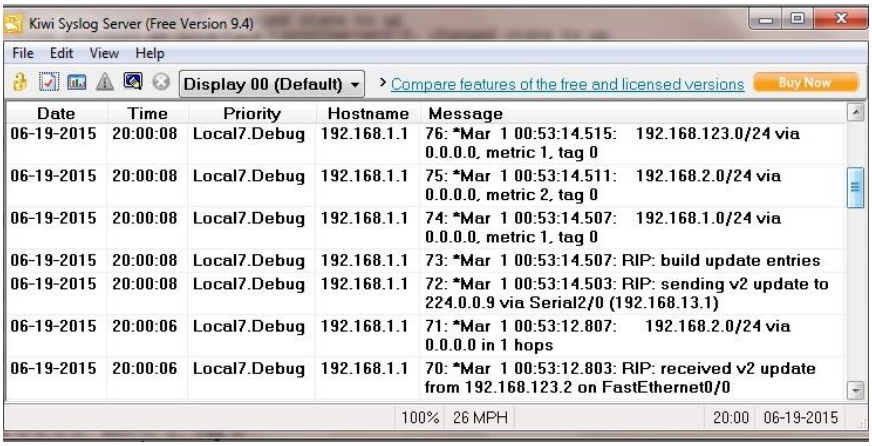


Hình 2 – Các thông điệp syslog của R1 nhận được trên Server

Thực hiện debug trên R1 để kiểm tra kết quả debug trên R1 cũng được xuất đến Server:

```
R1#debug ip rip <- Bật debug RIP
RIP protocol debugging is on
R1#
*Mar  1 00:53:00.743: RIP: received v2 update from 192.168.13.3 on Serial2/0
*Mar  1 00:53:00.747:      192.168.2.0/24 via 0.0.0.0 in 2 hops
*Mar  1 00:53:00.747:      192.168.3.0/24 via 0.0.0.0 in 1 hops
*Mar  1 00:53:00.751:      192.168.123.0/24 via 0.0.0.0 in 1 hops
R1#
*Mar  1 00:53:11.547: RIP: received v2 update from 192.168.123.3 on FastEthernet0/0
*Mar  1 00:53:11.547:      192.168.3.0/24 via 0.0.0.0 in 1 hops
*Mar  1 00:53:11.551:      192.168.13.0/24 via 0.0.0.0 in 1 hops
(...)
R1#undebug all <- Tắt debug
All possible debugging has been turned off
```

Kết quả debug trên R1 cũng đã xuất hiện đầy đủ trên thống kê của Server syslog (hình 3):



Hình 3 – Kết quả debug trên R1 đã được xuất đến Server

Thực hiện kiểm tra tương tự với R2.

3. Cấu hình syslog (2)

- Cấu hình trên R1 để các thông điệp log từ mức debug trở lên đều được lưu vào bộ đệm nội bộ, tuy nhiên, kích thước cấp phát tối đa cho bộ đệm nội bộ này là 8192 byte.
- Cấu hình để tốc độ phát các thông điệp syslog ra cổng console của R1 (kể cả các thông điệp debug) không được vượt quá 1 thông điệp trên 1 giây.

Cấu hình:

Trên R1:

```
R1(config)#logging buffered 8192 debugging
R1(config)#logging rate-limit console all 1
```

Kiểm tra:

Thực hiện tạo một vài thông điệp log trên R1:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*Mar    1  01:28:21.751:  %LINK-5-CHANGED:  Interface  FastEthernet0/0,  changed
state to administratively down
*Mar    1  01:28:22.751:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*Mar    1  01:28:28.495:  %LINK-3-UPDOWN:  Interface  FastEthernet0/0,  changed
state to up
*Mar    1  01:28:29.495:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to up
R1(config-if)#end
R1#
*Mar  1 01:28:33.319: %SYS-5-CONFIG_I: Configured from console by console
```

Kiểm tra bộ đệm nội bộ lưu trữ log trên R1:

```
R1#show logging
Syslog logging: enabled (12 messages dropped, 0 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.

    Console logging: level debugging, 40 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 6 messages logged, xml disabled,
```

```
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level debugging, 44 message lines logged
        Logging to 192.168.1.10  (tcp port 5000,  audit disabled,
              authentication disabled, encryption disabled, link down),
              39 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled

Log Buffer (8192 bytes):

*Mar  1 01:19:49.935: %SYS-5-CONFIG_I: Configured from console by console
*Mar   1  01:28:21.751:  %LINK-5-CHANGED:  Interface  FastEthernet0/0,  changed  state  to
administratively down
*Mar   1  01:28:22.751:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/0,
changed state to down
*Mar  1 01:28:28.495: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar   1  01:28:29.495:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/0,
changed state to up
*Mar  1 01:28:33.319: %SYS-5-CONFIG_I: Configured from console by console
```

Các thông điệp log đã được lưu trên bộ đệm của Router.

4. Cấu hình syslog (3)

- Cấu hình R1 và R2 đánh số thứ tự cho các thông điệp log.
- Cấu hình để R1 hiển thị thời điểm xảy ra log, sử dụng timestamp date-time:
  - Với các thông điệp debug, R1 hiển thị thời gian đến đơn vị mili giây.
  - Với các thông điệp khác, R1 thêm cả thông tin về năm vào thời gian phát ra thông điệp log.
- Cấu hình để R2 hiển thị thời điểm xảy ra log, sử dụng timestamp up-time.

Cấu hình:

Trên R1:

```
R1(config)#service timestamps debug datetime msec
R1(config)#service timestamps log datetime year
R1(config)#service sequence-numbers
```

Trên R2:

```
R2(config)#service timestamps debug uptime
R2(config)#service timestamps log uptime
R2(config)#service sequence-numbers
```

Kiểm tra:

Thực hiện tạo các thông điệp syslog trên R1 để kiểm tra kết quả cấu hình:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
000041: *Mar  1 2002 00:58:30: %LINK-5-CHANGED: Interface FastEthernet0/0,
changed state to administratively down
000042: *Mar  1 2002 00:58:31: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
000043: *Mar  1 2002 00:58:37: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
R1(config-if)#
000044: *Mar  1 2002 00:58:38: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up
R1(config-if)#end
R1#
000045: *Mar  1 2002 00:58:41: %SYS-5-CONFIG_I: Configured from console by
console
```

Các thông điệp syslog trên R1 đã được đánh số thứ tự và hiển thị timestamp có thêm cả năm trong đồng hồ hệ thống.

Thực hiện debug trên R1:

```
R1#debug ip rip
RIP protocol debugging is on
R1#
000046: *Mar  1 01:01:11.023: RIP: received v2 update from 192.168.12.1 on FastEthernet0/0
000047: *Mar  1 01:01:11.023:      192.168.1.0/24 via 0.0.0.0 in 1 hops
000048: *Mar  1 01:01:11.027:      192.168.12.0/24 via 0.0.0.0 in 1 hops
```

Có thể thấy rằng bên cạnh việc được đánh số thứ tự, các thông điệp debug của R1 còn được đánh dấu thời gian đến đơn vị milisecond đúng như yêu cầu.

Thực hiện tạo một vài thông điệp log và kiểm tra cách thức hiển thị các thông điệp này trên màn hình console của R2:

```
R2(config)#interface f0/0
R2(config-if)#shutdown
R2(config-if)#
000027: 00:53:25: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
000028: 00:53:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
```

```
R2(config-if)#no shutdown
R2(config-if)#
000029: 00:53:33: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R2(config-if)#
000030: 00:53:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R2(config-if)#end
R2#
000031: 00:53:39: %SYS-5-CONFIG_I: Configured from console by console

R2#show version | inc uptime
R2 uptime is 54 minutes
```

Các thông điệp log trên R2 đã được đánh số thứ tự và đánh dấu thời gian xuất hiện theo kiểu uptime đúng như yêu cầu.

5. Đồng bộ thời gian thực với NTP

- Cấu hình để R1 đóng vai trò là nguồn đồng bộ thời gian thực sử dụng stratum 5.
- Cấu hình để Router R2 đồng bộ thời gian thực trên đồng hồ của mình theo thời gian của R1.
- Các Router sử dụng source cho các gói tin NTP là địa chỉ IP trên cổng F0/1.

Cấu hình:

Trên R1:

```
R1(config)#ntp master 5
R1(config)#ntp source f0/1
```

Trên R2:

```
R2(config)#ntp server 192.168.1.1
R2(config)#ntp source f0/1
```

Kiểm tra:

Trước hết, thực hiện hiệu chỉnh đồng hồ trên các Router về một giá trị chung để rút ngắn thời gian đồng bộ giữa các Router:

```
R1#clock set 16:30:00 25 Jan 2020
R2#clock set 16:30:00 25 Jan 2020
```

Trên R1:

```
R1#show ntp status
Clock is synchronized, stratum 5, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D9315755.147FF5C4 (16:31:33.080 UTC Sun Jan 25 2020)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 15875.02 msec, peer dispersion is 15875.02 msec

R1#show ntp associations
```

```
     address         ref clock     st  when  poll reach  delay  offset    disp
*~127.127.7.1      127.127.7.1      4     2    64    3     0.0    0.00  7875.0
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Trên Router R2:

```
R2#show ntp status
Clock is synchronized, stratum 6, reference is 192.168.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0017 Hz, precision is 2**24
reference time is D9315AB2.66A48429 (16:32:54.400 UTC Sun Jan 25 2020)
clock offset is -89.1152 msec, root delay is 28.05 msec
root dispersion is 169.60 msec, peer dispersion is 80.44 msec
R2#show ntp associations

     address         ref clock     st  when  poll reach  delay  offset    disp
*~192.168.1.1      127.127.7.1      5    36   128  377    28.0  -89.12    80.4
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Các Router R2 và R3 đã đồng bộ thời gian thực theo Router R1 và nhận stratum bằng 6.

6. Xác thực NTP

- Cấu hình để R2 xác thực các gói tin NTP đến từ R1 với password là “CISCO”.

Cấu hình:

Trên R1:

```
R1(config)#ntp authentication-key 1 md5 CISCO
```

Trên R2:

```
R2(config)#ntp authenticate
R2(config)#ntp authentication-key 1 md5 CISCO
R2(config)#ntp trusted-key 1
```

7. Cấu hình SNMP (1)

- Cấu hình trên R1 và R2 cho phép NMS 192.168.1.10 đọc thông tin SNMP trên các thiết bị này, sử dụng community string “CISCORO”.
- Ngoài ra, cấu hình trên Router R1 cho phép NMS 192.168.1.10 được phép sửa đổi thông tin SNMP trên R1, sử dụng community string “CISCORW”.
- Chỉ Host 192.168.1.10 được truy vấn SNMP đến các Router. Các Router sẽ phát ra một thông điệp log nếu các Host không hợp lệ truy vấn SNMP đến Router

Cấu hình:

Trên R1:

```
R1(config)#access-list 1 permit 192.168.1.10
R1(config)#access-list 1 deny any log
R1(config)#snmp-server community CISCORO ro 1
R1(config)#snmp-server community CISCORW rw 1
```

Trên R2:

```
R2(config)#access-list 1 permit 192.168.1.10
R2(config)#access-list 1 deny any log
R2(config)#snmp-server community CISCORO ro 1
```

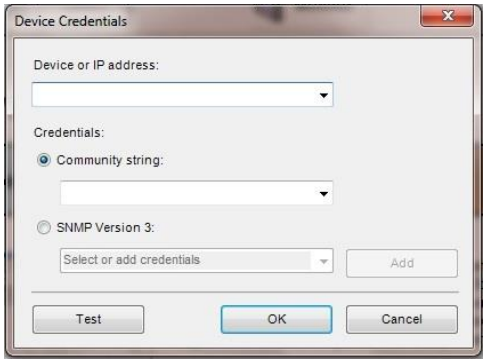
Kiểm tra:

Có thể sử dụng chương trình Solarwinds toolset để kiểm tra việc truy vấn thông tin SNMP trên các Router. Đây là một phần mềm có bản quyền, có thể tải bản dùng thử từ link: *http://www.solarwinds.com/engineers-toolset.aspx* .

Có nhiều tool trong chương trình này, có thể sử dụng một tool bất kỳ trong đó để thực hiện kiểm tra hoạt động SNMP trên các Router. Ví dụ, có thể sử dụng tool "Real Time Interface Monitor" (hình 4):

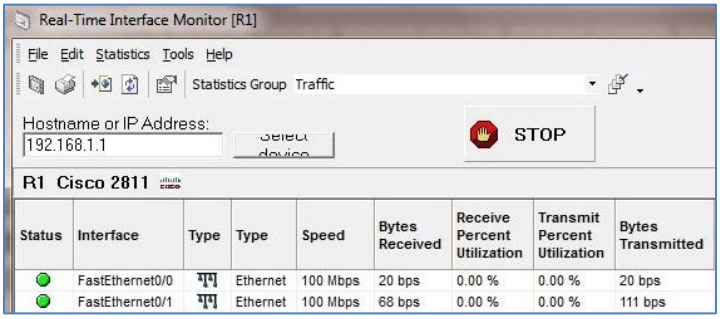
Hình 4 – Giao diện tool "Real – Time Interface Monitor"

Trên cửa sổ này, nhấn phím "Select device", một cửa sổ hiện ra yêu cầu nhập địa chỉ IP và community của thiết bị cần giám sát (hình 5):



Hình 5 – Địa chỉ IP và community cho Agent

Thực hiện nhập IP và community string tương ứng của thiết bị cần giám sát, chương trình sẽ truy vấn và hiển thị các thông tin về thiết bị được giám sát, ví dụ, R1 (hình 6):

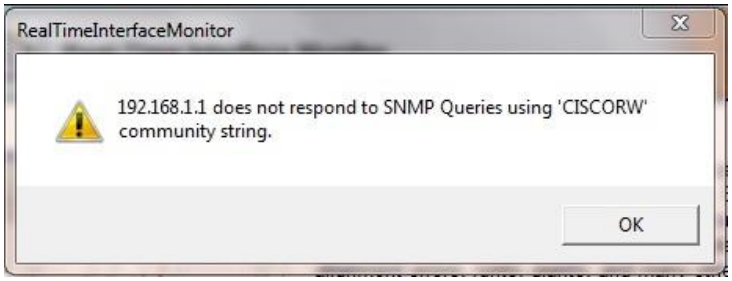


Hình 6 – Thông tin về các interface của Router R1

Thay đổi IP trên Management Server thành một địa chỉ khác, ví dụ 192.168.1.11/24 để kiểm tra ngoài 192.168.1.10, không một địa chỉ nào khác được phép truy vấn SNMP đến các Router (hình 7):

Hình 7 – Đổi địa chỉ trên NMS

Thực hiện truy vấn SNMP lại từ NMS, lần này việc truy vấn diễn ra không thành công (hình 8):



Hình 8 – Truy vấn SNMP không thành công.

Trên Router, một thông báo syslog thể hiện điều này:

```
*July 18 16:20:03.887: %SEC-6-IPACCESSLOGNP: list 1 denied 0 192.168.1.11 ->
0.0.0.0, 1 packet
```

Sau khi kiểm tra xong, cần lưu ý trả lại IP 192.168.1.10 cho Management Server.

8. Cấu hình SNMP (2)

- Cấu hình các Router R1 và R2 gửi trap về NMS 192.168.1.10. Việc gửi trap chỉ thực hiện khi các cổng chuyển trạng thái sang up hoặc down.
- Community sử dụng cho hoạt động trap và community trên các Router là "CISCOTRAP".

Cấu hình:

Trên R1 và R2:

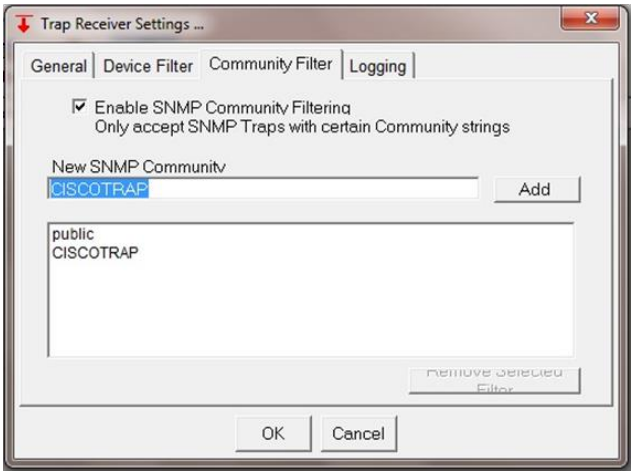
```
R1-2(config)#snmp-server enable traps snmp linkdown linkup
R1-2(config)#snmp-server host 192.168.1.10 CISCOTRAP
```

Kiểm tra:

Có thể sử dụng tool "Trap Receiver" trong bộ tool để kiểm tra (hình 9):

Hình 9 – Giao diện tool "SNMP Trap Receiver"

Chọn "Setting" trên cửa sổ chương trình để thiết lập việc tiếp nhận trap từ các Router. Các thông số thiết lập được chỉ ra trên hình 10:



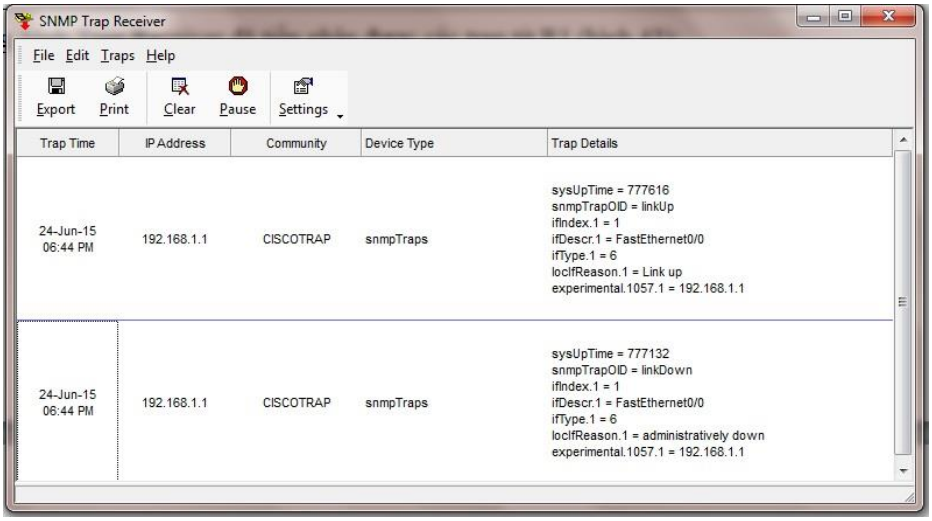
Hình 10 – Thiết lập các thông số cho tool "Trap Receiver"

Thực hiện shutdown/no shutdown cổng F0/0 của R1 để R1 gửi trap đến Trap Receiver:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*Jun  24  12:25:29.279:  %LINK-5-CHANGED:  Interface  FastEthernet0/0,  changed
state to administratively down
```

```
*Jun  24  12:25:30.279:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*Jun  24  12:25:35.491:  %LINK-3-UPDOWN:  Interface  FastEthernet0/0,  changed
state to up
*Jun  24  12:25:36.491:  %LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface
FastEthernet0/0, changed state to up
```

SNMP Trap Receiver đã tiếp nhận được các trap từ R1 (hình 11):



Hình 11 – Các trap nhận được từ R1

Có thể kiểm tra tương tự với hoạt động gửi trap từ R2.

9. Cấu hình Netflow

Thực hiện cấu hình tính năng Netflow trên Router R1:

- R1 sử dụng Netflow version 5.
- Kết quả Netflow được chuyển về Host quản lý 192.168.1.10, sử dụng port 9999.
- R1 thu thập thông tin của dữ liệu đi ra và đi vào cổng F0/0.

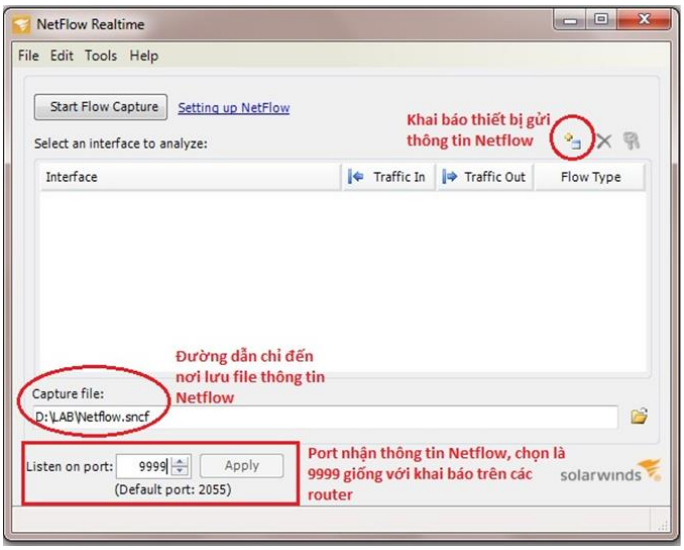
Cấu hình:

```
R1(config)#ip flow-export version 5
R1(config)#ip flow-export destination 192.168.1.10 9999

R1(config)#interface f0/0
R1(config-if)#ip flow ingress
R1(config-if)#ip flow egress
R1(config-if)#exit
```

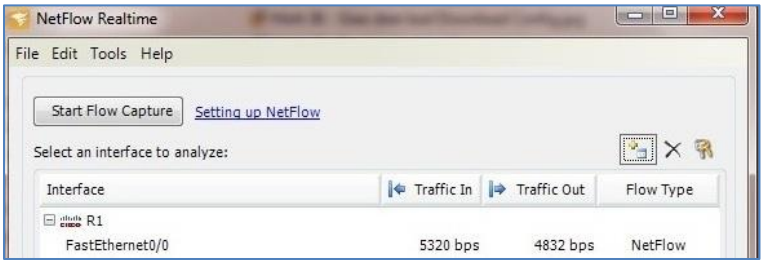
Kiểm tra:

Tương tự như các bước trên, có thể sử dụng công cụ "Netflow Realtime" của bộ tool để kiểm tra (hình 12):



Hình 12 – Giao diện tool "Netflow Real Time"

Sau khi khai báo hoàn tất, cổng F0/0 của R1 hiện ra trong danh sách được giám sát Netflow (hình 13):



Hình 13 – Cổng F0/0 của R1 trong danh sách giám sát

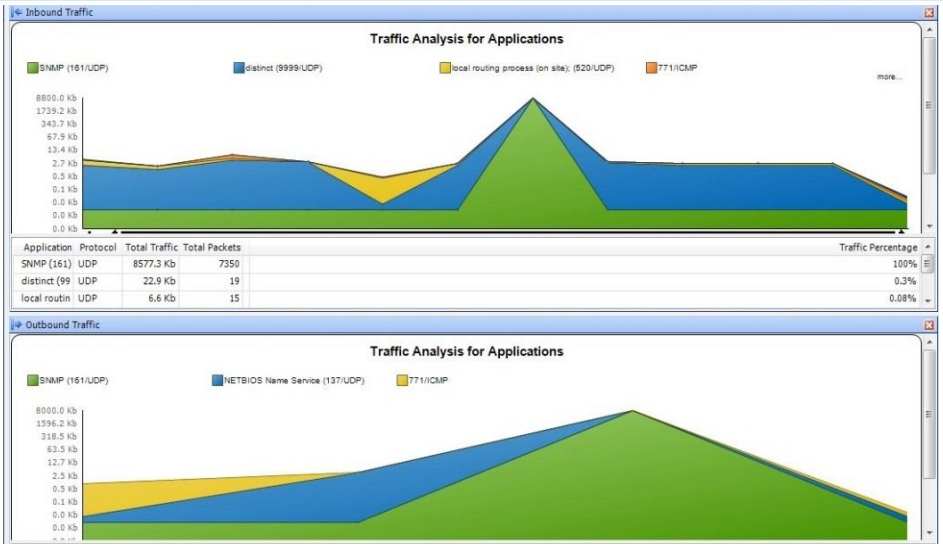
Trên cửa sổ giao diện này, nhấn "Start Flow Capture" để bắt đầu phân tích lưu lượng trên cổng F0/0 của R1.

Thực hiện khởi tạo một luồng dữ liệu đi ngang qua cổng F0/0 của R1:

```
R2#ping 192.168.1.10 repeat 100000 timeout  1

Type escape sequence to abort.
Sending 1000000, 100-byte ICMP Echos to 192.168.123.1, timeout is 1 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Kết quả phân tích Netflow (hình 14):



Hình 14 – Kết quả phân tích Netflow

Bên cạnh việc sử dụng chương trình phân tích Netflow bên ngoài có thể kiểm tra thông tin thống kê trực tiếp trên Router bằng cách sử dụng lệnh:

```
R1#show ip cache f0/0 flow
IP packet size distribution (1701370 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .003 .985 .008 .002 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  8 active, 4088 inactive, 876 added
  31404 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  8 active, 1016 inactive, 876 added, 876 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other          785      0.0        30   133      2.0      14.7      15.4
ICMP                83      0.0      9044   100     64.2      26.2      15.7
Total:             868      0.0       892   101     66.3      15.8      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1         192.168.1.10    Fa0/0*        192.168.123.3   01 0000 0000   462K
Fa0/1         192.168.1.10    Fa0/0*        192.168.123.3   11 E14D 00A1   500
```