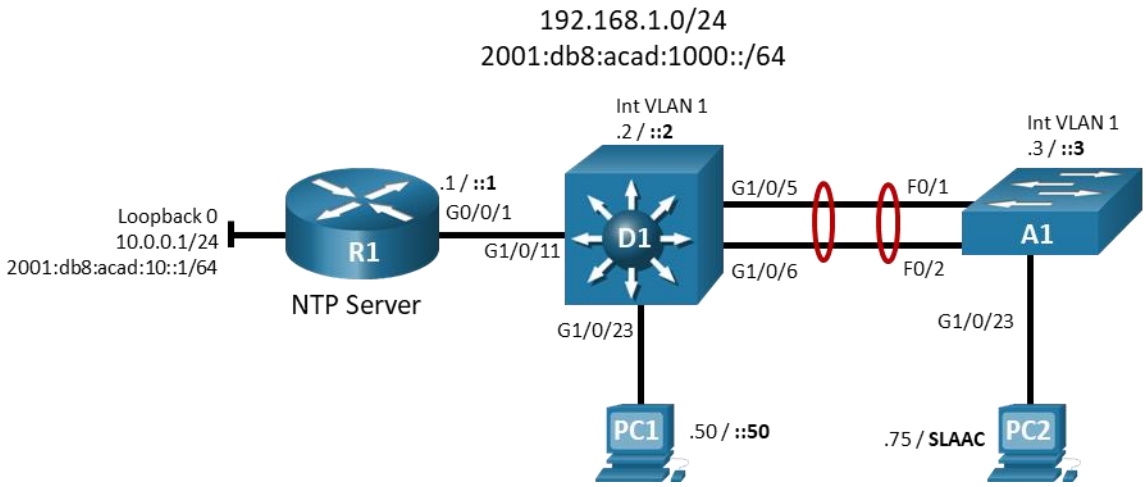
LAB – Triển khai Flexible Netflow

Sơ đồ:



Yêu cầu:

1. Cấu hình ban đầu:

- Đặt địa chỉ IP cho các interface trên thiết bị Routers trong global configuration mode theo quy hoạch IP được chỉ ra trên hình.

Cấu hình:

Trên R1:

```
R1(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#ipv6 unicast-routing
R1(config)#banner motd # R1, Implement Flexible Netflow #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#exec-timeout 0 0
R1(config-line)#password cisco123
R1(config-line)#login
R1(config-line)#exit
```

```
R1(config)#Interface g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:acad:1000::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface loopback 0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:acad:10::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ntp master 3
R1(config)#end
R1# copy running-config startup-config
```

Trên D1:

```
D1(config)#hostname D1
D1(config)# no ip domain lookup
D1(config)#ipv6 unicast-routing
D1(config)#banner motd # D1, Implement Flexible Netflow  #
D1(config)#line con 0
D1(config-line)#exec-timeout 0  0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#line vty 0 4
D1(config-line)#privilege level 15
D1(config-line)#exec-time 0 0
D1(config-line)#password cisco123
D1(config-line)#login
D1(config-line)#exit
D1(config)#interface vlan 1
D1(config-if)#ip address 192.168.1.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
```

```
D1(config-if)#ipv6 address 2001:db8:acad:1000::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip default-gateway 192.168.1.1
D1(config)#interface g1/0/23
D1(config-if)#spanning-tree portfast
D1(config-if)#switchport mode access
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface g1/0/11
D1(config-if)#spanning-tree portfast
D1(config-if)#switchport mode access
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface range g1/0/5-6
D1(config-if)#switchport mode trunk
D1(config-if)#channel-group 1 mode active
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ntp server 192.168.1.1
D1(config)#end
D1# copy running-config startup-config
```

Trên A1:

```
A1(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#ipv6 unicast-routing
A1(config)#ip domain name CCNPv8.CoPP.Lab
A1(config)#banner motd # A1, Implement Flexible Netflow #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#line vty 0 4
```

```
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#password cisco123
A1(config-line)#login
A1(config-line)#exit
A1(config)#interface vlan 1
A1(config-if)#ip address 192.168.1.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:acad:1000::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range f0/1-2
A1(config-if)#switchport mode trunk
A1(config-if)#channel-group 1 mode active
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface f0/-23
A1(config-if)#switchport mode access
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#ntp server 192.168.1.1
A1(config)#end
A1# copy running-config startup-config
```

2. Cấu hình và kiểm tra Flexible Netflow.

Quy trình làm việc của Flexible Netflow bao gồm bốn bước sau:

Bước 1: Tạo Flow record. Flow records xác định thông tin cần thu thập. Classic Netflow thì xác định các flow record có phù hợp với bộ nhớ đệm hay không, hoặc bạn có thể cấu hình các flow record của riêng mình để phù hợp với nhu cầu của bạn.

Bước 2: Tạo Flow exporter. Điều này xác định nơi thông tin thống kê đã được tổng hợp để gửi đi

Bước 3: Tạo Flow mornitor và kết hợp Flow records và Flow Exporters với chính nó.

Bước 4: Cấu hình các giao diện thích hợp cho bộ nhớ đệm đầu vào hoặc đầu ra được liên kết với Flow monitor.

Trong bài lab này, bạn sẽ cấu hình Flexible Netflow để gửi các thông tin thống kê về R1 interface g0/0/1 đến PC1.

2.1. Tạo flow records

Đối với flow record đầu tiên của chúng ta, chúng ta sử sử dụng ipv4 original-input flow record đã được định nghĩa từ trước.

Đối với flow record thứ 2, chúng ta sẽ tạo ra flow record dạng custom. Bởi vì flow record đầu tiên tập trung vào input traffic, và flow record thứ 2 tập trung vào output traffic.

Tạo một flow record dạng named CCNP8-CUSTOM-OUT.

```
R1(config)# flow record CCNP8-CUSTOM-OUT
```

Gán phần mô tả cho flow record

```
R1(config-flow-record)# description Custom Flow Record for outbound traffic
```

Cấu hình flow record khớp với phần mô tả của địa chỉ ipv4 và transport

```
R1(config-flow-record)# match ipv4 destination address
R1(config-flow-record)# match transport destination-port
```

Cấu hinh flow record để thu thập bytes và packets.

```
R1(config-flow-record)# collect counter bytes
R1(config-flow-record)# collect counter packets
```

Sử dụng câu lệnh **show flow record CCNP8-CUSTOM-OUT** để kiểm tra kết quả

```
R1# show flow record CCNP8-CUSTOM-OUT
flow record CCNP8-CUSTOM-OUT:
  Description:        Custom Flow Record for outbound traffic
  No. of users:       0
  Total field space:  14 bytes
  Fields:
    match ipv4 destination address
    match transport destination-port
    collect counter bytes
collect counter packets
```

2.2. Tạo flow exporter.

Cấu hình flow exporter để định nghĩa nơi mà thông tin cached đã được gửi. Tạo flow exporter dạng named CCNP8-COLLECTOR-HOST. Chỉ rõ thêm là exporter nên sử dụng Netflow version 9, và trỏ đến 192.168.1.50 udp port 9999.

```
R1(config)# flow exporter CCNP8-COLLECTOR-HOST
R1(config-flow-exporter)# destination 192.168.1.50
R1(config-flow-exporter)# export-protocol netflow-v9
R1(config-flow-exporter)# transport UDP 9999
R1(config-flow-exporter)# exit
```

Sử dụng câu lệnh **show flow exporter CCNP8-COLLECTOR-HOST** để kiểm tra kết quả.

```
R1# show flow exporter CCNP8-COLLECTOR-HOST
Flow Exporter CCNP8-COLLECTOR-HOST:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.1.50
    Source IP address:      192.168.1.1
    Transport Protocol:     UDP
    Destination Port:       9999
    Source Port:            63275
    DSCP:                   0x0
    TTL:                    255
Output Features:        Used
```

2.3. Tạo flow monitors.

Flow monitors liên kết flow record với flow exporter. Đối với bài tập của chúng ta, chúng ta cần tạo 2 flow monitors, mỗi cái cho từng flow record.

Sử dụng câu lệnh flow monitor CCNP8-INBOUND-MONITOR để tạo flow monitor đầu tiên và đặt tên là CCNP8-INBOUND-MONITOR. Là một phần của flow monitor, hãy chỉ định rằng netflow ipv4 orgirinal-input flow record, xuất cache đến exporter mỗi 30 giây, và xác định CCNP8-COLLECTOR-HOST là exporter.

```
R1(config)# flow monitor CCNP8-INBOUND-MONITOR
R1(config-flow-monitor)# record netflow ipv4 original-input
R1(config-flow-monitor)# cache timeout active 30
R1(config-flow-monitor)# exporter CCNP8-COLLECTOR-HOST
R1(config-flow-monitor)# exit
```

Sử dụng câu lệnh flow monitor CCNP8-OUTBOUND-MONITOR để tạo flow monitor thứ 2 và đặt tên nó là CCNP8-OUTBOUND-MONITOR. Là một phần của flow monitor, hãy chỉ định

rằng nó sẽ ghi lại CCNP8-CUSTOM-OUT flow record, xuất cache đến exporter mỗi 30 giây, và xác định CCNP8-COLLECTOR-HOST là exporter.

```
R1(config)# flow monitor CCNP8-OUTBOUND-MONITOR
R1(config-flow-monitor)# record CCNP8-CUSTOM-OUT
R1(config-flow-monitor)# cache timeout active 30
R1(config-flow-monitor)# exporter CCNP8-COLLECTOR-HOST
R1(config-flow-monitor)# exit
```

Sử dụng câu lệnh show flow monitor để kiểm tra kết quả

```
R1# show flow monitor
Flow Monitor CCNP8-INBOUND-MONITOR:
  Description:       User defined
  Flow Record:       netflow ipv4 original-input
  Flow Exporter:     CCNP8-COLLECTOR-HOST
  Cache:
    Type:                normal (Platform cache)
    Status:              not allocated
    Size:                200000 entries
    Inactive Timeout:    15 secs
    Active Timeout:      30 secs
    Trans end aging:   off

Flow Monitor CCNP8-OUTBOUND-MONITOR:
  Description:       User defined
  Flow Record:       CCNP8-CUSTOM-OUT
  Flow Exporter:     CCNP8-COLLECTOR-HOST
  Cache:
    Type:                normal (Platform cache)
    Status:              not allocated
    Size:                200000 entries
    Inactive Timeout:    15 secs
    Active Timeout:      30 secs
    Trans end aging:   off
```

2.4. Cấu hình interface cho flow caching.

Bước cuối cùng là cấu hình các interface thích hợp để chúng có thể lưu thông tin cache. Trong bài lab, chúng ta sẽ tập trung trên input và output từ Interface g0/0/0 trên R1. Sử dụng câu lệnh ip flow monitor <name><direction> trên interface g0/0/1 để chỉ rõ inbound và outbound flow monitors mà mình đã tạo ra.

```
R1(config)# interface g0/0/1
R1(config-if)# ip flow monitor CCNP8-INBOUND-MONITOR input
R1(config-if)# ip flow monitor CCNP8-OUTBOUND-MONITOR output
R1(config-if)# exit
```

2.5. Tạo vài traffic.

Để thu thập số liệu thống kê, chúng ta cần vài lưu lượng truy cập.

Từ PC2, Bắt đầu ping đến địa chỉ IPv4 và IPv6 của R1, ở phần này mình sẽ cấu hình size cho lệnh ping với kích thước mỗi gói tin là 1475 bytes.

Câu lệnh trên windows như sau:

```
C:\> ping 10.0.0.1 -t -l 1475
C:\> ping 2001:db8:acad:1000::1 -t -l 1475
```

Từ Switch A1, telnet đến R1, đăng nhập và để nguyên session đang chạy.

Từ switch D1, sử dụng extended ping utility để ping tới Loopback 0 của R1 sử dụng sweep range của 36 bytes đến 18024 bytes. Cấu hình repeat count là 1,000,000 và sweep interval là 1

```
D1# ping
Protocol [ip]:
Target IP address: 10.0.0.1
Repeat count [5]: 100000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface:
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
```

```
Sweep range of sizes [n]: y
Sweep min size [36]:
Sweep max size [18024]:
Sweep interval [1]:
Type escape sequence to abort.
Sending 89945, [36..18024]-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Trên PC1, Mở Wireshark và lọc **`ip.src == 192.168.1.1 && udp.dstport == 9999 && ! icmp`**. Bộ lọc này sẽ hiển thị các gói tin từ 192.168.1.1 UDP port 9999 đã được cấu hình trước đó và không có các gói tin ICMP.

2.6. Đợi 60 giây và sau đó kiểm tra kết quả.

Trên PC1, quan sát màn hình hiển thị Wireshark. Phải có lưu lượng truy cập phù hợp với bộ lọc đang được hiển thị.

Trên R1, Sử dụng câu lệnh **show flow monitor CCNP8-INBOUND-MONITOR statistics.**

```
R1# show flow monitor CCNP8-INBOUND-MONITOR statistics
  Cache type:                               Normal (Platform cache)
  Cache size:                               200000
  Current entries:                               2
  High Watermark:                               12

  Flows added:                                 103
  Flows aged:                                  101
    - Active timeout      (     30 secs)       38
    - Inactive timeout    (     15 secs)       63
```

Trên R1, sử dụng câu lệnh **show flow monitor CCNP8-INBOUND-MONITOR cache.** Lưu ý: Window traffic output sẽ thay đổi tùy thuộc vào thời gian lưu lượng truy cập sau 30 giâyvà được đưa vào bộ nhớ đệm

```
R1# show flow monitor CCNP8-INBOUND-MONITOR cache
  Cache type:                               Normal (Platform cache)
  Cache size:                               200000
  Current entries:                               1
  High Watermark:                               12
```

```
  Flows added:                                  112
  Flows aged:                                   111
    - Active timeout      (    30 secs)         43
    - Inactive timeout    (    15 secs)         68


IPV4 SOURCE ADDRESS:        192.168.1.75
IPV4 DESTINATION ADDRESS:   10.0.0.1
TRNS SOURCE PORT:           0
TRNS DESTINATION PORT:      2048
INTERFACE INPUT:            Gi0/0/1
FLOW SAMPLER ID:            0
IP TOS:                     0x00
IP PROTOCOL:                1
ip source as:               0
ip destination as:          0
ipv4 next hop address:      0.0.0.0
ipv4 source mask:           /0
ipv4 destination mask:      /0
tcp flags:                  0x00
interface output:           Null
counter bytes:              12024
counter packets:            8
timestamp first:            20:43:34.189
timestamp last:             20:43:41.263
```

Dừng tất cả các lệnh ping và thoát session telnet

3. Cấu hình và kiểm tra Netflow

3.1. Cấu hình Netflow

Cấu hình Netflow export version là version 9.

```
R1(config)# ip flow-export version 9
```

Cấu hình Netflow export đích đến là 192.168.1.50 port 9999

```
R1(config)# ip flow-export destination 192.168.1.50 9999
```

Trên interface G0/0/1 R1, cấu hình Netflow để monitor ingress và egress traffic.

```
R1(config)# interface g0/0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
R1(config-if)# exit
```

3.2. Tạo vài lưu lượng truy cập

Để thu thập số liệu thống kê, chúng ta cần vài lưu lượng truy cập.

Từ PC2, Bắt đầu ping đến địa chỉ IPv4 và IPv6 của R1, ở phần này mình sẽ cấu hình size cho lệnh ping với kích thước mỗi gói tin là 1475 bytes.

Câu lệnh trên windows như sau:

```
C:\> ping 10.0.0.1 -t -l 1475
C:\> ping 2001:db8:acad:1000::1 -t -l 1475
```

Từ Switch A1, telnet đến R1, đăng nhập và để nguyên session đang chạy.

Từ switch D1, sử dụng extended ping utility để ping tới Loopback 0 của R1 sử dụng sweep range của 36 bytes đến 18024 bytes. Cấu hình repeat count là 1,000,000 và sweep interval là 1.

```
D1# ping
Protocol [ip]:
Target IP address: 10.0.0.1
Repeat count [5]: 100000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface:
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]: y
Sweep min size [36]:
Sweep max size [18024]:
Sweep interval [1]:
```

```
Type escape sequence to abort.
Sending 89945, [36..18024]-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Trên PC1, Mở Wireshark và lọc **`ip.src == 192.168.1.1 && udp.dstport == 9999 && ! icmp`**. Bộ lọc này sẽ hiển thị các gói tin từ 192.168.1.1 UDP port 9999 đã được cấu hình trước đó và không có các gói tin ICMP.

3.3. Xác minh Netflow.

Sử dụng câu lệnh show ip flow interface để xác minh các interface tham gia và flow capture

```
R1# show ip flow interface
GigabitEthernet0/1
ip flow ingress
ip flow egress
```

Sử dụng câu lệnh show ip flow export để hiển thị host IP address và bao nhiêu flows đã được exported

```
R1# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.1.50 (9999)
  Version 9 flow records
  117 flows exported in 55 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
export packets were dropped due to encapsulation fixup failures
```

Sử dụng câu lệnh show ip cache flow để hiển thị thông tin flow

```
R1# show ip cache flow
IP packet size distribution (2597 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .172 .023 .070 .016 .012 .016 .016 .017 .016 .012 .012 .012 .012 .012 .012
```

```
    512   544   576 1024 1536 2048 2560 3072 3584 4096 4608
   .012 .012 .012 .172 .355 .000 .000 .000 .000 .000 .000


IP Flow Switching Cache, 278544 bytes
  3 active, 4093 inactive, 97 added
  2551 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  3 active, 1021 inactive, 93 added, 93 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
TCP-Telnet           3      0.0         7    42      0.0       0.8      15.5
UDP-NTP             36      0.0         1    76      0.0       0.6      15.7
UDP-other           19      0.0         6   106      0.0       5.1      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
ICMP                36      0.0        41   750      0.0       1.3      15.0
Total:              94      0.0        18   675      0.0       1.8      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
Gi0/1         192.168.1.50    Local         192.168.1.1     01 0000 0303
1
Gi0/1         192.168.1.75    Local         10.0.0.1        01 0000 0800
447
Gi0/1         192.168.1.75    Local         10.0.0.1        01 0000 0000
447
```

Bạn sẽ thấy các gói tin được thu thập trong Wireshark.

Dừng tất cả các lệnh ping và thoát telnet session.