# XÂY DỰNG CÁC BÀI TẬP TRIỂN KHAI HỆ THỐNG GIÁM SÁT MẠNG BẰNG NETFLOW ĐỂ PHỤC VỤ GIẢNG DẠY

*VÕ HỒ THU SANG*
*Khoa Tin học, Trường Đại học Sư phạm, Đại học Huế*
*Email: cyan1904@gmail.com*

**Tóm tắt:** Netflow là giao thức độc quyền của Cisco cho phép giám sát chi tiết các thành phần trong luồng lưu lượng mạng, từ đó khắc phục nhược điểm của giao thức quản trị mạng truyền thống SNMP. Trong điều kiện còn thiếu thiết bị chuyên dụng như switch, router… để thực hành xây dựng hệ thống mạng và giám sát hệ thống đó, chúng tôi đã nghiên cứu và xây dựng các bài tập nhằm giúp người học thực từng bước triển khai hoàn chỉnh hệ thống giám sát mạng với Netflow trên nền phần mềm mô phỏng mạng GNS3 đáp ứng nhu cầu giảng dạy học phần Quản trị mạng tại trường ĐHSP Huế.

**Từ khóa:** Netflow, Netflow v9, Mô phỏng Netflow trên GNS3.

## 1. MỞ ĐẦU

Sự phát triển về quy mô mạng IP đã kéo theo sự phát triển của nhiều loại ứng dụng và dịch vụ. Những loại dịch vụ này đặt ra yêu cầu cao về băng thông sử dụng, về hiệu suất và tính dự báo trước về chất lượng dịch vụ chẳng hạn như dịch vụ VoIP, các dịch vụ đa phương tiện hay dịch vụ mạng hướng an toàn. Những yêu cầu này cũng đòi hỏi phải có công nghệ tương ứng để hỗ trợ cung cấp thông tin giám sát mạng và sử dụng tài nguyên của các ứng dụng. Việc giám sát mạng có thể được thực hiện bởi giao thức SNMP để lấy thông tin về lưu lượng và tốc độ dữ liệu nhận và gởi trên các giao diện thiết bị từ đó cho biết mức độ sử dụng băng thông của hệ thống mạng cũng như cho phép người quản trị đưa ra quyết định về hoạch định khả năng của mạng. Tuy nhiên, SNMP không cho biết cụ thể ứng dụng nào đang sử dụng băng thông, địa chỉ IP hay host nào liên quan, các thông tin về loại dịch vụ, chất lượng dịch vụ. Netflow là giao thức đặc quyền được đề xuất bởi Cisco có thể giải quyết vấn đề này. Việc giám sát mạng dựa trên giao thức Netflow cho phép đặc tả rõ hơn về lưu lượng IP, hiểu được các luồng xuất phát từ đâu và như thế nào, đây chính là những thông tin quan trọng sử dụng trong vấn đề sửa lỗi, đánh giá hiệu xuất cũng như đánh giá tính sẵn sàng của toàn bộ hệ thống mạng.

Trong giảng dạy các học phần mạng máy tính, để triển khai hệ thống thiết bị thực gồm những thiết bị chuyên dụng như switch, router… sẽ đòi hỏi chi phí rất lớn và việc thiết kế và chạy thử nghiệm các hệ thống mạng lớn cũng không khả thi. Do vậy, để người học có thể thực hành trên thiết bị tương đương với thiết bị thực cũng như định hướng người học các bước triển khai hoàn chỉnh hệ thống giám sát mạng bằng Netflow, chúng tôi xây dựng các bài tập trên nền phần mềm mô phỏng mạng GNS3 để phục vụ giảng dạy học phần Quản trị mạng tại trường ĐHSP Huế - ĐHH.

Tạp chí Khoa học, Trường Đại học Sư phạm, Đại học Huế
ISSN 1859-1612, Số 02(50)/2019: tr. 107-117
Ngày nhận bài: 30/11/2018; Hoàn thành phản biện: 08/12/2018; Ngày nhận đăng: 10/12/2018

## 2. NỘI DUNG NGHIÊN CỨU

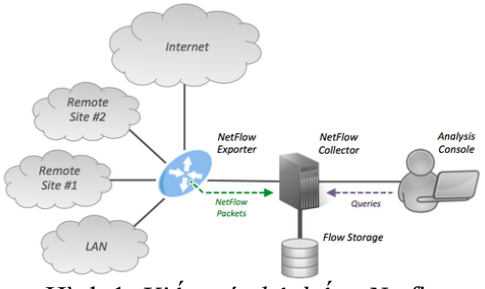
### 2.1. Sơ lược về giao thức Netflow

Việc quản trị các thiết bị mạng (switch, router…) và các dịch vụ được thực hiện truyền thống bằng giao thức quản trị mạng đơn giản SNMP. Mặc dù có thể giám sát được mức sử dụng băng thông và có các ưu điểm [1] như đơn giản quá trình quản lý, dễ dàng mở rộng và tương thích, thì nhược điểm của SNMP là không thể giám sát được thông tin chi tiết trong lưu lượng mạng nhằm xác định được cụ thể đối tượng nào đang sử dụng băng thông. Để đáp ứng yêu cầutrên, Cisco IOS Netflow ra đời với phiên bản đầu tiên được ghi nhận vào ngày 5/9/2001[3].

Netflow là một giao thức độc quyền của Cisco để tập hợp, gộp và lưu các dữ liệu luồng dữ liệu mạng. Netflow được nhúng trong các phần mềm hệ điều hành mạng trên các thiết bị như switch hay router và được hỗ trợ bởi tất cả các thiết bị Cisco. Dữ liệu được cung cấp bởi Netflow cho người quản trịcái nhìn chi tiết về lưu lượng mạng và băng thông mạng đang được sử dụng hơn là chú trọng và những kết quả của việc giám sát như giao thức SNMP. Netflow đã có 10 phiên bản, nhưng hiện nay 2 phiên bản sử dụng phổ biến là phiên bản 5 và phiên bản 9 [2][3]. Phiên bản 9 là phiên bản cải tiến nhất với việc sử dụng template trong định nghĩa các bảng ghi luồng nhờ đó thông tin luồng được định nghĩa linh động hơn thay vì phải cố định trước các trường của bản ghi như ở phiên bản trước đó, qua đó Netflow v9 cho phép thích hợp với nhiều định dạng dữ liệu thông qua cơ chế template như IPv6, Virtual Local Area Networks (VLAN) và Multiprotocol Label Switching (MPLS)[4]. Phiên bản 10 là phiên bản cải tiến từ phiên bản 9 và được IETF chấp nhận thành chuẩn quy định trong các RFC (5101, 5102).

### 2.2. Kiến trúc của hệ thống Netflow

Kiến trúc của một hệ thống Netflow gồm 3 thành phần gồm bộ phận xuất luồng, bộ phận tập hợp luồng và bộ phận quản trị [2][3] như ở hình 1.




Hình 1. *Kiến trúc hệ thống Netflow*

- Bộ phận xuất luồng: có thể là nhiều loại thiết bị khác nhau (switch, router, firewall…) hỗ trợ giao thức Netflow, chúng làm nhiệm vụ tạo dữ liệu và xuất dữ liệu đến bộ tập hợp luồng. Để triển khai Netflow có 2 cách tiếp cận gồm Netflow truyền thống (TNF) và Netflow linh hoạt (FNF). Trong phạm vi bài báo này chúng tôi đề cập đến cách tiếp cận TNF, với cách tiếp cận này, bộ phận xuất luồng sẽ khởi tạo các luồng và lưu các luồng vào thiết bị nhớ gọi là Netflow cache, sao cho trong mỗi luồng sẽ gồm các gói tin có chung 7 thuộc tính chính [5].Khi luồng không hoạt động sau một thời gian nhất định, hoặc tồn tại quá một khoảng thời gian được chỉ định trước trong cache, luồng sẽ được gom và đóng gói theo định dạng gói tin của phiên bản Netflow để gởi đến bộ phận tập hợp luồng.

- Bộ phận tập hợp luồng đảm thực hiện nhiệm vụ nhận các bản ghi từ bộ phận xuất luồng và thực hiện một số tác vụ quan trọng bao gồm lưu trữ luồng, loại bỏ dữ liệu

trùng lặp, nhận diện mẫu và phân tích hành vi, hoặc hỗ trợ các giải thuật và cơ chế để phân tích các luồng để dò tìm các nguy cơ về an ninh mạng. Dữ liệu Netflow được xuất tới bộ tập hợp sử dụng giao thức UDP. Địa chỉ IP của bộ tập hợp và số hiệu cổng đích phải được cấu hình trên các thiết bị (router, switch…) được giám sát.

- Bộ phận quản trị có nhiệm vụ cung cấp giao diện trực quan cho quản trị viên trong việc quản trị và phân tích các vấn đề mạng, gồm các tính năng chính như xem tổng quan các hoạt động của mạng, phân tích chuyên sâu để phát hiện các hành vi bất thường của mạng, Cảnh báo ngay lập tức khi xảy ra những điều kiện bất thường, cấu hình lại hệ thống phân tích Netflow…

Việc triển khai hệ thống giám sát mạng bằng Netflow bên cạnh ưu điểm [2][4] vẫn tồn tại nhược điểm: (1). Dữ liệu của Netflow chỉ giám sát được dữ liệu từ tầng 2 đến tầng 4 và phải xác định các ứng dụng qua số hiệu port của tầng Transport. Nhược điểm này có thể khắc phục bằng sự kết hợp giữa Netflow và công nghệ NBAR tích hợp các Cisco IOS [5]; (2). Dữ liệu của Netflow làm tăng tải cho thiết bị và lưu lượng mạng. Do vậy khi triển khai Netflow phải xét đến khả năng xử lý của thiết bị (RAM, CPU..), băng thông đường truyền để cấu hình các thông số Netflow trên thiết bị cũng như vị trí triển khai Netflow tại vị trí nào đểphù hợp nhất với topology của mạng đó [1].

### 2.3. Các bài tập triển khai hệ thống Netflow

Qua việc phân tích các thành phần của kiến trúc Netflow, cách thức hoạt động của các thành phần [2][3], chúng tôi nhận thấy việc triển khai hệ thống được thực hiện qua các bước:

- Xác định vị trí thiết bị triển khai Netflow

- Cấu hình ghi dữ liệu vào bộ nhớ cache và quản lý bộ nhớ cache.

- Cấu hình để xuất các luồng tới máy chủ tập hợp luồng.

- Phần mềm của bộ phận phân tích sẽ phân tích dữ liệu và tạo các báo cáo theo lịch sử và thời gian thực.

Để giúp người học hiểu rõ các bước và trực tiếp thực hành triển khai hệ thống Netflow, chúng tôi xây dựng nhóm các bài tập để triển khai hệ thống Netflow gồm 4 nhóm bài tập như sau:

- Nhóm bài tập 1: Cấu hình Netflow trên thiết bị; nhóm bài tập này mục đích để người học định hình tổng quan việc triển khai 1 hệ thống Netflow, bao gồm xác định thiết bị triển khai Netflow, vị trí triển khai bộ tập hợp, chỉ định các thông số đơn giản trên thiết bị bao gồm giao diện cổng trên thiết bị để cấu hình xuất luồng, cấu hình phiên bản Netflow, cấu hình địa chỉ bộ tập hợp và port ứng dụng; kiểm tra thông tin cấu hình qua chế độ CLI.

- Nhóm bài tập 2: Cấu hình quản lý cache trên thiết bị; nhóm bài tập này mục đích để người học hiểu ý nghĩa các thông số cấu hình cache và vai trò agrregation cache tới việc tối ưu băng thông giữa thiết bị và bộ tập hợp luồng, gồm các thông số xác định thời gian

hoạt động luồng, thời gian lưu lại của luồng trên cache, cấu hình aggregation cache và kiểm tra thông tin cache qua chế độ dòng lệnh CLI.

- Nhóm bài tập 3: Cấu hình phần mềm của bộ quản trị; Nhóm bài tập này nhằm mục đích người học thực hành cấu hình bộ phận quản trị để nhận dữ liệu từ bộ xuất luồng từ đó đọc các thông tin dữ liệu Netflow, tạo các thống kê, tạo các cảnh báo để kiểm tra và giám sát mức độ sử dụng băng thông của thiết bị, ứng dụng.

- Nhóm bài tập 4: Nhóm bài tập tổng hợp; Nhóm bài tập này nhằm mục đích để người học thực hành triển khai hệ thống Netflow hoàn chỉnh gồm phân tích yêu cầu, xây dựng hệ thống mạng hoặc dựa trên một topo mạng đã có để triển khai và giám sát hệ thống với Netflow Analyzer.

### *2.3.1. Môi trường mô phỏng*

Để mô phỏng các tình huống mạng chúng tôi sử dụng phần mềm mô phỏng GNS3 kết hợp với phần mềm giả lập máy ảo VMWare, với một số yêu cầu về phần cứng phần mềm khác như bảng dưới. Ngoài ra, để phù hợp với mục đích đã đặt ra là xây dựng hệ thống bài tập giúp người học hiểu rõ và thực hành từng bước để triển khai hệ thống Netflow chúng tôi giới hạn điều kiện thực hành các bài tập như sau: Triển khai TNF Netflow với phiên bản 9 trên thiết bị Router c7200; Sử dụng phần mềm Netflow Analyer 12 để giám sát và phân tích dữ liệu; đồng thời người học đã có kiến thức cơ bản về cấu hình router bao gồm cấu hình địa chỉ thiết bị, cấu hình định tuyến router; cấu hình NAT.

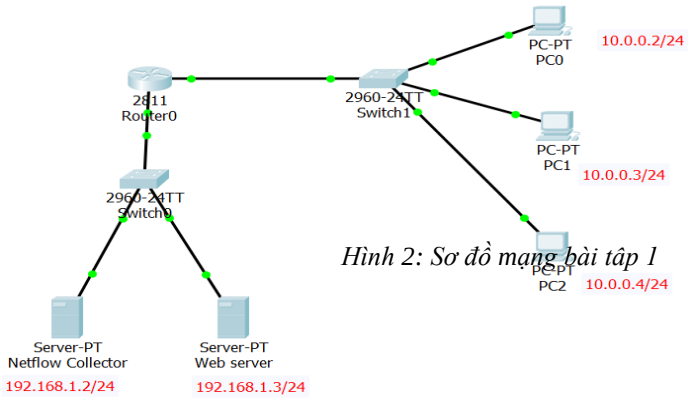
Bảng 1. *Các phần mềm và phần cứng sử dụng trong mô phỏng*

| STT | Phần cứng / phần mềm | Cấu hình tối thiểu | Mục đích sử dụng |
|---|---|---|---|
| | **Phần mềm** | | |
| 1. | GNS3 cài đặt cùng GNS3 VM (phiên bản 2.1.1) | CPU: Dual core hoặc hơn<br>Ram: 4GB<br>Storage: 1GB khả dụng | Mô phỏng hệ thống mạng |
| 2. | VMWare (Phiên bản 12.0.0) | CPU: x86<br>Ram: 2GB<br>Storage: 1 GB khả dụng | Cài đặt các máy tính ảo |
| 3. | Netflow Analyzers 12 | 2.4 GHz, Pentum4;<br>Ram: 4GB<br>Storage: 10GB khả dụng; OS: 64 Bit | Phần mềm giám sát và phân tích dữ liệu trên bộ phân tích Netflow |
| | **Phần cứng** | | |
| 4. | Máy tính desktop hay laptop | CPU: Dual core hoặc hơn<br>Ram: 8-16 GB<br>Storage: 40 GB khả dụng | |

### *2.3.2. Bài tập 1*

**- Thời lượng:** 2 tiết (1 tiết: cấu hình thiết bị trên GNS3; 1 tiết: cấu hình Netflow và kiểm tra thông tin cấu hình)

**- Mục đích:** Cấu hình bật tính năng Netflow trên thiết bị router; cấu hình giám sát lưu lượng trên các giao diện router; Kiểm tra thông tin Netflow Cache trên thiết bị router;




*Hình 2: Sơ đồ mạng bài tập 1*

**- Bài tập tình huống:** Cho sơ đồ mạng như hình vẽ 2, cấu hình Netflow version 9 để giám sát lưu lượng trên Router và cấu hình bộ tập hợp Netflow ở địa chỉ 192.169.1.2/24 số hiệu cổng UDP 9996.

**- Tập lệnh** [7]

| STT | Cú pháp lệnh | Ý nghĩa |
|---|---|---|
| 1. | Router(config)# **ip flow {ingress/egress}** | Bật tính năng Netflow trên một giao diện. **ingress** –Bắt lưu lượng đi vào tại một giao diện **egress** –Bắt lưu lượng được truyền đi từ một giao diện. |
| 2. | Router(config)# **ip flow-export destination**{*ip-address \| hostname*} *{udp-port }* | Chỉ định địa chỉ IP hoặc tên của bộ tập hợp Netflow và số hiệu cổng UDP mà bộ tập hợp Netflow đang chờ lắng nghe. |
| 3. | Router(config)# **ip flow-export version 9** | Cấu hình định dạng gói tin xuất Netflow phiên bản 9 |
| 4. | Router# **show ip cache flow** | Kiểm tra sự hoạt động của Netflow và hiển thị tóm tắt thông tin thống kê Netflow. |

**- Các bước cấu hình:**

1. Sử dụng GNS3 để mô phỏng hệ thống mạng như yêu cầu; cấu hình địa chỉ cho thiết bị;
2. Cấu hình bật tính năng Netflow trên giao diện của Router
3. Triển khai một web server và các máy con để tạo lưu lượng trên mạng (hoặc sử dụng đối tượng Ostinato trên GNS3 để tạo lưu lượng cho hệ thống mạng)
4. Cấu hình chỉ định địa chỉ IP của bộ tập hợp Netflow là 192.168.1.2/24 số hiệu UPD Port 9996.
5. Kiểm tra sự hoạt động của Netflow và đọc thông tin Netflow cache trên Router
6. Lưu cấu hình trên thiết bị router.

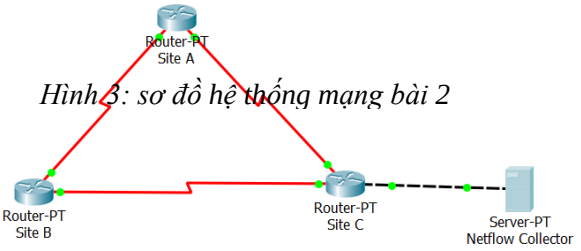
- **Biến thể của bài tập**: Thay đổi mô hình mạng để sinh viên quyết định vị trí cấu hình Netflow, giao diện cài đặt Netflow phù hợp; Yêu cầu tạo lưu lượng cụ thể trên Ostinato và kiểm tra thông tin đó trên Netflow Cache bằng chế độ CLI.

### *2.3.3. Bài tập 2*

- **Thời lượng:** 2 tiết (1 tiết: lắp đặt thiết bị, cấu hình địa chỉ, định tuyến thiết bị; 1 tiết cấu hình Netflow và kiểm tra thông tin cấu hình)

- **Mục đích:** Cấu hình main cache; aggregation cache và kiểm tra thông tin tin cấu hình cache theo yêu cầu.

- **Bài tập tình huống:** Sơ đồ mạng như hình vẽ 3 cấu hình Netflow và cấu hình main cache và cache aggregation trên router *(lược đồ và tham số theo yêu cầu cụ thể của giáo viên)* và cấu hình triển khai thiết bị collector Netflow tại site C.




*Hình 3: sơ đồ hệ thống mạng bài 2*

- **Tập lệnh** [7]

| STT | Cú pháp lệnh | Ý nghĩa |
|---|---|---|
| 1. | Router(config)# **ip flow-aggregation cache {as \| as-tos \| destination-prefix \| destination-prefix-tos \| prefix \| prefix-port \| prefix-tos \| protocol-port \| protocol-port-tos \| source-prefix \| source-prefix-tos}** | Bật chế độ cấu hình aggregation cache và cấu hình lược đồ cache tương ứng.<br>Từ khóa as cấu hình cache lược đồ cache AS<br>Từ khóa **as-tos** cấu hình cache lược đồ AS ToS cache.<br>Từ khóa **destination-prefix** cấu hình cache lược đồ destination prefix.<br>Từ khóa **destination-prefix-tos** cấu hình cache lược đồ destination prefix ToS.<br>Từ khóa **prefix** cấu hình cache lược đồ prefix.<br>Từ khóa **prefix-port** cấu hình cache lược đồ prefix port.<br>Từ **prefix-tos** cấu hình cache lược đồ prefix ToS.<br>Từ khóa **protocol-port** cấu hình cache lược đồ protocol port<br>Từ khóa **protocol-port-tos** cấu hình cache lược đồ protocol port ToS<br>Từ khóa **source-prefix** cấu hình cache lược đồ source prefix.<br>Từ khóa **source-prefix-tos** cấu hình cache lược đồ source prefix ToS. |
| 2. | Router(config-flow-cache)# **cache entries** *{number}* | Đối số number là số mục được cho phép trong cache aggregation. Giá trị này nằm trong khoảng từ 1024 đến 2000000. Giá trị mặc định là 4096. |
| 3. | Router(config-flow- | Đối số minutes chỉ định số phút mà một mục dữ liệu |

| | | |
|---|---|---|
| | cache)# **cache timeout active** *{minutes}* | hoạt động được cho phép tồn tại tối đa trong cache. Giá trị này nằm trong khoảng từ 1 đến 60 và mặc định là 30 phút. |
| 4. | Router(config-flow-cache)# **cache timeout inactive** *{seconds}* | Đối số seconds chỉ định thời gian tính bằng giây mà một mục dữ liệu trong cache không hoạt động được tồn tại trong cache. Giá trị này nằm trong khoảng từ 10 đến 600 giây. Giá trị mặc định là 15 giây. |
| 5. | Router#**show ip cache flow aggregation {*parameter*}** | Kiểm tra thông tin aggregation cache với 1 lược đồ cụ thể được chọn; với *parameter* nhận các giá trị và ý nghĩa giá trị như ở lệnh 1. |
| 6. | Router(config)# **ip flow-cache entries** *numbers* | Chỉ định số mục tối đa luồng được lưu trong main cache. Giá trị này nằm trong khoảng 1024 đến 524288. |
| 7. | Router(config)# **ip flow-cache timeout active** *{minutes}* | Đối số minutes chỉ định số phút mà một mục dữ liệu hoạt động được cho phép tồn tại tối đa trong cache. Giá trị này nằm trong khoảng từ 1 đến 60 và mặc định là 30 phút. |
| 8. | Router(config)# **ip flow-cache timeout inactive** *{seconds}* | Đối số seconds chỉ định thời gian tính bằng giây mà một mục dữ liệu trong cache không hoạt động được tồn tại trong cache. Giá trị này nằm trong khoảng từ 10 đến 600 giây. Giá trị mặc định là 15 giây. |

**- Các bước cấu hình:**

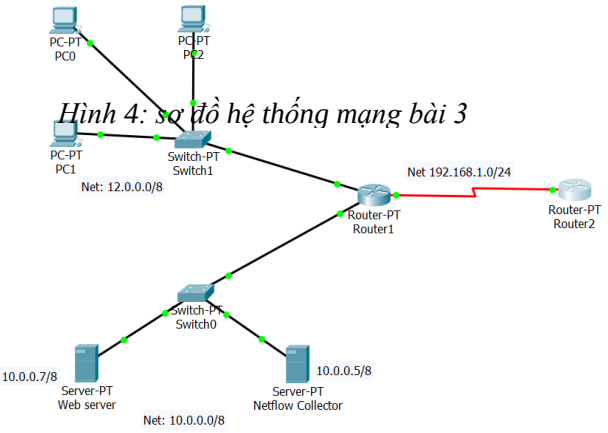
1. Sử dụng GNS3 để mô phỏng hệ thống mạng như yêu cầu; cấu hình địa chỉ cho thiết bị; Khởi tạo lưu lượng trên mạng với Ostinato;Cấu hình định tuyến giữa các router bằng giao thức định tuyến OSPF
2. Cấu hình chỉ định địa chỉ IP của bộ tập trung Netflow là 192.168.1.2/24
3. Cấu hình main cache bao gồm (thời gian tối đa luồng tồn tại và thời gian luồng không hoạt động) và kiểm tra thông tin main cache trên router Site C và kiểm tra thông tin main cache
4. Cấu hình Cache Aggregation theo một lược đồvà cấu hình quản lý cache aggregation
5. Kiểm tra sự hoạt động của Netflow và đọc thông tin Netflow cache trên Router

**- Biến thể của bài tập:** Đặt ra yêu cầu cụ thể đối với main cache và aggreagation cache để người học xác định thông số cấu hình theo yêu cầu cụ thể; ghi nhận và đối chứng các thông tin đã cấu hình qua kiểm tra cache ở chế độ CLI trên Router.

### *2.3.4. Bài tập 3*

**- Thời lượng:** 3 tiết (1 tiết: lắp đặt thiết bị, cấu hình địa chỉ, định tuyến/NAT trên thiết bị router; 2 tiết: cấu hình Netflow, kiểm tra thông tin cấu hình; cài đặt, cấu hình và kiểm tra thông tin trên phần mềm Netflow Analyzer)

- **Mục đích:** Cấu hình Netflow trên thiết bị, cài đặt và cấu hình giám sử dụng băng thông của các thiết bị và ứng dụng mạng với phần mềm Netflow Analyzer.




*Hình 4: sơ đồ hệ thống mạng bài 3*

- **Bài tập tình huống:** Một công ty có hệ thống mạng như hình 4; trong đó Router 1 nối với mạng nội bộ có dãy địa chỉ 12.0.0.0/8 và mạng DMZ gồm có server chạy các dịch vụ và Netflow Collector (địa chỉ 10.0.0.5/8 và số hiệu cổng 9996); Router 2 đại diện cho router biên kết nối đến mạng ngoài hoặc Internet (Trong bài tập này, kết nối mạng ảo trong GNS3 ra Internet qua card mạng thật máy tính); Cấu hình triển khai giám sát hệ thống mạng với Netflow; Cấu hình tạo các báo cáo và tạo các cảnh báo trên phần mềm Netflow Analyzer để quản lý giám sát băng thông của hệ thống mạng này.

- **Các bước cấu hình:**

1. Sử dụng GNS3 để mô phỏng hệ thống mạng như yêu cầu; Cài đặt một máy ảo chạy hệ điều hành Window 7 và nối vào GNS3;
2. Cấu hình địa chỉ cho thiết bị .Cấu hình NAT và default route trên router1 để mạng bên trong GNS3 kết nối Internet; Cấu hình kích hoạt Netflow trên router1; cấu hình quản lý cache; Cấu hình chỉ định địa chỉ IP của bộ tập trung Netflow là 10.0.0.5/8 và số hiệu port 9996.
3. Kiểm tra kết nối của các thiết bị và từ thiết bị đến Internet; sự hoạt động của Netflow;
4. Cài đặt Netflow Analyzer trên Server và thiết lập các cấu hình [6]:
   - Cấu hình Flow export: Kiểm tra lại thông số cổng bằng với giá trị đã cấu hình ở Router (9996).
   - Cấu hình quản trị dữ liệu qua Settings/Storage Settings
     + Raw Data: Bật On
     + Aggregated Data: cấu hình giá trị thống kê 10 bản ghi dữ liệu đầu tiên và thời gian lưu trữ dữ liệu là 2 tháng.
     + One minute storage: cấu hình thời gian lưu trữ dữ liệu 1 tháng để phục vụ thống kê theo thời gian thực.
   - Cấu hình Report: tạo 2 Schedule Report và Forensic Report theo yêu cầu
     + Schedule Report: Name (schR_Interface); Description (thống kê theo giao diện); Device Type (interface); Report Type (Traffic report); Report Format

(PDF); Report Date và Report Time: Thời điểm hiện tại; Report Period (Today); Mail Notification (Enable) và chỉ định địa chỉ mail nhận Report với Subject mặc định.

+ Forensic Report: Tạo thống kê chi tiết theo các tiêu chí theo yêu cầu Device Type (Interface); Device (10.0.0.1); Interface ( infIndex2); Criteria (địa chỉ nguồn 12.0.0.9); From và To: chỉ định khoảng thời gian cần thống kê;

- Trên DashBoard xem thống kê lưu lượng Traffic Summary; Top N Application; Top N Protocol; của các thiết bị và mức sử dụng băng thông của các Layer 4 Protocol; của Interface của các thiết bị tương ứng.

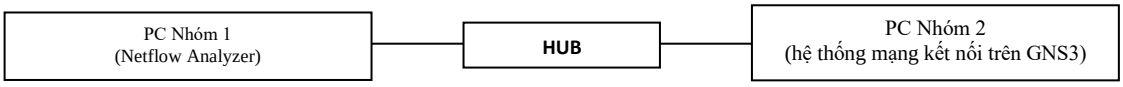
### *2.3.5. Bài tập 4*

**- Thời lượng:** 5 tiết (2 tiết: Lắp đặt thiết bị mô phỏng trên GNS3; cấu hình cho thiết bị (Địa chỉ, định tuyến, Nat…); 3 tiết cấu hình Netflow và kiểm tra thông tin cấu hình; cài đặt, cấu hình và kiểm tra thông tin trên phần mềm Netflow Analyzer).

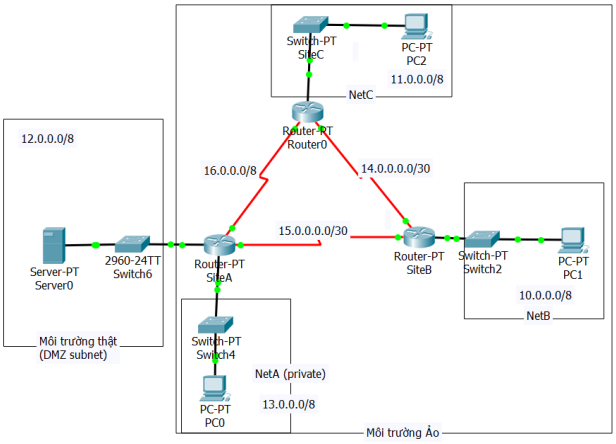
**- Mục đích:** Phân tích yêu cầu để lựa chọn phương án triển khai 1 hệ thống Netflow hoàn chỉnh và thực hiện giám sát hệ thống mạng đã cho. Nhóm bài tập tổng hợp này được xây dựng để người học thực hành làm việc nhóm trên 2 công việc chính độc lập: Cấu hình Netflow trên thiết bị; Cấu hình giám sát trên Netflow Analyzer theo kịch bản như sau:

**+ Nhóm 1:** Cấu hình Netflow giám sát hệ thống mạng ảo trên 1 máy tính chạy GNS3

**+ Nhóm 2:** cấu hình Netflow Analyzer trên 1 PC thật và kết nối với nhóm 1 theo mô hình:




**- Bài tập tình huống:** Hệ thống mạng gồm 3 chi nhánh A, B, C theo sơ đồ hình 5; Router 1 nối với mạng nội bộ có dãy địa chỉ 12.0.0.0/8 và mạng DMZ gồm có server chạy các dịch vụ và Netflow Collector (địa chỉ 10.0.0.5/8 và số hiệu cổng 9996); Các chi nhánh B, C lần lượt nối với các mạng nội bộ NetB và NetC có địa chỉ ở hình đã cho. Cấu hình Netflow để giám sát sử dụng băng thông của các thiết bị và ứng dụng cho hệ thống nói trên.




Hình 5. *Sơ đồ mạng bài tập 4*

1. Sử dụng GNS3 để mô phỏng hệ thống mạng như yêu cầu;
   - Toàn bộ nhóm Môi trường ảo được cài đặt trên GNS3 chạy trên PC nhóm 1;
   - Hệ thống mạng thật trong đó có PC đóng vai trò là Netflow Collector và cài đặt Netflow Analyzer được nối vào thiết bị Hub thật và nối vào card mạng thật của PC cài đặt một máy ảo chạy hệ điều hành Window 7 và nối vào GNS3;
2. Cấu hình địa chỉ cho các thiết bị theo yêu cầu;
3. Cấu hình định tuyến giữa các router với OSPF;
4. Cấu hình kích hoạt Netflow trên router1; Kiểm tra thông tin cấu hình cache trên router;
5. Cấu hình giám sát hệ thống trên Netflow Analyzer và quản lý thông tin giám sát sử dụng băng thông của các thiết bị và ứng dụng.

**- Biến thể của bài tập**: Thay đổi mô hình mạng và vị trí triển khai Netflow collector để người học thực hành xác định vị trí triển khai Netflow và cấu hình trên giao diện Router với lệnh tương ứng; Đặt ra yêu cầu giám sát sử dụng băng thông của thiết bị hay ứng dụng cụ thể và tạo các report và cảnh báo cho các đối tượng đó trên phần mềm Netflow Analyzer.

## 3. KẾT LUẬN

Giám sát luồng dữ liệu đang dần trở thành giáp pháp mang tính phổ biến để giám sát lưu lượng mạng tốc độ cao. Netflow được phát triển bởi Cisco là một trong những giải pháp giám sát luồng bên cạnh một số giải pháp luồng như sFlow, jFlow.. Đồng thời Netflow cũng khắc phục được nhược điểm mà giao thức SNMP truyền thống không làm được về giám sát chi tiết lưu lượng dữ liệu trong luồng. Trong điều kiện các thiết bị mạng chuyên dụng phục vụ cho học phần mạng còn hạn chế, cũng như triển khai và vận hành mạng lớn là không khả thi thì hệ thống bài tập thực hành trên GNS3 nhằm hướng dẫn người học từng bước triển khai hoàn chỉnh hệ thống Netflow là công cụ hiệu quả để người học kiểm nghiệm phần thuyết và rèn luyện kỹ năng thực hành qua đó nâng cao chất lượng dạy và học.

## TÀI LIỆU THAM KHẢO

[1] Douglas R. Mauro and Kevin J. Schmidt (2005). *Essential SNMP*, second editionO'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

[2] Mike Chapple, Ph.D (2012). *Netflow Security Monitoring For Dummies,*John Wiley & Sons Inc, 111 River Street.

[3] Americas Headquarters (2014). *NetFlow Configuration Guide, Cisco IOS Release 15S*, Cisco Systems, Inc.

[4] Rick Hofstede, Pavel Celeda, Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto and Aiko Pras (2014). *Flow Monitoring Explained: From Packet Capture to Data Analysis withNetFlow and IPFIX,* IEEE, Page(s): 2037 - 2064.

[5] https://www.cisco.com, *Application Monitoring Using NetFlow*, Technology Design Guide, 2013
[6] https://www.manageengine.com/products/netflow/help/, NetFlow Analyzer Help.
[7] https://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c.html, Cisco IOS Switching Services Configuration Guide

**Title:** BUIDING EXERCISES TO IMPLEMENT A NETWORK MONITORING SYSTEM WITH NETFLOW FOR TEACHING

**Abstract:** Netflow is a Cisco proprietary protocol that allows detailed monitoring of network traffic flows, thus overcoming the disadvantage of traditional SNMP protocol in monitoring bandwidth usage of devices and applications. Due to the shortage of real devices used for network administrating and monitoring, the system of exercises that enables learners to take steps to fully implement the network monitoring system with Netflow based on simulation software GNS3 was built to meet the demand of teaching network management module at Hue University of Education.

**Keywords:** Netflow, Netflow v9, Netflow simulation software on GNS3.