NETWORK VIRTUALIZATION

Mục lục

1. Giới thiệu

1.1. Phạm vi bài báo cáo

Bài báo cáo này tập trung vào việc nghiên cứu và phân tích về ảo hóa mạng (Network virtualization) và các ứng dụng của nó, đặc biệt là phần demo về SDN (Software-Defined Networking). Chúng ta sẽ đánh giá các giải pháp, công nghệ liên quan, cũng như tiềm năng phát triển của ảo hóa mạng trong tương lai. Bài báo cáo sẽ bao gồm các khía cạnh sau:

- Lý thuyết cơ bản về ảo hóa mạng và SDN, bao gồm định nghĩa, các loại ảo hóa mạng, kiến trúc SDN, ưu điểm và nhược điểm của cả hai.
- Ứng dụng của ảo hóa mạng trong các lĩnh vực như trung tâm dữ liệu, mạng di động, mạng vận chuyển và mạng doanh nghiệp.
- Phần demo về SDN bao gồm thiết kế, triển khai và đánh giá hiệu năng của mô hình mạng SDN. Demo sẽ minh họa cách tạo và quản lý các ảo hóa mạng thông qua SDN, cũng như các ứng dụng và kịch bản thực tế.

1.2. Giới thiệu về ảo hóa mạng

1.2.1. Bối cảnh

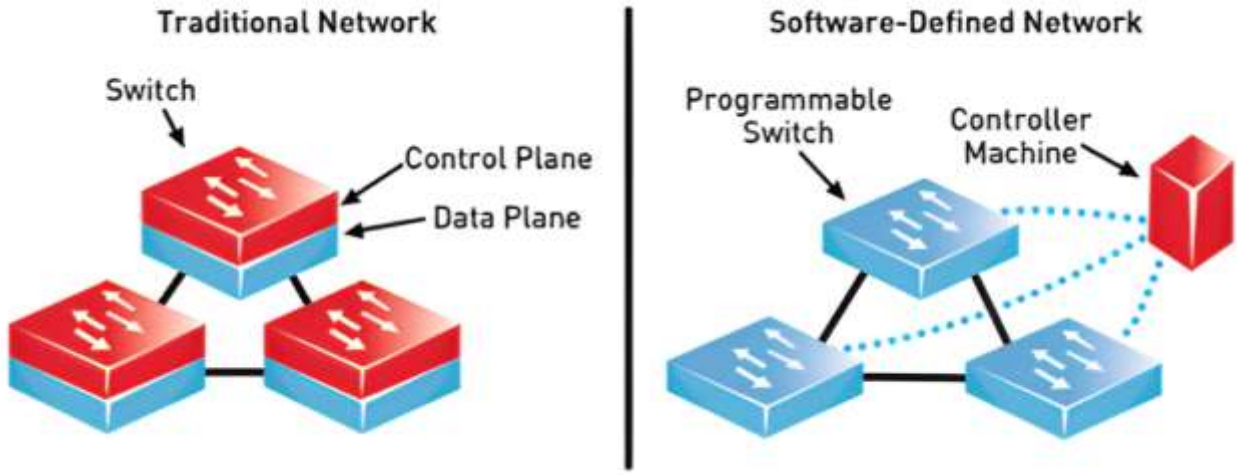
Trong thời đại phát triển của điện toán đám mây mang đến cho các tổ chức những lợi ích lớn nhờ khả năng nhanh gọn, tính linh hoạt cũng như sự hiệu quả nó mang lại, cũng không quá bất ngờ khi các tổ chức lớn nhỏ đều muốn có được những khả năng vượt trội ấy không chỉ bao gồm các hạ tầng cloud, edge cloud mà còn những hạ tầng sẵn có của họ.

Trên thực tế, các hạ tầng mạng và an ninh truyền thống mang đến nhiều khó khăn, công sức để thiết, thực thi, cũng như là quản lý. Ngoài ra, chi phí hay khả năng cũng là một trở ngại. Hiện nay, việc ảo hóa mạng được coi là một cách hiệu quả để khắc phục các vấn đề đã nêu.

1.2.2. Định nghĩa

Thuật ngữ “ảo hóa mạng” (Network Virtualization) chỉ việc trừu tượng hoá tài nguyên mạng từ phần cứng sang phần mềm. Mạng ảo hóa có thể chia một mạng vật lý thành nhiều mạng độc lập, riêng biệt hoặc kết hợp nhiều mạng vật lý thành một hệ thống

ảo. Các quản trị viên có thể triển khai các máy ảo mạng giữa các địa điểm khác nhau bằng công nghệ ảo hóa mạng mà không cần cấu hình lại mạng. Trên cơ sở hạ tầng mạng vật lý giống nhau, phần mềm xây dựng một lớp mạng cho phép nhiều lớp mạng ảo hoạt động. Việc ảo hóa hạ tầng mạng có thể giúp các doanh nghiệp cải thiện hiệu suất, tăng độ bảo mật, đồng thời giảm chi phí và độ phức tạp. Nó đặc biệt hữu ích trong môi trường điện toán đám mây, có nhiều khách hàng thuê chung một cơ sở hạ tầng vật lý nhưng yêu cầu tài nguyên mạng tách biệt và an toàn.



1.2.3. Tại sao nên ảo hóa mạng

Phương pháp ảo hóa mạng đã tái định nghĩa các quy chuẩn về cung cấp dịch vụ, từ những Datacenter bằng phần mềm, cho đến Cloud. Phương pháp này đã chuyển đổi những hạ tầng mạng cứng nhắc và không hiệu quả trở nên linh hoạt, dễ thích ứng và hiệu quả. Các hệ thống tinh vi cần có khả năng đáp ứng về mặt tốc độ và sự linh hoạt, đồng thời đáp ứng các yêu cầu cho các ứng dụng Cloud và mối đe dọa về bảo mật ngày càng tăng. Nhờ vào ảo hóa, ta có thể giảm thiểu được thời gian cần thiết để triển khai cơ sở hạ tầng cần thiết cho việc hỗ trợ một ứng dụng mới, nhờ đó các ứng dụng có thể được cập nhật hoặc triển khai chỉ trong vài phút.

1.3. Lợi ích của ảo hóa mạng

Ảo hóa mạng cho phép tạo ra nhiều mạng ảo trên cùng một cơ sở hạ tầng vật lý. Ảo hóa mạng có thể mang lại nhiều lợi ích cho các doanh nghiệp và tổ chức, bao gồm:

1.3.1. Giảm chi phí

Ảo hóa mạng cho phép các tổ chức kết hợp nhiều mạng vật lý thành một mạng ảo, giảm nhu cầu về cơ sở hạ tầng vật lý đắt tiền. Điều này giúp tiết kiệm chi phí đầu tư, bảo trì và hao tổn.

1.3.2. Độ linh hoạt khi triển khai hệ thống

Ảo hóa mạng cho phép các tổ chức dễ dàng mở rộng hoặc thu nhỏ mạng của họ để đáp ứng những nhu cầu thay đổi, qua đó giúp giảm thiểu sự lãng phí và tối ưu hóa hiệu suất của hệ thống. Ngoài ra, ảo hóa mạng cũng cho phép thay đổi và điều chỉnh cấu hình mạng một cách nhanh chóng và linh hoạt, không cần phải can thiệp vào thiết bị vật lý. Điều này đặc biệt có giá trị đối với các tổ chức có khối lượng công việc lớn hoặc khi có lượng nhu cầu sử dụng tăng cao trong thời gian cao điểm (Ví dụ như các dịch vụ online meeting trong thời điểm Covid).

1.3.3. Tăng tính bảo mật

Ảo hóa mạng có thể cải thiện bảo mật mạng bằng cách cho phép sử dụng các mạng riêng ảo (VPN) và cô lập lưu lượng truy cập giữa các mạng ảo khác nhau. Điều này giúp ngăn chặn sự xâm nhập và tấn công từ bên ngoài hoặc từ các môi trường khác. Ngoài ra, ảo hóa mạng cũng cho phép áp dụng các chính sách và quy tắc bảo mật riêng biệt cho từng môi trường, tăng cường khả năng kiểm soát và tuân thủ của mạng.

1.3.4. Đơn giản hóa việc quản trị

Ảo hóa mạng cho phép quản trị viên quản trị mạng của họ dễ dàng hơn, bằng cách trừu tượng hóa cơ sở hạ tầng vật lý cơ bản và có được một cái nhìn tổng quan về mạng. Điều này giúp đơn giản hóa kiến trúc của mạng, qua đó giảm thiểu sự phụ thuộc vào các nhà cung cấp thiết bị và các giao thức khác nhau.

1.3.5. Giảm thời gian theo dõi khi triển khai phần mềm mới

Với ảo hóa mạng, ta sẽ không tiêu tốn đến hàng ngày, hàng tuần để có thể triển khai được cơ sở hạ tầng cần thiết để hỗ trợ một ứng dụng mới. Các ứng dụng có thể được đưa vào hoạt động hoặc cập nhật chỉ trong thời gian ngắn.

1.4. Khó khăn khi triển khai ảo hóa mạng

Ảo hóa mạng là công nghệ phức tạp, do đó khi triển khai ảo hóa mạng người quản trị mạng sẽ gặp phải rất nhiều khó khăn. Báo cáo sẽ trình bày về một số khó khăn phổ biến như sau:

1.4.1. Khó khăn về kỹ thuật:

Ảo hóa mạng đòi hỏi các thiết bị mạng phải có khả năng hỗ trợ các giao thức và chuẩn mới, như VXLAN, NVGRE, MPLS, OpenFlow, v.v. Điều đó yêu cầu các quản trị viên nâng cấp hoặc thay thế các thiết bị mạng đã cũ nhưng vẫn hoạt động. Ngoài ra, việc thiết kế và cấu hình các mạng ảo cũng đòi hỏi kỹ năng và kiến thức của các kỹ sư mạng.

1.4.2. Khó khăn về tích hợp hệ thống:

Ảo hóa mạng phải làm việc liên tục và hiệu quả với các hệ thống khác trong môi trường IT như máy chủ ảo hóa, lưu trữ, bảo mật, v.v. Điều này đòi hỏi sự tương thích và liên kết giữa các giải pháp ảo hóa của các nhà cung cấp khác nhau. Ngoài ra, việc tích hợp ảo hóa mạng cũng phải đảm bảo không gây ra xung đột hoặc gián đoạn cho các dịch vụ và ứng dụng đang chạy trên hạ tầng mạng.

1.4.3. Khó khăn về quản trị:

Tuy ở trên ta đã đề cập rằng ảo hóa mạng sẽ giúp đơn giản hóa việc quản trị, nó đồng thời cũng tạo ra sự phức tạp khi số lượng và chủng loại của các mạng ảo ngày càng tăng. Việc quản trị mạng ảo cũng đòi hỏi kiến thức về các công cụ và phương pháp mới, có thể tự động hóa và tối ưu hóa các quy trình. Ngoài ra, việc quản trị mạng ảo cũng phải đảm bảo tính nhất quán và minh bạch giữa các mạng ảo và mạng vật lý.

1.4.4. Khó khăn về bảo mật:

Cũng như vấn đề quản trị, ảo hóa mạng tuy tạo ra những quy tắc bảo mật nâng cao thì cũng tạo ra những rủi ro mới. Việc bảo mật mạng ảo đòi hỏi các giải pháp và quy định tường lửa mới, có thể phát hiện và ngăn chặn các tấn công hiệu quả. Ngoài ra, việc bảo mật mạng ảo cũng phải tuân thủ các quy định và tiêu chuẩn về an toàn thông tin.

2. Cách thức hoạt động

Mạng ảo hóa tách các dịch vụ mạng khỏi phần cứng cơ bản và cho phép cung cấp ảo hoá toàn bộ một mạng. Tài nguyên mạng vật lý như Switch, Router, Firewall, Load Balancer, v.v. được gộp lại và cung cấp dưới dạng phần mềm, và chỉ yêu cầu chuyển tiếp gói tin Internet Protocol từ mạng vật lý cơ bản.

2.1. Software-Defined Networking (SDN):

Software-Defined Networking (SDN) là một công nghệ mạng ảo hóa mới, cho phép các quản trị viên mạng điều khiển và quản lý mạng bằng cách sử dụng các bộ điều khiển phần mềm, giúp tăng tính linh hoạt và hiệu quả trong việc triển khai và quản lý mạng.

SDN hoạt động bằng cách tách lớp điều khiển (Control Plane) và lớp dữ liệu (Data Plane) của thiết bị mạng. Lớp điều khiển được quản lý bởi một Controller, còn lớp dữ liệu được quản lý bởi các thiết bị mạng. SDN cho phép quản trị viên mạng tương tác với Controller bằng cách sử dụng API và giao diện đồ họa để tạo ra các quy định routing, tối ưu hóa mạng và cân bằng tải mạng.

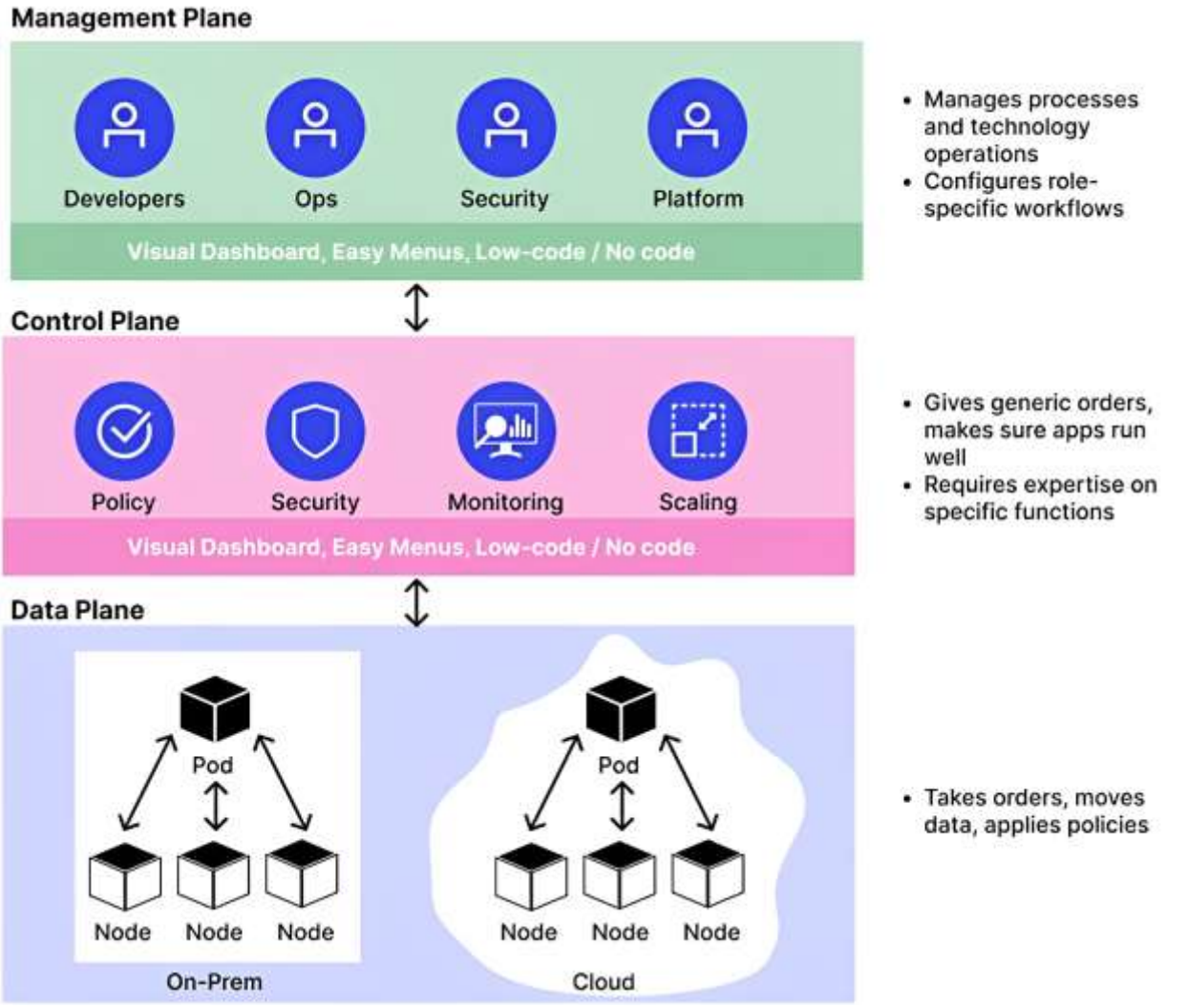
SDN giúp tăng tính linh hoạt và hiệu quả trong việc triển khai và quản lý mạng. Các quản trị viên mạng có thể triển khai các chính sách mạng mới một cách nhanh chóng và dễ dàng, mà không cần thay đổi phần cứng của thiết bị mạng. Điều này giúp tăng tính linh hoạt và tiết kiệm chi phí cho các tổ chức.

Ngoài ra, SDN còn cung cấp tính năng tối ưu hóa mạng. Trung tâm điều khiển SDN có thể phân tích và giám sát lưu lượng mạng để tối ưu hóa định tuyến và cân bằng tải, giúp tăng hiệu suất mạng và giảm độ trễ.

Control Plane và Data Plane:

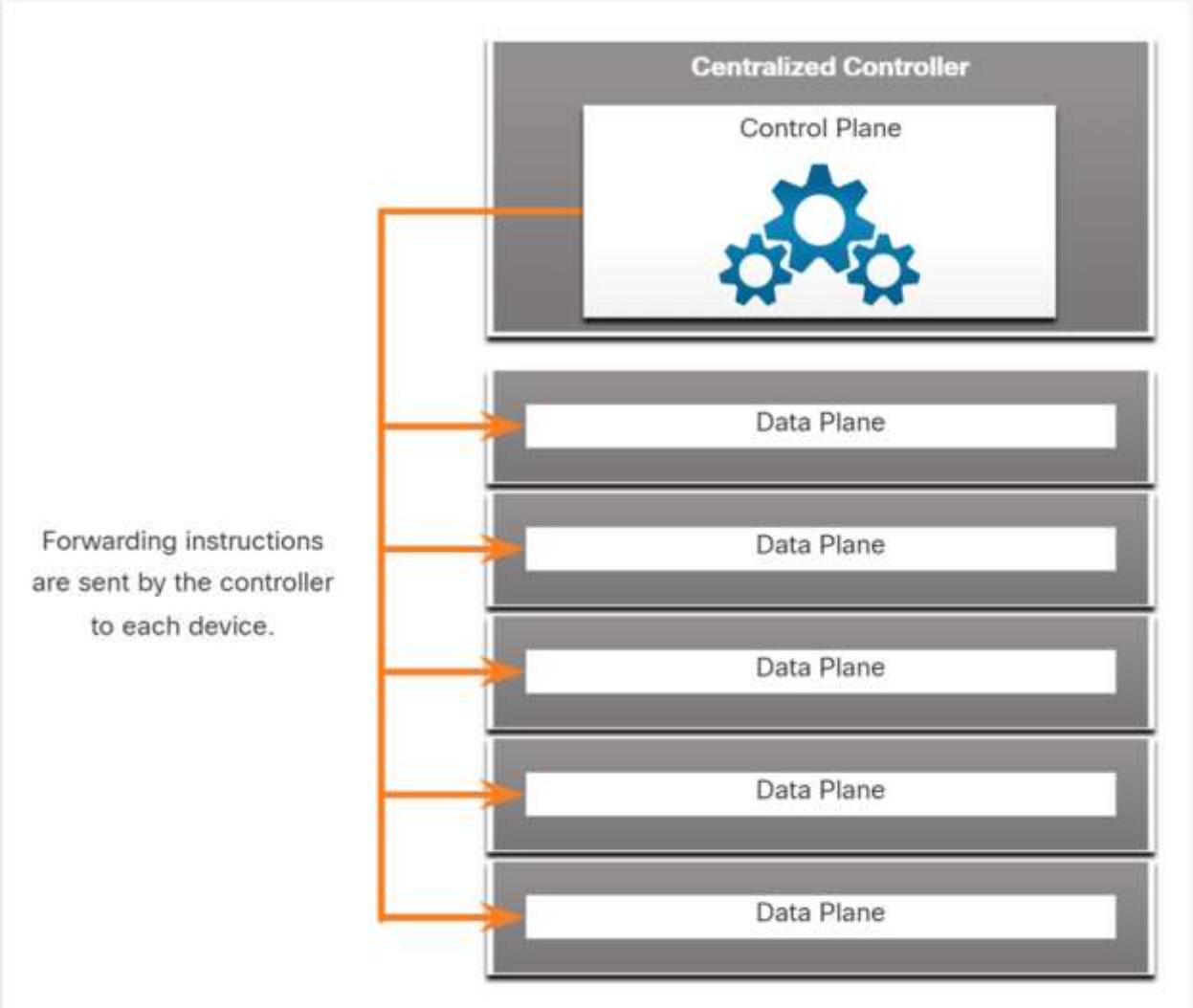
- **Control Plane:** Đây thường được coi là bộ não của một thiết bị. Nó được sử dụng để đưa ra quyết định chuyển tiếp. Control Plane chứa các cơ chế chuyển tiếp tuyến Lớp 2 và Lớp 3, chẳng hạn như bảng lân cận giao thức định tuyến (Routing Protocol Neighbor Tables), bảng cấu trúc liên kết (Topology Tables), bảng định tuyến (Routing Tables) IPv4/IPv6, STP và bảng ARP. Thông tin gửi đến Control Plane được xử lý bởi CPU.

- **Data Plane:** Thường là Switch Fabric kết nối các cổng mạng (Port) khác nhau trên thiết bị. Data Plane của mỗi thiết bị được sử dụng để chuyển tiếp các luồng lưu lượng (Traffic Flow). Router và Switch sử dụng thông tin từ Control Plane để chuyển tiếp lưu lượng đến ra khỏi Egress Interface thích hợp. Thông tin trong Data Plane thường được xử lý bởi bộ vi xử lí dành riêng cho Data Plane mà không cần CPU tham gia.
- **Management Plane**: chịu trách nhiệm quản lý thiết bị thông qua kết nối của thiết bị với mạng. Quản trị viên mạng sử dụng các ứng dụng như SSH, TFTP, SFTP hay HTTPS để truy cập vào Management Plane và cấu hình thiết bị.



SDN và bộ điều khiển trung tâm (Controller):

SDN về cơ bản là sự tách biệt giữa Control Plane và Data Plane. Chức năng Control Plane được loại bỏ khỏi từng thiết bị và được thực hiện bởi Controller. Controller truyền các chức năng của Control Plane tới từng thiết bị, và mỗi thiết bị chỉ tập trung vào việc chuyển tiếp dữ liệu trong khi bộ điều khiển tập trung quản lý luồng dữ liệu, tăng cường bảo mật và cung cấp các dịch vụ khác.



Các thành phần của SDN:

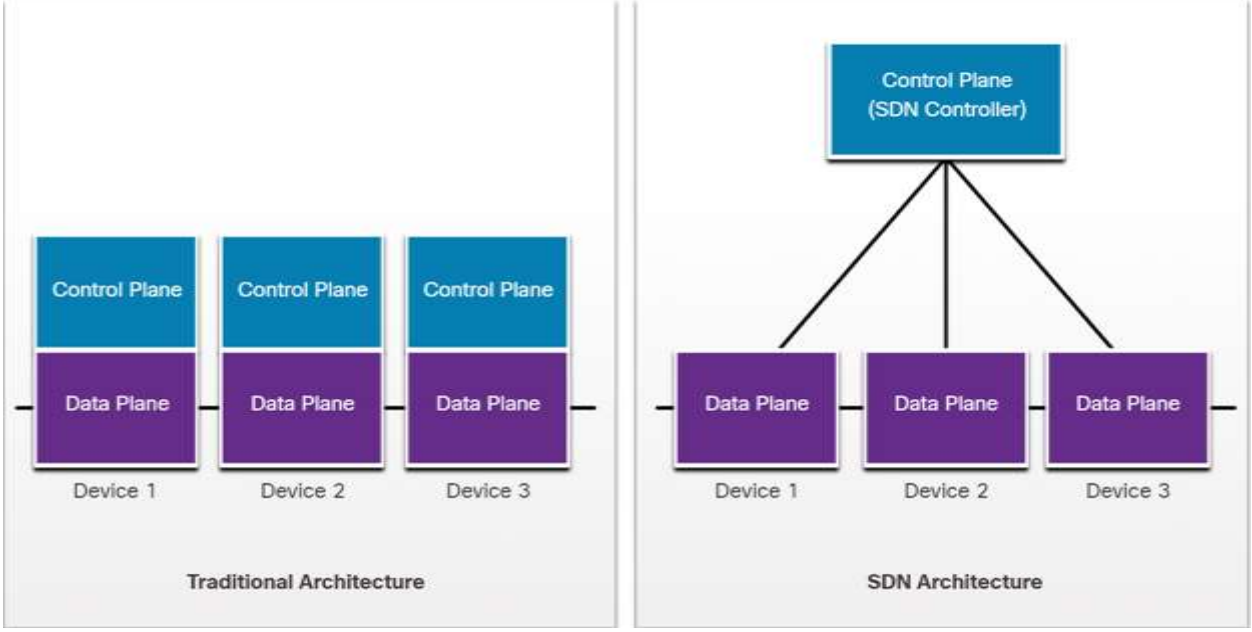
- **OpenFlow:** Là một yếu tố cơ bản trong việc xây dựng các giải pháp SDN, giúp quản lý lưu lượng giữa các Router, Switch, Wireless AP và Controller
- **OpenStack:** Cách tiếp cận này là một nền tảng ảo hóa và điều phối được thiết kế để xây dựng các môi trường đám mây có thể mở rộng và cung cấp giải pháp IaaS. OpenStack thường được sử dụng với Cisco ACI. Điều phối

(Orchestration) trong mạng là quá trình tự động hóa việc cung cấp các thành phần mạng như máy chủ, bộ lưu trữ, Switch, Router và ứng dụng.

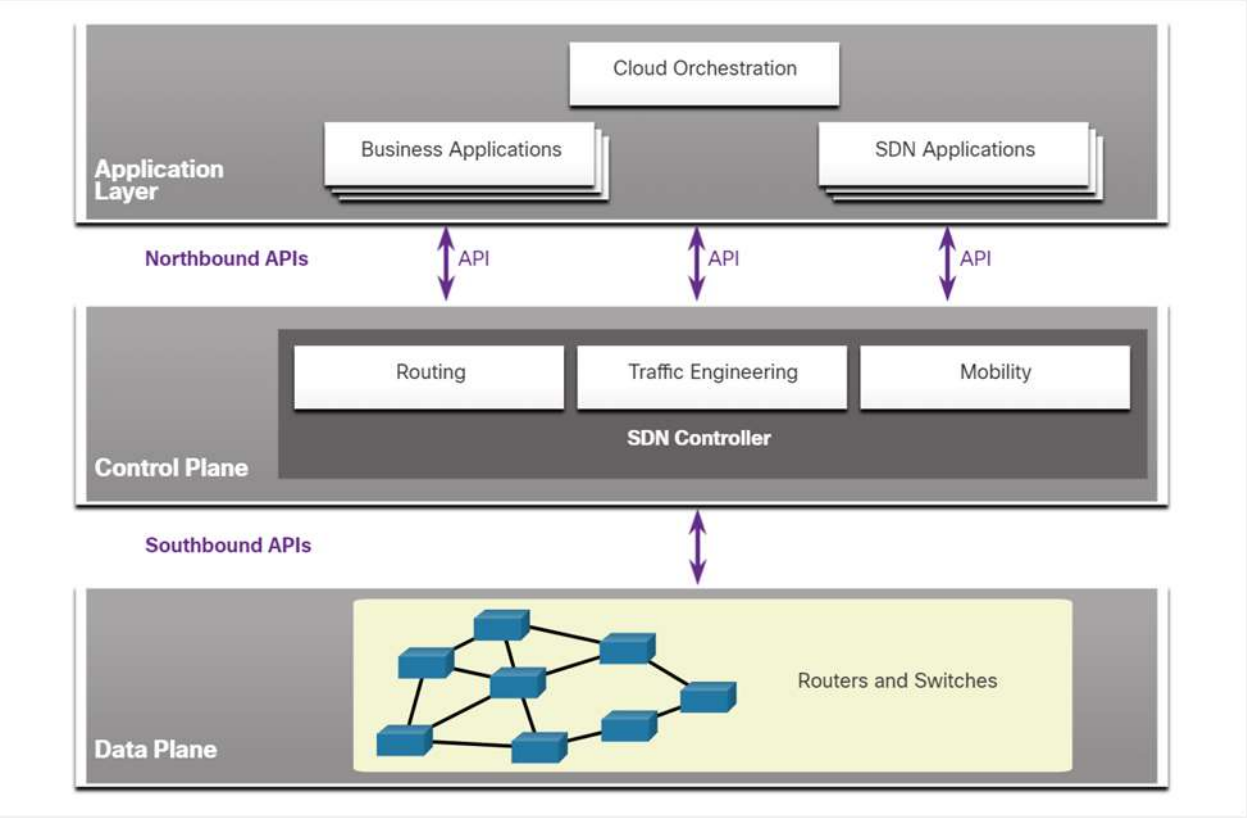
- Các thành phần khác - bao gồm Interface với Hệ thống Định tuyến (I2RS), TRILL, Cisco FabricPath (FP) và IEEE 802.1aq (SPB).

Kiến trúc truyền thống và kiến trúc SDN:

Trong kiến trúc Router và Switch truyền thống, các chức năng của Control Plane và Data Plane xảy ra trong cùng một thiết bị. Quyết định định tuyến và chuyển tiếp gói là trách nhiệm của hệ điều hành thiết bị. Trong SDN, việc quản lý Control Plane được chuyển sang một Controller trung tâm. Hình so sánh kiến trúc truyền thống và SDN:



SDN Controller là một thực thể logic cho phép quản trị viên mạng quản lý và ra lệnh các Data Plane của Router và Switch sẽ xử lý lưu lượng mạng như thế nào. Nó phối hợp, trung gian và tạo điều kiện giao tiếp giữa các ứng dụng và các phần tử mạng.

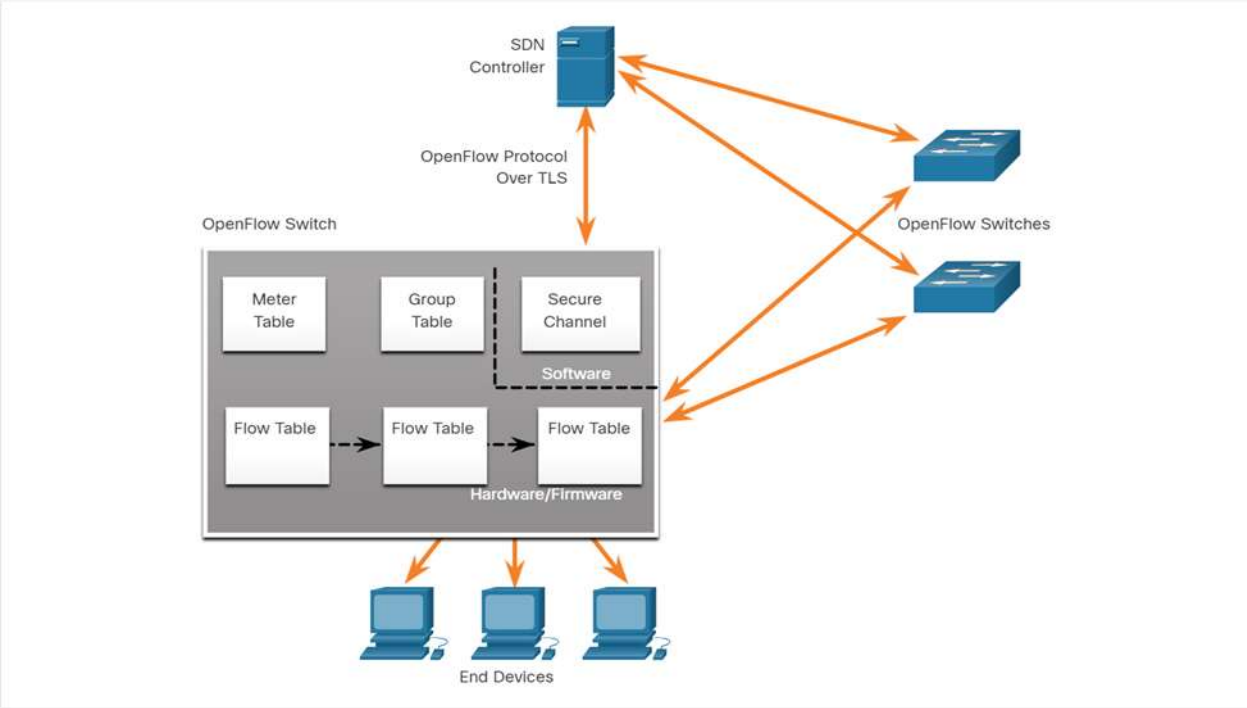


Lưu ý việc sử dụng API trong khuôn khổ SDN. API là một tập hợp các yêu cầu được tiêu chuẩn hóa xác định cách thích hợp để một ứng dụng yêu cầu dịch vụ từ một ứng dụng khác. SDN Controller sử dụng các Northbound API để giao tiếp với các ứng dụng upstream. Các API này giúp quản trị viên mạng định hình lưu lượng và triển khai các dịch vụ. Các Southbound API được sử dụng để xác định hành vi của các Data Plane trên các Router và Switch downstream.

SDN Controller and Operations:

SDN Controller xác định các luồng dữ liệu giữa Control Plane trung tâm và các Data Plane trên các router và switch riêng lẻ. Mỗi luồng (Flow) đi qua mạng trước tiên phải được phép từ SDN Controller. Nó xác minh rằng giao tiếp được cho phép theo chính sách mạng (Network Policy). Nếu bộ điều khiển cho phép một luồng, nó sẽ tính toán lộ trình cho luồng đó và thêm entry cho luồng đó trong mỗi Switch dọc theo đường dẫn.

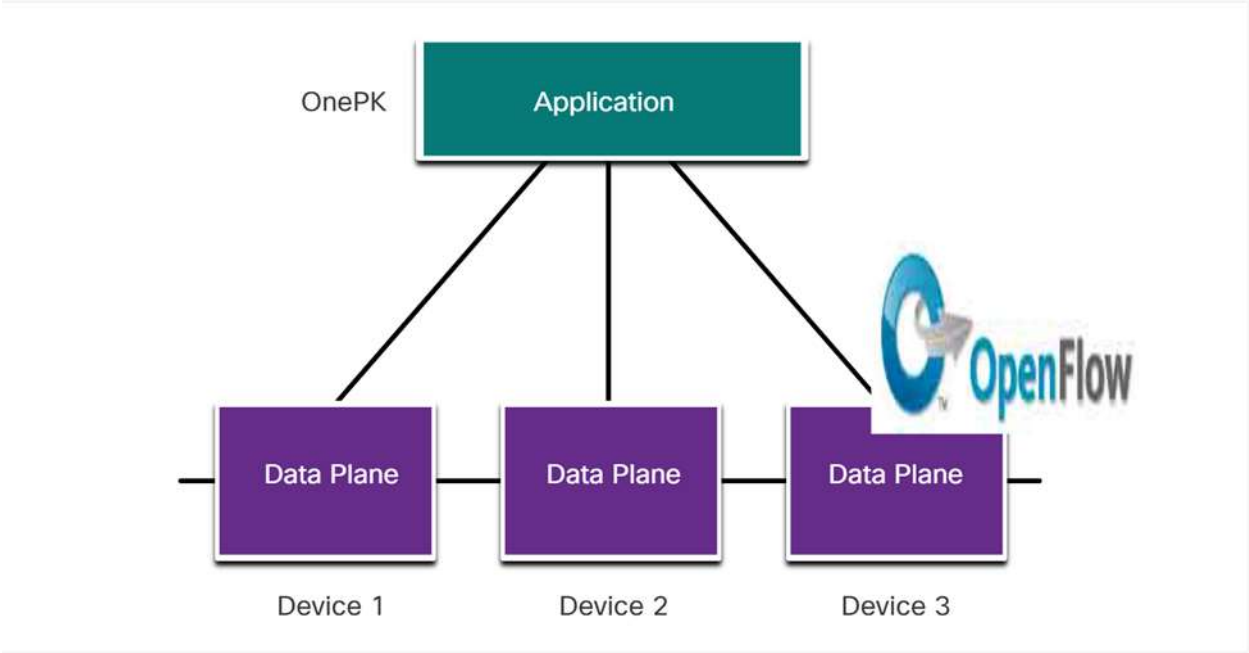
Tất cả các chức năng phức tạp được thực hiện bởi bộ điều khiển. Bộ điều khiển điền vào các Flow Table. Các switch quản lý các bảng lưu lượng.



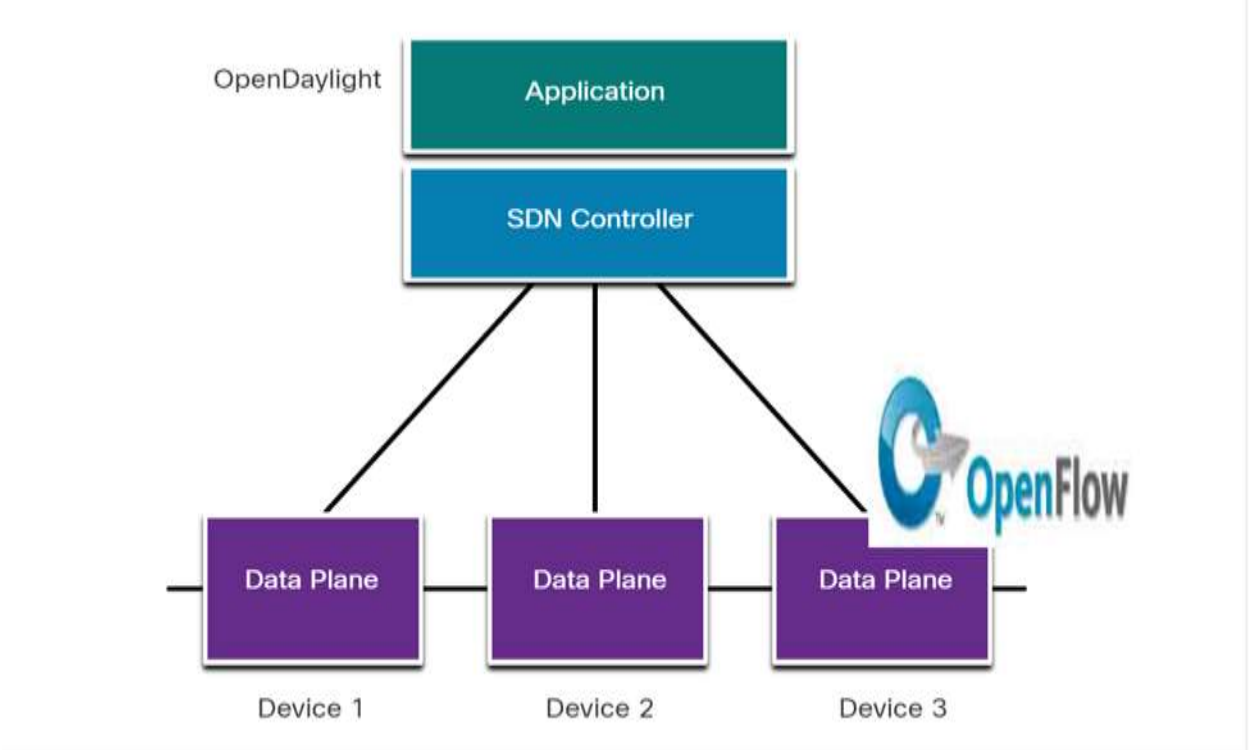
Trong mỗi Switch, một loạt các bảng được triển khai trong phần cứng hoặc Firmware được sử dụng để quản lý các luồng gói thông qua Switch. Đối với Switch, một luồng là một chuỗi các gói khớp với một entry cụ thể trong Flow Table.

Các loại SDN:

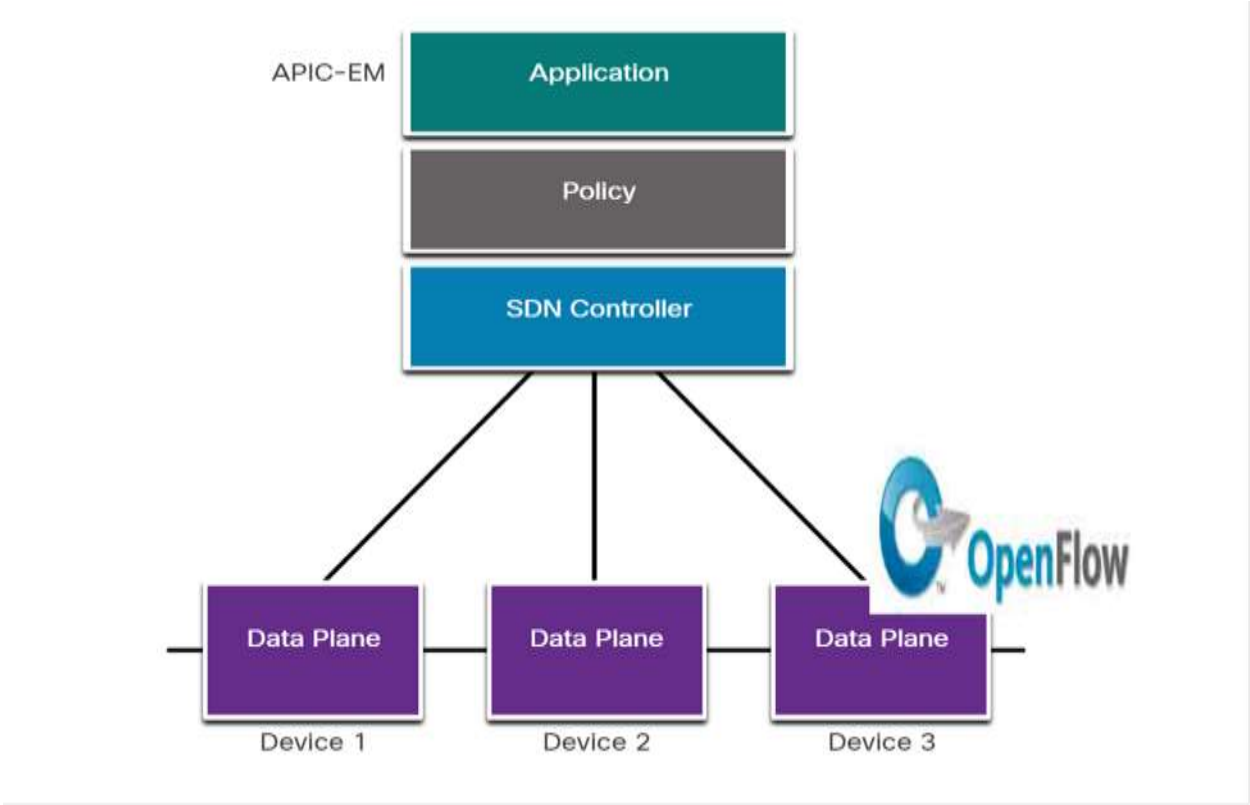
- **Device-based SDN:** Trong loại SDN này, các thiết bị có thể lập trình được bằng các ứng dụng chạy trên chính thiết bị hoặc trên máy chủ trong mạng, như thể hiện trong hình. Cisco OnePK là một ví dụ về Device-based SDN. Nó cho phép các lập trình viên xây dựng các ứng dụng bằng C và Java với Python để tích hợp và tương tác với các thiết bị của Cisco.



- **Controller-based SDN:** Loại SDN này sử dụng bộ điều khiển tập trung có thông tin về tất cả các thiết bị trong mạng. Các ứng dụng có thể giao tiếp với bộ điều khiển chịu trách nhiệm quản lý thiết bị và điều khiển các luồng lưu lượng trên toàn mạng. OpenDaylight là một ví dụ về loại SDN này.



- **Policy-based SDN:** Loại SDN này tương tự như Controller-based SDN trong đó bộ điều khiển tập trung có chế độ xem tất cả các thiết bị trong mạng. Policy-based SDN bao gồm một Policy Layer bổ sung hoạt động ở mức trừu tượng cao hơn. Nó sử dụng các ứng dụng tích hợp để tự động hóa các tác vụ cấu hình nâng cao thông qua các quy trình được hướng dẫn và GUI thân thiện với người dùng. Cisco APIC-EM là một ví dụ về loại SDN này.

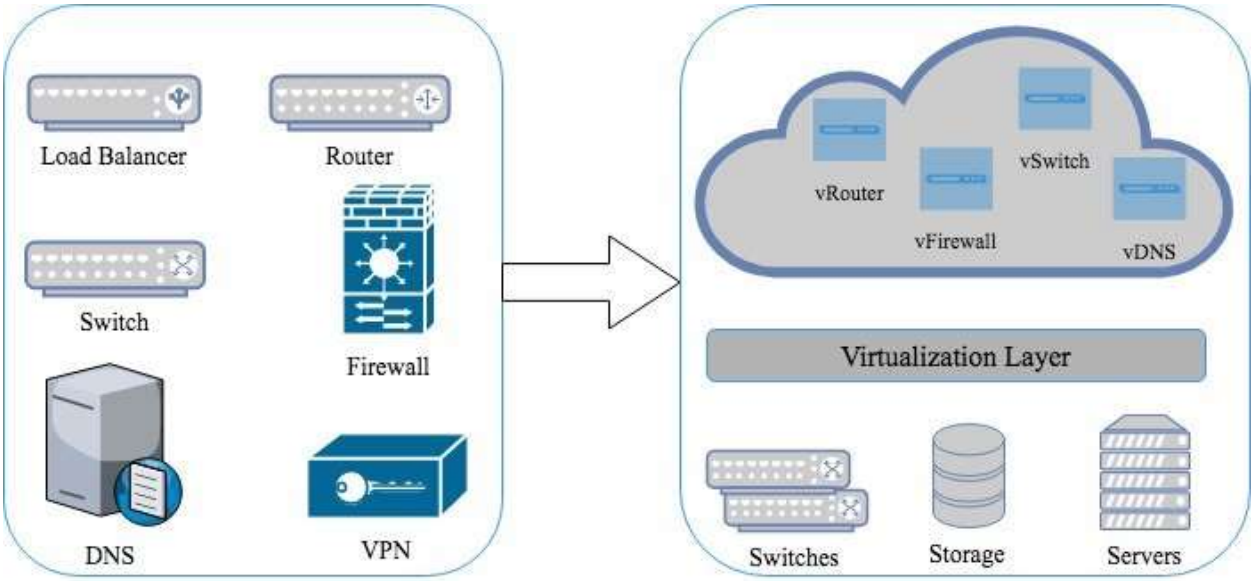


2.2. Network Function Virtualization (NFV):

Network Function Virtualization (NFV) là một công nghệ mạng ảo hóa cho phép các chức năng mạng được triển khai dưới dạng các máy ảo trên nền tảng phần cứng thông thường, thay vì sử dụng các thiết bị mạng vật lý truyền thống. NFV sử dụng các máy chủ phần cứng tiêu chuẩn để cài đặt các chức năng mạng ảo (Virtual Network Function - VNF), qua đó có thể được theo dõi và mở rộng dựa trên nhu cầu sử dụng.

NFV cho phép các chức năng mạng, chẳng hạn như NAT, Firewall, Intrusion Detection, DNS, Caching, v.v. được cài đặt trên các máy ảo, giúp tăng tính linh hoạt và hiệu quả trong việc triển khai và quản lý mạng. Các thiết bị vật lý lúc này không còn là các

phần cứng độc quyền của các hãng nữa, mà có thể là các server, switch và thiết bị lưu trữ được sản xuất hàng loạt theo các tiêu chuẩn công nghiệp chung. Việc này sẽ giúp ta giảm chi phí đầu tư và sự phụ thuộc vào các thiết bị phần cứng chuyên biệt của từng hãng. Đồng thời, các nhà mạng có thể khởi tạo, điều phối và di dời các hàm chức năng mạng, các dịch vụ mạng một cách linh hoạt, từ đó tận dụng tốt hơn hạ tầng phần cứng đã đầu tư. Không chỉ chi phí đầu tư mà cả chi phí vận hành, bảo dưỡng và nâng cấp thiết bị sau này cũng sẽ được cắt giảm đáng kể.



Traditional Network Approach NFV Approach

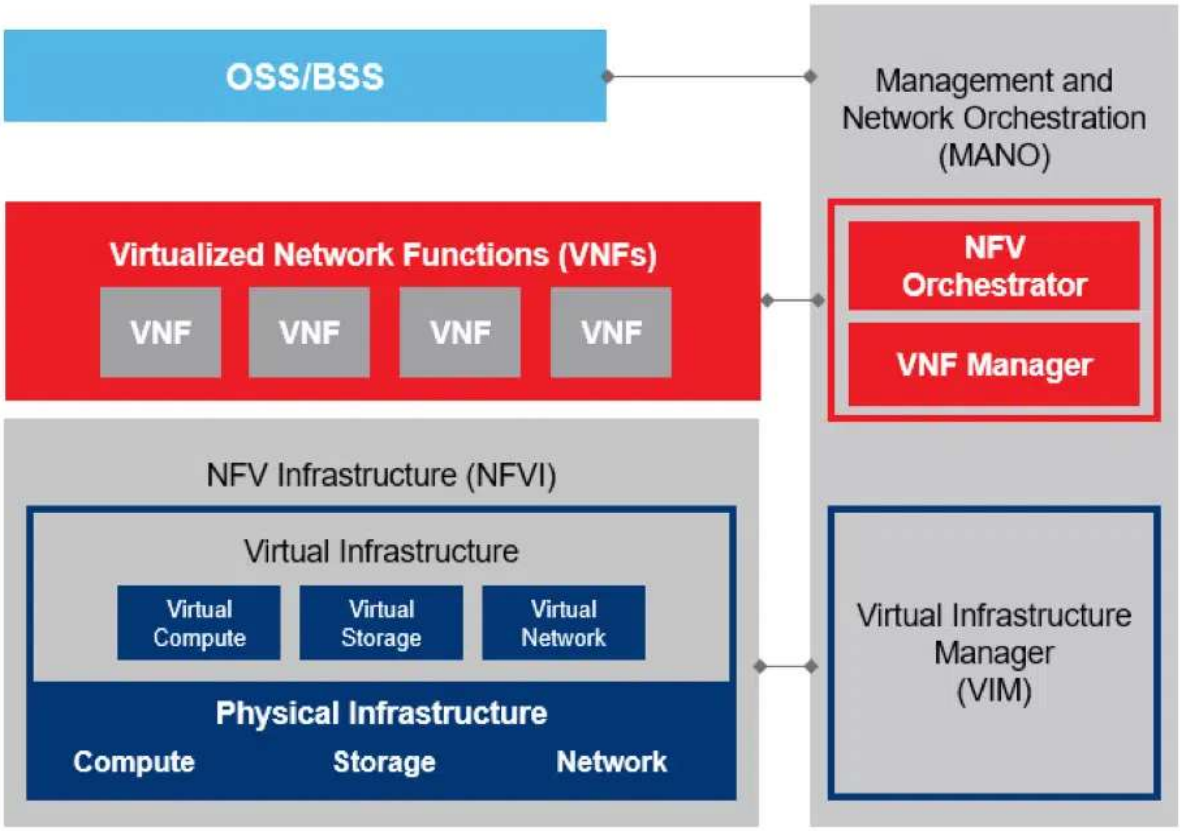
Các chức năng mạng trong NFV được triển khai trên các máy ảo thông qua một môi trường ảo hóa, như KVM (Proxmox, Unraid) hoặc VMware (ESXi). Các chức năng mạng này được cài đặt trên các máy ảo và được quản lý bởi một trung tâm điều khiển (Ví dụ như VMware vCenter), giúp tối ưu hóa việc cấu hình, triển khai và quản lý các chức năng mạng.

Kiến trúc NFV bao gồm ba thành phần chính: Chức năng mạng ảo hóa (VNF), Cơ sở hạ tầng NFV (NFVI) và Quản lý và điều phối NFV (MANO). Các VNF đóng gói các chức năng mạng dưới dạng các phiên bản phần mềm, NFVI cung cấp cơ sở hạ tầng ảo hóa cơ bản và MANO quản lý vòng đời của các VNF và điều phối việc triển khai và cấu hình của chúng.

NFV bao gồm các thành phần chính:

- **Chức năng mạng ảo hóa (Virtual Network Functions - VNF):** Là các ứng dụng phần mềm thực hiện các chức năng mạng cụ thể, như tường lửa, cân bằng tải, hoặc định tuyến. Các VNF có thể chạy trên bất kỳ hạ tầng phần cứng nào và có thể được kết hợp để tạo ra một dịch vụ mạng hoàn chỉnh.
- **Cơ sở hạ tầng NFV (NFV Infrastructure - NFVI):** Bao gồm các phần cứng và phần mềm cung cấp môi trường để các VNF hoạt động. NFVI bao gồm các máy chủ, mạng, và hệ thống lưu trữ, cũng như phần mềm quản lý ảo hóa. NFVI trừu tượng hóa các tài nguyên phần cứng và cung cấp một môi trường ảo hóa để chạy các VNF.
- **Quản lý và điều phối NFV (NFV Management and Orchestration - NFV MANO):** Là hệ thống quản lý chịu trách nhiệm cho việc triển khai, quản lý, và điều phối các VNF và NFVI. NFV MANO bao gồm ba thành phần chính:
    - *NFV Orchestrator (NFVO):* quản lý vòng đời, quản lý tài nguyên và xác thực cũng như ủy quyền các yêu cầu tài nguyên NFVI.
    - *VNF Manager (VNFM):* kiểm soát việc quản lý vòng đời của các phiên bản VNF, cung cấp vai trò điều phối và thích ứng cho cấu hình và báo cáo hoạt động của NFVI và Hệ thống quản lý mạng.
    - *Virtualized Infrastructure Manager (VIM):* kiểm soát và quản lý các tài nguyên cơ sở hạ tầng.

Operation Support System/Business Support System (OSS/BSS): OSS dành cho quản lý mạng, lỗi, cấu hình và dịch vụ trong khi BSS được sử dụng để quản lý tùy chỉnh, sản phẩm và đơn hàng. OSS/BSS của một nhà điều hành cũng có thể được tích hợp với Quản lý và điều phối NFV.



Quy trình hoạt động của NFV bắt đầu bằng việc triển khai các VNF trên NFVI. NFV MANO quản lý và điều phối quá trình này, bao gồm việc khởi tạo, cấu hình, và quản lý vòng đời của các VNF.

Ví dụ, để triển khai một tường lửa ảo, tường lửa được triển khai như một VNF trên NFVI. Sau đó, NFV MANO quản lý và điều phối tường lửa, bao gồm việc khởi tạo, cấu hình, và quản lý vòng đời của nó. Tường lửa có thể được điều chỉnh linh hoạt để đáp ứng nhu cầu thay đổi của mạng. NFV MANO cũng quản lý và điều phối NFVI, bao gồm việc quản lý tài nguyên, cấu hình và quản lý vòng đời của các phần cứng và phần mềm trong NFVI.

2.3. SDN và NFV

Nếu như khái niệm NFV xuất phát từ nhu cầu của các nhà cung cấp dịch vụ muốn giảm bớt chi phí đầu tư các thiết bị phần cứng bằng cách ảo hóa các thiết bị mạng để có thể triển khai các dịch vụ mạng trên phần cứng phổ thông, thì SDN lại xuất phát từ các

trường đại học, viện nghiên cứu, data center muốn tách bạch việc điều khiển mạng khỏi các thiết bị vật lý, để dễ dàng cấu hình, quản lý tập trung một lượng lớn các thiết bị này.

Về bản chất, hai công nghệ này là độc lập với nhau. Bên này có thể áp dụng được vào thực tiễn mà không cần phụ thuộc vào bên kia. Thật khó để nói được SDN hay NFV, công nghệ nào tốt hơn vì chúng phục vụ cho những mục đích khác nhau.

Vài nét so sánh giữa SDN và NFV:

Tiêu chí so sánh	SDN	NFV
Mục đích	Phân tách giữa control plane và data plane, quản lý tập trung, cấu hình mạng bằng cách lập trình	Chuyển dời các chức năng mạng từ phần cứng chuyên dụng sang các thiết bị phổ thông.
Đối tượng phục vụ	Các viện nghiên cứu, trung tâm dữ liệu	Các nhà cung cấp dịch vụ mạng.
Thiết bị	Máy chủ, thiết bị chuyển mạch phổ thông	Máy chủ, thiết bị chuyển mạch và lưu trữ phổ thông
Ứng dụng	Điều phối mạng. Quản lý luồng traffic đi qua các thiết bị.	Ảo hóa các thiết bị mạng như: router, firewall, CDN,… Khởi tạo và triển khai hàng loạt các thiết bị ảo.
Tổ chức chuẩn hóa	Open Networking Forum	ETSI NFV Working Group

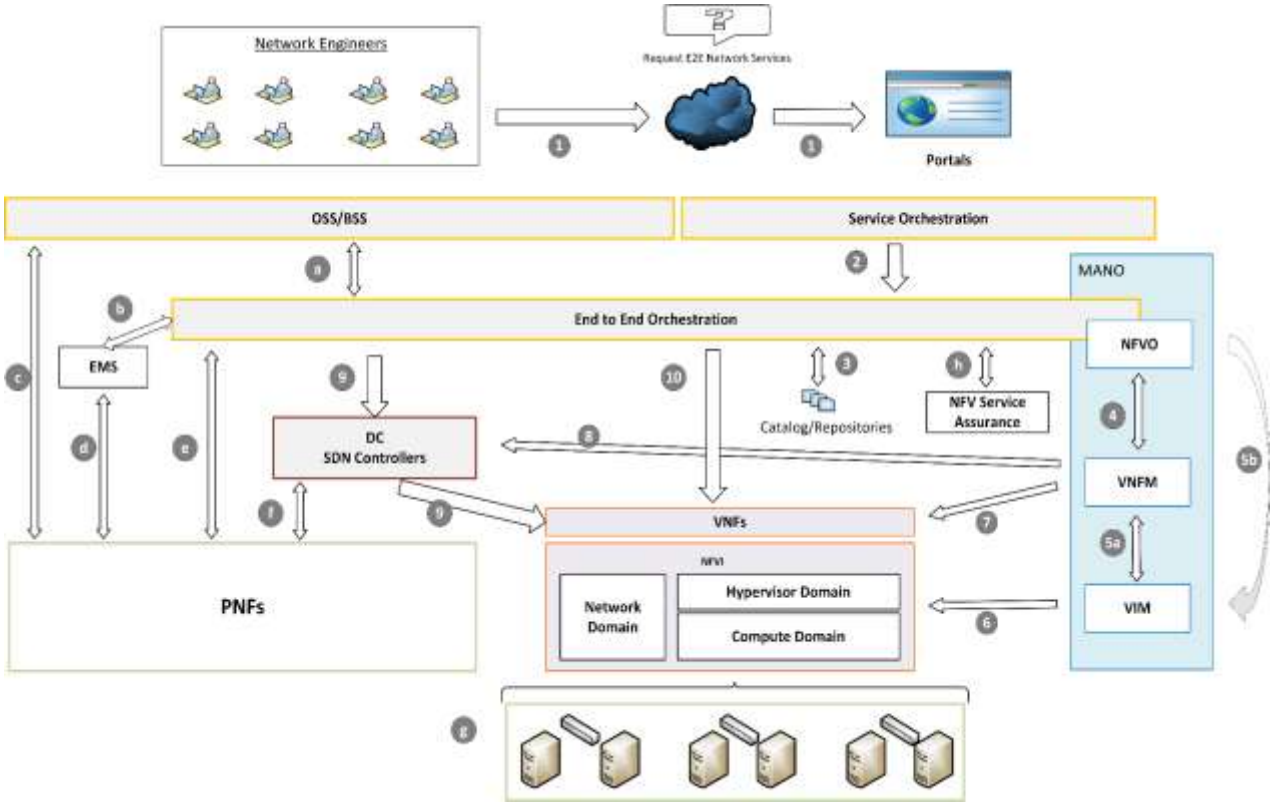
Mục tiêu chung của cả SDN và NFV là điều khiển hạ tầng mạng dễ dàng hơn, tiết kiệm chi phí và hạn chế việc tương tác trực tiếp với các thiết bị phần cứng. Như vậy, ta có thể thấy rằng hai công nghệ này không hề đối chọi với nhau mà còn lại bổ sung, hoàn thiện lẫn nhau, tạo nên 1 giải pháp hoàn chỉnh cho ngành viễn thông.

Việc quản lý tập trung của SDN kết hợp với khả năng ảo hóa các thiết bị mạng của NFV sẽ đem lại những lợi ích vô cùng lớn với hạ tầng viễn thông. Đặc biệt là việc chuẩn bị cho công nghệ 5G sắp tới thì việc ứng dụng 2 công nghệ này tạo nên nền tảng cho 5G (theo như AT&T).

Kết hợp SDN và NFV:

Mục tiêu chính của công nghệ NFV chính là khởi tạo và cấu hình các thiết bị mạng một cách nhanh chóng. Tuy công nghệ NFV có thể điều chỉnh luồng dữ liệu khi khởi tạo các thiết bị mạng nhưng khó có thể điều chỉnh lại các luồng dữ liệu đã được thiết lập này. Chưa kể đến một số tính năng nâng cao như lọc gói tin, header, QoS thì các giải pháp NFV hiện nay vẫn còn thiếu rất nhiều tính năng và không thể so sánh được với công nghệ SDN, vốn chuyên dùng để điều chỉnh các luồng dữ liệu.

Chính vì vậy, kết hợp SDN vào hạ tầng NFV chính là lời giải đáp cho vấn đề này.



Mô hình kiến trúc tổng quan 1 hạ tầng NFV + SDN do Verizon đề ra

(xem bảng chú thích bên dưới)

Trong mô hình này việc điều chỉnh luồng dữ liệu sẽ được chia làm 2 giai đoạn:

- **Giai đoạn 1:** là giai đoạn khởi tạo ban đầu do khối MANO của NFV đảm nhận. Cụ thể, thông tin về đường mạng, các liên kết giữa các VNF/VNFC cũng như việc kết

nối chúng lại thành VNFFG rồi từ đó trở thành NS hoàn chỉnh sẽ được thể hiện trong các tập tin đặc tả. Khối MANO sẽ đọc cái tập tin này, cấp phát tài nguyên rồi khởi tạo thành dịch vụ mạng hoàn chỉnh.

- **Giai đoạn 2:** là giai đoạn sau khởi tạo. Sau khi hệ thống đã được triển khai hoàn chỉnh, việc điều chỉnh luồng lúc này sẽ được giao cho SDN Controller phụ trách. Khi xuất hiện luồng dữ liệu thỏa các tập rule đã định nghĩa từ trước, SDN Controller sẽ điều chỉnh luồng dữ liệu đi qua các node VNF theo một lộ trình đã được định sẵn trong các VNFFG. Người điều khiển hoàn toàn có thể lập trình sẵn hoặc điều chỉnh lại các tập rule để điều chỉnh luồng cho thích hợp với yêu cầu dịch vụ.

Bảng chú thích 1:

STT	Mô tả
1	Network Engineers khởi tạo một dịch vụ hoàn chỉnh thông qua portal (giao diện đồ họa hoàn chỉnh). Portal này sẽ có sẵn danh sách các dịch vụ mà hệ thống hỗ trợ (NAT, VPN, Load Balancer…) cùng các thông số đi kèm.
2	Các thông tin, thông số của dịch vụ được End-to-End Orchestrator (EEO) tiếp nhận.
3	EEO lấy thông tin mô tả dịch vụ (End-to-End Service Descriptor) từ các file template được định nghĩa trước. Việc này nhằm xác định lượng tài nguyên cần thiết và vị trí cài đặt các VNF mới.
4	NFVO (lúc này là một thành phần trong EEO) và VNFM liên lạc với nhau để thực hiện các bước chuẩn bị để khởi tạo VNF như: kiểm tra lượng tài nguyên khả dụng, cấp phép cấp phát tài nguyên,..
5a	VNFM liên hệ với VIM để yêu cầu tạo các máy ảo cần thiết để cho VNF chạy lên. (VNFM driven).
5b	NFVO liên hệ với VIM để yêu cầu tạo các máy ảo cần thiết để cho VNF chạy lên. (NFVO driven).
6	VIM liên hệ với NFVI để yêu cầu tài nguyên phần cứng cần thiết nhằm khởi tạo VM.
7	VNFM tiến hành cài đặt VNF lên các VM vừa được tạo.

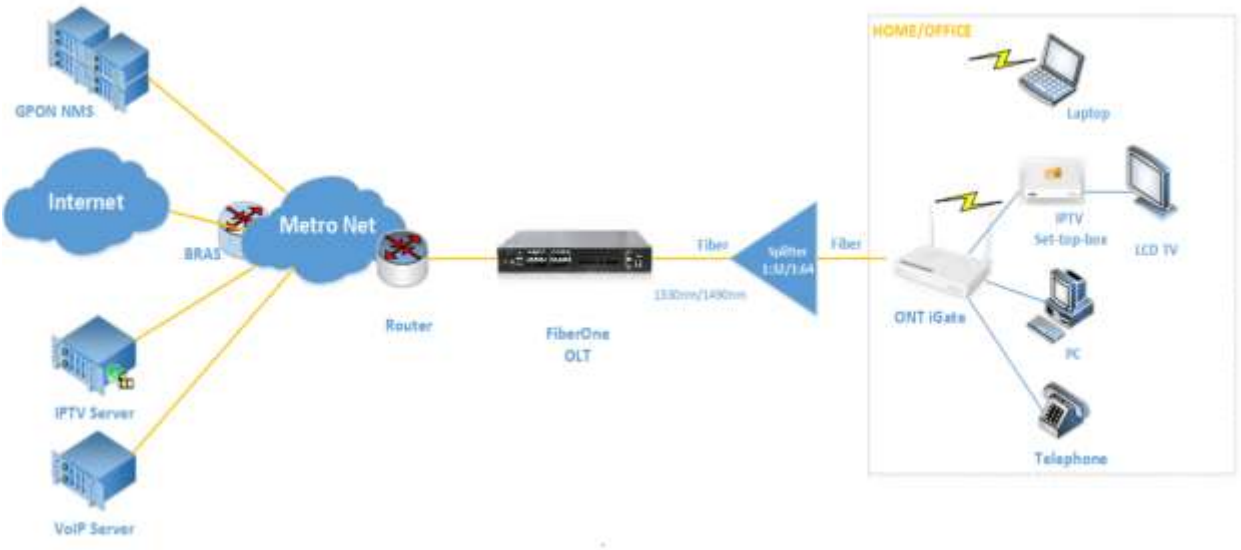
8	Đối với những VNFs nào gồm nhiều VM, VNFM sẽ yêu cầu SDN Controller để tạo kết nối giữa các VM trong cùng một VNF.
9	EEO yêu cầu SDN Controller để tạo kết nối giữa các VNF lại thành một chuỗi dịch vụ hoàn chỉnh.
10	EEO cung cấp các thông tin đặc thù của khách hàng xuống cho các hàm dịch vụ mạng. Ví dụ như tập rule đối với Firewall, IDS,..

Bảng chú thích 2:

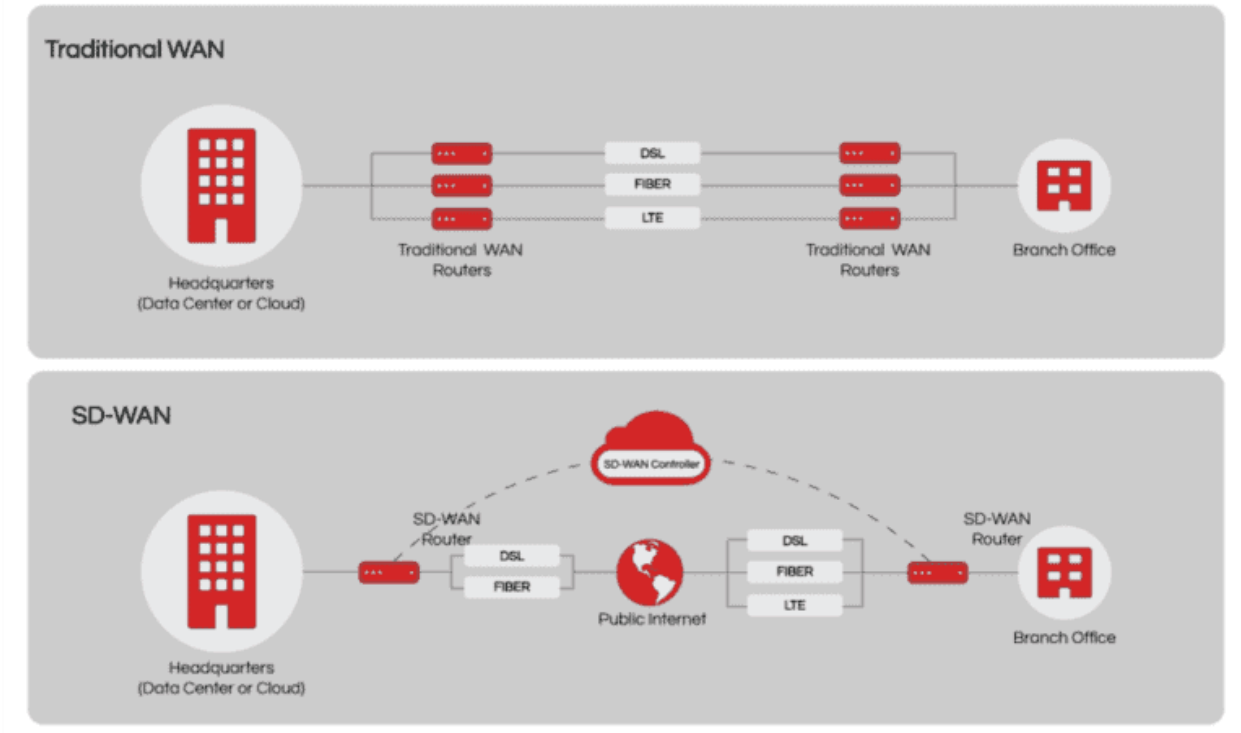
Luồng	**Mô tả**
a	OSS/BSS liên hệ với EEO để yêu cầu dịch vụ
b	EEO thông qua EMS để quản lý các thiết bị mạng vật lý (PNFs)
c	OSS/BSS quản lý trực tiếp các PNFs bên dưới
d	EMS quản lý PNFs
e	EEO quản lý trực tiếp PNFs bên dưới
f	SDN Controller tạo kết nối giữa PNFs – PNFs hoặc giữa PNFs – VNFs. Tận dụng lại hạ tầng mạng sẵn có.
g	Phần cứng bên dưới của NFVI gồm các switch, server có hiệu năng cao, ko phụ thuộc vào công nghệ của các hãng (high volume servers, switches).
h	Service Assurance (SA) thu thập thông tin alarm, monitor hệ thống. Những thông tin này có thể được dùng để sửa lỗi, phân tích tình hình…

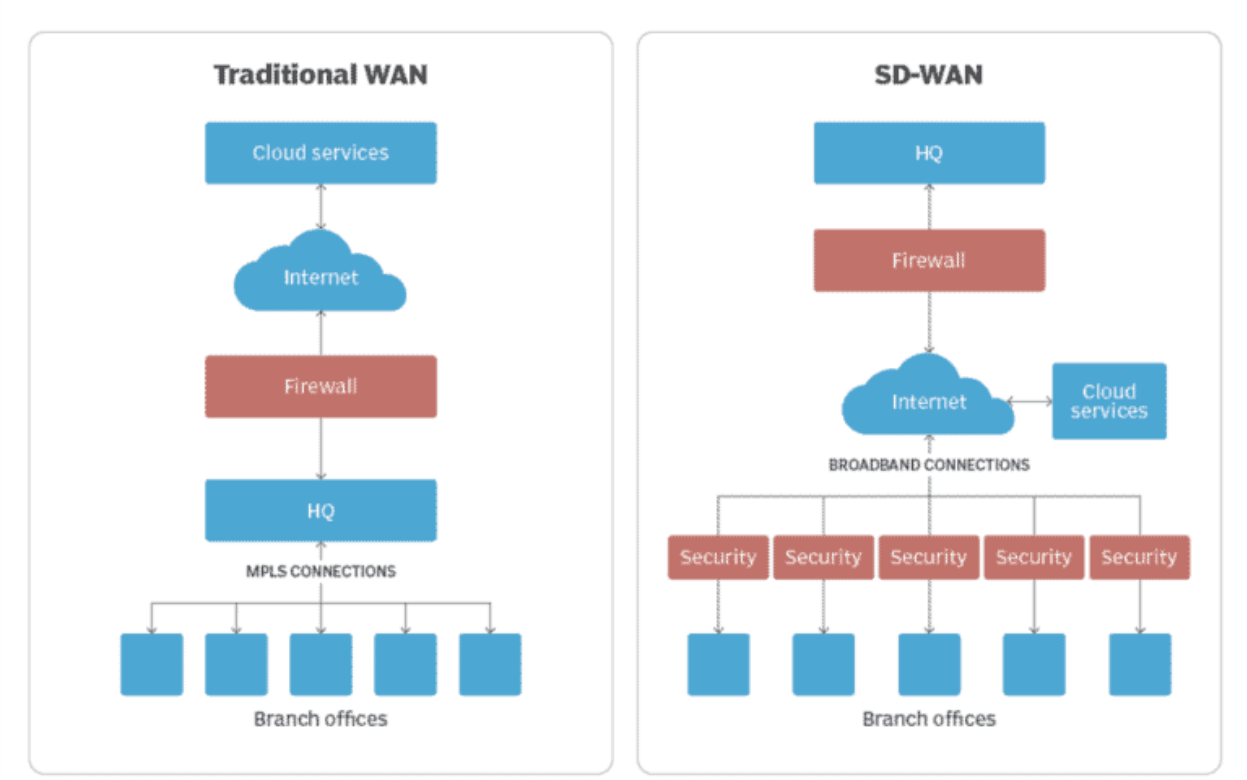
3. Mô hình triển khai ảo hóa mạng thực tế

- Các ISP ở Việt Nam chia các dịch vụ như Internet, Truyền hình (IPTV), Điện thoại (VoIP) thành các mạng khác nhau, được tag VLAN khác nhau, sau đó thiết lập VLAN cho các cổng ở thiết bị đầu cuối của khách hàng (ONU)



- FPT Cloud Edge đang cung cấp giải pháp SD-WAN, sử dụng thiết bị EdgeConnect của Aruba để giúp các doanh nghiệp đơn giản hóa việc triển khai kết nối WAN giữa các văn phòng, đồng thời tận dụng mọi kết nối internet có sẵn, nhờ đó cải thiện hiệu năng kết nối WAN đồng thời giảm thiểu chi phí phát sinh khi thay thế các hình thức triển khai mạng WAN riêng tư như MPLS (Multiprotocol Label Switching) truyền thống.





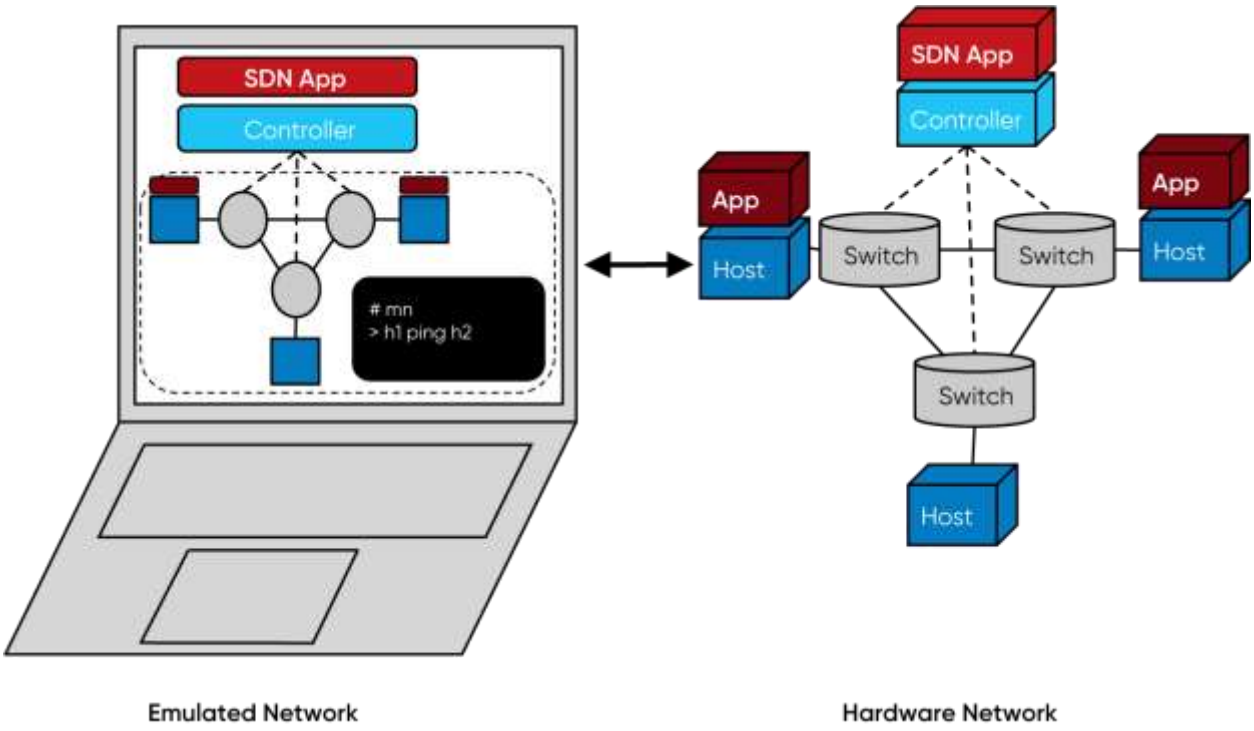
4. Demo

4.1. Mục đích

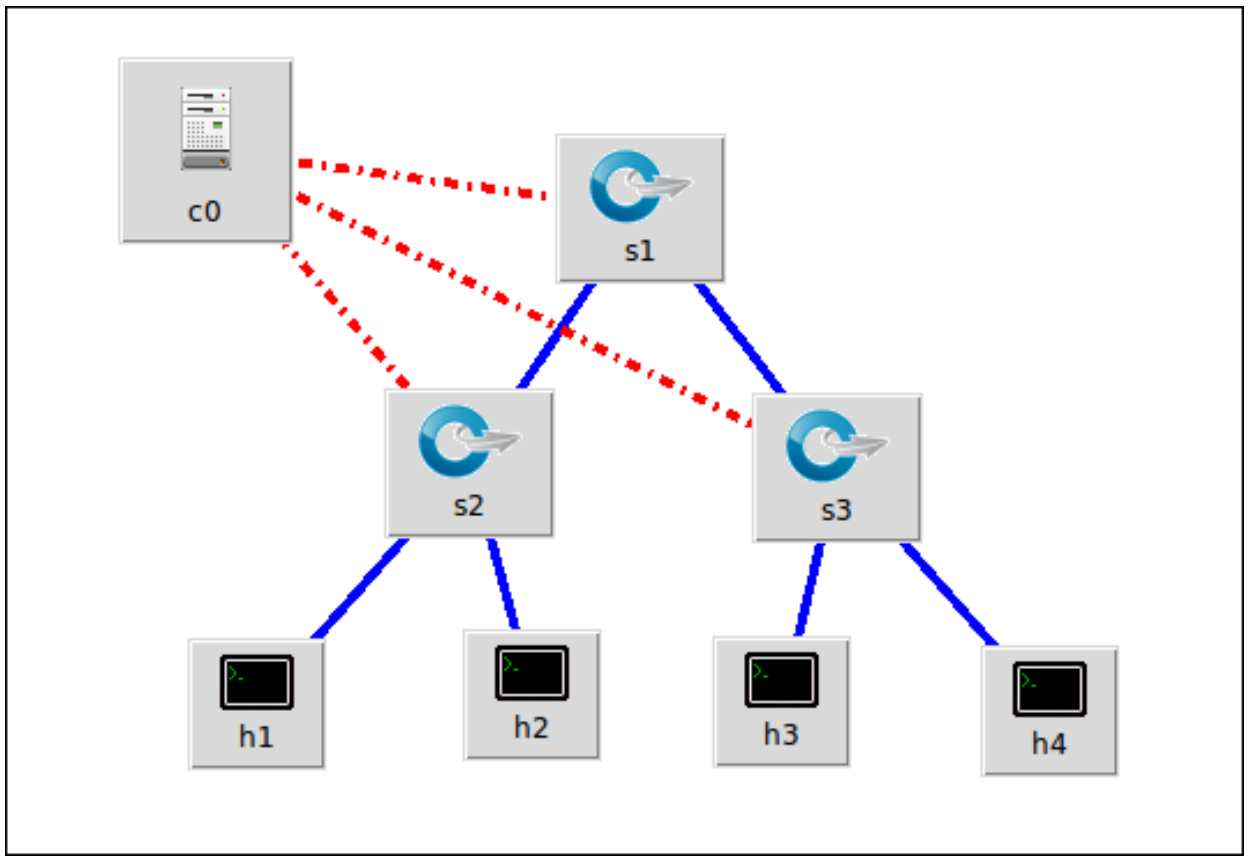
Demo giới thiệu về khả năng triển khai một mô hình SDN bằng Mininet với cấu hình có sẵn, có thể dễ dàng thay đổi, mở rộng hoặc thu nhỏ theo nhu cầu, đồng thời giới thiệu khả năng tích hợp các thiết bị vật lý, qua đó máy khách có thể tham gia vào mạng đã triển khai như một mạng truyền thống. Ngoài ra demo còn giới thiệu về cách tích hợp một Controller ngoài sử dụng giao thức OpenFlow nhằm điều khiển mạng đã triển khai.

4.2. Lý thuyết

4.2.1. Mininet



Mininet là một công cụ giả lập mạng, bao gồm tập hợp các host đầu cuối, các switch, router và các link, chạy trên một Linux Kernel. Mininet sử dụng công nghệ ảo hóa (ở mức đơn giản) để tạo nên hệ thống mạng hoàn chỉnh, chạy chung trên cùng một kernel và user code. Các host ảo, switch, liên kết và các controller trên mininet là các thực thể được giả lập bằng phần mềm thay vì phần cứng.

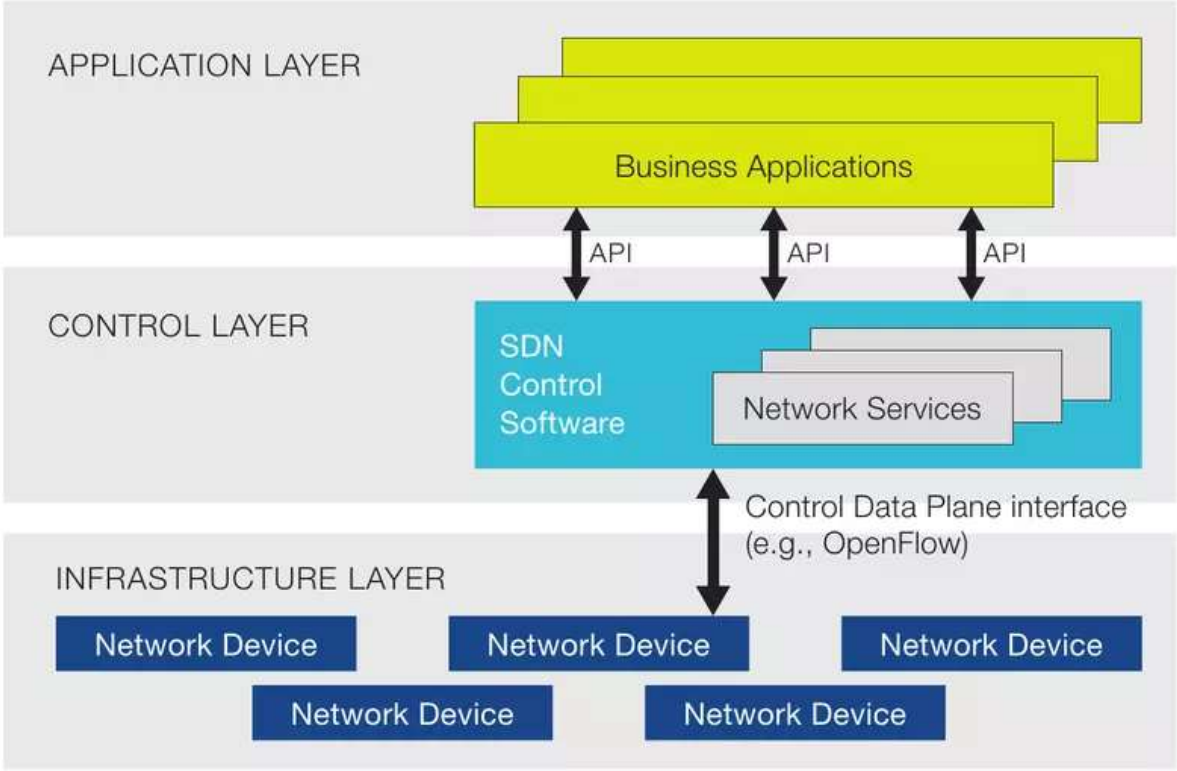


Mininet cho phép tạo và tùy chỉnh topo mạng nhanh chóng; chạy được các dịch vụ thực như web servers, TCP monitoring, Wireshark; tùy chỉnh được việc chuyển tiếp gói tin. Mininet không yêu cầu cấu hình đặc biệt gì về phần cứng để chạy, có thể cài trên máy vật lý hoặc VM bất kỳ.

4.2.2. Kiến trúc SDN

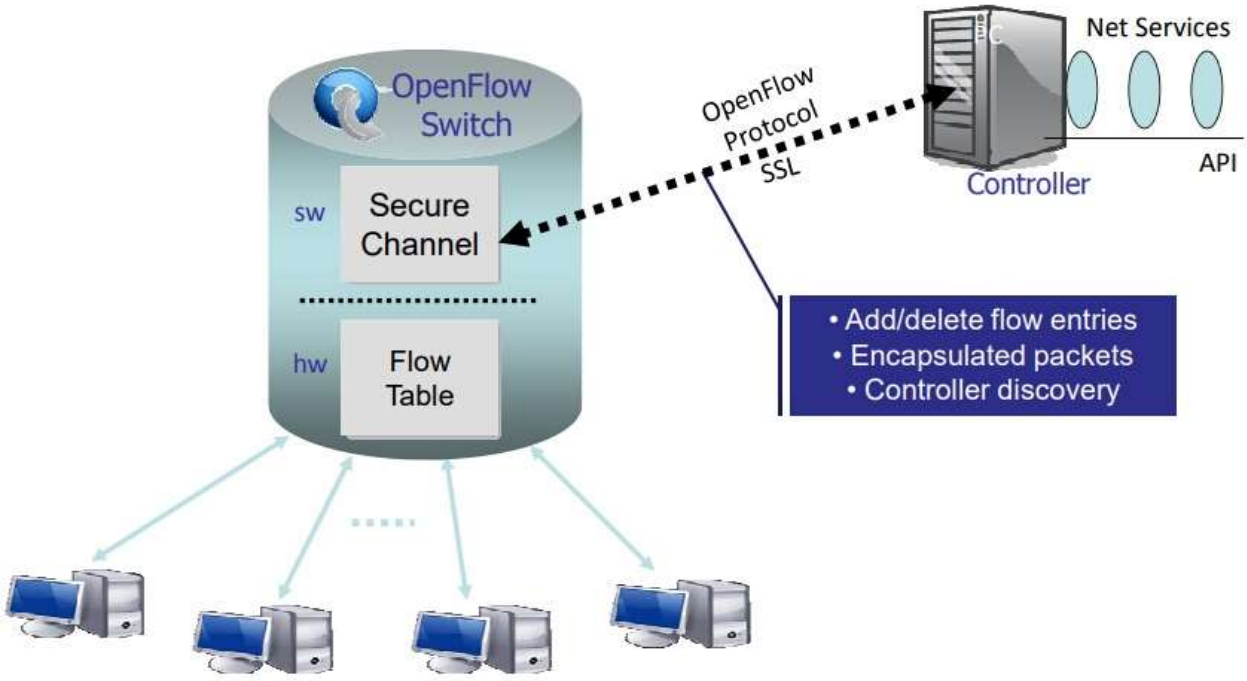
- Lớp ứng dụng: Là các ứng dụng được triển khai trên mạng, giao tiếp với lớp điều khiển thông qua các API, từ đó cho phép lớp ứng dụng cấu hình lại mạng (điều chỉnh các tham số trễ, băng thông, định tuyến, v.v.) thông qua lớp điều khiển.
- Lớp điều khiển: Là nơi tập trung các bộ điều khiển, thực hiện việc điều chỉnh cấu hình mạng theo các yêu cầu từ lớp ứng dụng và khả năng của mạng. Các bộ điều khiển này có thể là phần mềm.
- Lớp cơ sở hạ tầng: Là các thiết bị mạng vật lý hoặc ảo hóa, thực hiện việc chuyển tiếp gói tin theo sự điều khiển của lớp điều khiển. Một thiết bị mạng

có thể hoạt động theo sự điều khiển của nhiều bộ điều khiển khác nhau, điều này giúp tăng cường khả năng ảo hóa của mạng.

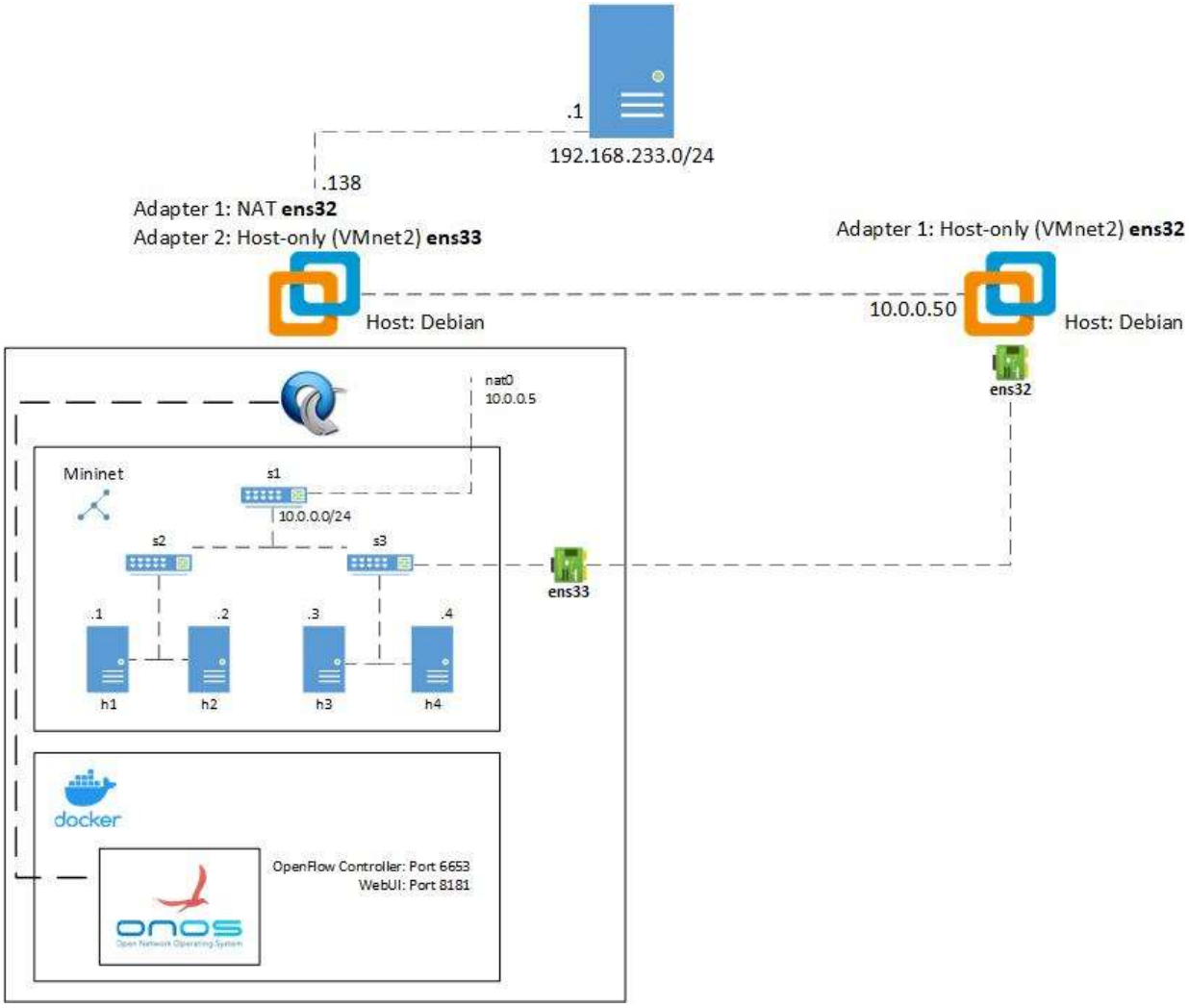


4.2.3. OpenFlow

OpenFlow là một giao thức mạng phần mềm được sử dụng trong việc quản lý và điều khiển các mạng mở. Được phát triển bởi Open Networking Foundation (ONF), OpenFlow đã trở thành một tiêu chuẩn quan trọng trong việc xây dựng Software-Defined Networking (SDN), cung cấp khả năng giao tiếp giữa lớp điều khiển và lớp chuyển tiếp trong kiến trúc SDN. Thay vì dựa vào các thiết bị mạng truyền thống, OpenFlow chuyển trọng tâm điều khiển vào một bộ điều khiển tách biệt, gọi là OpenFlow Controller. Bộ điều khiển này quản lý việc chuyển tiếp các gói tin trong mạng bằng cách gửi các chỉ thị OpenFlow tới các công tắc mạng (switches) tương ứng.


OpenFlow
Switch
sw
Secure
Channel
hw
Flow
Table
OpenFlow
Protocol
SSL
Net Services
API
Controller
• Add/delete flow entries
• Encapsulated packets
• Controller discovery

4.3. Topology


.1
192.168.233.0/24
.138
Adapter 1: NAT ens32
Adapter 2: Host-only (VMnet2) ens33
Host: Debian
Adapter 1: Host-only (VMnet2) ens32
10.0.0.50
Host: Debian
ens32
nat0
10.0.0.5
Mininet
s1
10.0.0.0/24
s2
s3
ens33
.1
.2
.3
.4
h1
h2
h3
h4
docker
OpenFlow Controller: Port 6653
WebUI: Port 8181
onos

Tài liệu tham khảo

"CCNA Module 13 - Network Virtualization."

"[NFV] Phần 1 - Giới thiệu về NFV." *CloudCraft*, 17 April 2018, https://cloudcraft.info/nfv-phan-1-gioi-thieu-ve-nfv/.

"[NFV] Phần 2 - Kiến trúc của NFV." *CloudCraft*, 11 July 2018, https://cloudcraft.info/nfv-phan-2-kien-truc-cua-nfv/.

"[NFV] NFV và SDN." *CloudCraft*, 12 July 2018, https://cloudcraft.info/nfv-va-sdn/.

Santana, Gustavo AA. "VMware NSX® Network Virtualization Fundamentals." *VMware*, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-network-virtualization-fundamentals-guide.pdf.

"Van-Hoang-Kha/Software-Defined-Networking: Software Defined Networking." *GitHub*, https://github.com/Van-Hoang-Kha/Software-Defined-Networking.