Software Defined Networking

Tugberk Goc
Student Id: 115200084

Table of Contents

1. Software-Defined Networking

Software-defined networking (SDN) is an architecture that intends to make networks agile, flexible and adaptable. The objective of SDN is to improve network control by enabling enterprises and service providers to react rapidly to changing business necessities.

In a software-defined networking, a network engineer or administrator who has access to the system can change traffic from a centralized control console without having to touch individual switches in the network such as Cisco switches. The centralized SDN controller directs the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices.

This process is a move away from traditional network architecture, in which individual network devices make traffic decisions based on their configured routing tables.

2. SDN architecture

A regular portrayal of SDN design contains three layers: the application layer, the control layer and the infrastructure layer.

SDN architecture separates the network into three distinguishable layers, connected through northbound and southbound APIs.

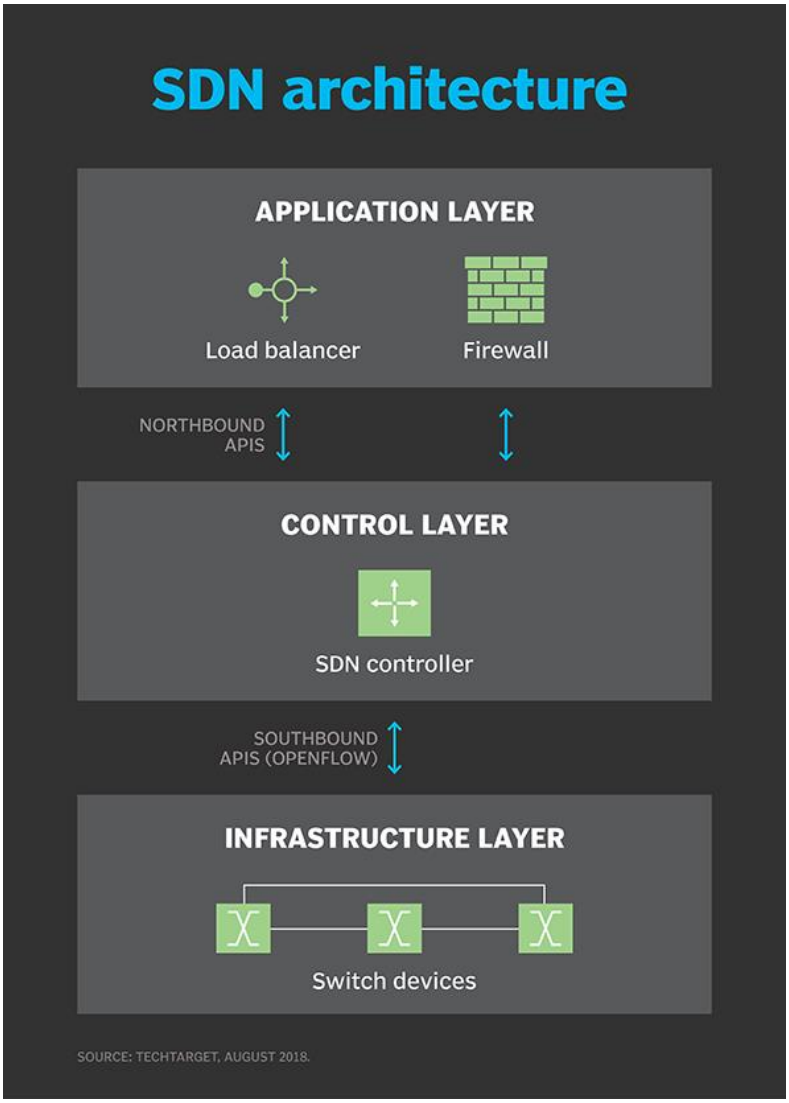


Figure 01: SDN Architecture

2.1 Application Layer

The application layer, not surprisingly, contains the typical network applications or functions organizations use, which can include intrusion detection systems, load balancing or firewalls. Where a traditional network would use a specialized appliance, such as a firewall or load balancer, a software-defined network replaces the appliance with an application that uses the controller to manage data plane behavior.

2.2 Control Layer

The control layer represents the centralized SDN controller software that acts as the brain of the software-defined network. This controller resides on a server and manages policies and the flow of traffic throughout the network.

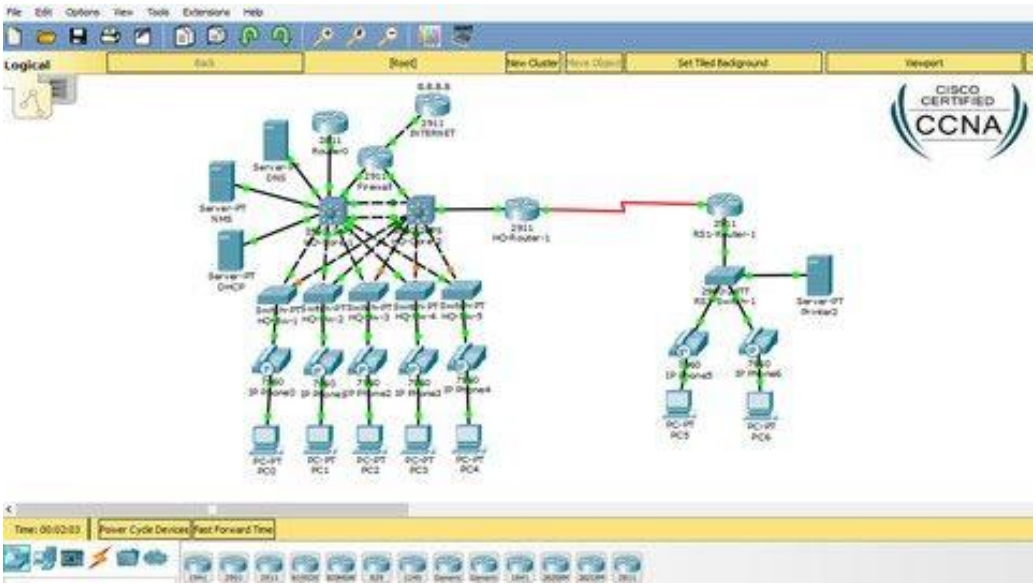


Figure 02: Cisco Packet Tracer

2.3 Infrastructure Layer

The infrastructure layer is made up of the physical switches in the network.

These three layers communicate using northbound and southbound application programming interfaces (APIs). This help them to manage their data transfer with certain rules. Northbound Interface is referred for communication with upper which is Application Layer and it would be in general realized through RESTful APIs. Southbound Interface is referred for communication with lower which is Infrastructure layer and it would be in general realized through southbound protocols such as OpenFlow, Netconf, Ovsdb and so on.

3 How SDN Works

SDN encompasses several types of technologies, including functional separation, network virtualization and automation through programmability.

Originally, SDN technology focused solely on separation of the network control plane from the data plane. While the control plane makes decisions about how packets should flow through the network, the data plane actually moves packets from place to place.

In a classic SDN scenario, a packet arrives at a network switch, and rules built into the switch's proprietary firmware tell the switch where to forward the packet. These packet-handling rules are sent to the switch from the centralized controller.

The switch -- also known as a data plane device -- queries the controller for guidance as needed, and it provides the controller with information about traffic it handles. The switch sends every packet going to the same destination along the same path and treats all the packets the exact same way.

Software-defined networking uses an operation mode that is sometimes called adaptive or dynamic, in which a switch issues a route request to a controller for a packet that does not have a specific route. This process is separate from adaptive routing, which issues route requests through routers and algorithms based on the network topology, not through a controller.

The virtualization aspect of SDN comes into play through a virtual overlay, which is a logically separate network on top of the physical network. Users can implement end-to-end overlays to abstract the underlying network and segment network traffic. This micro segmentation is especially useful for service providers and operators with Multi-tenant cloud environments and cloud services, as they can provision a separate virtual network with specific policies for each tenant.

4 Benefits of SDN

With SDN, an administrator can change any network switch's rules when necessary -- prioritizing, deprioritizing or even blocking specific types of packets with a granular level of control and security. This is especially helpful in a cloud computing multi-tenant architecture, because it enables the administrator to manage traffic loads in a flexible and more efficient manner. Essentially, this enables the administrator to use less expensive commodity switches and have more control over network traffic flow than ever before.

Other benefits of SDN are network management and end-to-end visibility. A network administrator need only deal with one centralized controller to distribute policies to the connected switches, instead of configuring multiple individual devices. This capability is also a security advantage because the controller can monitor traffic and deploy security policies. If the controller deems traffic suspicious, for example, it can reroute or drop the packets.

SDN also virtualizes hardware and services that were previously carried out by dedicated hardware, resulting in the touted benefits of a reduced hardware footprint and lower operational costs.

Additionally, software-defined networking contributed to the emergence of software-defined wide area network (SD-WAN) technology. SD-WAN employs the virtual overlay aspect of SDN technology, abstracting an organization's connectivity links throughout its WAN and creating a virtual network that can use whichever connection the controller deems fit to send traffic.

5. Challenges with SDN

Security is both a benefit and a concern with SDN technology. The centralized SDN controller presents a single point of failure and, if targeted by an attacker, can prove detrimental to the network.

Ironically, another challenge with SDN is there's really no established definition of "software-defined networking" in the networking industry. Different vendors offer various approaches to SDN, ranging from hardware-centric models and virtualization platforms to hyper-converged networking designs and controllerless methods.

Some networking initiatives are often mistaken for SDN, including white box networking, network disaggregation, network automation and programmable networking. While SDN can benefit and work with these technologies and processes, it remains a separate technology.

SDN technology emerged with a lot of hype around 2011, when it was introduced alongside the OpenFlow protocol. Since then, adoption has been relatively slow, especially among enterprises that have smaller networks and fewer resources. Also, many enterprises cite the cost of SDN deployment to be a deterring factor.

Main adopters of SDN include service providers, network operators, telecoms and carriers, along with large companies, such as Facebook and Google, all of which have the resources to tackle and contribute to an emerging technology.

6. SDN Use Cases & Cisco Packet Tracer

Some use cases for SDN include:

- DevOps -- An approach based on software-defined networking can facilitate DevOps by automating app updates and deployments, including automating IT infrastructure components as the DevOps apps and platforms are deployed.
- Campus networks -- Campus networks can be difficult to manage, especially with the ongoing need to unify Wi-Fi and Ethernet networks. SDN controllers can benefit campus networks by

offering centralized management and automation, improved security and application-level quality of service across the network.

- Service provider networks -- SDN helps service providers simplify and automate the provisioning of their networks for end-to-end network and service management and control.
- Data center security -- SDN supports more targeted protection and simplifies firewall administration. Generally, an enterprise depends on a traditional perimeter firewall to secure its entire datacenter. However, a company can create a distributed firewall system by adding virtual firewalls to protect the virtual machines. This extra layer of firewall security helps prevent a breach in one virtual machine from jumping to another. Also, SDN centralized control and automation allow the admin to view, modify and control network activity to reduce the risk of a breach to begin with.

Cisco Packet Tracer is a software-defined networking tool which is created by Cisco Company and uses for Cisco switches. It uses for controlling software defined networking architecture. (See Appendix A)

7. The Impact of SDN

Software-defined networking has had a major impact on the management of IT infrastructure and network design. As SDN technology matures, it not only changes network infrastructure design, it also changes how IT views its role, since IT management is more heavily involved throughout the decision process and redefines the entire IT infrastructure.

SDN architectures can make network control programmable, often using open protocols, such as OpenFlow. Because of this, enterprises can apply globally aware software control at the edges of their networks to access network switches and routers rather than the closed and proprietary firmware generally used to configure, manage, secure and optimize network resources.

While SDN deployments are found in every industry, the impact of the technology is strongest in technology-related fields and financial services.

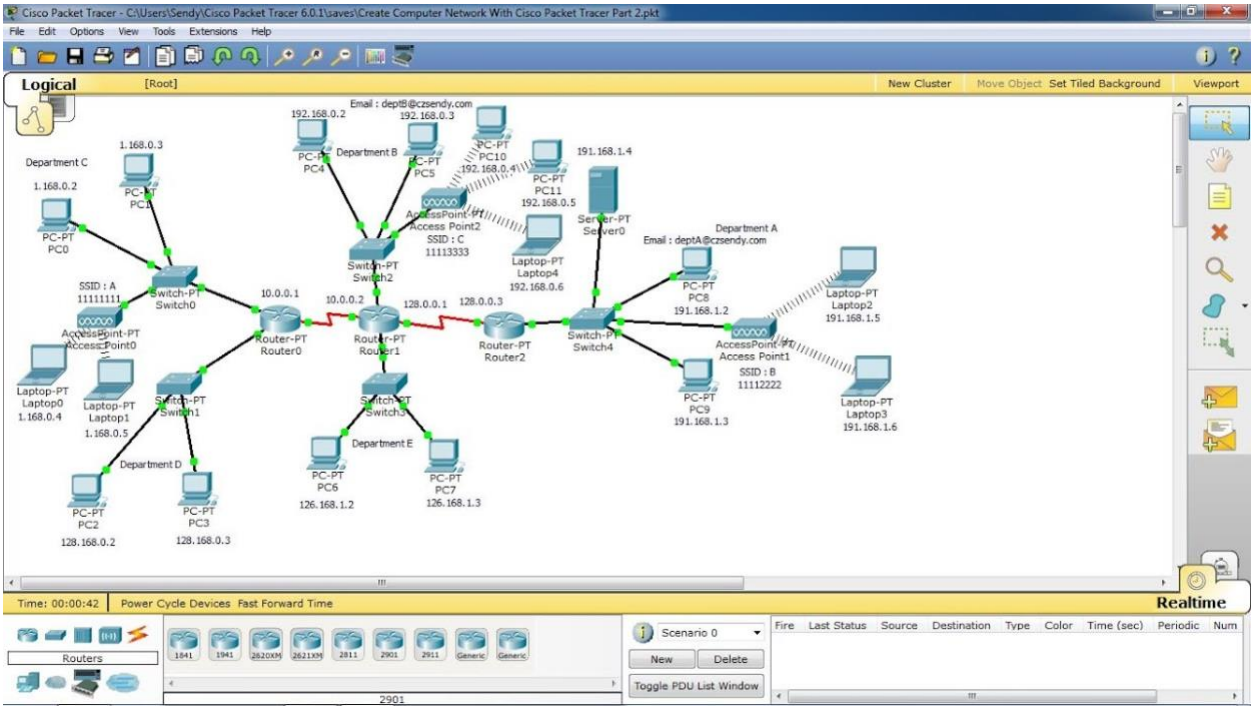
SDN is having an impact on the way telecommunications companies operate. For example, Verizon uses SDN to combine all its existing service edge routers for Ethernet and IP-based services into one platform.

The goal is to simplify the edge architecture, enabling Verizon to enhance operational efficiency and flexibility to support new functions and services. SDN will help Verizon improve network management and ultimately offer better services to its customers.

Success in the financial services sector hinges on connecting to large numbers of trading participants, low latency and a highly secure network infrastructure to power financial markets worldwide.

Nearly all of the participants in the financial market depend on legacy networks that, in part, are non-predictive, hard to manage, slow to deliver and have huge security vulnerabilities. With SDN technology, however, organizations in the financial services sector can build predictive networks to enable more efficient and effective platforms for financial trading apps.

APPENDIX A


Cisco Packet Tracer - C:\Users\Sendy\Cisco Packet Tracer 6.0.1\saves\Create Computer Network With Cisco Packet Tracer Part 2.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Department C
1.168.0.2
1.168.0.3
PC-PT PC0
PC-PT PC1
SSID : A
11111111
Switch-PT Switch0
Access Point-PT Access Point0
Laptop-PT Laptop0
1.168.0.4
Laptop-PT Laptop1
1.168.0.5
Department D
PC-PT PC2
128.168.0.2
PC-PT PC3
128.168.0.3
Switch-PT Switch1
10.0.0.1
Router-PT Router0
10.0.0.2
Router-PT Router1
128.0.0.1
128.0.0.3
Router-PT Router2
Switch-PT Switch3
Department E
PC-PT PC6
126.168.1.2
PC-PT PC7
126.168.1.3
Email : deptB@czsendy.com
192.168.0.2
192.168.0.3
Department B
PC-PT PC4
PC-PT PC5
Switch-PT Switch2
PC-PT PC10
192.168.0.4
Access Point-PT Access Point2
SSID : C
11113333
PC-PT PC11
192.168.0.5
191.168.1.4
Server-PT Server0
Laptop-PT Laptop4
192.168.0.6
Switch-PT Switch4
Department A
Email : deptA@czsendy.com
PC-PT PC8
191.168.1.2
Access Point-PT Access Point1
SSID : B
11112222
PC-PT PC9
191.168.1.3
Laptop-PT Laptop2
191.168.1.5
Laptop-PT Laptop3
191.168.1.6
Time: 00:00:42
Power Cycle Devices Fast Forward Time
Realtime
Routers
1841
1941
2620XM
2621XM
2811
2901
2911
Generic
Generic
2901
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num

REFERENCES

Arora, H. (2018) *Software Defined Networking (SDN) - Architecture and Role of OpenFlow* [online] available from <https://www.howtoforge.com/tutorial/software-defined-networking-sdn-architecture-and-role-of-openflow/>

Rouse, M. (2019) *What Is Software-Defined Networking (SDN)? - Definition from WhatIs.Com* [online] available from <https://searchnetworking.techtarget.com/definition/software-defined-networking-SDN>

Wikipedia Contributors (2019) *Packet Tracer* [online] available from <https://en.wikipedia.org/wiki/Packet_Tracer>