SDN

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. SDN can create and control a virtual network – or control a traditional hardware – via software.

While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server.

Why Software-Defined Networking is important?

SDN represents a substantial step forward from traditional networking, in that it enables the following:

- **Increased control with greater speed and flexibility:** Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.
- **Customizable network infrastructure:** With a software-defined network, administrators can configure network services and allocate virtual resources to change the network infrastructure in real time through one centralized location. This allows network administrators to optimize the flow of data through the network and prioritize applications that require more availability.
- **Robust security:** A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

The key difference between SDN and traditional networking is infrastructure: SDN is software-based, while traditional networking is hardware-based. Because the control plane is software-based, SDN is much more flexible than traditional networking. It allows administrators to control the network, change configuration settings, provision resources, and increase network capacity — all from a centralized user interface, without the need for more hardware.

There are also security differences between SDN and traditional networking. Thanks to greater visibility and the ability to define secure pathways, SDN offers better security in many ways. However, because software-defined networks use a centralized controller, securing the controller is crucial to maintaining a secure network.

How does Software-Defined Networking (SDN) work?

Here are the SDN basics: In SDN (like anything virtualized), the software is decoupled from the hardware. SDN moves the control plane that determines where to send traffic to software, and leaves the data plane that actually forwards the traffic in the hardware. This allows network administrators who use software-defined networking to program and control the entire network via a single pane of glass instead of on a device by device basis.

There are three parts to a typical SDN architecture, which may be located in different physical locations:

Applications, which communicate resource requests or information about the network as a whole

Controllers, which use the information from applications to decide how to route a data packet

Networking devices, which receive information from the controller about where to move the data

Physical or virtual networking devices actually move the data through the network. In some cases, virtual switches, which may be embedded in either the software or the hardware, take over the responsibilities of physical switches and consolidate their functions into a single, intelligent switch. The switch checks the integrity of both the data packets and their virtual machine destinations and moves the packets along.

Benefits of Software-Defined Networking (SDN)

Many of today's services and applications, especially when they involve the cloud, could not function without SDN. SDN allows data to move easily between distributed locations, which is critical for cloud applications.

Additionally, SDN supports moving workloads around a network quickly. For instance, dividing a virtual network into sections, using a technique called network functions virtualization (NFV), allows telecommunications providers to move customer services to less expensive servers or even to the customer's own servers. Service providers can use a virtual network infrastructure to shift workloads from private to public cloud infrastructures as necessary, and to make new customer services available instantly. SDN also makes it easier for any network to flex and scale as network administrators add or remove virtual machines, whether those machines are on-premises or in the cloud.

Finally, because of the speed and flexibility offered by SDN, it is able to support emerging trends and technologies such as edge computing and the Internet of Things, which require transferring data quickly and easily between remote sites.

How is SDN different from Traditional Networking?

The key difference between SDN and traditional networking is infrastructure: SDN is software-based, while traditional networking is hardware-based. Because the control plane is software-based, SDN is much more flexible than traditional networking. It allows administrators to control the network, change configuration settings, provision resources, and increase network capacity—all from a centralized user interface, without adding more hardware.

There are also security differences between SDN and traditional networking. Thanks to greater visibility and the ability to define secure pathways, SDN offers better security in many ways. However, because software-defined networks use a centralized controller, securing the controller is crucial to maintaining a secure network, and this single point of failure represents a potential vulnerability of SDN.

What are the different models of SDN?

While the premise of centralized software controlling the flow of data in switches and routers applies to all software-defined networking, there are different models of SDN.

- **Open SDN:** Network administrators use a protocol like OpenFlow to control the behavior of virtual and physical switches at the data plane level.
- **SDN by APIs:** Instead of using an open protocol, application programming interfaces control how data moves through the network on each device.
- **SDN Overlay Model:** Another type of software-defined networking runs a virtual network on top of an existing hardware infrastructure, creating dynamic tunnels to different on-premise and remote data centers. The virtual network allocates bandwidth over a variety of channels and assigns devices to each channel, leaving the physical network untouched.
- **Hybrid SDN:** This model combines software-defined networking with traditional networking protocols in one environment to support different functions on a network. Standard networking protocols continue to direct some traffic, while SDN takes on responsibility for other traffic, allowing network administrators to introduce SDN in stages to a legacy environment.