Network Virtualization Technologies

Network virtualization is the transformation of a network that was once hardware-dependent into a network that is software-based. Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud. Network virtualization is dividing or combining hardware resources that the users can make use of, and every user has his own specific perspective, these resources can be nodes or links. Network virtualization became one of the most important technologies recently, the architecture and base platform of a NV hardware is crucially looked at for its importance in implementing an advanced consumer service. It also an important part is to follow the technical requirements when implementing the system. There are different types of network virtualization as mentioned below.

**VLAN (Virtual local area networks)**

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area. VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most frequently. VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other. VLANs tend to be flexible because they are based on logical connections, rather than physical.

One or more network switches may support multiple, independent VLANs, creating Layer 2 (data link) implementations of subnets. A VLAN is associated with a broadcast domain. It is usually composed of one or more network switches

**VXLAN (Virtual Extensible LAN)**

VXLAN is an encapsulation protocol that provides data center connectivity using tunneling to stretch Layer 2 connections over an underlying Layer 3 network.

In data centers, VXLAN is the most used protocol to create overlay networks that sit on top of the physical network, enabling the use of virtual networks. The VXLAN protocol supports the virtualization of the data center network while addressing the needs of multi-tenant data centers by providing the necessary segmentation on a large scale.

The VXLAN tunneling protocol that encapsulates Layer 2 Ethernet frames in Layer 3 UDP packets, enables you to create virtualized Layer 2 subnets, or segments, that span physical Layer 3 networks. Each Layer 2 subnet is uniquely identified by a VXLAN network identifier (VNI) that segments traffic. The entity that performs the encapsulation and decapsulation of packets is called a VXLAN tunnel endpoint (VTEP). To support devices that can’t act as a VTEP on their own, like bare-metal servers, a Juniper Networks device can encapsulate and de-encapsulate data packets. This type of VTEP is known as a hardware VTEP. VTEPs can also reside in hypervisor hosts, such as kernel-based virtual machine (KVM) hosts, to directly support virtualized workloads. This type of VTEP is known as a software VTEP.

VXLAN is very similar to VLAN, which also encapsulates layer 2 frames and segments networks. The main difference is that VLAN uses the tag on the layer 2 frame for encapsulation and can scale up to 4000 VLANs. VXLAN, on the other hand, encapsulates the MAC in UDP and can scale up to 16 million VXLAN segments. But VXLAN provides the following advantages over VLAN Increases scalability in virtualized cloud environments as the VXLAN ID is 24 bits, which enables you to create up to 16 million isolated networks. This overcomes the limitation of VLANs having the 12 bits VLAN ID, which enables you to create a maximum of 4094 isolated networks.

**SDN(Software Defined Networking)**

Software-defined networking (SDN) technology is an approach to network management  that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like  cloud computing than traditional network management.[]](https://en.wikipedia.org/wiki/Software-defined_networking#cite_note-ReferenceA-1) SDN is meant to address the fact that the static architecture of traditional networks is decentralized and complex while current networks require more flexibility and easy troubleshooting. SDN attempts to centralize network intelligence in one network component by disassociating the forwarding process of network packets (data plane) from the routing process (control plane). The control plane consists of one or more controllers, which are considered the brain of the SDN network where the whole intelligence is incorporated. However, the intelligent centralization has its own drawbacks when it comes to security, scalability and elasticity[]](https://en.wikipedia.org/wiki/Software-defined_networking#cite_note-ReferenceA-1) and this is the main issue of SDN.

**NFV (Network functions virtualization)**

Network functions virtualization which is also network function virtualization or NFV is a network architecture concept that leverages the IT virtualization technologies to virtualize entire classes of network node functions into building blocks that may connect, or chain together, to create and deliver communication services.

NFV relies upon traditional server- virtualization techniques such as those used in enterprise IT. A virtualized network function, or VNF, is implemented within one or more virtual machine or containers running different software and processes, on top of commercial off the shelf (COTS) high-volume servers, switches, and storage devices, or even cloud computing infrastructure, instead of having custom hardware appliances for each network function thereby avoiding vendor lock-in.

SDN architecture mainly focuses on data centers where as NFV is targeted at service providers or operators. SDN separates control plane and data forwarding plane by centralizing control and programmability of network. NFV helps service providers or operators to virtualize functions like load balancing, routing, and policy management by transferring network functions from dedicated appliances to virtual servers. SDN uses OpenFlow as a communication protocol. There is no protocol determined yet for NFV. Various enterprise networking software and hardware vendors are initiative supporters of SDN. Telecom service providers or operators are prime initiative supporters of NFV. SDN applications run on industry-standard servers or switches. NFV applications run on industry-standard servers.