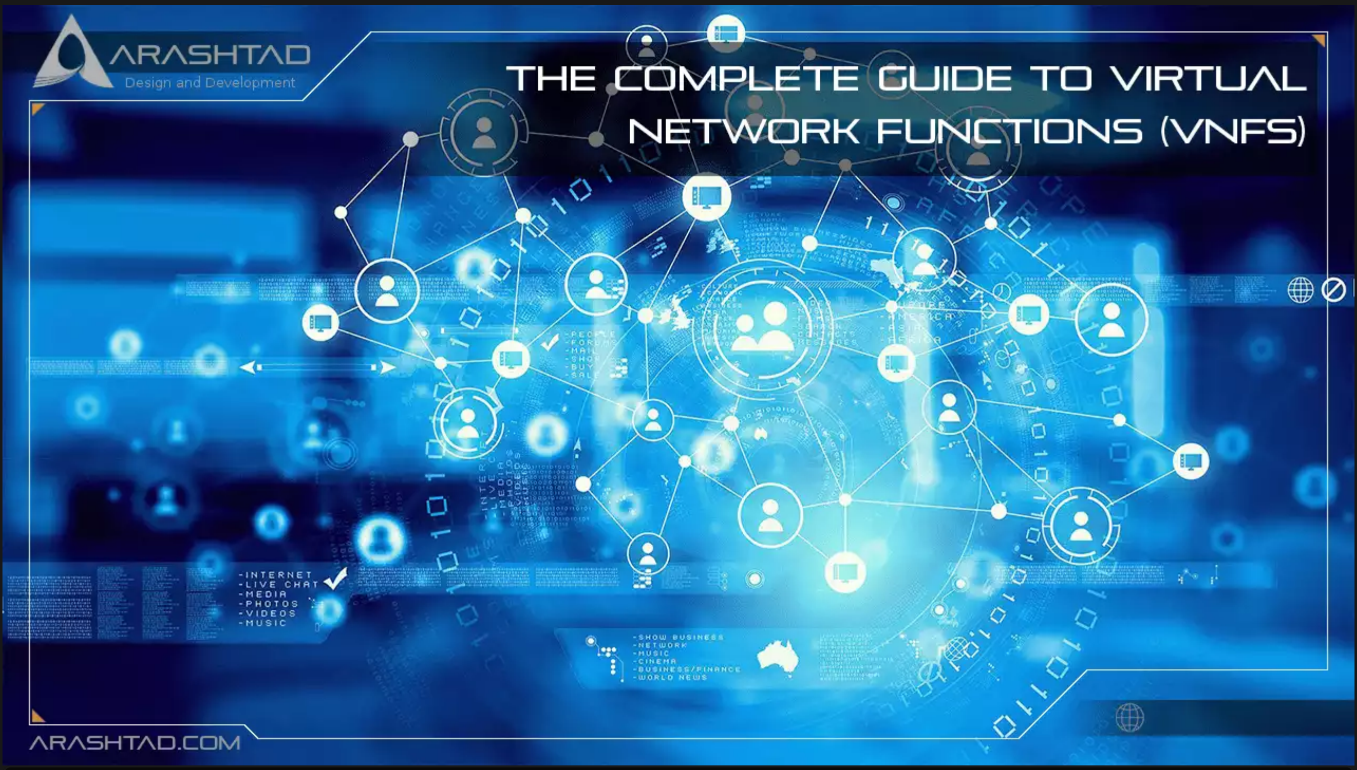
The Complete Guide to Virtual Network Functions (VNFs)

No comments



Using individual Virtual Network Functions (VNFs), a fully virtualized environment can be constructed by connecting or combining them as building blocks. On top of hardware networking infrastructure, VNFs run on virtual machines (VMs). They can run on multiple hardware boxes using all of their resources. In this article, we will discuss the architecture and components of VNFs, their advantages and limitations, and how they differ from NFV.

What Are Virtual Network Functions (VNFs)?

To achieve agility, flexibility, and dynamic scaling in network infrastructure, Network functions virtualization (NFV) and Software-defined networking (SDN) are being used in technology transformation. Software-defined networking (SDN) allows network administrators and operators to take complete control of their networks, and NFV replaces the network equipment with a virtualized infrastructure. On this virtual infrastructure, Virtual Network Functions (VNFs) will run and host. Virtual Network Functions are movable and scalable software implementations of network devices that are virtualized.

Now multiple vendors are offering Virtual Network Functions as a solution for various network functions, hosted on Commercial Off-the-Shelf (COTS) compute, networking, and storage infrastructure.

Virtual Network Functions Components

1- Switching: CG-NAT, BNG, routers.

2- Traffic analysis: QoE measurement, DPI.

3- Edge Devices: Broadband remote access server, IP Edge, vCPE.

4- Tunneling gateway elements: IPSec/SSL VPN gateways.

5- Signalling: IMS, SBCs.

6- Application-level optimization: Load Balancers, CDNs.

7- Security functions: spam protection, virus scanners, firewalls.

8- Set-top boxes and home routers.

The network functions virtualization environment (NFV) involves joining multiple individual VNFs together to form a single super service. VNFs are built for different network functions. They can be used individually or together as part of super service. They can also be developed and deployed quickly by service providers.

Overview of Cloud-Native VNFs

The creation of cloud-native VNFs is a solution for vendors, and to have all cloud-native characteristics in VNFs is a revolution in software development. Microservices and containerized functions are part of cloud-native VNFs designed explicitly for orchestration. They are also managed dynamically. The primary difference between cloud-native VNFs and traditional VNFs is their scalability and self-management capabilities. The cloud-native VNF API solved the limitations mentioned above of traditional VNF and Cloud-native VNF APIs are capable of enabling the following:

1- Installing and configuring automatically

2- Self-healing or fault-tolerant

3- Automatically upgrade and update VNFs to apply for new patches and releases.

4- Automate scaling based on network requirements.

5- By reducing unnecessary resources, simplified management and standard reduce power consumption.

6- A VNF can be shared within an NFV environment.

7- Managing capacity, errors, and performance of VNFs automatically.

8- It is possible to share and reuse processes within VNFs.

Cloud-Native VNFs Architecture

Virtual network functions run on NFV infrastructure (NFVi). NFV orchestrators orchestrate virtual network functions. virtual network functions are software images.

Image not found or type unknown

vnf The Complete Guide to Virtual Network Functions (VNFs)

EM (Element Management)

It is responsible for managing the functional aspects of VNFs, namely FCAPS (Fault, Configuration, Accounting, Performance, and Security Management). VNFs are managed using proprietary interfaces. There may be one Element management system (EMS) per VNF or one Element management system (EMS) managing multiple VNFs. The EMS itself could be a VNF.

Virtual Network Functions Manager

Managing a VNF instance's life cycle is done by VNF Manager. It can handle a single VNF or multiple VNFs. It also performs FCAPS for virtual components of a VNF. the difference between EM and VNFM is that EM manages functional components, while VNF Manager controls virtual components.

NFVI (Network Function Virtualization Infrastructure)

Virtual Network Functions are run in an environment called NFVI. It consists of physical resources, a virtualization layer, and virtual resources, which are described below.

Memory, Compute, and Networking Resources

This category includes any storage server or the physical server that belongs to NFVI.

Virtual Memory, Virtual Compute, and Virtual Networking Resources

The virtual part of NFVI abstracts resources from their physical counterparts.

Virtualization Layer

Generally, this is known as a "Hypervisor" that abstracts physical resources into virtual resources.

Advantages of Virtual Network Functions

The traditional way of installing new network functions and services is on proprietary hardware and manually configuring them on a device-by-device basis. network engineers enable and configure the required functions within dedicated appliances. Using service chaining, engineers would need to manually connect each dedicated appliance so that certain functions could be performed in sequence.

The virtualization infrastructure eliminates the need for expensive purpose-built hardware by virtualizing these functions in software. In addition, new functions can be deployed as VMs or containers more quickly and efficiently. In addition to increasing network scalability and agility, VNFs can also optimize network resource utilization. Other VNF benefits include: reducing overall energy consumption; reducing physical data center space requirements due to the replacement of physical hardware with VNFs; An overall reduction in operating expenses and a long-term reduction in cooling and power requirements.

Challenges of Virtual Network Functions

Network functions virtualization (NFV) and VNFs have been plagued with a lack of standardization from major vendors for years, as with all technology. By releasing a variety of specifications and guidelines for vendors to follow, the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) for NFV is working to solve this problem. NFV/VNF vendors who do not adhere to these standards will face difficulties when implementing nonstandard NFV architectures and VNF deployment templates. Besides standardization concerns, VNF also faces the following challenges:

1- When building and operating VNFs in the virtualized hypervisor or container environments, network teams must overcome a deployment and management learning curve.

2- Traditional network monitoring tools can cause network teams to lose monitoring and management visibility.

3- The layered software approach of VNFs might obfuscate security visibility and traceability, which may lead to new cybersecurity challenges.

4- Lastly, replacing physical network functions (PNF) with virtualized functions requires a significant upfront infrastructure investment.

NFV vs. VNF: What's the difference?

NFV and virtual network functions can sometimes be used interchangeably by networking professionals, which can confuse them. However, when we examine the NFV specifications outlined by ETSI, it becomes clear the two acronyms have related but distinct meanings.

First, we should note that network functions are typically components of a network infrastructure that provide well-defined functional behavior, such as intrusion detection, intrusion prevention, or routing. Using a VNF, a network function can be implemented using software decoupled from its underlying hardware. This can lead to more agile networks, resulting in significant Opex and Capex savings. In contrast, NFV is usually a concept or principle that refers to software-defined network functions independent of any specific hardware platform and to a formal network virtualization initiative led by some of the largest telecommunication operators in the world. As part of ETSI, these companies aim to develop and standardize an overarching, comprehensive NFV framework, as shown below, at a high level. VNFs may be deployed on top of NFV infrastructure, which may span multiple physical locations. In summary, NFV is an overarching concept within ETSI's NFV framework, whereas VNFs are building blocks.

Conclusion

In this article, you learned about Virtual Network Functions and their architecture and components. Network operators can easily manage and expand their network capabilities on demand by utilizing virtual, software-based applications where physical boxes once stood in the network architecture. In this way, operators can balance the load, scale up and down, and move functions between distributed hardware resources. With continual updates, customers will always be able to use the latest software.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.

Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP **NEWSLETTER** **RSS FEED**