Business Network Virtual Network Infrastructure (VNI)

Frequently Asked Questions

What is Network Functions Virtualization?

Forrester defines network function virtualization (NFV) as the ability for a programmable orchestration and automation system to set up and tear down software-based/virtual network functions (VNFs) to match the demands of users, devices, applications, data, or business (see Figure 1). Examples include security and load balancing. These network services can exists as a virtual service instantiated through VNF running on x86 hardware within a hypervisor or container environment.

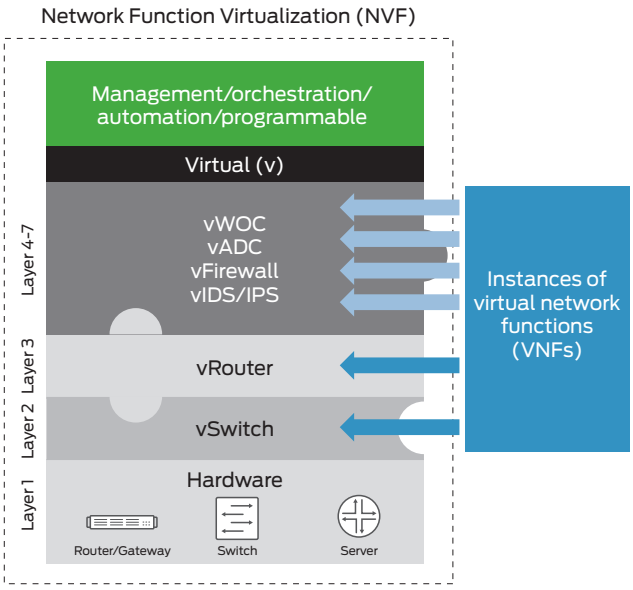

Figure 1: Network Function Virtualization is built on hardware, Virtual Network Functions, and software tools.

What components make up NFV?

For an NFV implementation to be successful, infrastructure and operations (I&O) professionals need an architectural framework that provides a clear set of interfaces, elements, features, and capabilities. While various organizations have delivered some of these, the European Telecommunications Standards Institute (ETSI) defines the most complete and comprehensive set of requirements, such as MANO and NFVi, and its architectural framework serves as a high-level starting point (see Figure 2).

What are the key benefits of an NFV-based model compared to a fixed physical network appliances model?

NFV has multiple advantages:

- **Elasticity and flexibility:** NFV provides a platform that allows the business to spin networking services up and down or in and out to match the needs the company.
- **Optimized network infrastructure:** NFV platforms only use resources when needed, so there is no need to overprovision. Without NFV, I&O professionals are forced to build infrastructure based on current demands and then add a buffer over the highest expected run rate to provide some overhead. The problem with this approach is that, on average, hardware devices only use about 25% of their capacity, so companies are spending for capacity they don't use. Worst of all, they are stuck with it until the next refresh cycle—on average, five to seven years.
- **Multi-tenant environment:** Hardware has one administrator and basically one team to manage the entire underlying infrastructure. NVF can support a multi-tenant platform that enables different professionals to leverage VNFs based on their needs. For example, in Forrester's Zero Trust model, security professionals can spin up virtual firewalls and set policies for specific applications or data without disrupting the rest of the VNFs or infrastructure.
- **Pay-per-use model:** Network hardware infrastructure is designed for worst-case scenarios, such as peak demands or failures, and not current run rates. With VNFs, usage can be aligned with demand and billed accordingly.
- **Simplicity:** Multiple VNFs can be leveraged within a single link or physical device, reducing operational waste and security holes. This benefit is particularly valuable when service chaining. In the hardware world, every hardware service requires a set of physical connections; for I&O teams following best practices, redundancy will be needed for each new service. This leads to an exponentially growing set of physical connections, architecture, policies, and management as multiple services are linked to support service chaining.

- **Increased trust levels:** NFV environments enable security controls to be placed around each piece of data, application, user, and device. Forrester calls this Zero Trust. It is not feasible to use physical security devices to secure applications and data residing in virtual platforms, especially those offered as infrastructure-as-a-service.
- **Improve operational efficiency and speed:** The technology management team can ignite and extinguish services at fraction of the time with VNFs compared to hardware networking appliances.

What are some of the biggest misconceptions in the market about an NFV-based model?

The biggest market misconceptions surrounding NFV stem from simple misunderstandings. For instance, 53% of networking and telecom respondents to a recent Forrester survey confused NFV with software-defined networking (SDN); they thought SDN involved software instances of routers, switches, firewalls, and other network functions. The situation is even worse for enterprises, where I&O teams don't really understand what exactly NFV is or the precise value it will provide them. While many of the terms are interrelated, these acronyms provide different values. To get the greatest value, enterprise I&O first have to understand what these acronyms are and what they stand for so they can ask for the right solution. Toward that end, Forrester has created a "Decode the New Networking Alphabet Soup" report to help clear up the confusion.

Why are enterprises beginning to embrace an NFV-based model?

Enterprises, per se, aren't embracing NFV-models as much as enterprise I&O teams are. Enterprise application developers have been using VNFs for some time. Forrester's Business Technographics Application Developer survey indicates 63% of mobile application developers use virtual network services to test mobile applications. Many I&O professionals have heard from their counterparts or seen the benefits they derive from using VNFs, generating interest in NFV-based models that offer many of benefits listed in question 1.

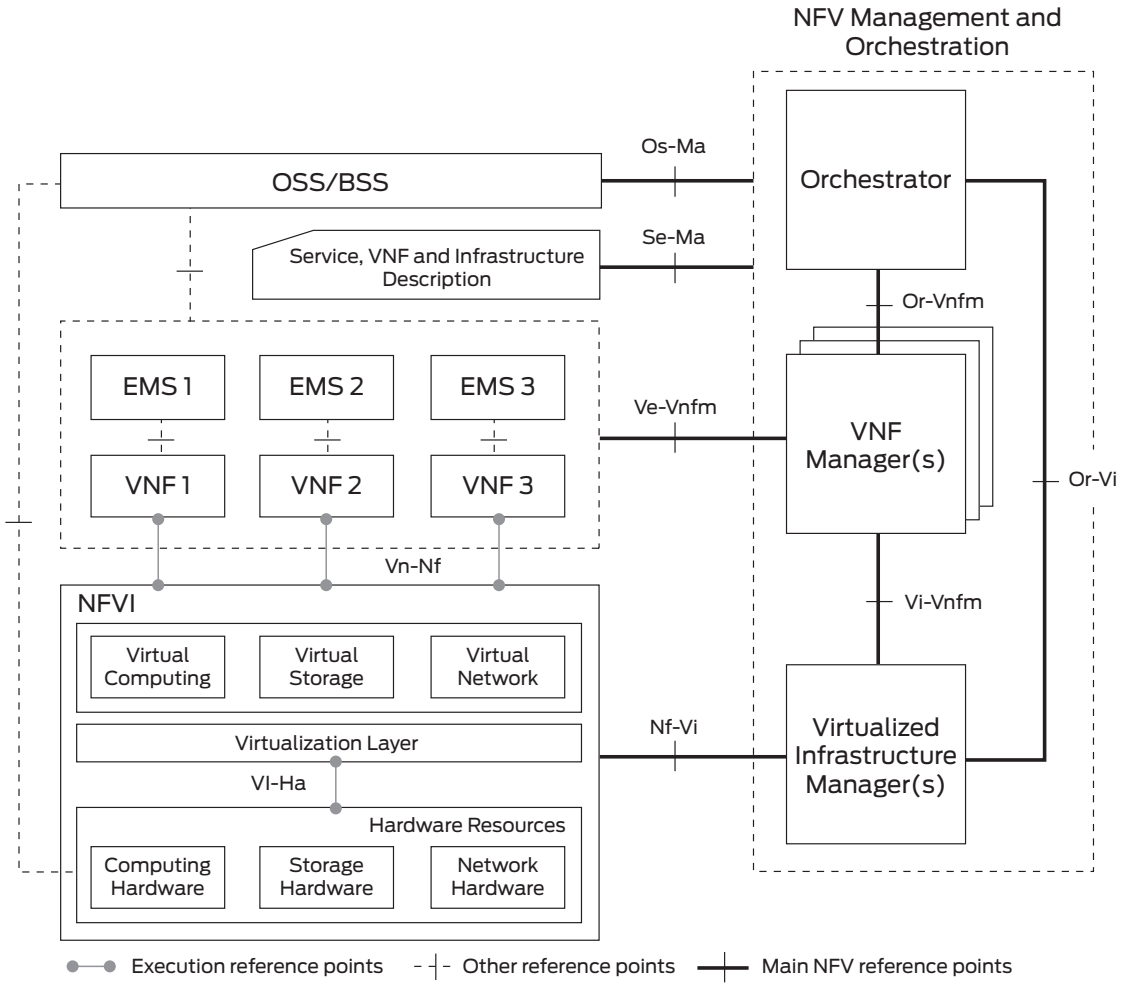

Figure 2: ETSI NFV architecture and interfaces.

Source: ETSI

Are there unique benefits that retail and branch banking organizations can achieve by adopting an NFV approach to the network?

Both branch banking and retail could benefit from NFV to:

- Match business resources to the customer's lifecycle. Business activities parallel their customer's life. At certain times a day, month, and year, businesses will see an increase of activities related to when people get paid, their days off, and holidays. An NFV platform allows I&O professionals to spin up or spin down services to match the actual or anticipated activity level at each remote location and optimize operating costs.
- Enhance customer experiences. Customers now expect a delightful customized experience inside the remote location or through the mobile application or webpage. While online and mobile apps have become common, these interfaces offer little differentiation. The physical location is a new differentiation point; customers will expect these businesses to deliver a customized experience when they come through the door. Those facilities will deploy a plethora of services to support the digital customer experience and enhance business operations in those locations. I&O professionals could leverage switching, optimization, security, and other networking services to support digital displays, facial recognition cameras, or business tablets.
- Highly distributed. Both the retail and banking industries have shifted to opening more micro-sized locations, seasonal pop-ups, and mobile branches. Royal Bank of Scotland uses banking vans to increase its presence in small towns. NFV platforms can help customers overcome some of the following challenges: physical constraints to accommodate hardware; costs of deploying all the hardware needed for each site; the resources required to set up the hardware and maintain it; or the management of the hardware.
- Secure financial transactions and customer data. Both types of businesses face significant pressures to control risk along with securing financial transactions and customer data. With more data collection and interactive services in these locations, security controls that traditionally resided in data centers now reside at the location. NFV makes it easier to set up and disperse them so micro perimeters can be set up to protect customers, their privacy, and their data.

What are key the recommendations for getting started with NFV?

Enterprise I&O professionals can improve the effectiveness and agility of the network and their organizations, but only if teams complete the following first:

- **Identify challenges.** To get the most out of NFV or any technology, teams should identify the current issues that NFV could solve and any potential obstacles that would reduce the effectiveness of NFV.
- **Define their goals and metrics.** Many I&O professionals get caught up in the "shiny ball" syndrome. So as not to waste precious resources implementing new technology, I&O organizations should define their goals before investigating an NFV infrastructure.
- **Organizational readiness.** Organizational readiness is critical. Other teams have automated their process and incorporated new technology. Use Forrester's "Infrastructure Transformation Playbook for 2015" to assess your networking team's readiness.
- **Prioritize services.** Not all services are created equal, and neither are the resources needed to use or maintain them. A cross-functional team should put a list together of the services that will be supported by NFV.
- **Visibility strategy.** The lack of ubiquitous visibility prevents proactive monitoring and inhibits fault seeking. Use the five parts of Forrester's "TechRadar™: Business Technology Monitoring" to assemble your business technology monitoring road map.
- **Management.** Nothing is gained if manual controls are used to manage VNFs. NFV needs a sophisticated management system that can orchestrate and manage the life cycle of virtual services from inception to day-to-day service operation.
- **APIs.** All the solutions highlight APIs, but having them is only the beginning. Use Forrester's "How to Manage APIs for Customer Engagement" to create a well-managed API delivery life cycle and comprehensive production monitoring and management.
- **Deployment strategy.** VNFs can exist in many different locations: on networking hardware and x86 bare metal servers; in networking hardware; hypervisors; cloud platforms; and containers. I&O professionals should have a full understanding of all the platforms and what will be used so they can choose the right solution.

Underlining hardware strategy. VNFs can only provide "good enough" capabilities that must be supplemented with business-critical aspects. Underlays provide this. There needs to be management, control, and visibility between the virtual and physical worlds.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

9030309-001-EN Feb 2017