Enterprise Network Functions Virtualization

Enterprise Network Functions Virtualization Architecture

Q. What is network functions virtualization (NFV)?

A. Network functions virtualization (NFV) is becoming the next disruptive wave in networking. NFV is an architectural approach that focuses on decoupling individual services such as Network Address Translation (NAT), access control lists (ACLs), quality of service (QoS), Layer 3 routing, intrusion prevention systems (IPSs), intrusion detection systems (IDSs), and more from the underlying hardware platform. Allowing such functions to run inside virtual machines on top of standard x86 resources increases deployment flexibility in the network. NFV is typically accompanied by software-defined networking (SDN) approaches (network controllers and orchestration) to offer automation and rapid service deployment of networking functions, thus promising to significantly contribute to network OpEx reductions.

Q. What is Enterprise NFV, and how is it different?

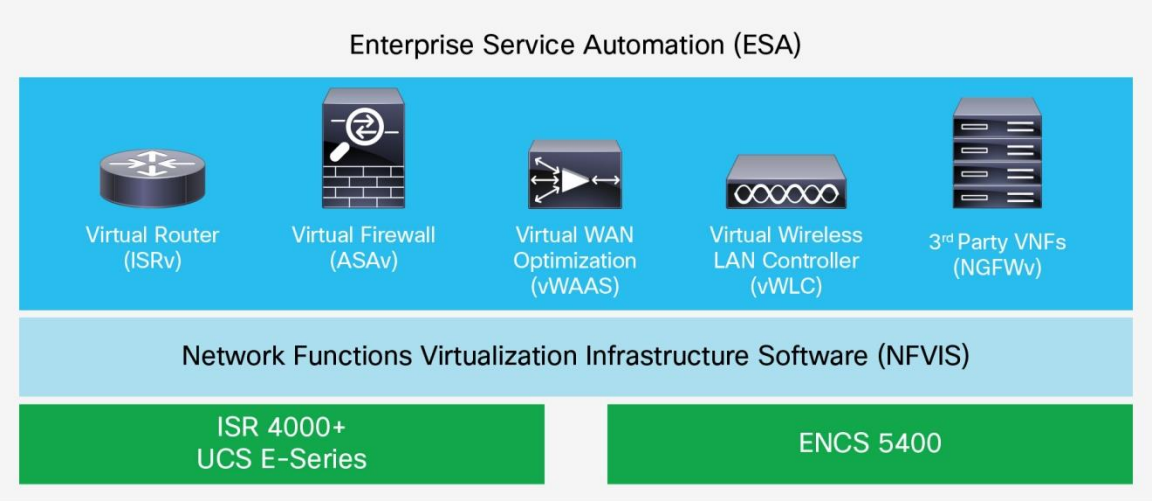
A. Cisco® Enterprise NFV is an end-to-end solution addressing all requirements for deploying virtualized network and application services from orchestration and management to the virtualization software package as well as options for different hardware platforms.

The Cisco Enterprise NFV solution reduces the operational complexity of such branch environments by running the required networking functions as software on standard x86-based hosts. In particular, the Cisco Enterprise NFV solution:

- Reduces the number of hardware elements to be managed at the branch, thus minimizing the need to perform costly site visits for hardware installations or upgrades
- Increases speed of deployment for networking services by offering a software only–based approach to service delivery
- Automates the deployment, management, and operations of branch functions, thus diminishing operational expenses
- Facilitates the deployment of best-in-class functions by taking an open approach to networking
- Enhances network operations flexibility by using virtualization techniques such as virtual machine moves, snapshots, or upgrades

Figure 1 shows the Enterprise NFV solution architectural layers.

Figure 1. Different Architectural Layers of Enterprise NFV Solution



Q. What are the benefits of Enterprise NFV?

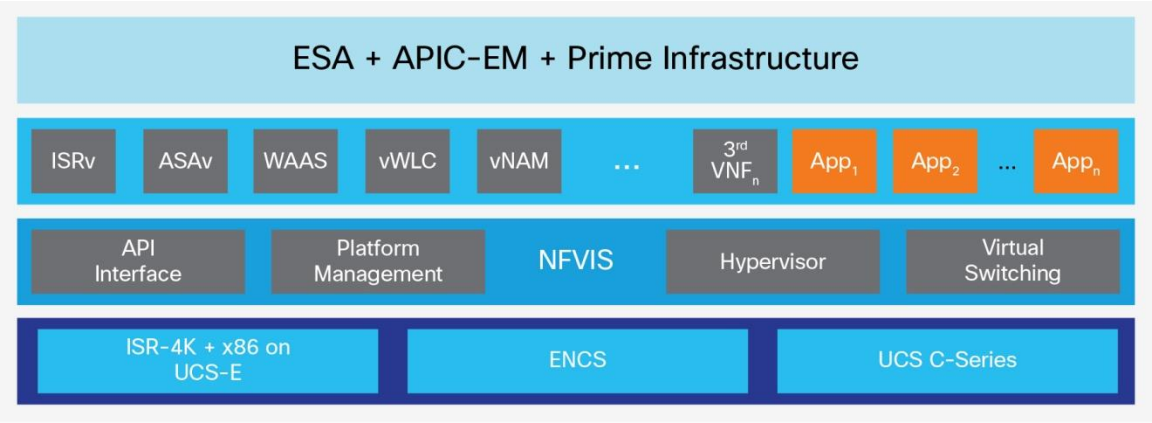
A. Although there are a number of benefits to virtualizing the branch, Enterprise NFV also simplifies day-to-day operations by providing an easy-to-use central orchestration portal. It enables customers to reduce the number of devices they have to deploy and manage at each location and to roll out new services quickly. Enterprise NFV also gives you the freedom of choosing the appropriate deployment hardware platform, from the Cisco UCS E-Series running on a Cisco 4000 Series Integrated Services Routers (ISRs) platform to Cisco 5400 Enterprise Network Compute System.

Q. What are the architectural components of Enterprise NFV?

A. The Cisco Enterprise NFV delivers a fully functional virtualized solution for network and related application services (see Figure 2). The main building blocks of the solution are:

- An orchestration environment to allow easy automation of the deployment of virtualized network services consisting of multiple VNFs
- The virtualized network functions (VNFs) that provide the desired network functionality or even nonnetworking software applications required at a deployment location
- The NFV Infrastructure Software (NFVIS) platform to facilitate the deployment and operation of VNFs and hardware components
- X86-based compute resources to provide the CPU, memory, and storage required to deploy and operate VNFs and run applications

Figure 2. Main Components of Cisco Enterprise NFV Solution



Enterprise NFV Management

Q. What are the different management options for Enterprise NFV?

A. Management and orchestration functionality in the Cisco Enterprise NFV solution is provided by the Cisco Enterprise Service Automation (ESA) and Cisco APIC-EM and Cisco Prime™ Infrastructure platforms. ESA automates your ability to deploy VNFs at multiple sites all at once using a convenient portal and pre-established templates. It also allows VNFs to intercommunicate with one another by service chaining them together.

The app runs on top of the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), the Cisco SDN controller.

ESA can map a particular network configuration profile to a region and populate each site in the region with the common attributes they share. This is done automatically across both virtual and physical branch sites.

With central, one-touch orchestration for the entire virtualized network, including third-party VNFs, ESA offers a standardized site design, centralized provisioning, service chaining, lifecycle management, and automated monitoring of the Cisco Enterprise NFV solution. All functions needed to design, provision, and manage your network are on a single, fully integrated platform.

Q. How is orchestration of the VNFs done?

A. ESA, through its use of central policy, enables services to be deployed and configurations enforced more easily across the enterprise.

Centralized policy is created by building profiles using configuration templates. Customers can create templates for both virtualized and physical services using an intuitive graphical service editor. Alternatively, service templates can be selected from a library of standard validated service designs (Cisco Validated Designs) using the intelligent template selection engine of ESA.

When a new branch instance is brought up for the first time, it can use plug and play (PnP) to register with the Cisco Enterprise NFV orchestration and management system. After being registered, the orchestrator matches the platform data to the profile provisioned in ESA to provision the system. The controller using an open REST API transported over HTTPS then implements the interaction initiated by ESA. A package of instructions and metadata that also contains a day-0 configuration file for VNFs is included as part of the provisioning that allows the VNFs to be activated. This decoupling of elements allows the Cisco Enterprise NFV orchestration and management architecture to scale efficiently.

Q. How can I monitor different aspects of my network?

A. APIC-EM with Cisco Prime Infrastructure (APIC-EM/PI) provides the controller and monitoring functionality for Cisco Enterprise NFV. Services defined and associated with a particular site deployment in ESA are instantiated using open APIs by APIC-EM/PI. After the VNFs or applications are instantiated, ongoing operation can also be monitored by APIC-EM/PI, with local support from NFVIS.

Q. Does ESA support my existing ISR routers?

A. Yes. ESA supports both physical and virtual router provisioning. ESA can provision physical ISR 4000 series routers as well as provision ISRv on NFVIS.

Virtual Network Functions

Q. What Cisco VNFs are supported in Enterprise NFV?

A. The Cisco Enterprise NFV solution offers an open environment for the virtualization of both network functions and applications in the enterprise branch.

The following Cisco VNFs are supported now:

- Cisco Integrated Services Virtual Router (ISRv) for virtual routing
- Cisco ASAv for virtual firewall
- Cisco vWAAS for virtualized WAN optimization
- Cisco vWLC for a virtualized wireless LAN controller

Q. What is the Cisco® Integrated Services Virtual Router (ISRv)?

A. The Cisco® ISRv is a Virtual form-factor Cisco IOS-XE router that delivers comprehensive WAN gateway and network services functions into virtual environments. Using familiar, industry-leading Cisco IOS® XE Software networking capabilities (same features present on Cisco ISR4000 series and ASR1000 series physical routers), the Cisco ISRv enables enterprises to deliver WAN services to their remote locations using Cisco Network Functions Virtualization (NFV) technology.

Q. Are third-party VNFs supported?

A. Yes. The Cisco Enterprise NFV solution offers an open and extensible environment, which will support 3rd party VNFs. KVM-based VNFs as well as applications running in a Linux or Windows environment (e.g., DNS/DHCP, web server, active directory) have the potential to integrate with NFVIS and be supported by ESA and APIC-EM/PI.

Q. Which 3rd party VNFs are supported?

A. An initial set of select 3rd party VNFs will be supported during the Enterprise NFV GA release. Support for additional 3rd party VNFs will be announced with subsequent releases.

Q. What are VNF requirements to run on NFVIS?

A. NFVIS uses KVM and associated libraries to run virtual applications. In essence, any application that supports stock qcow images can run on NFVIS.

NFV Infrastructure Software

Q. What is NFVIS?

A. The Cisco Enterprise NFV solution introduces a virtualized software platform. The platform software in the solution is NFVIS, which extends Linux by packaging additional functions for VNF lifecycle management, monitoring, device programmability, and hardware acceleration.

Q. Is NFVIS a hypervisor?

A. NFVIS has multiple components and functions. One of the components it packages is KVM, which is a hypervisor for virtualization. Additional components of NFVIS are:

- **OS kernel:** Drives the underlying hardware platforms (for example, Cisco UCS servers, Cisco UCS E-Series, x86 enhanced network elements) and hosts the virtualization layer for VNFs, virtual switching API interfaces, and management.
- **Virtualization support:** The hypervisor for virtualization is based on KVM and includes QEMU, Libvirt, and other associated processes.
- **Virtual switching:** Enables multiple VNFs to share physical interface resources and to allow for traffic to be passed within the x86 host between VNFs.
- **VM lifecycle management:** Support to bring up VNFs dynamically as well as to control their liveliness.
- **PnP:** A client to automate the bring-up of any NFVIS-based host. The PnP client can thus communicate with a PnP server running in the APIC-EM controller and be loaded with the right host configuration.
- **Web server:** Enables connectivity into NFVIS using HTTPS, which is particularly used to support local management tools and orchestration APIs.
- **Device management:** Tools packaged into NFVIS to support device management, including a resource manager.
- **Statistics:** Tools such as syslogd, snmpd, and collected to assist in statistics collection and reporting.

Q. How can I connect to NFVIS?

A. NFVIS also supports a web-based management device portal. From this portal, the user can upload VNF packages, implement lifecycle management turned services up and/or down, connect to VNF consoles, and monitor critical parameters. This portal contains dashboards showing the platform resource utilization and VNF service status. From the status dashboard, a window may be opened for connecting to the VNF console.

Q. Can I upgrade individual components of NFVIS?

A. No. End users will not be allowed to upgrade individual components of NFVIS. NFVIS will be a prepackaged installable ISO that the end user will deploy. All components packaged within NFVIS will be tested and qualified prior to NFVIS release.

Q. How is VM lifecycle management handled?

A. NFVIS comes prepackaged with ECS-Lite, which supports bring-up of VNFs dynamically as well as to control their liveliness.

Q. What is the use case for PnP in NFVIS?

A. When a new branch instance is brought up for the first time, it can use PnP in NFVIS to register with the Cisco Enterprise NFV orchestration and management system. After being registered, the orchestrator matches the platform data to the profile provisioned in ESA to provision the system. The controller then implements the interaction initiated by ESA. A package of instructions and metadata that also contains a day-0 configuration file for VNFs is included as part of the provisioning that allows the VNFs to be activated. This entire sequence of events allows customers to truly experience a zero-touch deployment model.

Q. Can NFVIS monitor the hardware components?

A. Yes, NFVIS can monitor all hardware status such as CPU, memory, disk, and network utilization.

Q. Does NFVIS provide VM monitoring?

A. Yes, NFVIS also monitors the health of VNFs running on it using an internal management bridge. CPU, memory, and disk monitoring are performed by NFVIS.

Q. Can I run an application on NFVIS?

A. NFVIS allows for the hosting of 3rd party and customer VMs (virtual machines). These VMs should be QCOW images and run on KVM. However, because of shared resources on the hardware platform we advise monitoring and base lining to develop an understanding of performance impact. NFVIS comes included with basic monitoring tooling.

NFVIS does not allow for 3rd party and customer processes to be running at the non-hypervisor level. Linux shell access to NFVIS is not provided to the operator and a VM will need to be used.

Hardware Options

Q. What are the different branch hosting platforms?

A. There are a few choices when it comes to branch hosting platforms. Choice includes Cisco 4000 Series ISRs with a Cisco UCS E-Series blade and Cisco 5400 Enterprise Network Compute System.

Q. Is Enterprise NFV still relevant for customers who use non-Ethernet interface to terminate their WAN?

A. Yes. Customers who want interface diversity like T1, DSL, 4G-LTE etc, while at the same time want to take advantage of the benefits that Enterprise NFV offers should look to deploy an ISR4000 Series, which provides the required flexibility in terms of the interfaces supported, along with UCS E-series compute blade running NFVIS. Customers can now run their VNFs on NFVIS inside of the UCS E-Series compute blade.

Q. Where can I run NFVIS?

A. NFVIS has been tested to run on Cisco UCS E-Series and Cisco 5400 Enterprise Network Compute System patforms.

Q. Is NFVIS supported on generic off-the-shelf x86 servers?

A. The goal of NFVIS is to support and run on generic third-party x86 hardware. However, at this time, it is supported only on the Cisco UCS E-Series and ENCS platforms.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-736831-02 02/17