Cisco vWAAS on KVM

This chapter contains the following sections:

About Cisco vWAAS on KVM

Cisco vWAAS on RHEL KVM (Red Hat Enterprise Linux Kernel-based Virtual Machine) is a virtual WAAS appliance that runs on a KVM Hypervisor. The Cisco vWAAS on RHEL KVM solution extends the capabilities of ISR-WAAS and vWAAS running on Cisco UCS-E Series.

Consider the following about Cisco vWAAS on RHEL KVM:

- **Cisco vWAAS on RHEL KVM** is available for vWAAS with WAAS Version 6.2.1 and later.
- **Cisco vWAAS on KVM on CentOS** (Linux Community Enterprise Operating System) is available for vWAAS on WAAS Version 6.2.3x and later.

Note The CDP protocol is not supported for Open Virtual Switch (OVS) on RHEL KVM on CentOS, therefore the **show cdp** command cannot be used for vWAAS on RHEL KVM on CentOS.

- The network and disk paravirtualized drivers are common to ISR-WAAS. For more information on resource allocation for vWAAS and vCM models, see ESXi Server Datastore Memory and Disk Space for vWAAS and vCM Models in Chapter 1, “Introduction to Cisco vWAAS.”

Note All general vWAAS features are supported, but some features specific to ISR-WAAS, such as ONE-P integration, are not supported.

- Resource configurations (vCPU, memory, disk) use the profiles from vWAAS that support number of connections of vWAAS models 150, 200, 750, 1300, 2500, 6000, 12000, and 50000, and that support number of managed nodes of vCM models 100, 500, 1000, and 2000. vWAAS-150 supported on Cisco EHWIC (Enhanced High-Speed WAN Interface Card) and NIM modules.
- For vWAAS with WAAS Version 6.2.3x and later, there is inline vWAAS support for the OVS switch, with additional settings in vWAAS. For example

1. Install CentOS 7.2 on UCS-C240.
2. Configure OVS switch on KVM host.
3. Deploy KVM vWAAS OVAs iwth OVS switch on KVM host.
4. Power off the vWAAS.
5. Add two additional interfaces.
6. Using the virt-manager, map the bridge ID in vWAAS:

   ```
   [root@localhost kvm]# virsh edit vwaas-name
   ```

   Domain vWAAS XML configuration changed.
7. Using the virt-manager, edit the virtual type:

   ```
   virtualport type='openvswitch'/
   ```
8. Sample output:

```
<interface type='bridge'>
      <mac address='52:54:00:ea:3f:7b'/>
      <source bridge='br2'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
    </interface>
<interface type='bridge'>
      <mac address='52:54:00:7f:7c:99'/>
      <source bridge='br3'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0'/>
    </interface>
```

System Requirements for vWAAS on KVM

vWAAS on RHEL KVM has a predefined configuration with specific requirements for CPU and memory. However, there are some features that are customizable. Table 4-1 shows the supported configuration for vWAAS on RHEL KVM, and, where applicable, highlights the customizable features.

Note Data disk size will vary according to the model shown in Table 7-4, "Hardware Requirements for vWAAS with Akamai Connect". While deploying RHEL KVM, Cisco vWAAS/vCM needs to verify that enough disk space is available in the respective partition.

Table 4-1 vWAAS on RHEL KVM Supported Configuration

Feature/Component	Description
Platform	Three-disk platform of: • 10GB system • 4GB flash • Data disk (customizable, depending on number of connections)
RHEL version for vWAAS on KVM	RHEL 7.2
Memory Requirements	• vWAAS-150: 4 GB • vWAAS-200: 4 GB • vWAAS-750: 4 GB • vWAAS-1300: 6 GB • vWAAS-2500: 8 GB • vWAAS-6000: 11 GB • vWAAS-12000: 18 GB • vWAAS-50000: 48 GB
Interception Method	WCCP (Web Cache Communication Protocol) or Appnav
Device Emulation	vWAAS on RHEL KVM uses QEMU-KVM.
Management	WAAS CM and serial console
Licensing	For information on Cisco vWAAS licensing, please contact your Cisco account representative.
MAC address	Customizable

Installing Cisco vWAAS on KVM

This section contains the following topics:

Cisco vWAAS on KVM Installation Files

Cisco vWAAS on RHEL KVM is deployed as a tar archive (tar.gz). Table 4-2 shows the files included for deploying Cisco vWAAS on RHEL KVM, and for deploying Cisco vWAAS on NFVIS (Network Function Virtualization Infrastructure Software). For more information on Cisco NFVIS and Cisco NFV (Network Function Virtualization), see the *Cisco Enterprise Network Functions Virtualization Solution Overview*.

Table 4-2 Installation Files for RHEL KVM and NFVIS Deployments

Installation Files	RHEL KVM Installation	NFVIS Installation
• **Cisco signature envelope file** Verifies that this deployment is from Cisco.	X	X
• **Manifest file with checksums**	X	X
• **image_properties.xml** A VM configuration template file used on the Cisco NFVIS platform.		X
• **package.mf** template file and **bootstrap-cfg.xml** These two files work together on the Cisco NFVIS platform with the image_properties.xml file as Day-0 configuration template.		X
• **INSTRUCTIONS.TXT** Describes the procedure for deploying the virtual instance and for using the launch.sh file.	X	
• **launch.sh** file For details on how to use this script, see Using the Launch Script to Deploy vWAAS on KVM.	X	
• **vm.xml** Configuration file needed for vWAAS deployment using virtual bridge or Open Virtual Switch (OVS) present in host mac.	X	
• **VM disk images** A 4 GB flash disk, 10 GB system disk, and data disk (data disk size is dependent on your connection profile).	X	X
• **ezdeploy.sh** file The script used to deploy vWAAS on UCS-E. For details on how to use this script, see Using the EzDeploy Script to Deploy vWAAS on KVM on UCS-E.	X	

Using the Launch Script to Deploy vWAAS on KVM

To use the launch script (launch.sh) to deploy Cisco vWAAS on RHEL KVM, follow these steps:

Step 1 Launch the vWAAS VM. (You must have root permissions to launch the vWAAS VM.)

Step 2 Create a new directory to hold the extracted contents of **tar.gz**.

Step 3 Copy **tar.gz** into the specified directory.

Step 4 To extract the **tar.gz** gzip file, use the **tar -zxvf Cisco-KVM-vWAAS-200-6.2.0.b-80.tar.gz** command.

The contents of the tar.gz file are:

- INSTRUCTIONS.TXT
- Disk-0.qcow
- Disk-1.qcow
- Disk-2.qcow
- vm_tap.xml

- vm_macvtap.xml
- launch.sh
- ezdeploy.sh
- ezdeploy.qstatus.exp

Step 5 To launch vWAAS, run the **launch.sh** script:

a. To check the prerequisite conditions, use the **./launch.sh check** command.

b. To launch vWAAS using the OVS bridge, use the **./launch.sh** *vm-name* **bridge** *bridge1-name bridge2-name* command.

- *bridge1-name* and *bridge2-name*—The OVS bridges already created in the host.

Note Before using the **./launch.sh** *vm-name* **bridge** *bridge1-name bridge2-name* command, verify that the OVS bridges are created and in working state.

c. To launch vWAAS using macvtap, use the **./launch.sh vm-name macvtap** *interface1-name interface2-name* command,

- *vm-name*—The specified name of the vWAAS VM.
- *interface1-name* and *interface2-name*—The specified Ethernet interfaces of the host machine.

Step 6 The vWAAS is launched

Step 7 To view the vWAAS, use the VM GUI or the **virsh list** command.

Step 8 To connect to the console, use the VM GUI or the **virsh console** *vm-name* command.

Step 9 To power down the vWAAS, use the **virsh destroy** *vm-name* command.

Step 10 To undefine the vWAAS:

a. Use the **virsh undefine** *vm-name* command.

b. Remove the directory with the specified *vm-name*.

Note If you want to create another vWAAS of the same model, follow this procedure again for a different vWAAS. The specified directory, for example, “Basic,” will then have two VMs, “Basic1” and “Basic2.” Disks for these VMs will be stored in the subdirectories “Basic1” and “Basic2,” respectively.

Using the EzDeploy Script to Deploy vWAAS on KVM on UCS-E

Use the EzDeploy script for simplified deployment of a vWAAS. Note that the EzDeploy script is not used for the vCM.

The following are prerequisites for launching the EzDeploy script:

- To launch the vWAAS VM, you must have root permission.
- The following software and utility packages must be installed before using the EzDeploy script:
  - QEMU
  - Libvirt

  - Genisoimage
  - Expect script (required only if you choose to run EzDeploy's capability for auto-monitoring WAAS CM registration status)
- Verify the following:
  - There is enough disk and RAM memory to deploy another vWAAS.
  - Compatibility of software versions.
  - Availability and readiness of network connectivity.

Note Because EzDeploy leverages the launch.sh script to launch a vWAAS, the launch.sh script, as well as all the necessary files associated with it, must be present, intact, and not manually removed or manually moved elsewhere.

To use the EzDeploy script (ezdeploy.sh) to deploy Cisco vWAAS on RHEL KVM on UCS-E, follow these steps:

Step 1 Launch the vWAAS VM.

Step 2 Create a new directory to hold the extracted contents of **tar.gz**.

Step 3 Copy **tar.gz** into the specified directory.

Step 4 To extract the **tar.gz** gzip file, use the **tar -zxvf Cisco-KVM-vWAAS-200-6.2.0.b-80.tar.gz** command.

The contents of the tar.gz file are:

- INSTRUCTIONS.TXT
- Disk-0.qcow
- Disk-1.qcow
- Disk-2.qcow
- vm_tap.xml
- vm_macvtap.xml
- launch.sh
- ezdeploy.sh
- ezdeploy.qstatus.exp

Step 5 Run the **ezdeploy.sh** script:

a. During execution of hte ezdeploy.sh, you are prompted for bootstrap configuration parameters:

  - vWAAS KVM name—The name is dependent on whether or not you provide the vWAAS' bootstrap configuration.

    If you do not provide the vWAAS' bootstrap configuration, the name is set as the name of the guest KVM to be created. not the vWAAS' host name.

    If you provide the vWAAS' bootstrap configuration, vWAAS' host name is set and used in both instances.
  - vWAAS' local IP address and mask
  - Default GW IP address: an address on the ISR-4000 series RP reachable by the vWAAS and having external network connectivity
  - IP address of the WAAS CM with which the vWAAS will register

- One NTP server address, without authentication. If you want to have authentication or multiple NTP servers, use the WAAS CM to configure these after the vWAAS is powered up.
- (Optional) DNS server address

The ezdeploy.sh script performs a validation before accepting each parameter.

b. After input collection is completed, the following information is saved:

- The bootstrap configuration is saved in the file **bootstrap-cfg.xml** in the directory created for this KVM.
- The execution log and error log of the script are saved in the file **ezdeploy-log.txt** in the directory created for this KVM.
- For the vWAAS in this KVM, the error log is saved in **errorlog/ezdeploy-errorlog.txt**.

Note By default, all configuration and error logs saved in the specified KVM directory are *not* deleted, even if they have recorded errors, so allow for debugging. If you do not want to generate log files, you must confirm this choice at the end of the script execution, after input entry.

c. After completion of the EzDeploy script, the vWAAS is fully up and running. Registration with the specified WAAS CM and the NTP server are automatically started after installation of their corresponding CLIs.

d. To view the vWAAS, use the VM GUI or the **virsh list** command.

e. To connect to the console, use the VM GUI or the **virsh console** *vm-name* command.

f. To power down the vWAAS, use the **virsh destroy** *vm-name* command.

g. To undefine the vWAAS:

- Use the **virsh undefine** *vm-name* command.
- Remove the directory with the specified *vm-name*.

Traffic Interception Guidelines for vWAAS on KVM

For traffic interception for Cisco vWAAS on KVM, you can use WCCP (WCCP GRE or WCCP L2) or Appnav.

Note When you use any of the traffic interception methods for vWAAS on KVM, you must disable Generic Receive Offload (GRO) on the Cisco UCS NIC. Use the command **ethtool -K** ***nic_interface_name*** **gro off** on KVM host to disable GRO. For example: **`ethtool -K enp3s0f2 gro off`**. If you do not disable GRO, traffic is not recognized, and packets are discarded.

If you upgrade the UCS NIC firmware to the latest version, you do not need to disable the GRO parameter.

For more information on configuring traffic interception methods, see the *Cisco Wide Area Application Services Configuration Guide*.

Downgrade Consideration for vWAAS on KVM

Cisco vWAAS on KVM is used with WAAS Version 6.2.1 and later. You cannot downgrade Cisco vWAAS on KVM or vCM on KVM devices to a version earlier than WAAS Version 6.2.1.

vWAAS in Cisco Enterprise NFV

This section has the following topics:

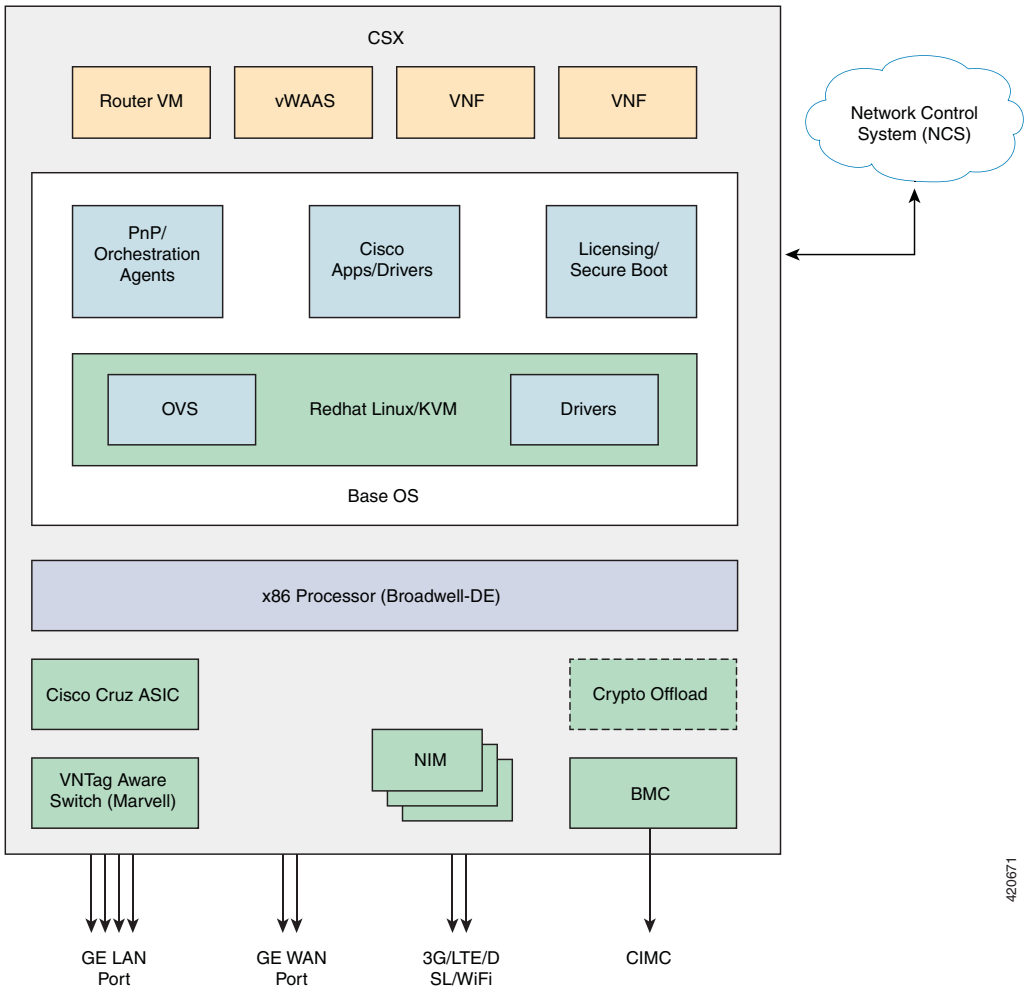
About vWAAS in Cisco Enterprise NFV

Cisco Enterprise Network Functions Virtualization (NFV) converts your critical network functions into software, making it possible to deploy services in minutes, and to create multiple virtual branch offices at once. Cisco Enterprise NFV also reduces your number of network appliances, decreases management complexity, and shrinks real estate requirements.

vWAAS in the Cisco Enterprise NFV (Network Functions Virtualization) solution offers enterprise customers the ability to virtualize the WAN optimization solution on top of x86 host platforms, USC E-Series server module the Cisco 4000 Series Integrated Services Routers (ISR), or on the Cisco ENCS Series.

As shown in Figure 4-1, vWAAS operates as a Virtual Network Function (VNF) within the Cisco Enterprise NFV.

Figure 4-1 vWAAS as VNF in Cisco Enterprise NFV



Operating Considerations for vWAAS in Cisco Enterprise NFV

Consider the following for vWAAS in Cisco Enterprise NFV:

- vWAAS must run on the NFV operating system based on Linux CentOS 7.2 or 7.3, depending on Cisco NFVIS version used.
- As part of Day 0 configuration, vWAAS supports configuration drive for Day 0 configuration, and supports specifying device IP, IP default gateway, Central Manager IP address, hostname, and NTP addresses.
- vWAAS supports WCCP and AppNav-XE traffic interception methods.
- vWAAS supports all existing vWAAS functionality per WAAS Version 6.2.1 and later.
- All vWAAS models are supported for Cisco Enterprise NFV, provided enough resources are available to deploy.
- vCM models are not supported for Cisco Enterprise NFV.

Cisco Enterprise NFV Features

This section describes the following Cisco Enterprise NFV features:

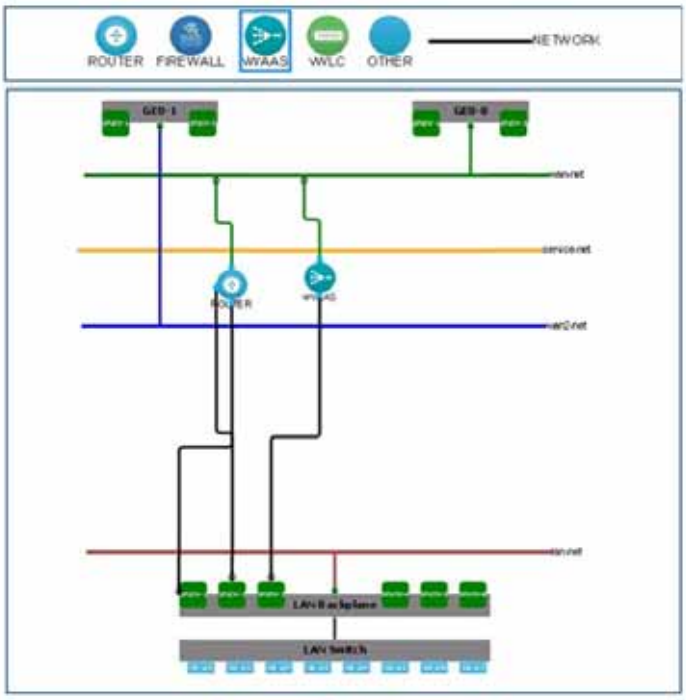
- Enterprise NFV Hosting Platforms and Host OS
- Enterprise NFV VNFs and Applications
- Enterprise NFV Service Chaining
- Enterprise NFV Orchestration and Management

Enterprise NFV Hosting Platforms and Host OS

This section describes features of the hosting platform and host operating system (OS) provided by Cisco Enterprise NFV.

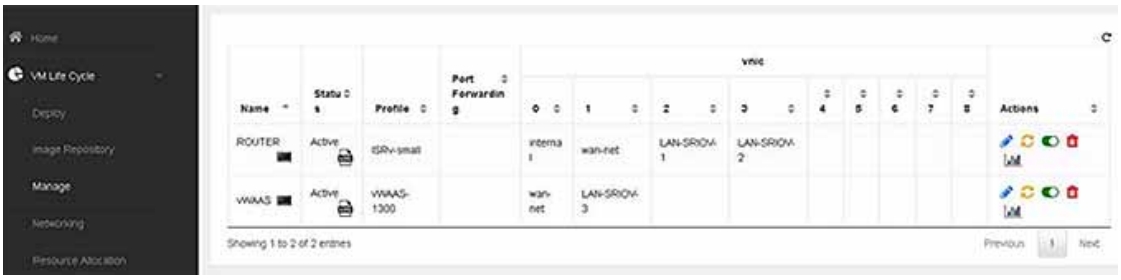
- Figure 4-2 shows a typical deployment of vWAAS in Cisco Enterprise NFV.

Figure 4-2 Typical Deployment of vWAAS in Cisco Enterprise NFV



- Use the NFVIS portal to log in to vWAAS on NFVIS. Navigate to VM Life Cycle > Manage > vWAAS Instance. Figure 4-3 shows the menu options and vWAAS instance.

Figure 4-3 vWAAS on NFVIS Login Path and vWAAS Instance



- Hosting Platforms—The Cisco Enterprise NFV hosting platform provides the hardware resources to run virtualized network functions and applications. Supported hosting platforms include:
  - Standard x86 server such as the UCS C-Series
  - ISR-4000 Series router with integrated UCS E-Series module
  - ENCS platform
- Host Operating System (OS)—Network Functions Virtualization Infrastructure Software (NFVIS) delivers the host OS functionality. NFVIS builds on top of a KVM Linux environment, with added plug-and-play (including device authentication), local GUI, and VNF and application life-cycle management capabilities.

  For a complete description of the Cisco Enterprise NFV Hardware and NFVIS requirements, see the *Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide*.

Note MacVTAP for VM-VM traffic is not supported for Cisco Enterprise NFV.

Enterprise NFV VNFs and Applications

With Cisco Enterprise NFV, there are two types of functions that can be virtualized in the branch, VNFs—such as routing, firewall, NAT, caching, WAN optimization, and applications—such as printer servers and LDAP servers.

Support for VNFs and applications also includes support for third-party (non-Cisco) networking functions and applications, so that even a multi-vendor branch environment that is based applications from different vendors can be simplified by consolidating these functions in software on a single x86 host platform.

Enterprise NFV Service Chaining

Service chaining, also known as service function chaining, orchestrates flows through several virtual switches in the host system. Rather than executing multiple features onto a packet flow in one functional block, the features are chained and successively applied to the packet flow. This allows for more granular services, and for easier functional configuration and management, fostering a multi-vendor VNF environment.

For service chaining on Cisco Enterprise NFV, the following features are also supported:

- Traffic Interception—Layer 2 or Layer 3 packet interception by WCCP or AppNav
- Bridged Service Chaining—VLAN or Ethernet support for bridged service chaining

Enterprise NFV Orchestration and Management

You can manage and orchestrate the Cisco Enterprise NFV solution with the Enterprise Services Automation (ESA). The ESA upon APIC-EM and Prime Infrastructure. Orchestration takes on the task of onboarding a new functionality into the branch, whether or not the branch is being activated from scratch.

There are two types of management for Cisco Enterprise NFV:

- vWAAS as a VNF running on NFVIS
- WAAS management as an optimizer

Any VNF or application onboarded onto an Enterprise NFV solution interfaces with the host at different levels, including the following:

- Physical—CPU, memory, storage
- OS—Linux version, file formats
- Network Interface—packet drivers, Layer 2 frame formats, Layer 3 packet formats
- Management—management interfaces, failure detection and reporting, statistics reporting

The orchestration and management feature also addresses Day 1 configuration and Day 2 ongoing management.

Table 4-3 shows the drivers supported for Cisco Enterprise NFV, and Table 4-4 shows the interfaces supported.

Table 4-3 Drivers Supported for Cisco Enterprise NFV

Driver Support	Description
Supported drivers	• NFVIS—VirtIO • CSP 2100—VirtIO and e1000
Driver version	• Must work under QEMU and Libvirt
Virtio	Must be compatible with QEMU or Libvirt.
Intel NICs	ENCS—Intel XL710; i350 (WAN for ENCS) UCS—Intel i350, Broadcom 5709
SR-IOV support for WAN-connected VNFs	UCS—Intel VF Drivers: IGBVF ENCS—Intel VF Drivers: IGBVF
SR-IOV support for ENCS (for VM-VM hardware offload)	Intel VF Drivers: i40evf
PCIe Pass-through support for WAN-connected VNFs	UCS—Intel VF Drivers: IGB ENCS—Intel VF Drivers: IGB
(Optional) Support for NICs	• UCS—Intel i350, Broadcom 5709, Cisco eNIC • ENCS—Intel XL710; i350 (WAN for ENCS) • CSP 2100—Intel i350, Intel X520, Intel XL710

Driver Support	Description
(Optional) For WAN-connected VMs	• SR-IOV – UCS—Intel i350, Broadcom 5709, Cisco eNIC – ENCS—Intel VF Drivers: IGBVF – CSP 2100—Intel VF Drivers: IGBVF, i40evf • PCIe-Pass Through support – UCS—Intel i350, Broadcom 5709, Cisco eNIC – ENCS—Intel VF Drivers: IGBVF – CSP 2100— •
(Optional) For VM-VM hardware offload	• SR-IOV – UCS—N/A – ENCS—Intel VF Drivers: i40evf – CSP 2100—Intel VF Drivers: IGBVF, i40evf

Table 4-4 Interfaces Supported for Cisco Enterprise NFV

Interface Support	Description
Maximum number of vNIC adapters per VNF (excluding Management)	NFVIS: 8 CSP 2100: 10
Minimum number of vNIC adapters per VNF	1
Maximum number of MAC addresses per VNF	256
Maximum number of VLANs	64
Layer 2 Ethernet Frames accepted	UCS • OVS: Any frame supported by OVS • SR-IOV—Any supported frame format ENCS • OVS: Any frame supported by OVS • SR-IOV—Any supported frame format ENCS • OVS: Any frame supported by OVS • SR-IOV—Any supported frame format

Interface Support	Description
Support for Ethernet Frame sizes greater than 1518 B	UCS • OVS—Allowed • SR-IOV—Allowed ENCS • OVS—Allowed • SR-IOV—Allowed **Note** VMs and applications must support path MTU discovery for frame sizes greater than 1518 B.
Number of IP Addresses (without management)	64*4
Data Plane Development Kit (DPDK) support	UCS—Allowed ENCS—Allowed CSP 2100—Not allowed

Cisco Enterprise NFV Licensing

Consider the following guidelines for Cisco Enterprise NFV licensing:

- For Cisco VNFs, the licensing model we recommend is Smart-Licensing. To streamline deployment, we recommend that VNFs support licensing configuration via Day-0 bootstrapping.
- VMs are independently licensed. NFVIS generates each VM with a Unique Universal ID (UUID).