



# Possibilities

#CiscoLive

# SD-WAN and Network Functions Service Chaining

Alexey Romanov  
Consulting Engineer  
DGTL-BRKENS-1100

**CISCO** *Live!*

June 2-3, 2020 | [ciscolive.com/us](https://ciscolive.com/us)

#CiscoLive



# Agenda

- Introduction
  - SD-WAN Architecture Overview
  - ENCS Platform Overview
- VNF Service Chaining in SD-WAN
  - VNF and Network Types
  - Virtual Branch Design Scenarios
- Virtual Branch Management
  - Automation of Service Chain Deployments
  - SD-WAN Operations Cycle
- Takeaways



# SD-WAN Architecture Overview

# Cisco SD-WAN Architecture

## Orchestration Plane

- First point of authentication
- Distributes list of vSmarts/ vManage to all vEdge routers
- Facilitates NAT traversal

## Management Plane

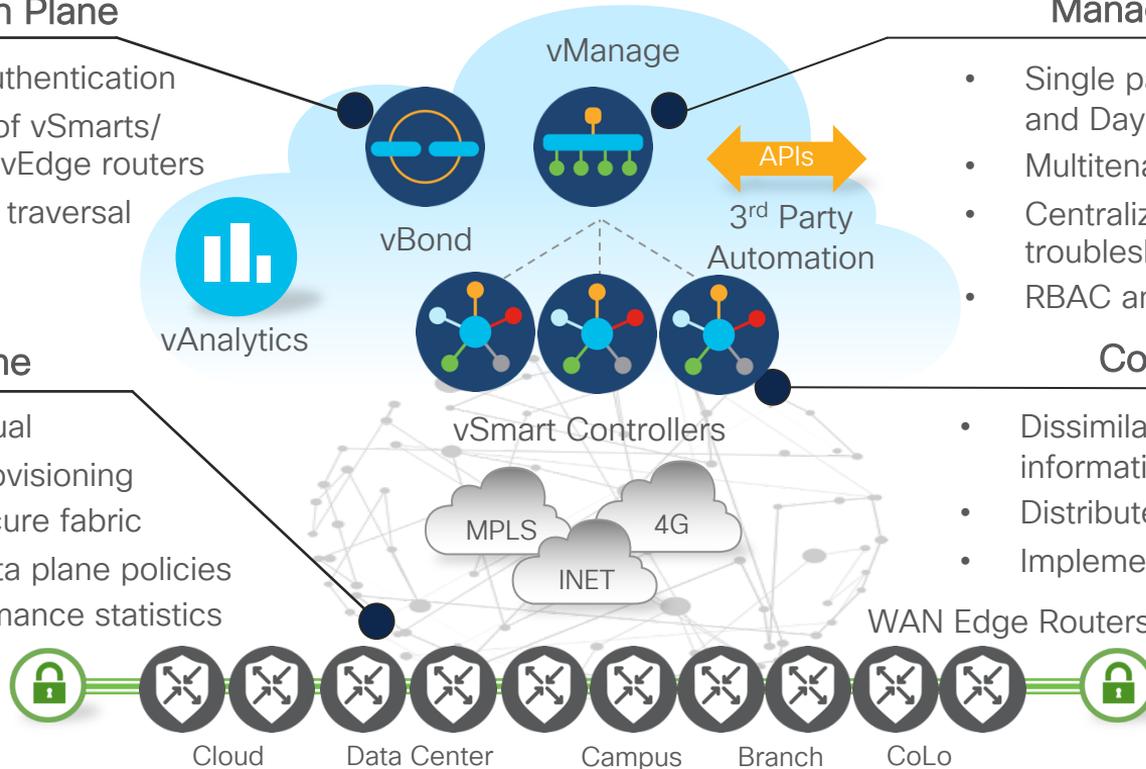
- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant or single-tenant
- Centralized provisioning, troubleshooting and monitoring
- RBAC and APIs

## Data Plane

- Physical or virtual
- Zero Touch Provisioning
- Establishes secure fabric
- Implements data plane policies
- Exports performance statistics

## Control Plane

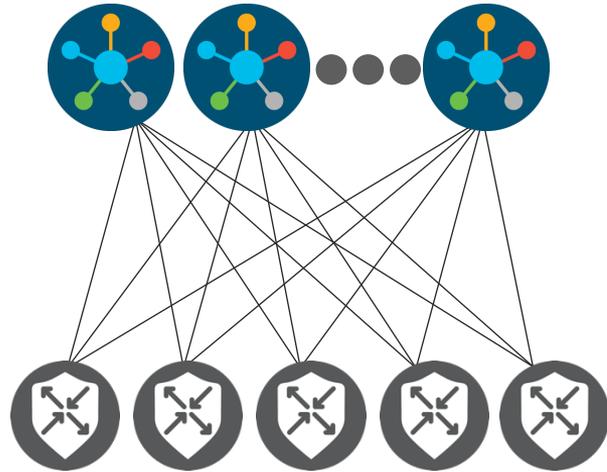
- Dissimilates control plane information between vEdges
- Distributes data plane policies
- Implements control plane policies



# Network-wide Control Plane

## Cisco SD-WAN

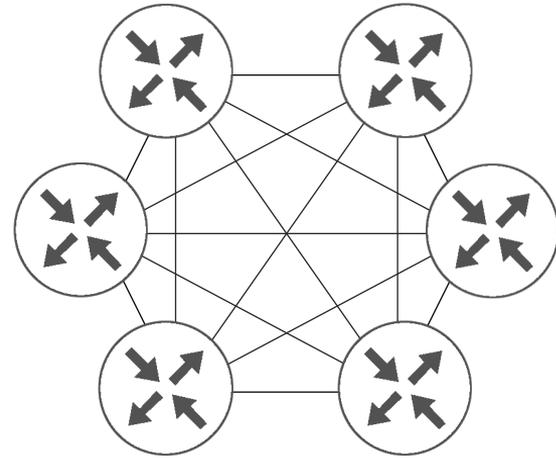
Network Control Plane



Data Plane + Local Control Plane

$O(n)$  Control Complexity  
High Scale

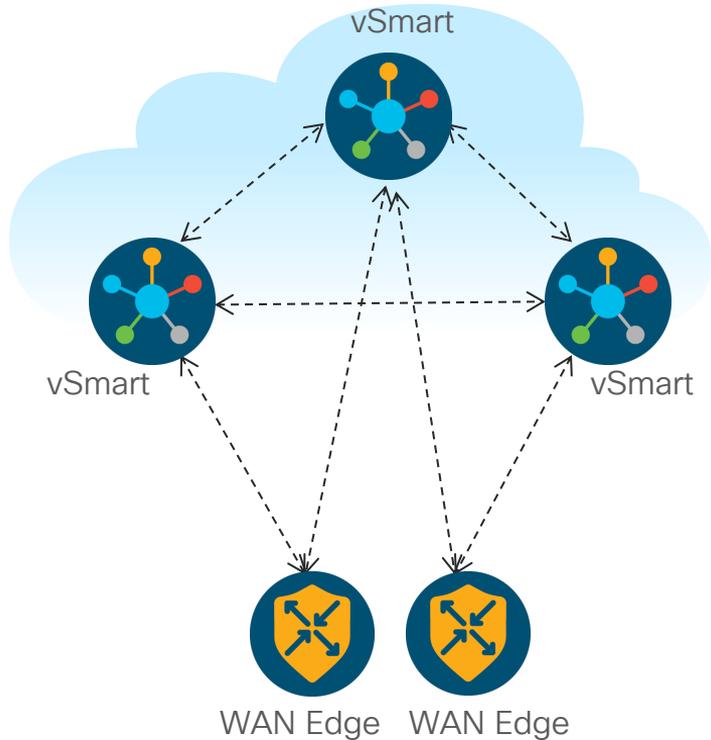
## Traditional



Integrated Control and Data Plane

$O(n^2)$  Control Complexity  
Limited Scale

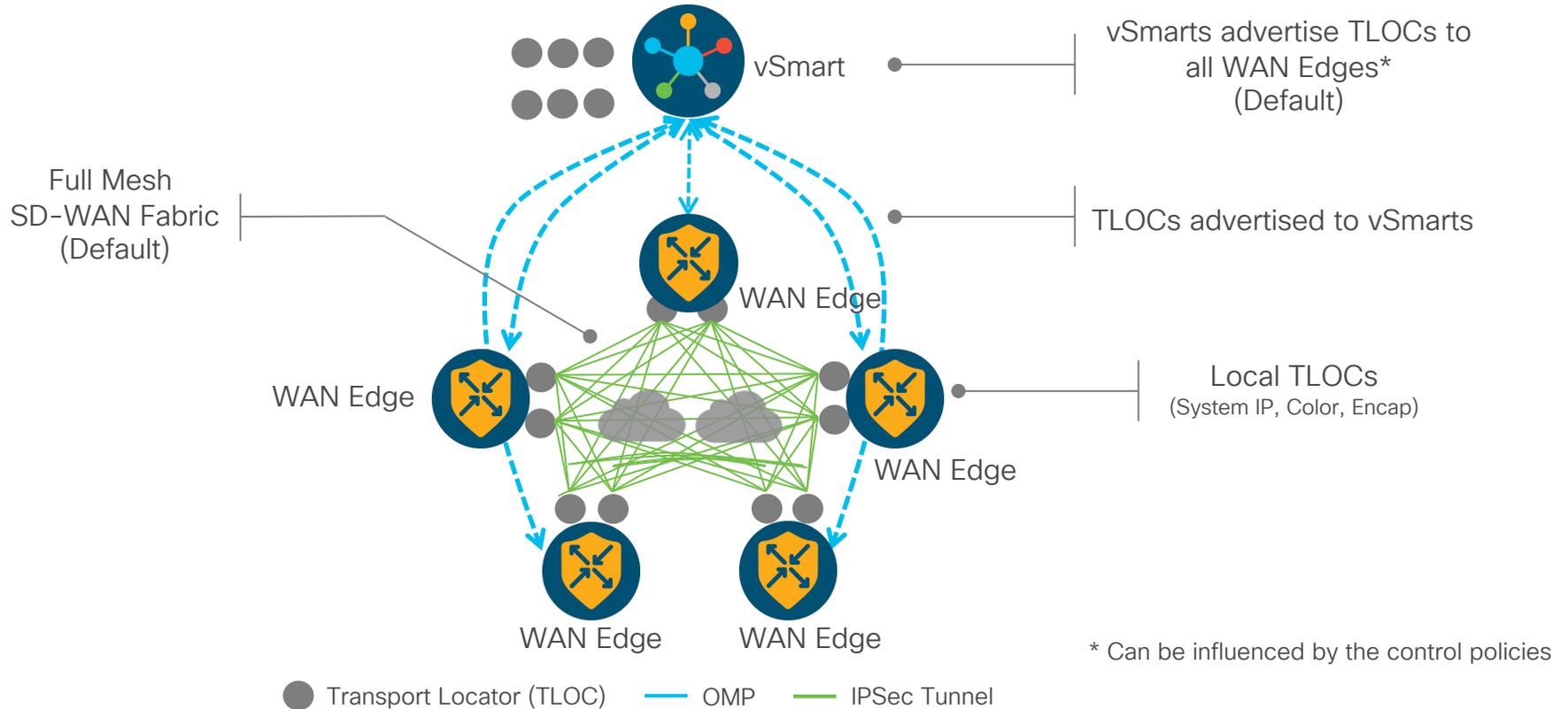
# Overlay Management Protocol (OMP)



Note: WAN Edge routers need not connect to all vSmart Controllers

- TCP based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside TLS/DTLS connections
- Leverages address families to advertise reachability for TLOCs, unicast/multicast destinations, service routes, BFD up/down stats and Cloud onRamp for SaaS probe stats
- Distributes IPsec encryption keys, and data and app-aware policies

# Transport Locators (TLOCs)





# vManage Demo



# ENCS Platform Overview

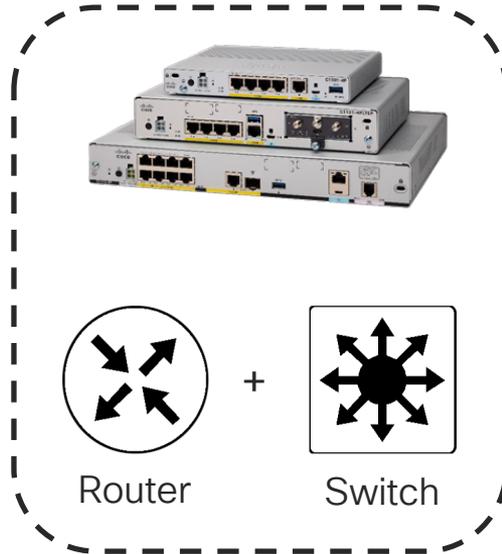
# What is Enterprise Network Compute System?

Small Office/Home office  
SOHO device



Unified  
Computing  
System  
(UCS)

+



=



Enterprise Network  
Compute System  
(ENCS)

# Platform Built for Enterprise NFV

- ENCS 5000 Series for the Branch

Best of Routing  
& Compute

Complete  
Virtualized Services

Open for Third Party  
Services and Apps

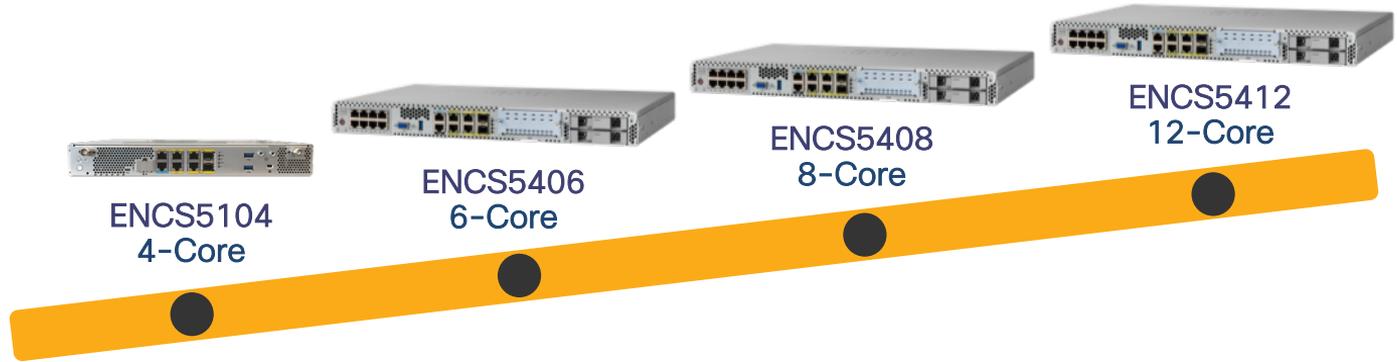
• **Enterprise Network Compute System** •

ENCS 5100 Series



ENCS 5400 Series

# ENCS 5000 Series - Chassis Options



	ENCS 5104	ENCS 5406	ENCS 5408	ENCS 5412
CPU	4-core, 3.4GHz	6-core, 1.9GHz	8-core, 2.0GHz	12-core, 1.5GHz
PoE	No	No	200W	200W
Capacity Guidance	ISRv + 1 VM	ISRv + 2 VMs	ISRv + 3 VMs	ISRv + 5 VMs



# NFV and NFVIS

# What and Why Network Function Virtualisation?

Prior to NFV - physical appliance per network function in each branch



Router



Firewall



WAN optimization

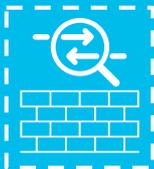


Wireless LAN Controller

NFV gives an opportunity to combine multiple network functions in one ENCS device



Virtual Router  
(ISrV, CSR, vEdge)



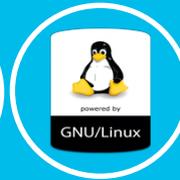
Virtual Firewall  
(ASA v, NGFW v)



Virtual WAN  
Optimization  
(vWAAS)



vWireless LAN  
Controller  
(WLC)



Third-Party  
applications/VNFs

# Purpose built Network Hypervisor Enterprise NFV Infrastructure Software (NFVIS)



## Network Hypervisor

- Supports segmentation of virtual networks
- Abstract CPU, memory, and storage resources



## Zero-Touch Deployment

- Automatic connection to PnP server
- Highly secure connection to the orchestration system
- Easy day-0 provisioning



## Security

- Secure Chain of Trust
- Secure overlay for management and monitoring
- VNF secure boot
- Role Based Access Control



## Lifecycle Management

- Provisioning and launch of VNFs
- Stop and restart services
- Dynamically add and remove services
- Failure monitoring and recovery
- VNF Backup Restore



## Service Chaining

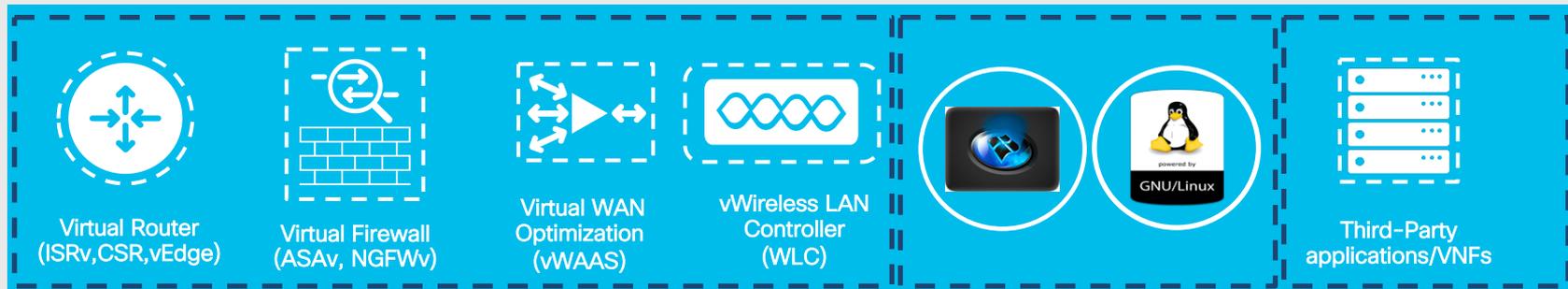
- Elastic service insertion
- PNIC tracking and VNIC update
- Multiple independent service paths based on applications or user profiles
- Host and VM Statistics, Packet Capture



## Open API

- Programmable API for service orchestration
- Rest and NETCONF API
- Netconf Notification

# Network Functions Virtualization Infrastructure Software (NFVIS)



Network Functions Virtualization Infrastructure Software (NFVIS)

Enterprise Network Compute System (ENCS)



# ENCS Demo

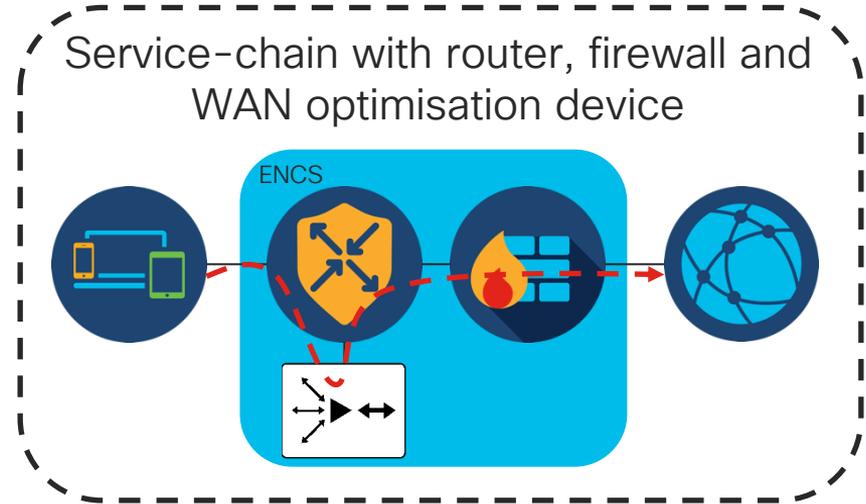
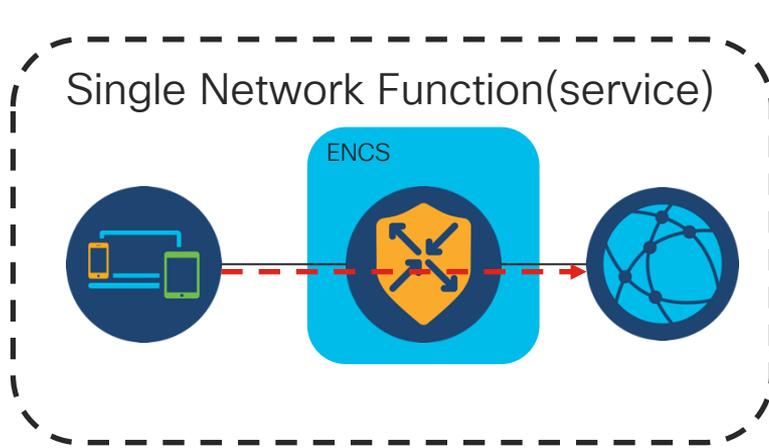


# VNF Service Chaining in SD-WAN



# VNF and Network Types

# What is Service Chain?



---▶ Traffic flow

# Where Do We Start With Virtual Branch Design?

- What Virtual Functions do we need?
- What are the bandwidth requirements?
- Single-homed, dual-homed, multi-homed site?
- L2 or L3 connectivity on the LAN side?

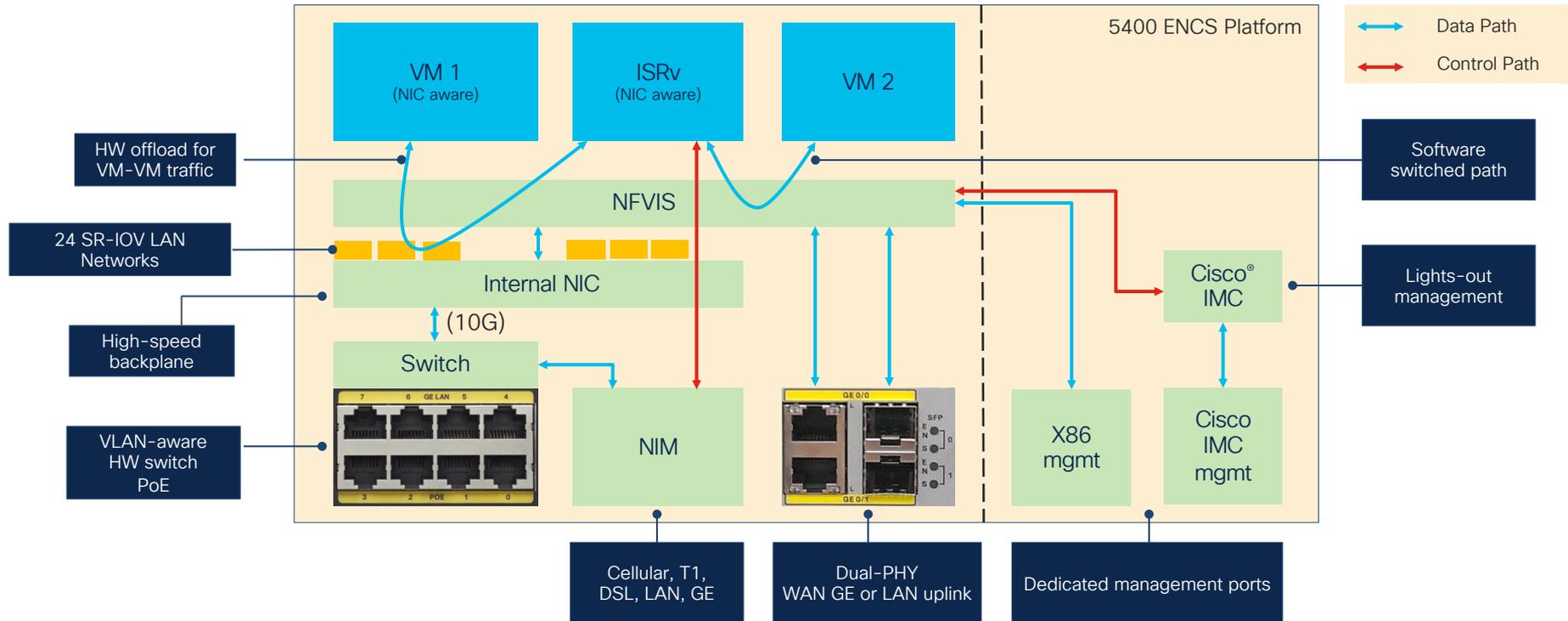
# What SD-WAN Relevant VNFs are Certified?

- Firewalls:
  - ASA v, FTD v, Checkpoint Cloud Guard, FortiGate, NETSCOUT vAED, Palo Alto VM
- Routers:
  - ISR v, vEdge Cloud
- WAN Optimisation:
  - vWAAS and Riverbed SteelHead

# Interface Types

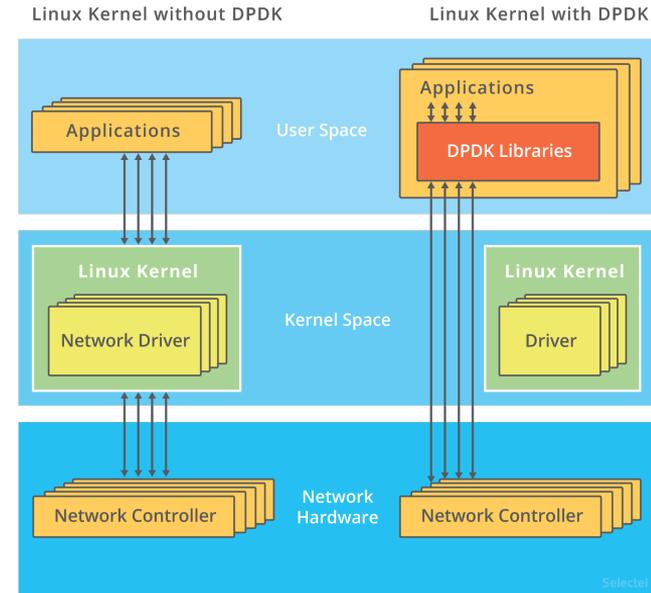
- Open vSwitch(OVS)/virtio - bridges and virtual networks for service chaining between VMs
- SR-IOV - High performance networks
- DPDK - Data Plane Development Kit skips the Linux kernel by processing packets directly in the user space.
- PCI Passthrough - dedicating the entire NIC to the VNF directly

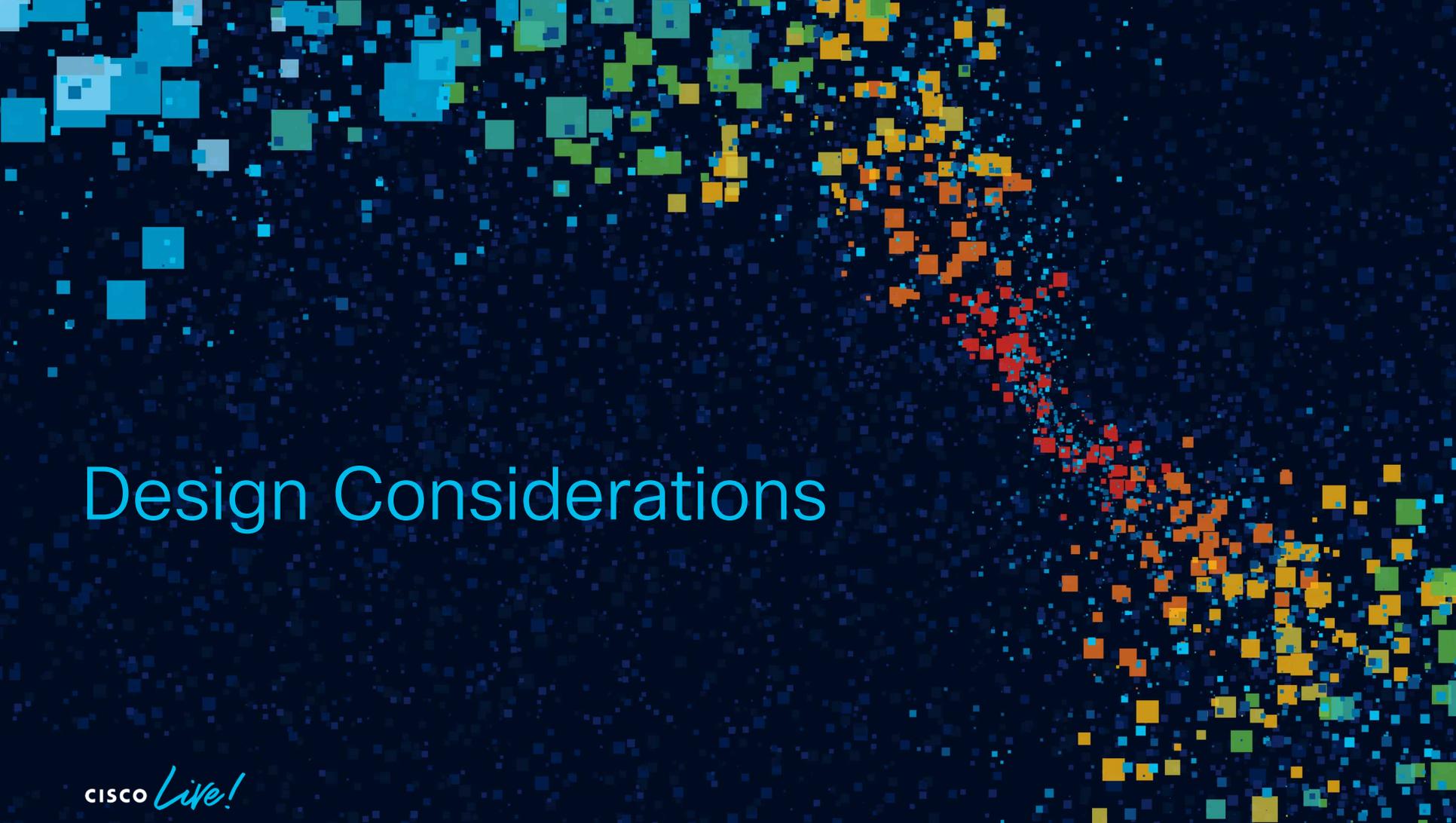
# 5400 ENCS Internal Networking



# Data Plane Development Kit (DPDK)

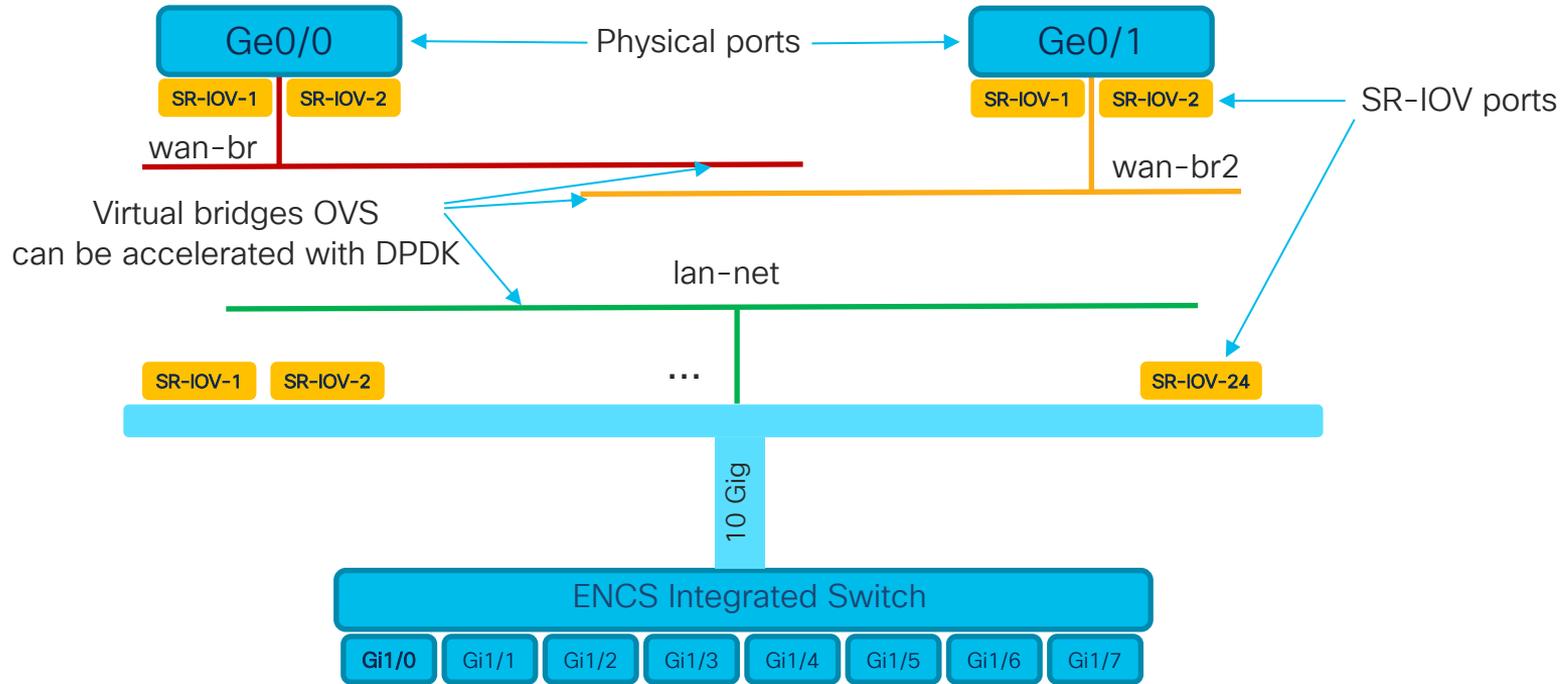
- DPDK skips the Linux kernel by processing packets directly in the user space.
- DPDK reserves a CPU that is constantly polling for new packets.
- Additional resources allocated – 1 CPU and 1 GiB of RAM



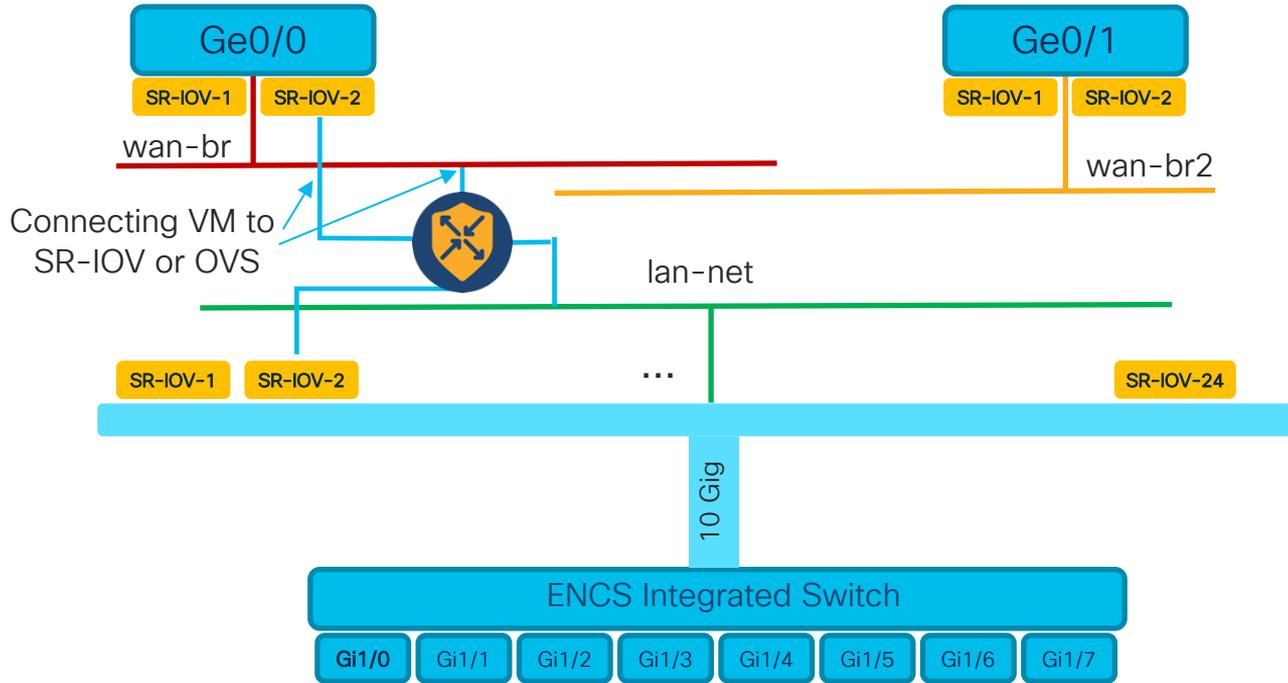


# Design Considerations

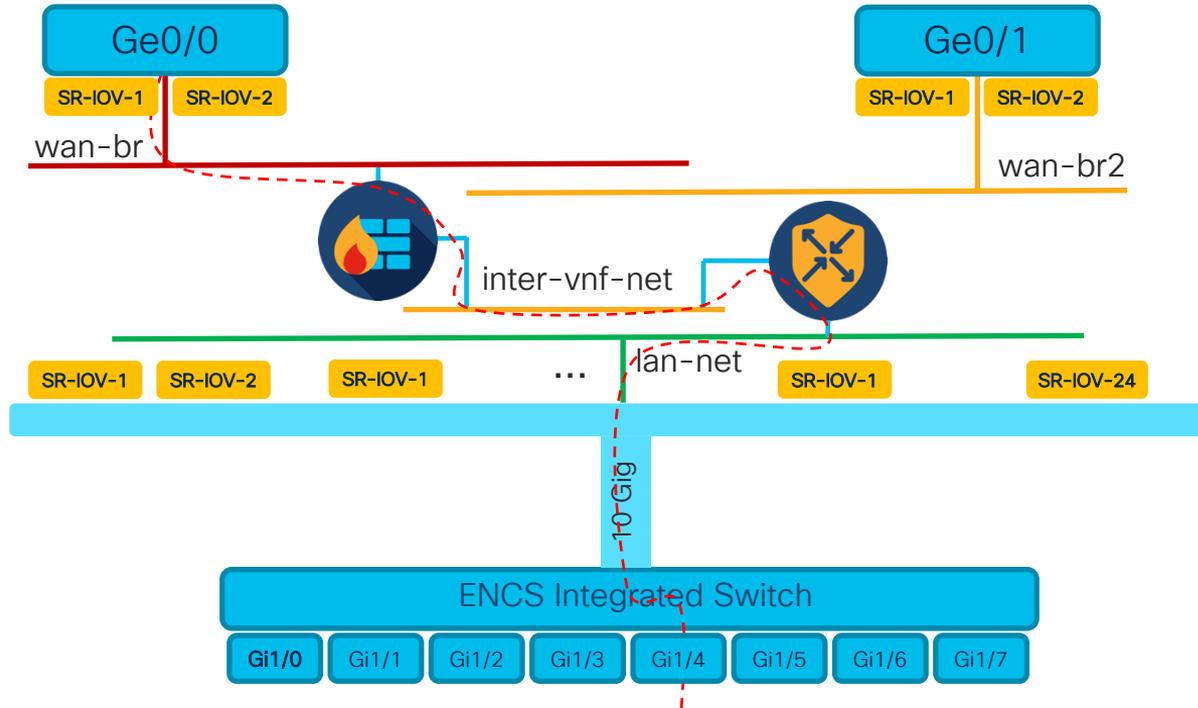
# How to Read the GUI?



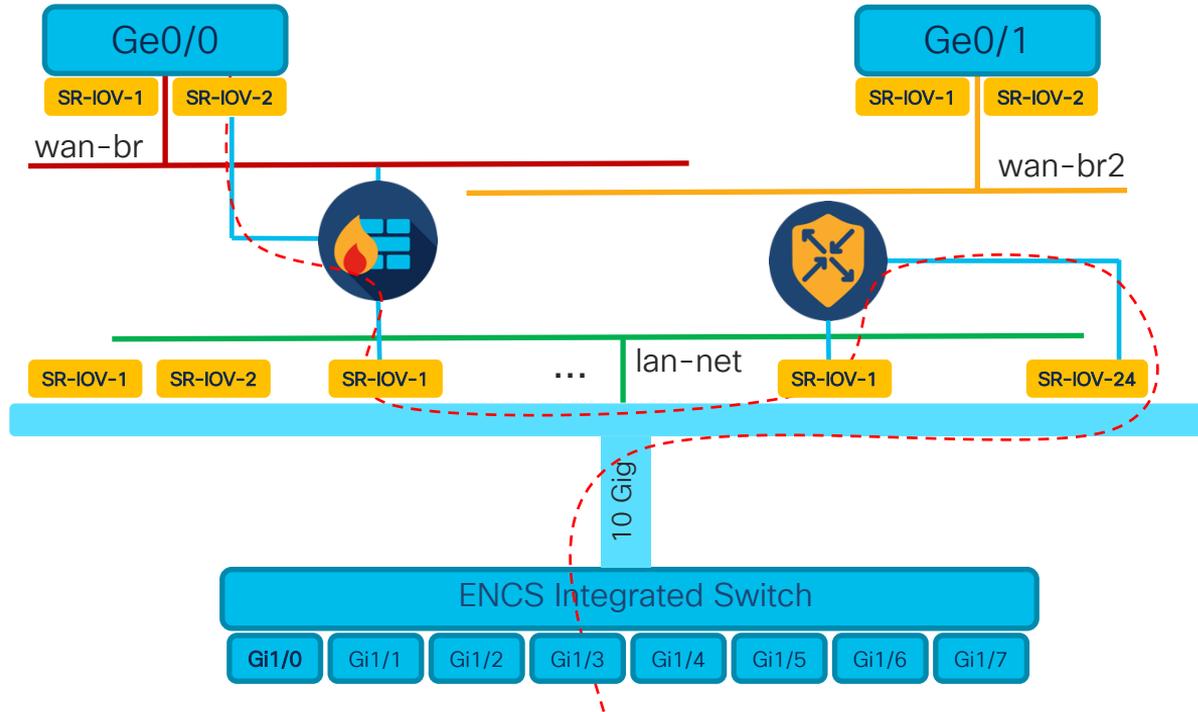
# Adding VNF to the Picture



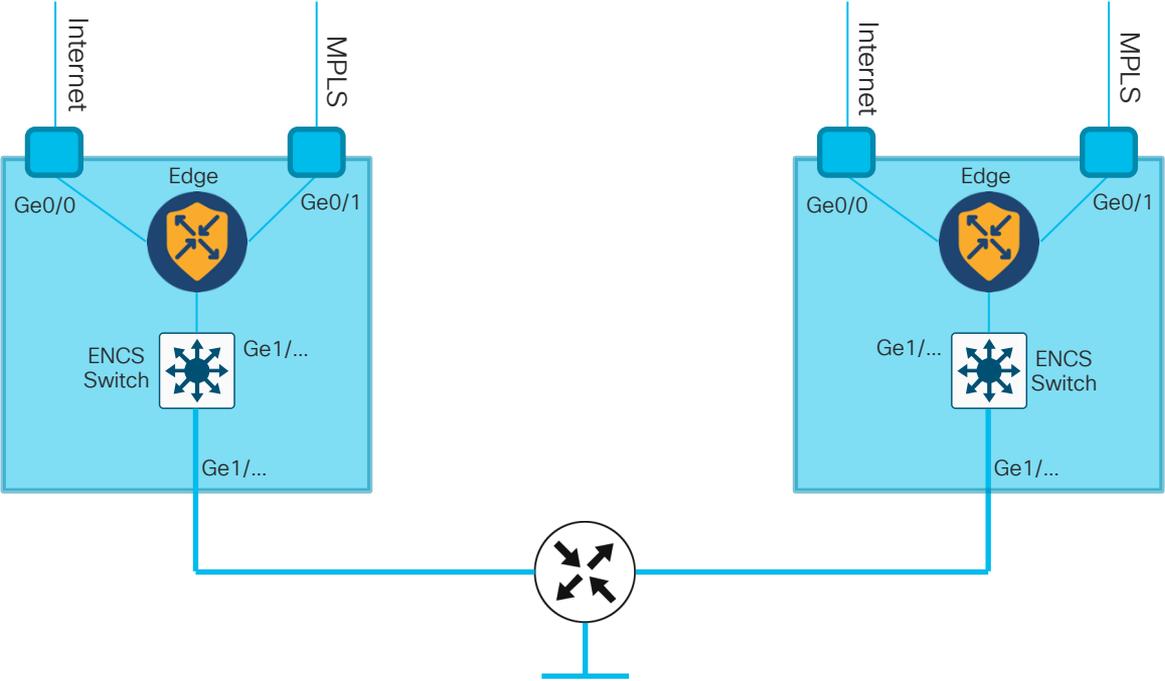
# Connecting Multiple VNFs



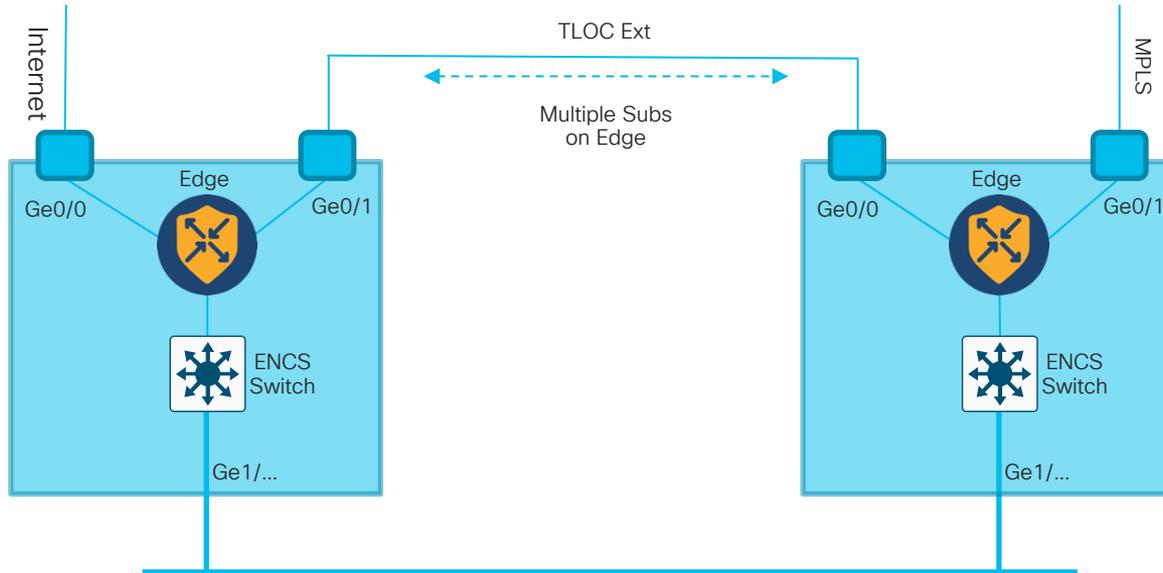
# Connecting Multiple VNFs



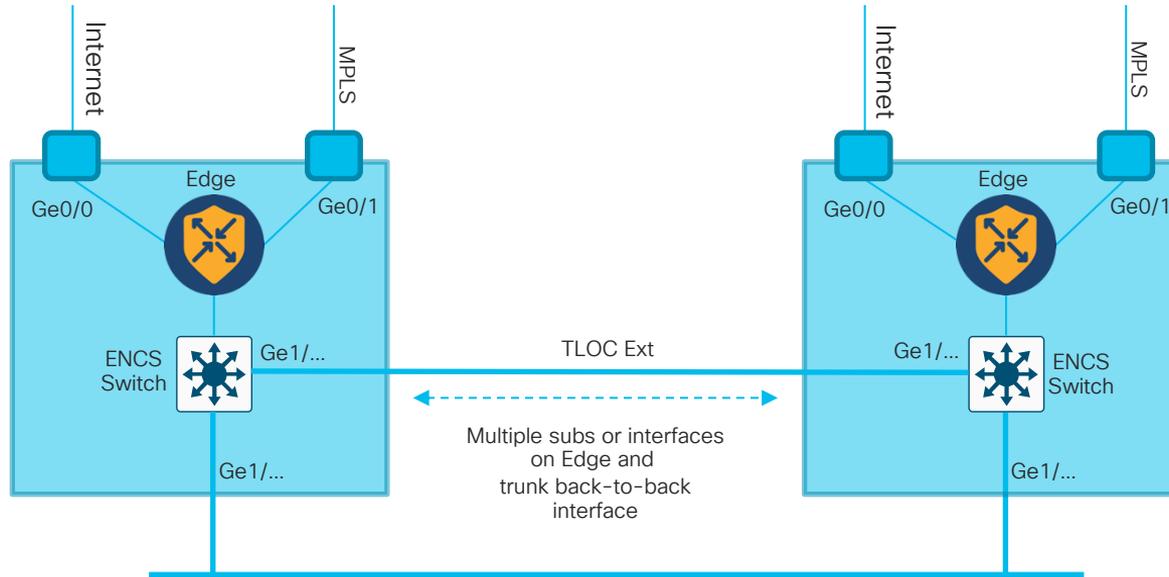
# Multi-Homed Site - L3 on the LAN side



# TLOC Extension Options

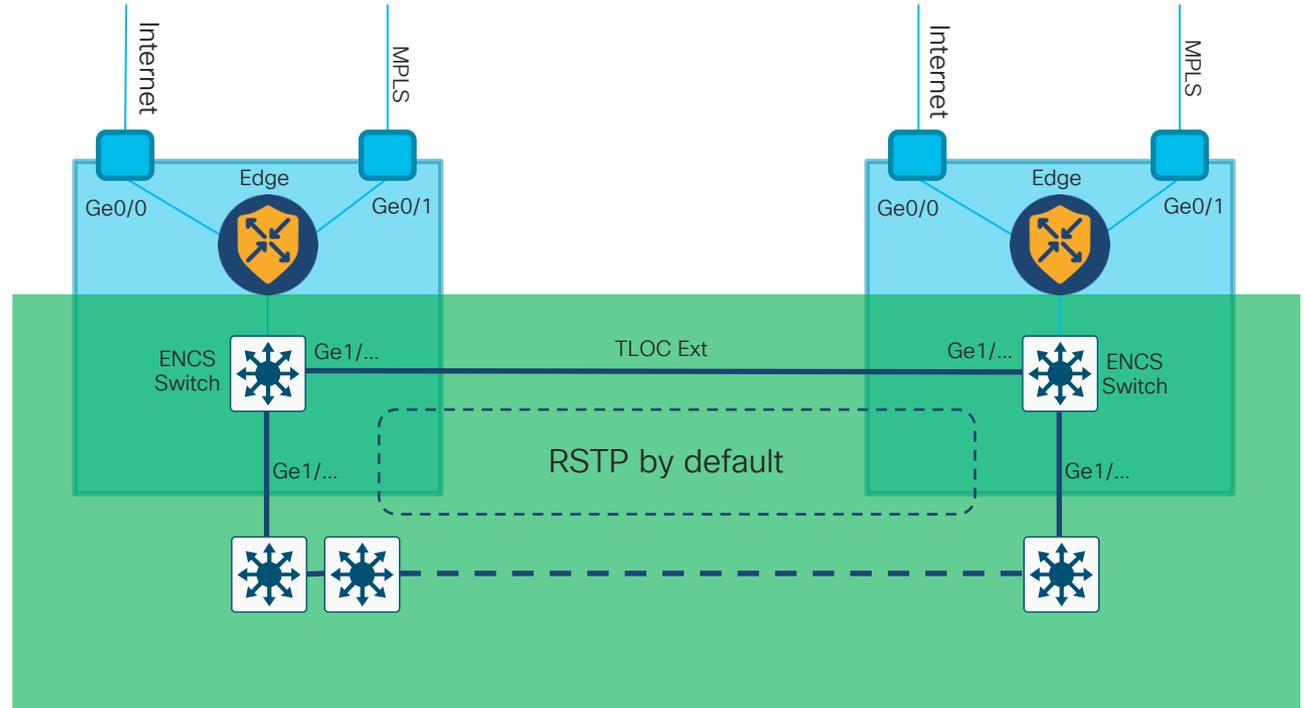


# TLOC Extension Options Cont.



# Spanning Tree Design

- Based on the LAN connectivity you might need to plan L2 domain design
- RSTP is the default spanning-tree mode
- RPVST is not supported
- MST is configurable via CLI



# Using VLANs

# Configuring VLANs on Virtual Networks

The screenshot shows the NFWIS configuration page for a virtual network named 'lan-net'. The interface includes a left-hand navigation menu with options like Home, VM Life Cycle, Deploy, Image Repository, Manage, Networking, Resource Allocation, VM Monitoring, Notifications, Host, About, Switch, ENPV Channel, and Make a Wish. The main configuration area is titled 'Networks & Bridges' and features a 'Submit' button. A table below the configuration form lists existing networks and their configurations.

**Network Configuration Form:**

- Network: lan-net
- Mode: trunk
- Vlan: |
- Native Vlan: trunk
- Bridge: Existing (selected) / Create New
- Interface: Select available interfa

**Networks & Bridges Table:**

Network	Mode	Vlans	Native Vlan	Bridge	Interfaces	Actions
lan-net	trunk			lan-br	int-LAN	
wan-net	trunk			wan-br	GEO-0	
wan2-net	trunk			wan2-br	GEO-1	

Showing 1 to 3 of 3 entries

# Configuring VLANs on SR-IOV prior to 3.12

- SR-IOV is configured as trunk by default
- Configuration changes on SR-IOV should be applied before attaching VM to SR-IOV port
- If you don't want to change NFVIS configuration you can just configure sub-interface on the VM

Configure SRIOV port in NFVIS:

```
conf t
networks network GE0-0-SRIOV-1
trunk true
native-vlan [ 10 ]
vlan [ 100 200 ]
```

```
networks network GE0-0-SRIOV-2
trunk false
vlan [ 100 ]
```

# Configuring VLANs on SR-IOV starting 3.12

NFVIS

ENCS5408/K9 NFVIS-3.12.3-FC4

Wed Apr 29, 03:00:39 PM Welcome admin

administrators

SRIOV Networks

SRIOV Network: GEO-0-SRIOV-1

Interface: GEO-0

Mode: trunk

Vlan:   
access   
trunk

Networks & Bridges

Starting 3.12 you can change SRIOV configuration in:  
VM Life Cycle->Networking tab

SRIOV Networks

Show 5 entries

	SRIOV Network	Interface	Mode	VLAN	Actions
<input type="checkbox"/>	GEO-0-SRIOV-1	GEO-0	trunk		
<input type="checkbox"/>	GEO-0-SRIOV-2	GEO-0	trunk		
<input type="checkbox"/>	GEO-1-SRIOV-1	GEO-1	trunk		
<input type="checkbox"/>	GEO-1-SRIOV-2	GEO-1	trunk		
<input type="checkbox"/>	LAN-SRIOV-1	LAN Switch	trunk		

Showing 1 to 5 of 28 entries

Previous 1 2 3 4 5 6 Next

# Adding VLANs to the Switch

Once you configured VLAN on the ENCS Switch port, don't forget to add it to VLAN list

The screenshot displays the Cisco DNA Center interface. On the left is a navigation sidebar with options like Home, VM Life Cycle, Deploy, Image Repository, Manage, Networking, Resource Allocation, VM Monitoring, Notifications, Host, Switch, About, ENFV Channel, and Make a Wish. The main area is divided into three sections:

- SwitchPort Table:** A table listing switch ports and their configurations. The row for GigabitEthernet1/2 is highlighted with a red box, showing it is configured for access mode and VLAN 100. A blue arrow points from the text on the left to this row.
- VLAN List:** A section titled 'VLAN' showing a list of configured VLANs. The entry '1,100' is highlighted with a red box, and a blue arrow points from the text on the left to it. Below the entry is an 'Edit' button.
- Spanning Tree Table:** A table showing spanning tree statistics for various ports. The row for port 1/2 shows non-zero values for IN-UCAST, OUT-UCAST, IN-MCAST, OUT-MCAST, IN-BCAST, and OUT-BCAST.

SwitchPort	Description	Status	MAC Address	PortType	VLAN	Speed	RXBytes	PktDrop
GigabitEthernet1/0		down	00:b7:71:d9:52:25	access	1	1000	0	0
GigabitEthernet1/1		down	00:b7:71:d9:52:26	access	1	1000	0	0
GigabitEthernet1/2		down	00:b7:71:d9:52:27	access	100	1000	39452	0
GigabitEthernet1/3		down	00:b7:71:d9:52:28	access	1	1000	0	0
GigabitEthernet1/4		down	00:b7:71:d9:52:29	access	1	1000	0	0
GigabitEthernet1/5		down	00:b7:71:d9:52:2a	access	1	1000	0	0
GigabitEthernet1/6		down	00:b7:71:d9:52:2b	trunk	1,30,40	1000	0	0
GigabitEthernet1/7		down	00:b7:71:d9:52:2c	access	1	1000	0	0

PORT	IN-UCAST	OUT-UCAST	IN-MCAST	OUT-MCAST	IN-BCAST	OUT-BCAST
1/0	0	0	0	0	0	0
1/1	0	0	0	0	0	0
1/2	1275313999	1431535137	57373	1681333	39452	35451
1/3	0	0	0	0	0	0
1/4	0	0	0	0	0	0
1/5	0	0	0	0	0	0
1/6	0	0	0	0	0	0
1/7	0	0	0	0	0	0



# Image Management and VNF deployment

# VM Image Packaging

- Converting qcow2 and img images into tar.gz
- Adds SR-IOV drivers to images
  - ISRV package “.tar.gz” is available on cisco.com
  - To create vEdge Cloud package you need build-in tool in the NFVIS GUI or use python script in the CLI
- A tar.gz file containing
  - qcow2 disk image (\*.qcow)
  - Image properties file (Image\_properties.xml)
  - Package Manifest (package.mf)

# VM Image Package Files

- Image properties file (Image\_properties.xml)
  - VM Type
  - Resource requirement (vCPU, Memory etc.,)
  - Profile

```
<?xml version="1.0" encoding="UTF-8"?>
<image_properties>
  <vnf_type>ROUTER</vnf_type>
  <name>ISRV</name>
  <version>RELVER</version>
  <bootup_time>600</bootup_time>
  <root_file_disk_bus>virtio</root_file_disk_bus>
  <root_image_disk_format>qcow2</root_image_disk_format>
  <vcpu_min>1</vcpu_min>
  <vcpu_max>8</vcpu_max>
  <memory_mb_min>4096</memory_mb_min>
  <memory_mb_max>8192</memory_mb_max>
  <vnic_max>8</vnic_max>
  <vnic_names>vnics:1:GigabitEthernet2</vnic_names>
  <vnic_names>vnics:2:GigabitEthernet3</vnic_names>
  <vnic_names>vnics:3:GigabitEthernet4</vnic_names>
  <vnic_names>vnics:4:GigabitEthernet5</vnic_names>
  <vnic_names>vnics:5:GigabitEthernet6</vnic_names>
  <vnic_names>vnics:6:GigabitEthernet7</vnic_names>
  <vnic_names>vnics:7:GigabitEthernet8</vnic_names>
  <root_disk_gb_min>8</root_disk_gb_min>
  <root_disk_gb_max>8</root_disk_gb_max>
  <console_type_serial>true</console_type_serial>
  <sriov_supported>true</sriov_supported>
  <sriov_driver_list>igb</sriov_driver_list>
  <sriov_driver_list>igbvf</sriov_driver_list>
  <sriov_driver_list>i40evf</sriov_driver_list>
  <pcie_supported>true</pcie_supported>
  <pcie_driver_list>igb</pcie_driver_list>
  <pcie_driver_list>igbvf</pcie_driver_list>
  <pcie_driver_list>i40evf</pcie_driver_list>
  <monitoring_supported>true</monitoring_supported>
  <monitoring_methods>ICMPping</monitoring_methods>
  <low_latency>true</low_latency>
  <privileged_vm>true</privileged_vm>
  <cdrom>true</cdrom>
```

```
<bootstrap_file 1>ovf-env.xml</bootstrap_file 1>
<bootstrap_file 2>iosxe_config.txt</bootstrap_file 2>
<custom_property>
  <tech_package>ax</tech_package>
  <tech_package>security</tech_package>
  <tech_package>ipbase</tech_package>
  <tech_package>appx</tech_package>
</custom_property>
<custom_property>
  <ngio>enable</ngio>
</custom_property>
<profiles>
  <profile>
    <name>ISRV-mini</name>
    <description>ISRV-mini</description>
    <vcpus>1</vcpus>
    <memory_mb>4096</memory_mb>
    <root_disk_mb>8192</root_disk_mb>
  </profile>
  <profile>
    <name>ISRV-small</name>
    <description>ISRV-small</description>
    <vcpus>2</vcpus>
    <memory_mb>4096</memory_mb>
    <root_disk_mb>8192</root_disk_mb>
  </profile>
  <profile>
    <name>ISRV-medium</name>
    <description>ISRV-medium</description>
    <vcpus>4</vcpus>
    <memory_mb>4096</memory_mb>
    <root_disk_mb>8192</root_disk_mb>
  </profile>
</profiles>
<default_profile>ISRV-small</default_profile>
</image_properties>
```

# VM Image Package Files Cont.

- Bootstrap Configuration file (ovf-conf.xml)
  - Login username and password
  - Mgmt interface

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="com.cisco.csr1000v.config-version.1" oe:value="1.0"/>
    <Property oe:key="com.cisco.csr1000v.enable-ssh-server.1" oe:value="True"/>
    <Property oe:key="com.cisco.csr1000v.login-username.1" oe:value="cisco"/>
    <Property oe:key="com.cisco.csr1000v.login-password.1" oe:value="cisco!srv123!"/>
    <Property oe:key="com.cisco.csr1000v.mgmt-interface.1" oe:value="GigabitEthernet1"/>
    !!!GigabitEthernet1-nicid(0)-int-mgmt-interface-don't change ip address or don't shutdown
    <Property oe:key="com.cisco.csr1000v.mgmt-ipv4-addr.1" oe:value="{NICID_0_IP_ADDRESS}/24"/>
    <Property oe:key="com.cisco.csr1000v.mgmt-ipv4-network.1" oe:value=""/>
    <Property oe:key="com.cisco.csr1000v.license.1" oe:value="{TECH_PACKAGE}"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0001" oe:value="vrf definition Mgmt-intf"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0002" oe:value="address-family ipv4"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0003" oe:value="exit-address-family"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0004" oe:value="address-family ipv6"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0005" oe:value="exit-address-family"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0006" oe:value="exit"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0007" oe:value="interface GigabitEthernet1"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0008" oe:value="vrf forwarding Mgmt-intf"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0009" oe:value="ip address ${NICID_0_IP_ADDRESS} ${NICID_0_NETMASK}"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0010" oe:value="no shut"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0011" oe:value="exit"/>
    <Property oe:key="com.cisco.csr1000v.ios-config-0012" oe:value="ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 ${NICID_0_GATEWAY}"/>
  </PropertySection>
</Environment>
```

# VM Image Package Files Cont.

- Package Manifest (package.mf)
  - Checksum
  - File type, name

```
<!-- shasum - for calculating checksum -->
<PackageContents>
  <File_Info>
    <name>isrv-ucmk9.16.10.2-vga.qcow2</name>
    <type>root_image</type>
    <sha1_checksum>9a61ef4e7c79fe6f6d6cf9fa5b3651dac7780624</sha1_checksum>
  </File_Info>
  <File_Info>
    <name>image_properties.xml</name>
    <type>image_properties</type>
    <sha1_checksum>3f78a87d67cfd55e9ba108e7b36b119e0534ef16</sha1_checksum>
  </File_Info>
  <File_Info>
    <name>isrv_ovf_env.xml</name>
    <type>bootstrap_file_1</type>
    <sha1_checksum>aad802de6ef10dc4b4b4c13d7d5d9991e4d89a8c</sha1_checksum>
  </File_Info>
</PackageContents>
```

# Image Packaging GUI

The screenshot displays the NFVIS Image Packaging GUI. The interface is organized into a sidebar on the left and a main content area on the right. The sidebar includes navigation options such as Home, VM Life Cycle, Image Repository, Deploy, Manage, Networking, Resource Allocation, VM Monitoring, Notifications, Host, Switch, About, ENFV Channel, and Make a Wish. The main content area is titled 'NFVIS' and shows the 'Image Packaging' tab selected. The configuration fields are as follows:

- Package Name:** Required Field
- VM Version:** Required Field
- VM Type:** Router
- Srlov Driver(s):** × igb × igbvf × i40evf
- Local/Upload Raw Images (.qcow2/.img):** Local (selected)
- Raw Disk File Bus:** virtio
- Thick Disk Provisioning:** No
- Local/Upload Bootstrap Files:** Local (selected)
- Monitored:** No
- Bootstrap Cloud Init Drive:** cdrom
- Bootstrap Cloud Init Bus:** ide

A 'Submit' button is located at the bottom right of the configuration area.

# Image Packaging GUI Cont.

Image Registration    Browse Datastore    USB Upload    **Image Packaging**

Package Name

VM Version

VM Type

Dedicate Cores(Optimize)

Serial Console

Sriov Driver(s)

Local  Upload Raw Images (.qcow2/.img)

Drop Files or Click

#	Name	Upload Progress	Size	Status
---	------	-----------------	------	--------

Raw Disk File Bus

Thick Disk Provisioning

Local  Upload Bootstrap Files

Select local files

Monitored

Bootstrap Cloud Init Drive

Bootstrap Cloud Init Bus

▶ Advanced Configuration

# Image Packaging GUI Cont.

Image Registration      Browse Datastore      USB Upload      Image Packaging

VM Packages 

Package Name	File Name	Status	Image Placement	Action
vEdge-SRIOV-19.2	vEdge-SRIOV-19.2.tar.gz	COMPLETE	datastore1(internal)	<a href="#">Register</a> <a href="#">Download</a> <a href="#">Delete</a>

Showing 1 to 1 of 1 entries

Previous 1 Next

# Image Packaging CLI

- VM packaging utility located in VM Life Cycle->Image Repository->Browse Datastore->data->intdatastore->vmpackagingutility
- The VM packaging utility contains the following
  - `nfvpt.py` – It is a python based packaging tool that bundles the VM raw disk image/s along with VM specific properties.
  - `image_properties_template.xml` – This is the template file for the VM image properties file, and has the parameters with default values. If the user provides new values to these parameters while creating the VM package, the default values get replaced with the user-defined values.
  - `nfvis_vm_packaging_utility_examples.txt` – This file contains examples on how to use the image packaging utility to package a VM image.
- `nfvpt.py -o isrv.16.10.04 -i isrv-universalk9.16.10.04.qcow2 -n ISRV.16.10.04 -t ROUTER -r 16.10.04 --monitored true --privileged true --bootstrap ovf-env.xml:file1,ios-xe.txt:file2 --min_vcpu 2 --max_vcpu 8 --min_mem 4096 --max_mem 8192 --min_disk 8 --max_disk 8 --vnic_max 8 --optimize true --profile ISRV-small,"ISRV small profile",2,4096,8192 --profile ISRV-medium,"ISRV medium profile",4,4096,8192 --default_profile ISRV-small --sriov_list igb,igbvf,i40evf --custom key:PASSWORD,val:secret`

# VM Deployment

# Deploying VM

Drag and drop VM type or new virt/io network to the area below

NFVIS  
ENC5412/K9 NFVIS-3.9.2-FC4

Mon Sep 30, 09:20:04 AM Welcome admin administrators

### VM Deployment

Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.

ROUTER FIREWALL VWAAS VWLC OTHER NETWORK

GE0-0 (SRIOV-1, SRIOV-2) | GE0-1 (SRIOV-1, SRIOV-2)

wan-net  
glue-network  
int-net  
service-net  
ROUTER

Deploy

#### Image Registration Status

Name	Status
isrv-ucmk9.16.12.1b.tar.gz	ACTIVE
vEdgeCloud-SRIOV.tar.gz	ACTIVE
viptela-edge-18.3.1-genericx86-64.qcow2	ACTIVE
viptela-edge-18.3.5-genericx86-64.qcow2	ACTIVE
viptela-edge-19.1.0-genericx86-64.qcow2	ACTIVE

#### VM Status Overview

##### VM Deployment Status

Name	Status
ROUTER	Active

# Deploying VM Cont.

Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.

VM Deployment

ROUTER FIREWALL vWAAS vWLC OTHER NETWORK

ROUTER

lan-net

wan-net

wan2-net

lan-net

LAN Backplane

LAN Switch

GE 1/0 GE 1/1 GE 1/2 GE 1/3 GE 1/4 GE 1/5 GE 1/6 GE 1/7

Deploy

VM Import

### VM Details

VM Name *	ROUTER	VM name
Image	SDWANImage	Image you are going to use
Profile	ISRv-small	Resource allocation profile or flavour, also defines maximum performance in terms of tunnels and throughput
VNC Password		
TECH PACKAGE	ax	Technology package licence type
NIM	ENABLE	NIM support
Port Number	22	Management configuration, port forwarding, internal MGMT bridge and management ip from the configured subnet
External Port Range	22000-22000	
Source Bridge	MGMT	
Deployment Disk	datastore1(internal)	
Management IP	10.0.0.10	

▼ Add Bootstrap Config

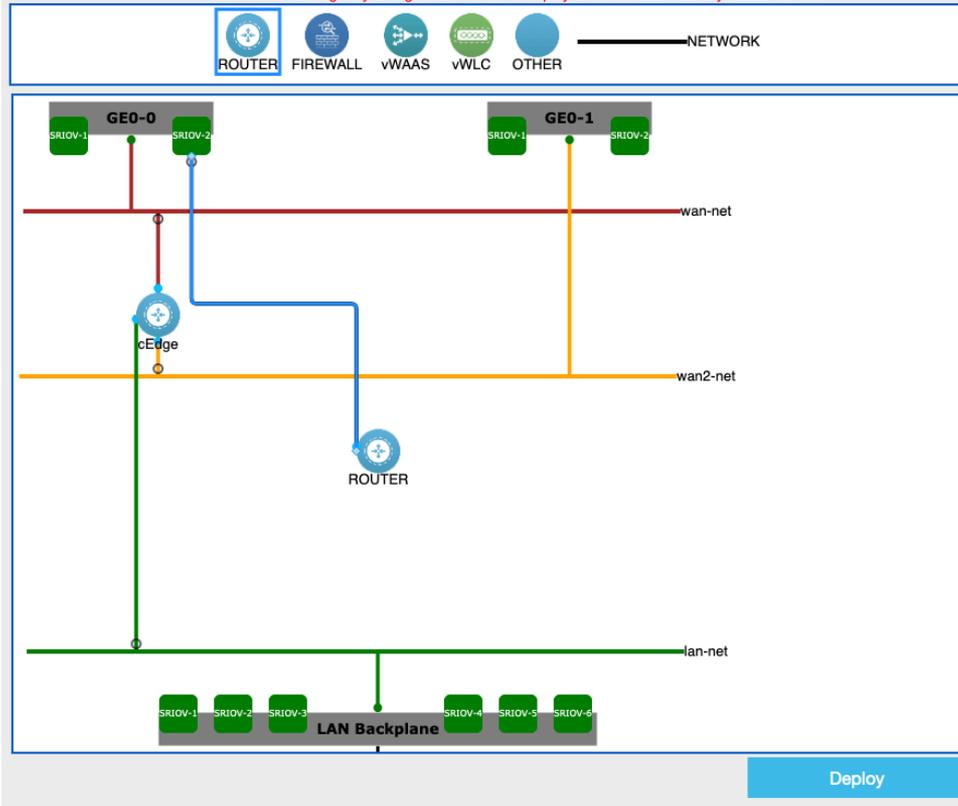
Bootstrap File Name

Bootstrap Payload

► Add Storage

# Deploying VM Cont.

Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.



### VM Import

#### vNIC Details

VM Name	ROUTER
Network Name	GE0-0-SRIOV-2
vNIC id	GigabitEthernet3

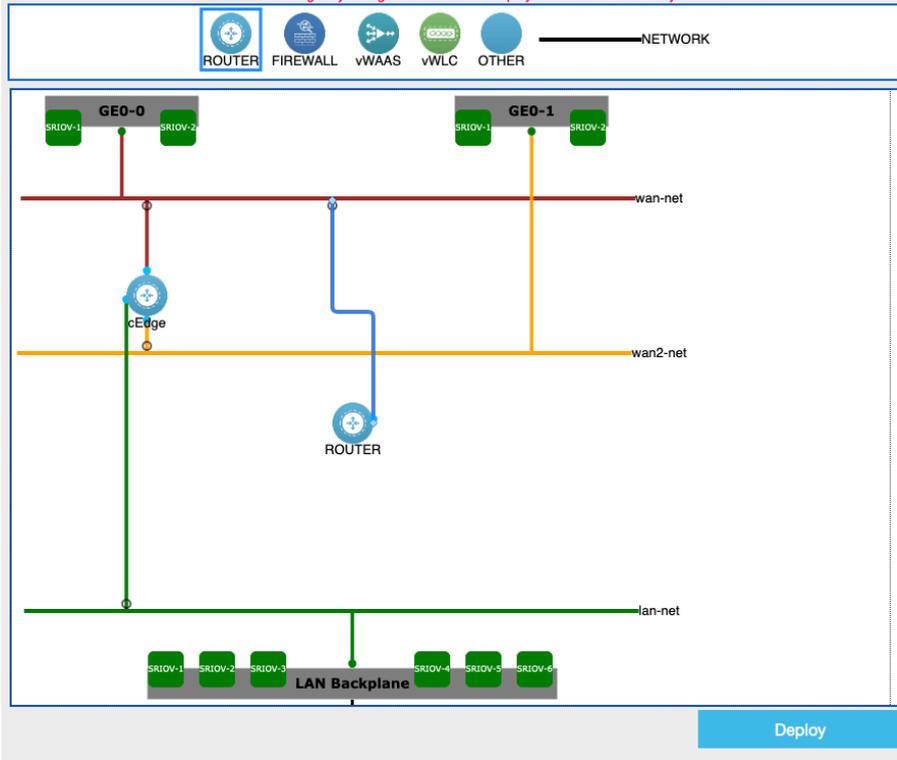
Annotations on the right side of the vNIC details panel:

- Blue arrow pointing to **GE0-0-SRIOV-2**: ENCS SR-IOV interface
- Blue arrow pointing to **GigabitEthernet3**: VM interface

A blue **Deploy** button is located at the bottom of the panel.

# Deploying VM Cont.

Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.



### VM Import

#### vNIC Details

VM Name	ROUTER
Network Name	wan-net
vNIC id	GigabitEthernet2
Model	virtio

Virtual network name

VM interface

Type of the virtual interface

# vEdge Cloud and ISRv Flavours

- vEdge Cloud using 1 core for the system and the rest for the forwarding, you can have 2 flavours 2 cores or 4 cores
- vEdge Cloud gives better performance with 8 Gig of RAM
- ISRv will also take 1 core for OS others for forwarding
- ISRv can allocate additional cores for security features which require use of containers

# Interface Performance

- SRIOV and DPDK in theory should provide performance close to interface speed, in reality performance is affected by feature set, DPI, Firewall, IPS etc. it all slows down the maximum performance and needs to be tested.
- OVS is capable to provide performance up to a few hundred Mbps with same remarks regarding feature set.
- PCI path-though same as SRIOV and DPDK
- VNF can have performance limitations, also important to look at the datasheet before deploying high performance interfaces.

# Monitored VM Caveat

- When VM is monitored – it is connected to internal NFVIS management network.
- If this address is not reachable, NFVIS will reload the VM (be careful applying template from vManage).
- If after 3 reloads VM is not reachable on this management interface, it will be moved to the error state even being fully operational.
- If VM is not monitored first interface you create will be management interface

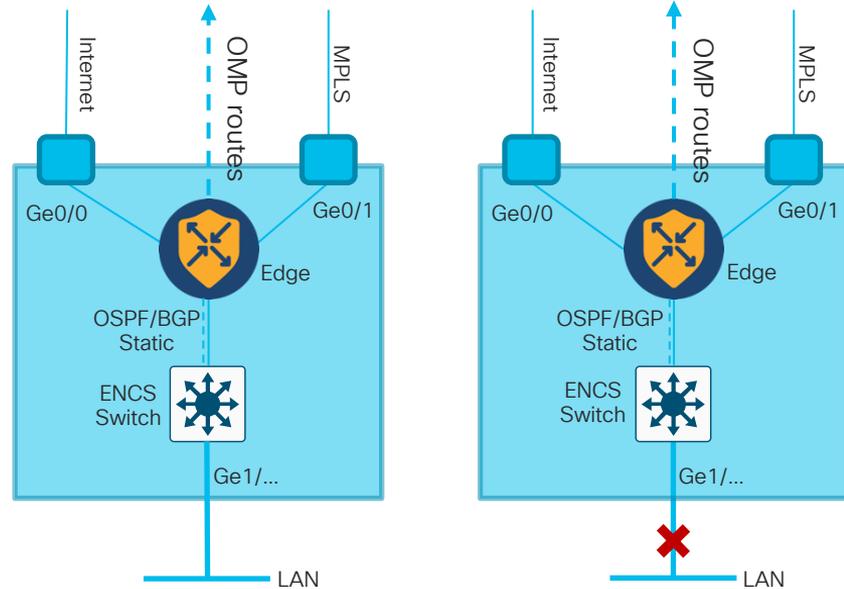
# VM Deployment Demo



# High Availability Design Considerations

# LAN Failure

- OMP update time is equal to routing protocol timers
- BFD is not supported on SD-WAN VNFs till 20.2/17.3
- WAN bandwidth can be utilised but traffic is dropped on the remote end



# VRRP LAN Failure

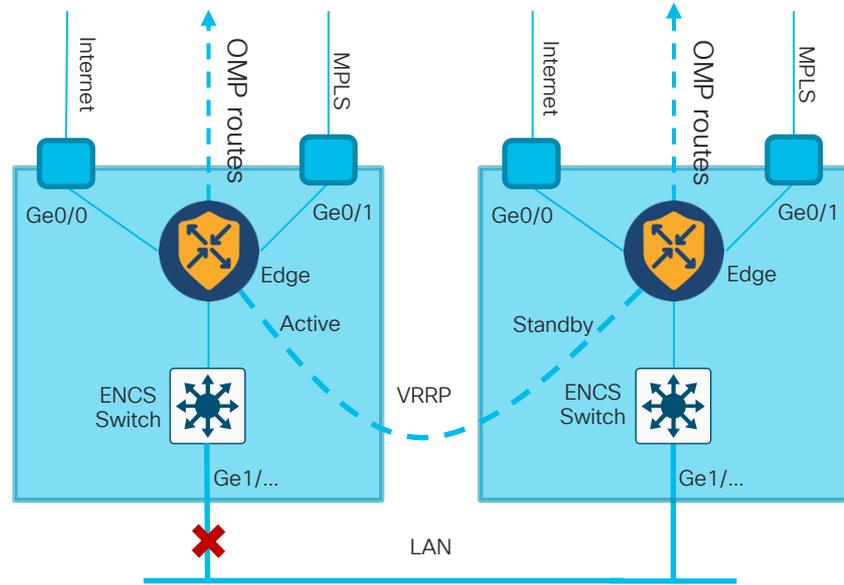
Port tracking is developed to resolve this issue.

Configuration example:

```
conf t
switch
interface gi1/...
track-state <vm_name> <NICID>
```

To find NICID:

```
show vm_lifecycle deployments
<vm_name>
```



# VRRP LAN Failure

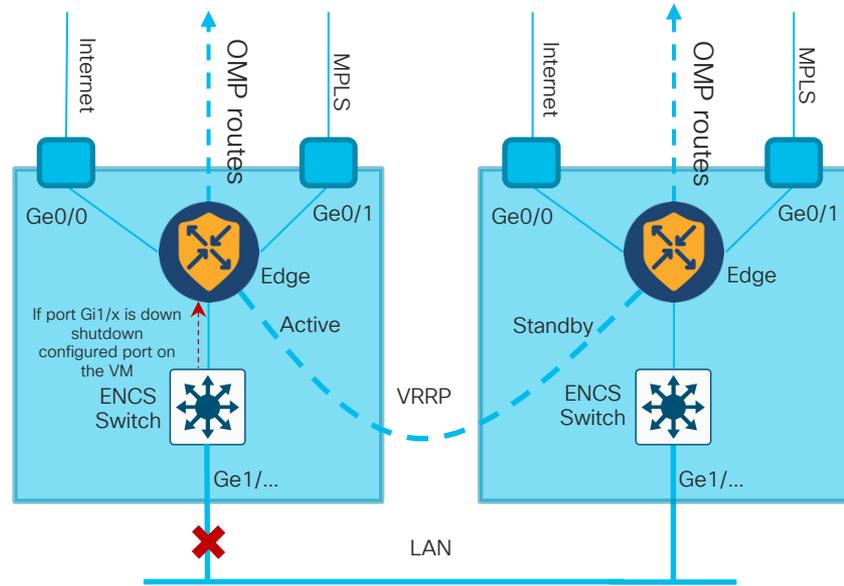
Port tracking is developed to resolve this issue.

Configuration example:

```
conf t
switch
interface gi1/...
track-state <vm_name> <NICID>
```

To find NICID:

```
show vm_lifecycle deployments
<vm_name>
```



# VRRP LAN Failure

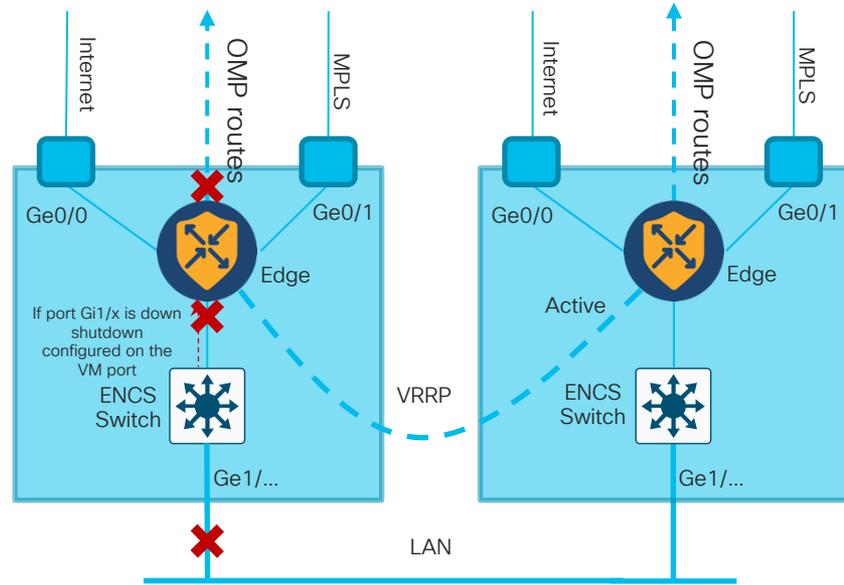
Port tracking is developed to resolve this issue.

Configuration example:

```
conf t
switch
interface gi1/...
track-state <vm_name> <NICID>
```

To find NICID:

```
show vm_lifecycle deployments
<vm_name>
```



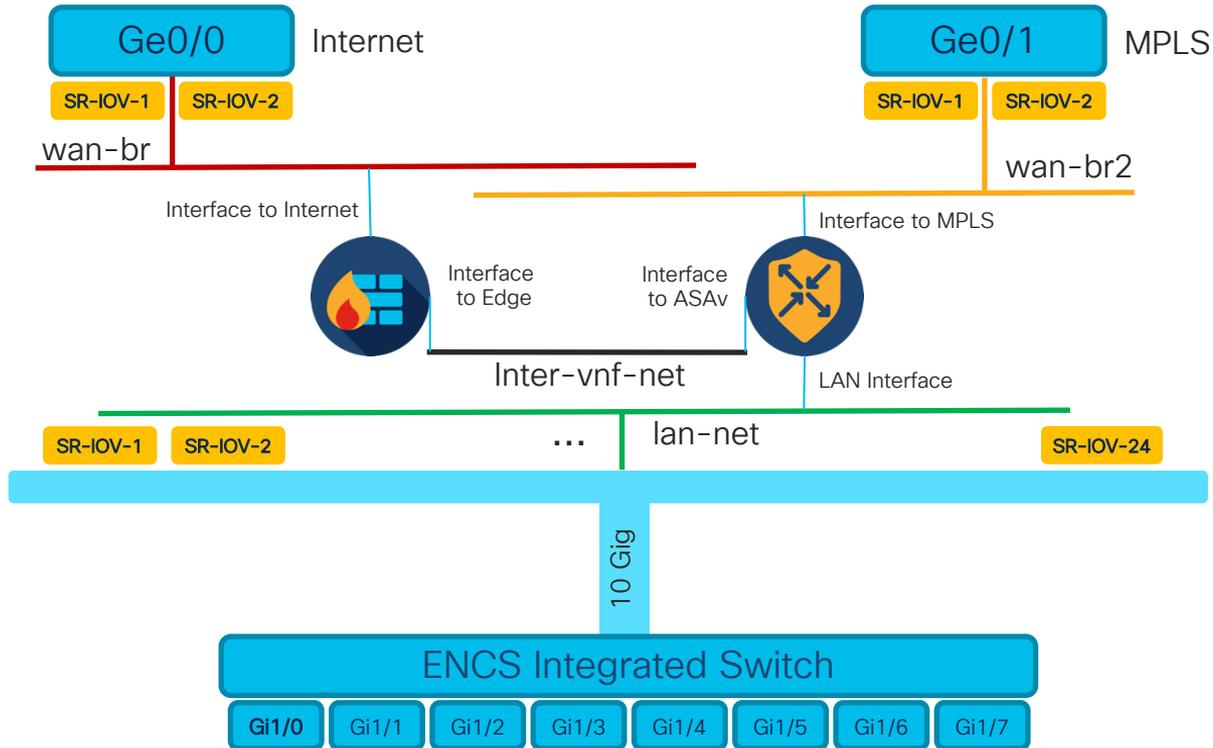
# Few Caveats For vEdge Cloud

- For vEdge Cloud VRRP on SRIOV is supported starting 19.2 but due to Intel NIC packet processing, additional fixes in the drivers needed and full support expected in NFVIS 4.2.1 July 2020
- Port tracking for SRIOV is supported on NFVIS 3.12.3
- DPI supports ~140k flows per CPU.

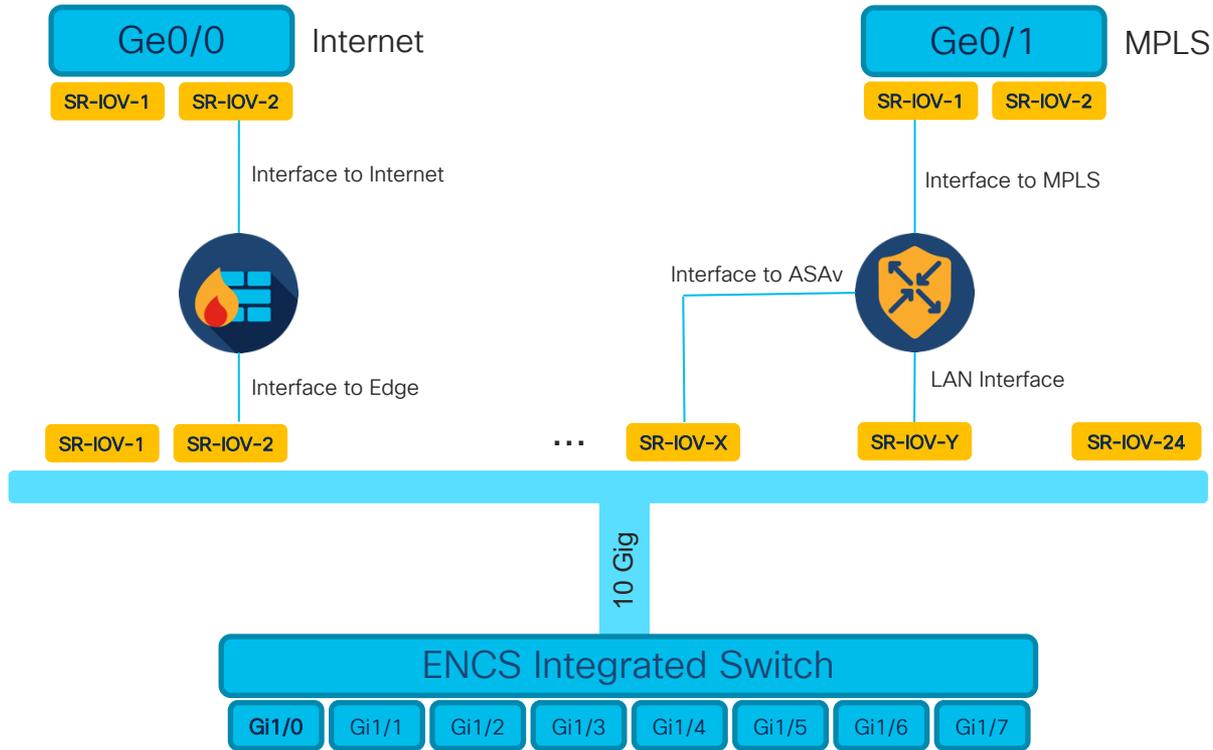


# Virtual Branch Design Scenarios

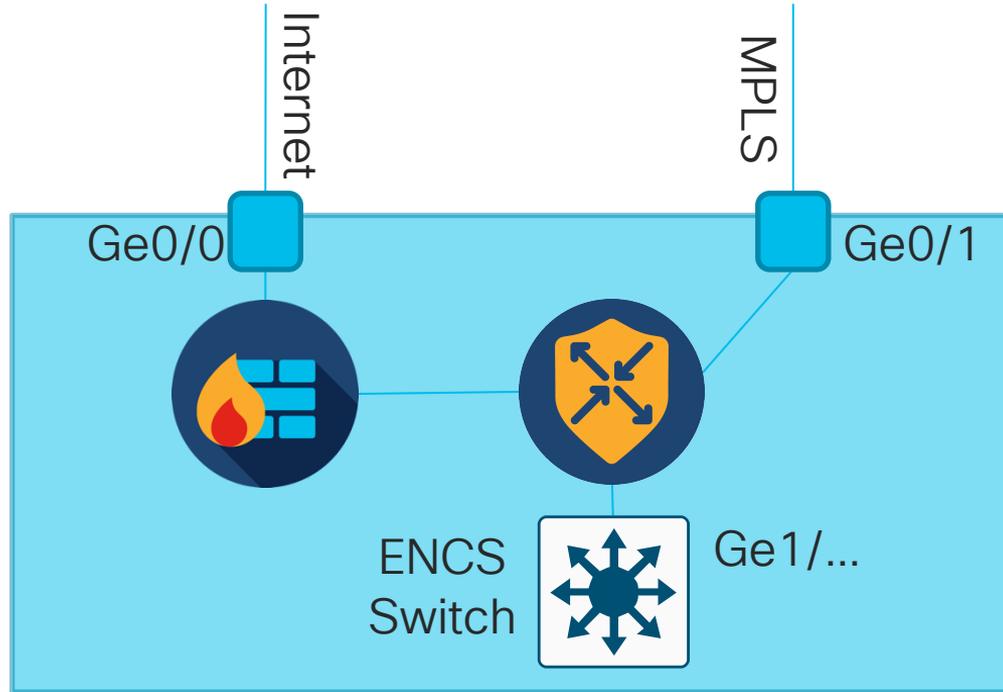
# vEdge/ISRv + ASA v + OVS



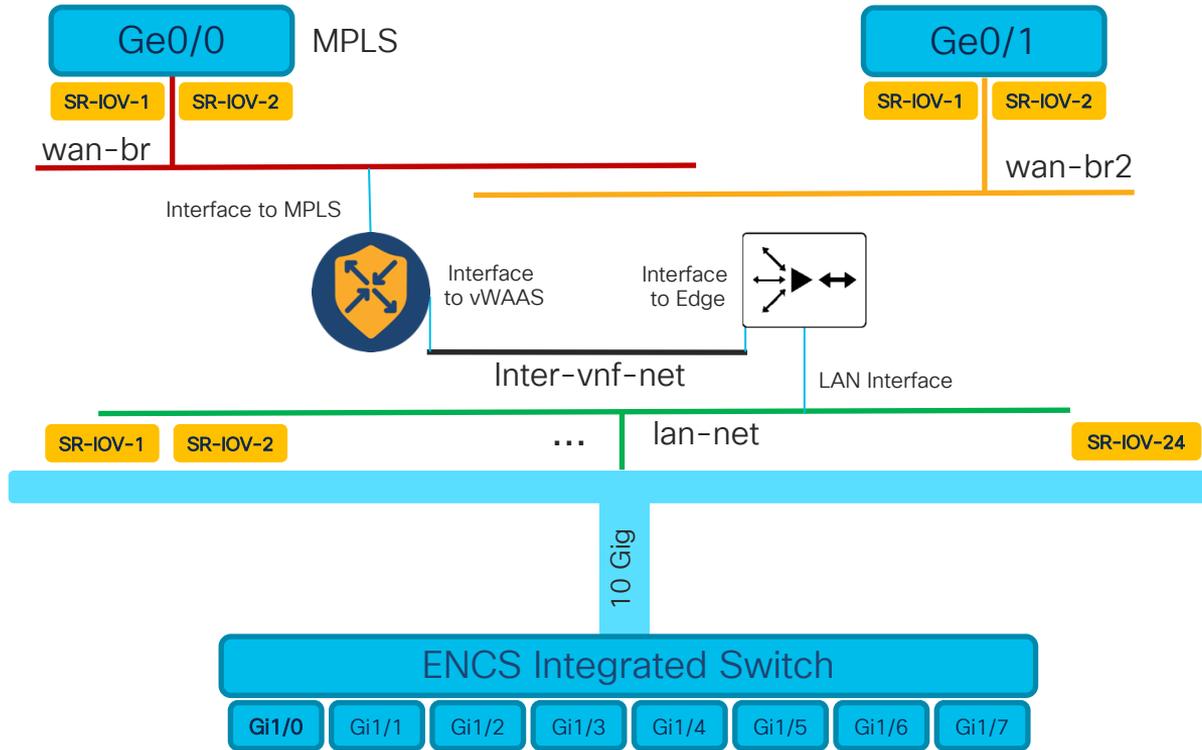
# vEdge/ISRv + ASA v + SRIOV



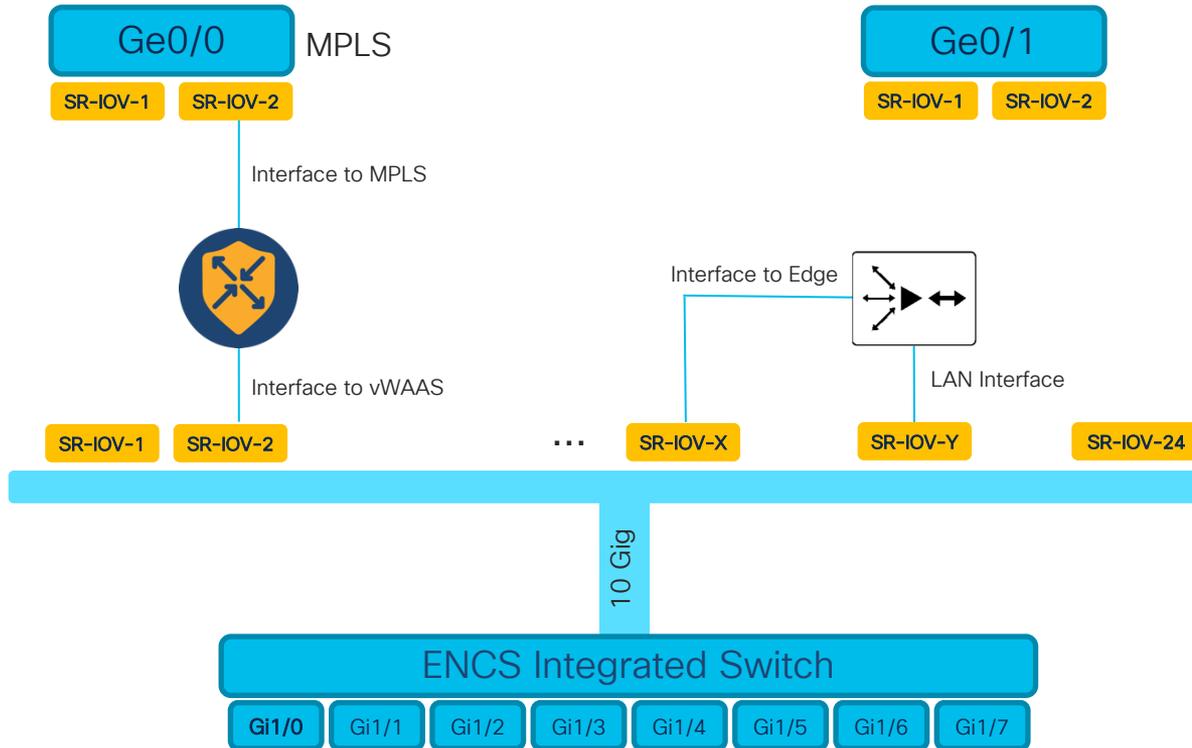
# vEdge/ISRv + ASA v



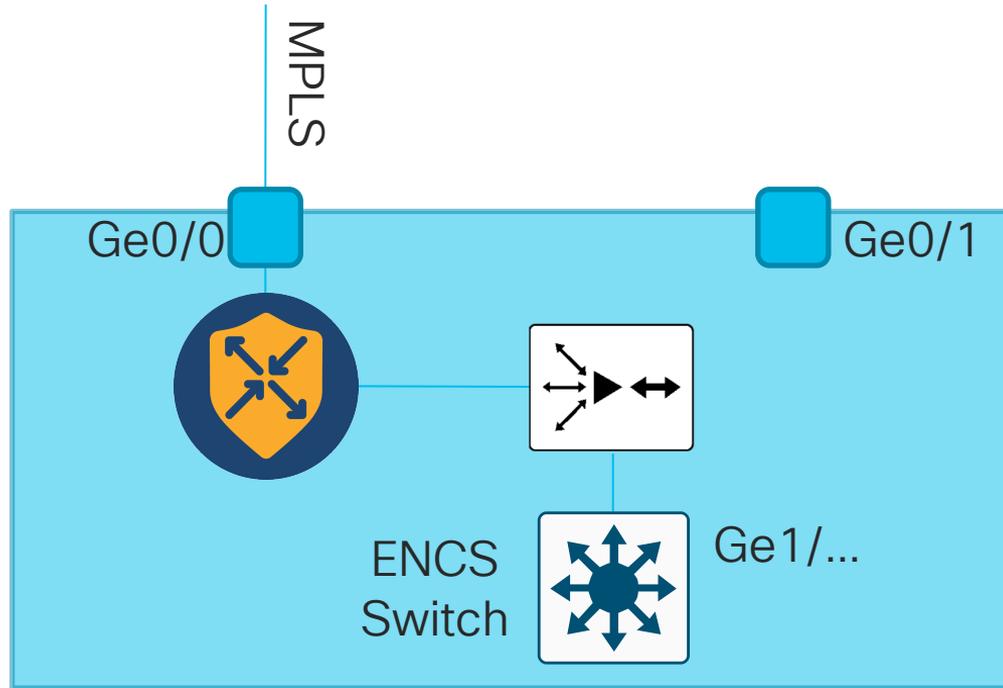
# vEdge/ISRv + vWAAS/SteelHead In-path + OVS



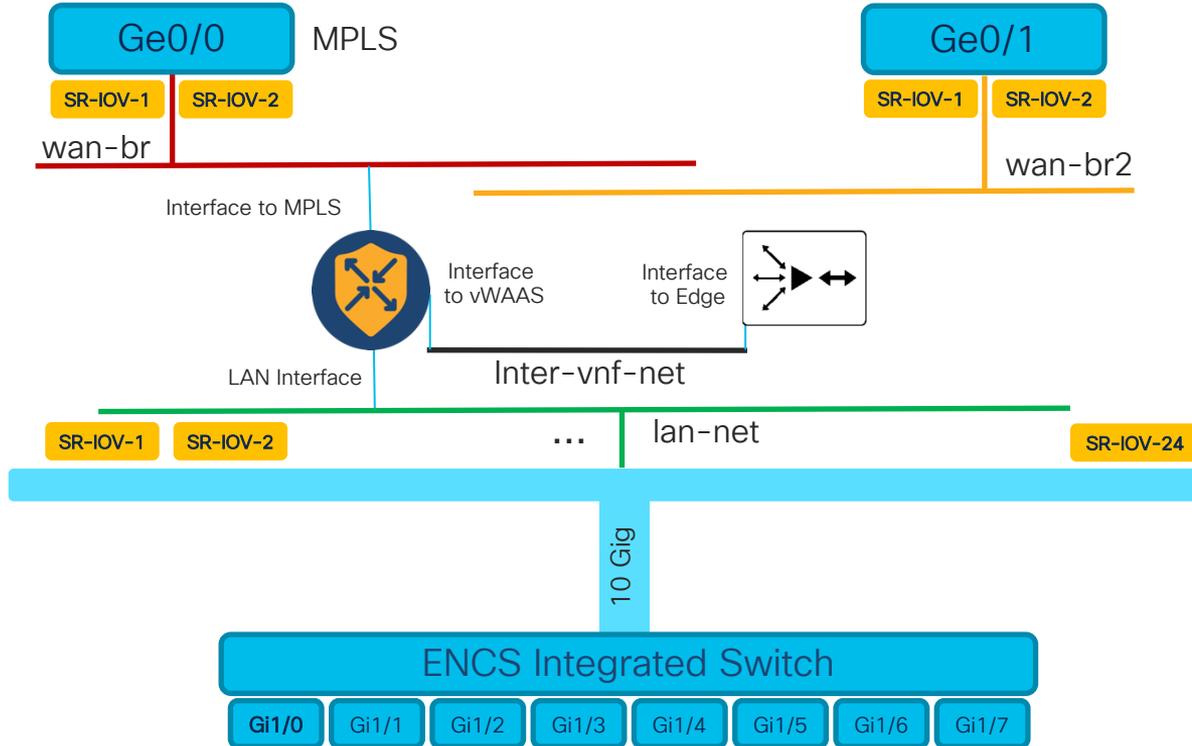
# vEdge/ISRv + vWAAS/SteelHead In-path + SRIOV



# vEdge/ISRv + vWAAS/SteelHead In-path

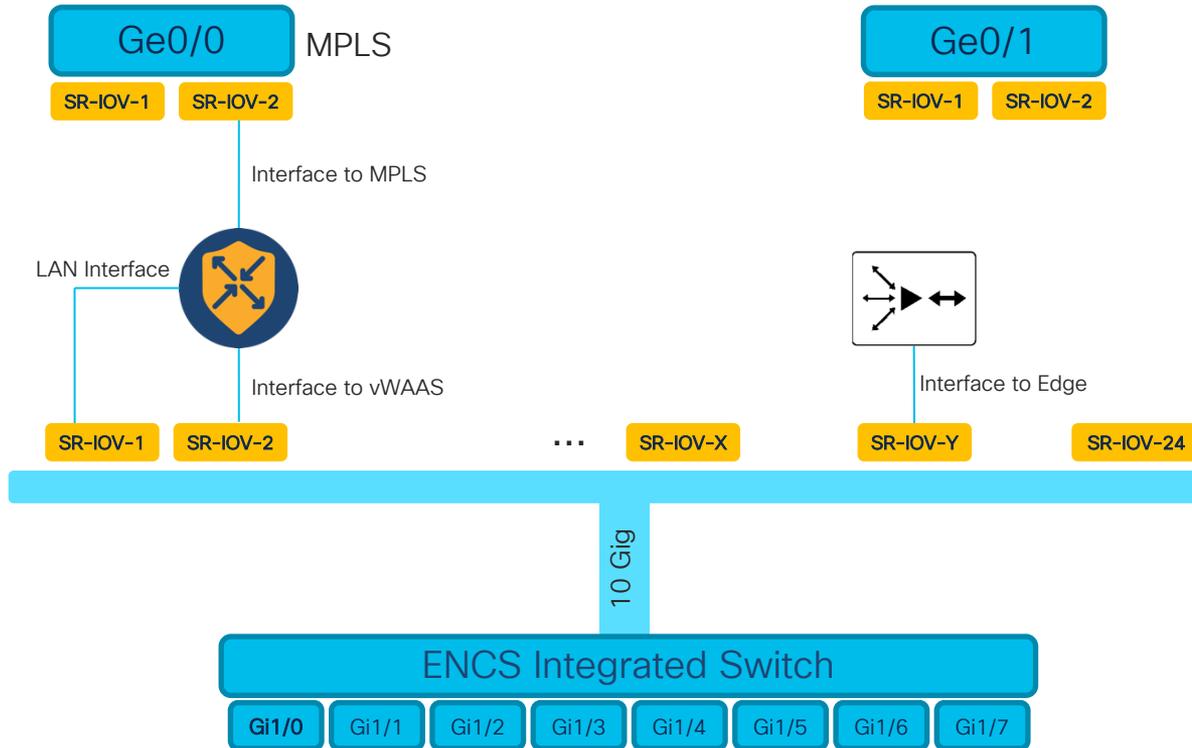


# ISRV + vWAAS Out-of-path + OVS



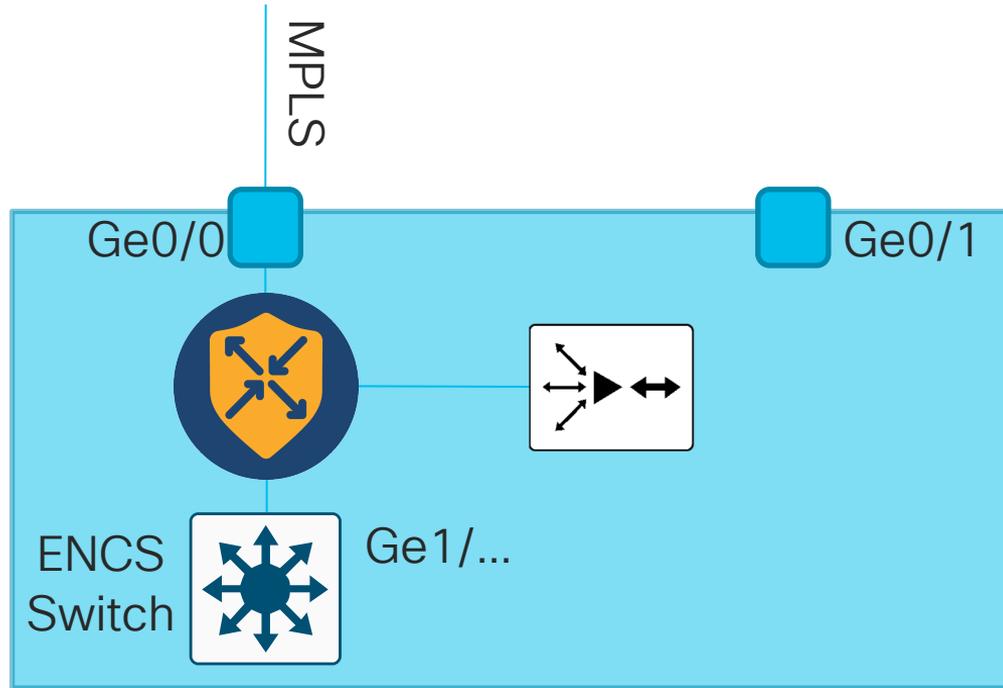
\*Supported starting 20.1/17.2.1 with AppNav-XE and full SD-WAN WAAS integration

# ISRv + vWAAS Out-of-path + SRIOV



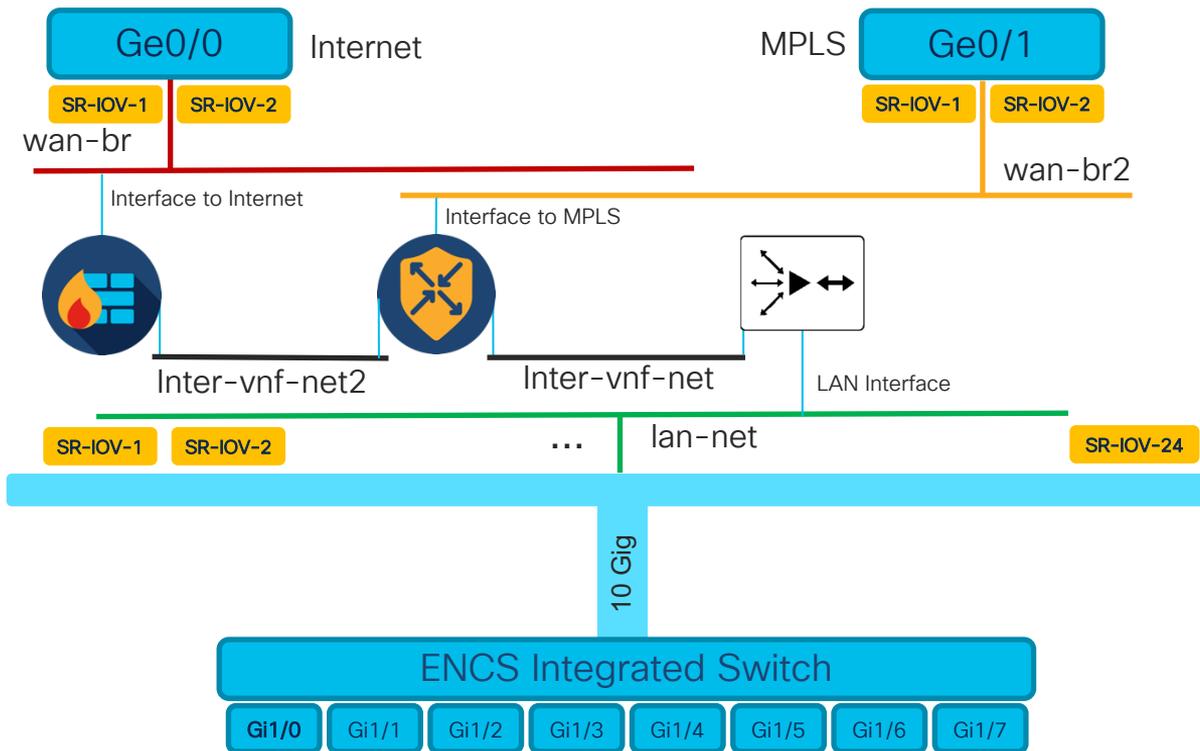
\*Supported starting 20.1/17.2.1 with AppNav-XE and full SD-WAN WAAS integration

# ISRv + vWAAS Out-of-path

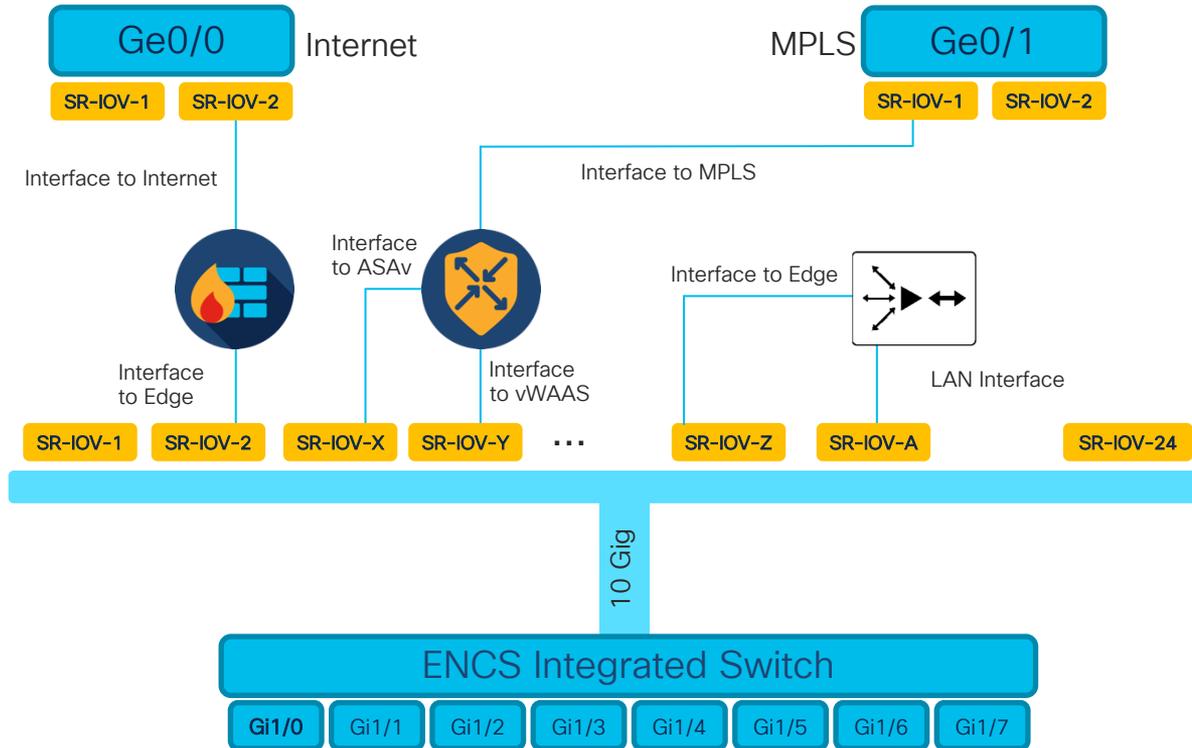


\*Supported starting 20.1/17.2.1 with AppNav-XE and full SD-WAN WAAS integration

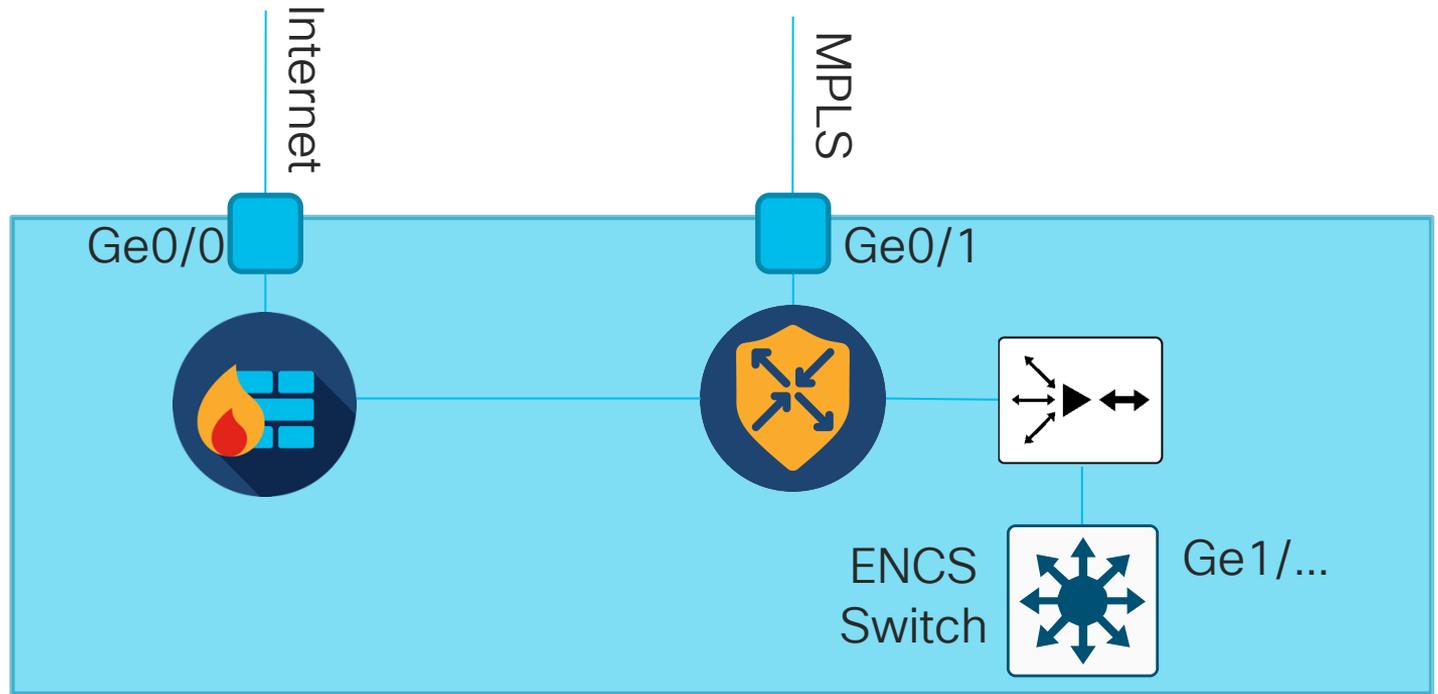
# vEdge/ISRv + vWAAS/SteelHead In-path + ASA v + OVS



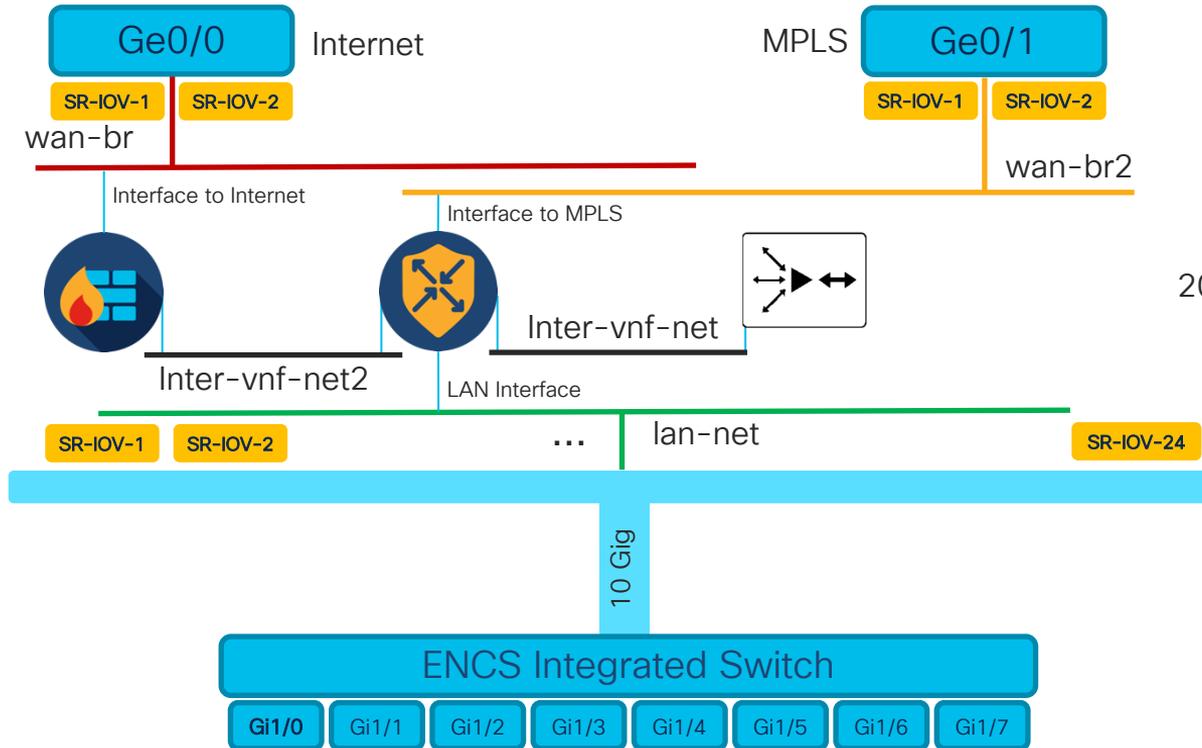
# vEdge/ISRv + vWAAS/SteelHead In-path + ASA v + SRIOV



# vEdge/ISRv + vWAAS/SteelHead In-path + ASA v



# ISRv + vWAAS Out-of-path + ASAv + OVS

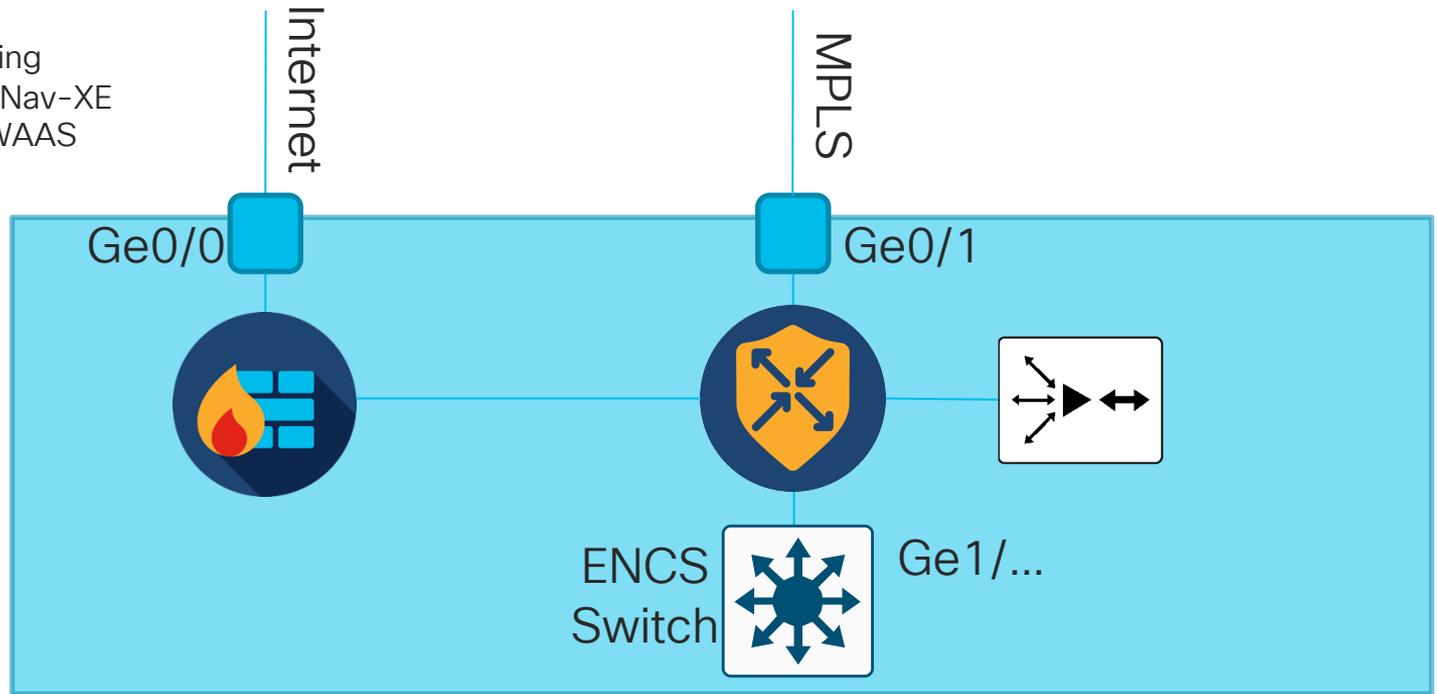


\*Supported starting 20.1/17.2.1 with AppNav-XE and full SD-WAN WAAS integration

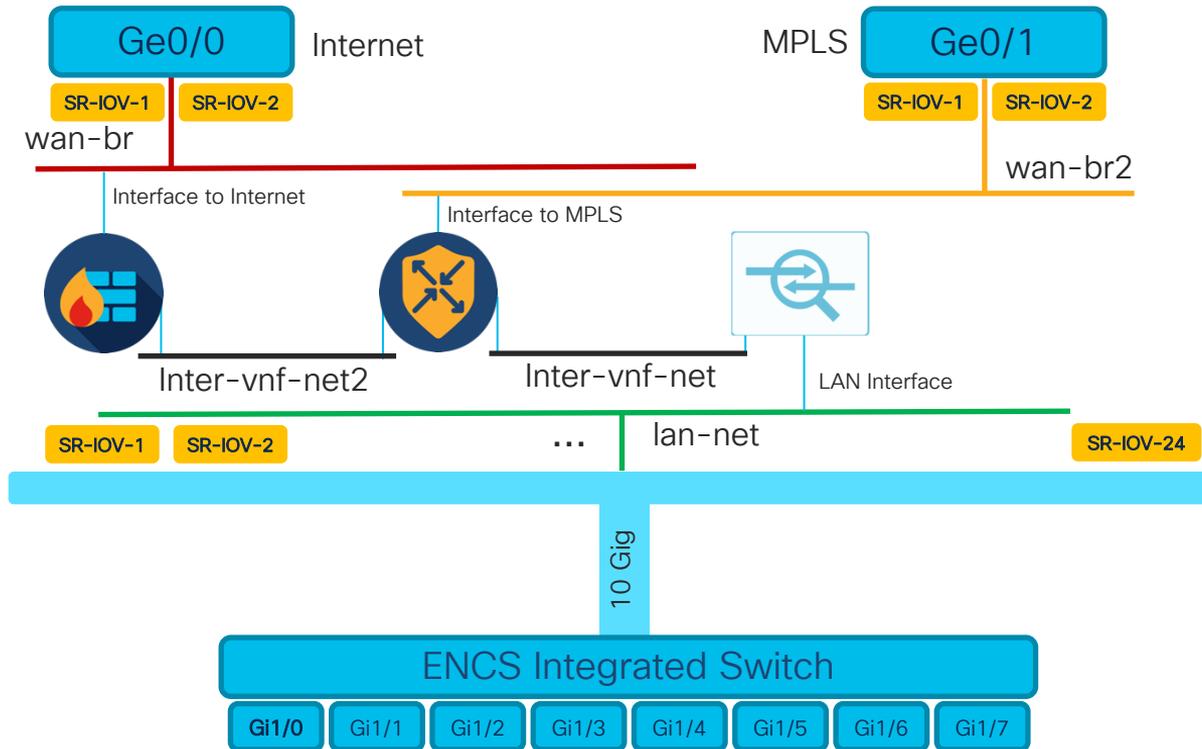


# ISRv + vWAAS Out-of-path + ASA v

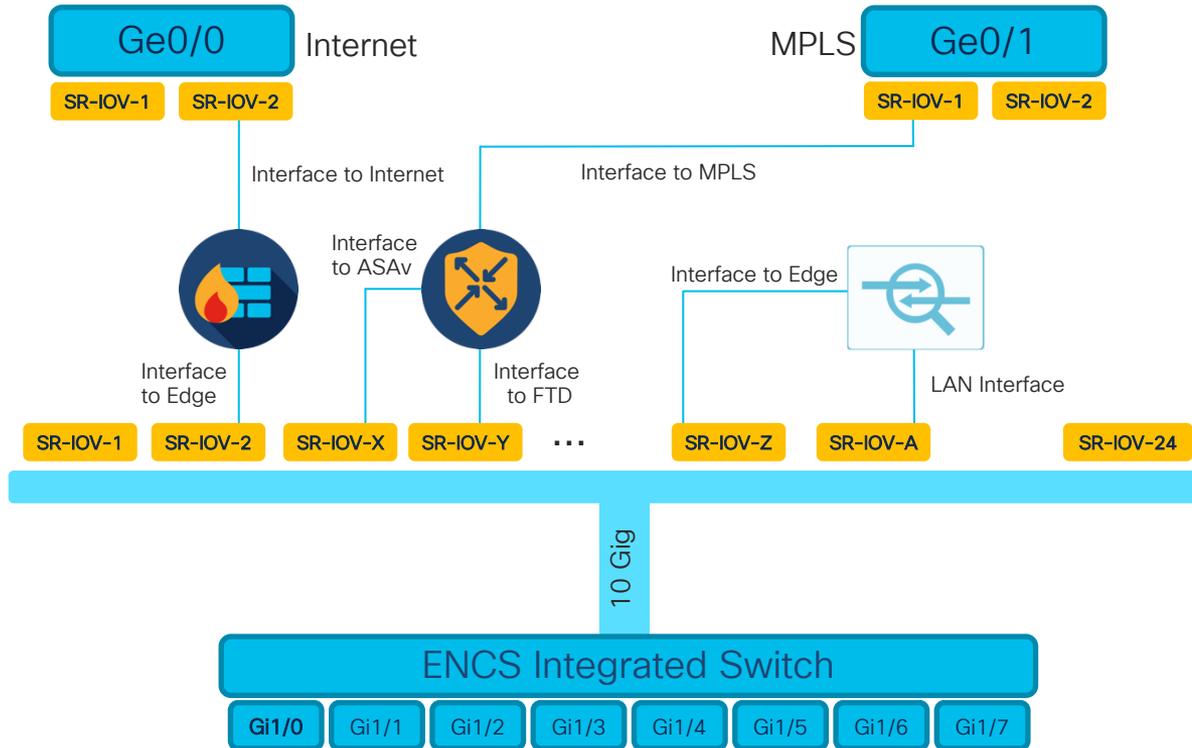
\*Supported starting 20.1/17.2.1 with AppNav-XE and full SD-WAN WAAS integration



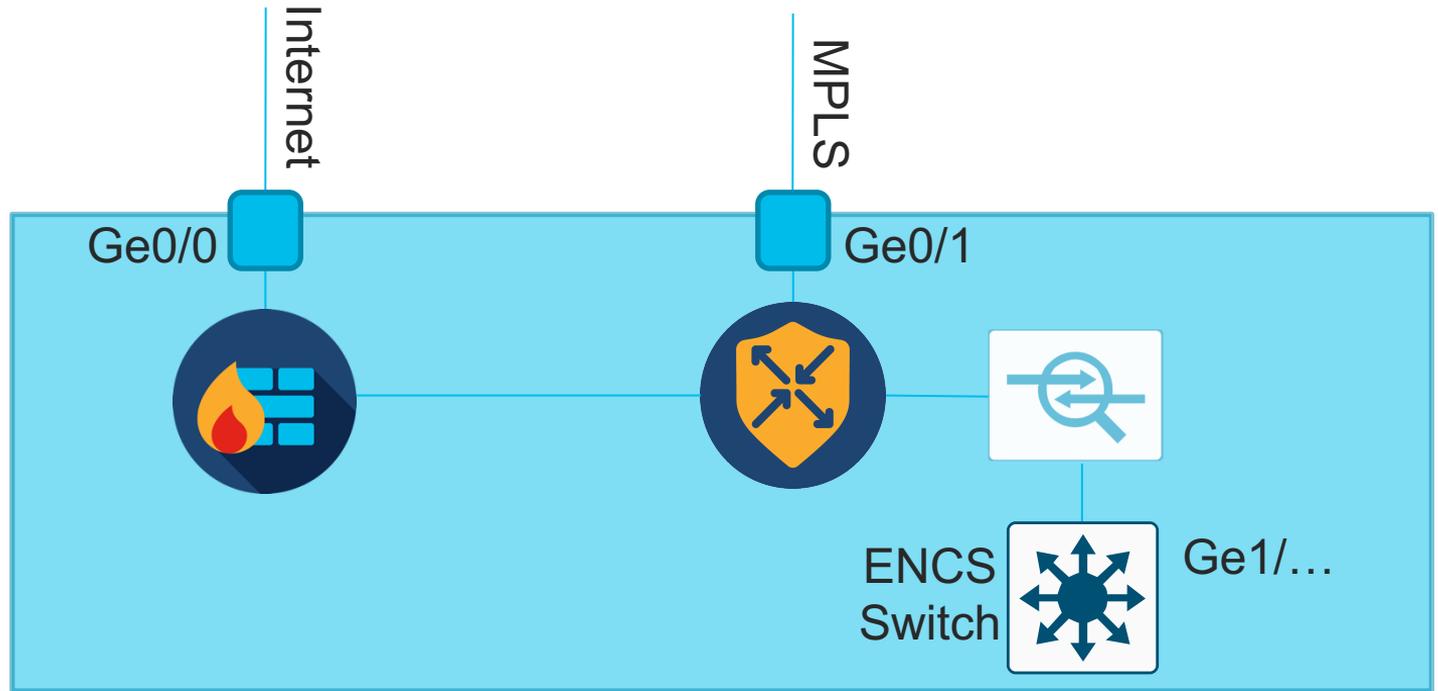
# vEdge/ISRv + FTD + ASA v + OVS



# vEdge/ISRv + FTD + ASA v + SRIOV



# vEdge/ISRv + FTD + ASA v





# Virtual Branch Management

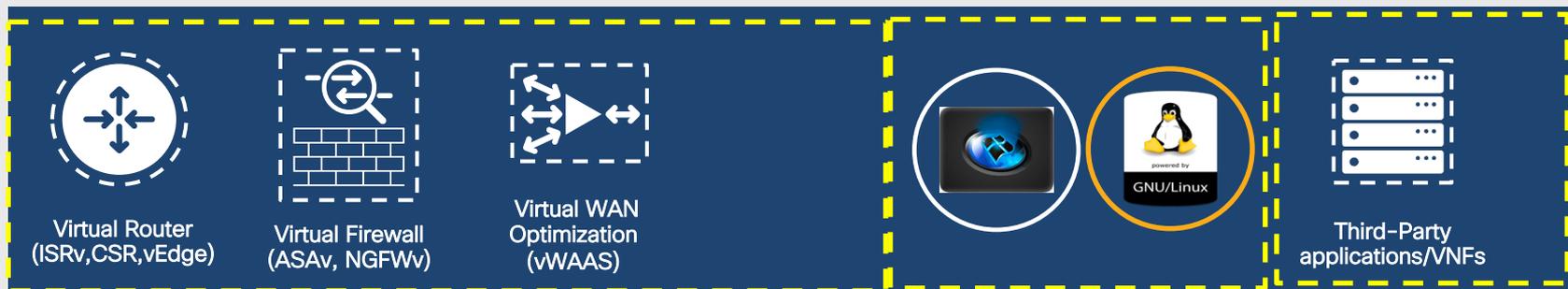


# Automation of Service Chain Deployments

# Software Defined Branch

## Deploy Services on Any Platform

vManage / Cisco DNA Center / Network Service Orchestrator/ MSX



Network Functions Virtualization Infrastructure Software (NFVIS)

Cisco 4000 Series ISR +  
UCS® E-Series

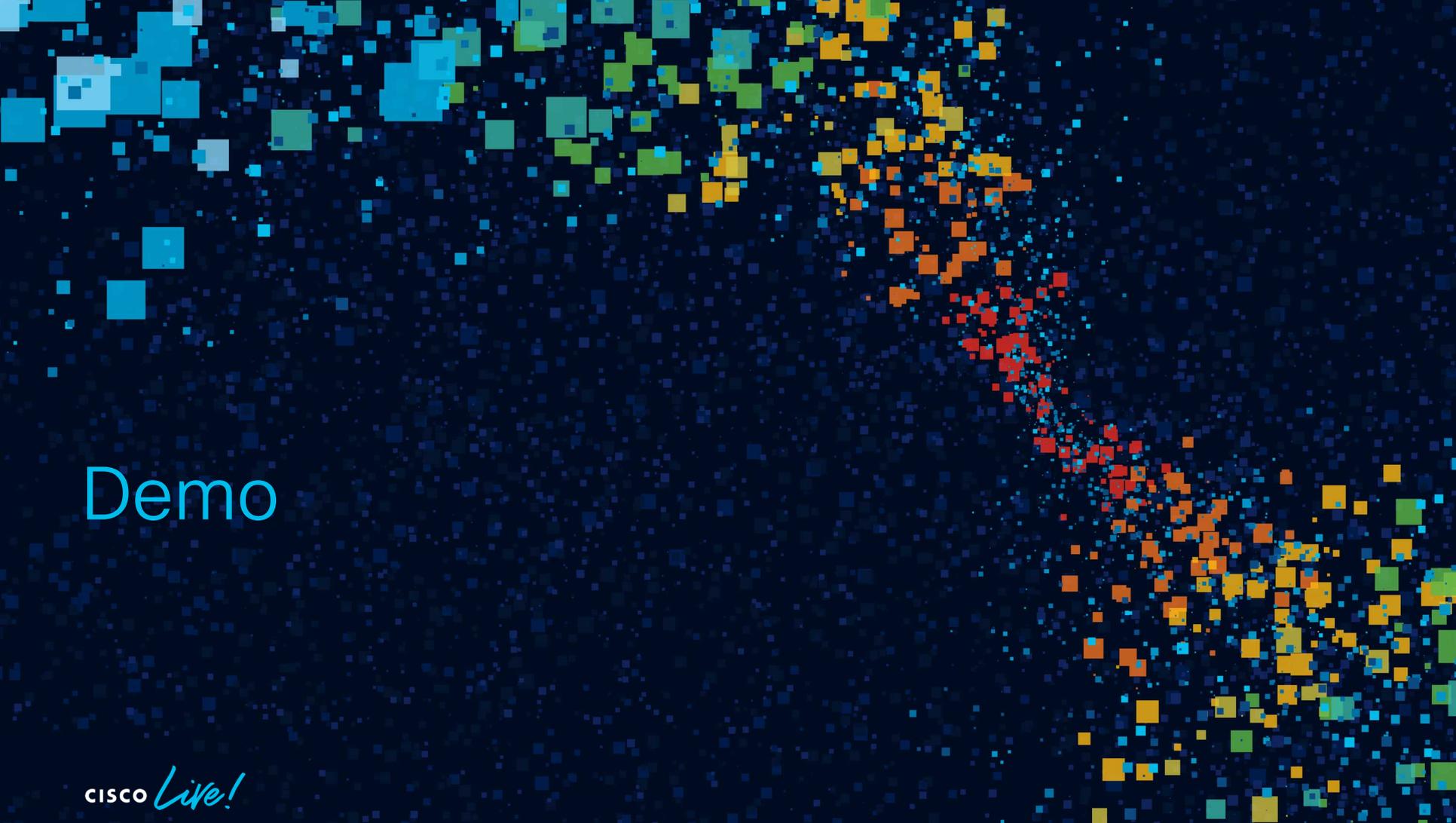
Enterprise Network  
Compute System  
(ENCS)

CSP-5000  
UCS-M5 C-Series

Select  
3rd Party Hardware

# Orchestrators

- Network Service Orchestrator(NSO)
  - Using NETCONF for device configuration
  - CLI management and configuration, requires programming skills
- Managed Services Accelerator (MSX)
  - Using NSO under the hood
  - User friendly Graphical Interface
- DNA Center
  - Using REST for configuration
  - User friendly Graphical Interface
- vManage (Coming soon)
  - Using NSO under the hood
  - Build-in SD-WAN solution



Demo

CISCO *Live!*



# SD-WAN Operations Cycle

# Virtual Device Onboarding

To add virtual routers like ISRv, CSR, vEdge Cloud to vManage log in to the Plug and Play portal, click Add Software Devices:

The screenshot displays the Cisco Software Central Plug and Play Connect interface. The main page shows the 'Add Software Device(s)' section with a progress indicator for STEP 1: Identify Device(s). A modal window titled 'Identify Device' is open, showing the following fields:

- Base PID: VEDGE-CLOUD-DNA
- Quantity: 15
- Controller Profile: ENTERPRISE-VBOND
- Description: Enter short optional description for this device.

The 'Save' button is highlighted in blue, indicating the completion of the device identification process.

# Virtual Device Day 1 Config

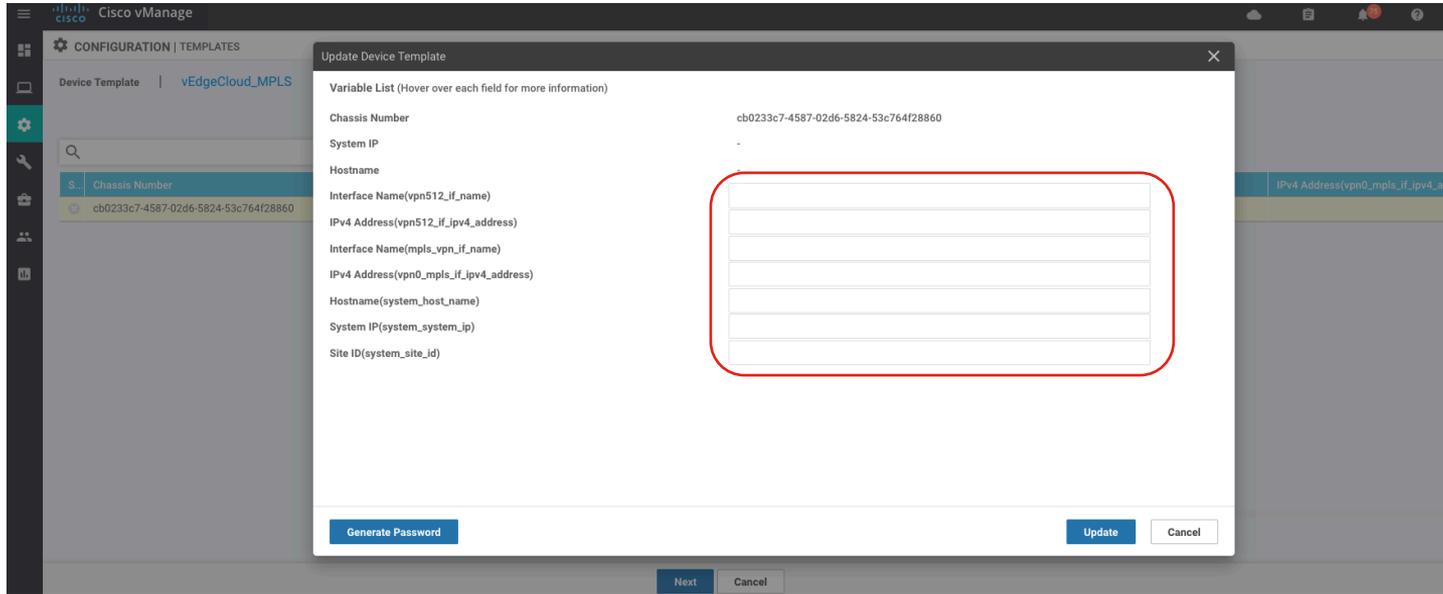
Attach available token to the template

The screenshot shows the Cisco vManage interface for configuring templates. A table lists various templates with columns for Name, Description, Type, Device Model, Feature Templates, Devices Attached, Updated By, Last Updated, and Template Status. A dialog box titled 'Attach Devices' is open, showing a list of available devices with their names and device IPs. One device IP, 'ab36794c-3045-cb78-9bc5-db35d8c1f46e', is highlighted with a red box. A blue arrow points from the text 'Attach available token to the template' to this highlighted IP. Another blue arrow points from the same text to a right-pointing arrow button in the dialog box. The dialog box also has a 'Selected Devices' section which is currently empty.

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status
ISR4331-basic-DIA	ISR4331 initial config DIA	Feature	ISR4331	15	0	admin	05 Nov 2019 2:21:15 PM CET	In Sync
ISR4331-basic-DIA-UTD	ISR4331 initial config DIA_UTD	Feature	ISR4331	15	0	admin	24 Oct 2019 10:32:31 PM CET	In Sync
DSL-C1117-4PM	repro for DSL controller	Feature	C1117-4PM	10	0	admin	22 Mar 2019 8:54:11 PM CET	In Sync
test_vedge_template	test_vedge_template	Feature	vEdge Cloud	9	0	admin	08 Jun 2019 9:10:38 PM CET	In Sync
C1121X-8PLTEP_Firewall_test	test	Feature	C1121X-8PLTEP	12	0	admin	30 Aug 2019 3:53:04 PM CET	In Sync
4431_test	testing PMTU	Feature	ISR4431	10	0	wmartowi	27 Jan 2020 1:30:51 PM CET	In Sync
c1111-8p_243_basic	0m	Feature	C1111-8P	16	1	iomeljan	07 Apr 2020 3:59:13 PM CET	In Sync
ISR4331-utd-larysa-test								
c1111-8te-om								
c1111-8p_template								
WDAAR-C1121X-TEMPLAT								
ASR1001-HX-ENK								
vEdgeCloud_MPLS								
ISR4331-basic								
ASR1001-HX-FW								
c1111-8te-tmikula								
CSR1kv-enk								
ISR4331-test								
ISR4331-udutt								
vEdge2000-enk-test								
ISR4331-enk_v2								
ISR4331-enk								
ISR4331-basic-utd								
udutt_AMP_test_1								
vEdge5000_Internet								
WDAAR-ISR4331-Policy								
ISR4331-tmikula-test	ISR4331-tmikula-test	Feature	ISR4331	21	0	admin	05 Oct 2019 8:49:59 PM CET	In Sync
ISR4331-Larysa-test-ppope	ISR4331-Larysa-test	Feature	ISR4331	16	0	larysa	16 Feb 2020 2:42:25 PM CET	In Sync

# Virtual Device Day 1 Config

Fill all the variables:



# Virtual Device Day 1 Config

Schedule configuration:

The screenshot shows the Cisco vManage interface for configuring a device template. The main area displays the configuration preview for the 'vEdgeCloud\_MPLS' template, which is applied to 1 device. The configuration includes system settings, user groups, and AAA configurations.

**CONFIGURATION | TEMPLATES**

Device Template: vEdgeCloud\_MPLS (Total: 1)

Device list (Total: 1 devices)

cb0233c7-4587-02d6-5824-53c764f28860

Configure Device Rollback Timer

Configure Preview | Config Diff

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

```
viptela-system:system
device-model      vedge-cloud
host-name         vEdge-Cloud
system-ip        1.2.3.4
domain-id        1
site-id          150
admin-tech-on-failure
no route-consistency-check
sp-organization-name "CALO - 100589"
organization-name  "CALO - 100589"
clock timezone Europe/Brussels
vbond 192.168.0.231 port 12346
aaa
auth-order local radius tacacs
usergroup basic
  task system read write
  task interface read write
!
usergroup netadmin
!
usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
!
user admin
password $6$51wKBQ==$wT2\Ua9B5reDP16gB8s\4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6sy1G6qnLABTrnE96HJJKF60Rq1
```

Back | **Configure Devices** | Cancel

# Virtual Device Day 1 Config

While provisioning VM on ENCS you can apply this bootstrap config

The screenshot shows the Cisco vManage interface with the 'Generate Bootstrap Configuration' dialog box open. The dialog has two tabs: 'Cloud-Init' (selected) and 'Encoded String'. The 'Cloud-Init' tab shows a text area with configuration content and a 'Download' button. The background shows a table of WAN Edge List devices.

State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	Hostname	System IP	Site ID	Mode	Assigned Template
	vEdge Cloud	cb0233c7-4587-02d6-5824-53c764f28...	Token - 81483a1f4cffe...	NA	NA	-	-	-	vManage	vEdgeCloud_M...
	vEdge Cloud	38161129-ef67-2a09-1613-abfc6fb50427	Token						CLI	
	vEdge 100 B	1920C403181095	100095						CLI	
	vEdge Cloud	c56a10e5-3a13-4ffc-70a4-dd81e914fe18	Token						CLI	
	vEdge Cloud	1fafac1f-aa46-54a4-cf81-99a3bf04e91	0233						CLI	
	vEdge 100 B	1920C403182838	100092						CLI	
	vEdge 1000	110G528180107	100124						CLI	
	vEdge 100 B	1920C403181450	1000A08						CLI	
	vEdge 1000	110G528180076	10012474						CLI	
	vEdge 2000	260E1122180113	10009E65						CLI	
	vEdge 1000	110G528180111	1001249D						CLI	
	vEdge 100 B	1920C403182840	10009FC6						CLI	
	vEdge 2000	260E1124180287	1001277C						CLI	
	vEdge 5000	193A1216180038	4418F419						CLI	
	vEdge 2000	260E1124180083	1000E58D						CLI	
	vEdge 1000	110G528180103	1001246D						CLI	

The screenshot shows the 'VM Details' configuration page. The 'Bootstrap File Name' field is set to 'ciscoedwan\_cloud\_init.cfg' and the 'Bootstrap Payload' field contains the configuration content from the dialog box.

VM Name \* cEdge  
Image isrv-universalk9.16.09.01a-vga-qcow2  
Profile isrv  
VNC Password  
Deployment Disk datastore1(internal)  
Add Bootstrap Config  
Bootstrap File Name ciscoedwan\_cloud\_init.cfg  
Bootstrap Payload Content-Type: multipart/mixed; boundar  
ya"=====8646069924485761024====  
761024====  
MIME-Version: 1.0

Generate bootstrap config

# Decommission WAN Edge

If you need to free previously allocated token use “Decommission WAN Edge” option, if you choose “Delete WAN Edge” you will have to sync smart account to use this token once again.

CONFIGURATION | DEVICES

WAN Edge List    Controllers

Change Mode    Upload WAN Edge List    Export Bootstrap Configuration    Sync Smart Account

Search Options    Total Rows: 60

State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	Hostname	System IP	Site ID	Mode	Assigned Template	
	vEdge Cloud	cb0233c7-4587-02d6-5824-53c764f28...	Token - 81483a1f4cff6...	NA	NA	--	--	--	vManage	vEdgeCloud_MPLS	...
	vEdge Cloud	38161129-ef67-2a09-1613-a8fc6fb50427	Token - 77b79833386b...	NA	NA	--	--	--			Running Configuration
	vEdge 100 B	1920C403181095	1000569E	NA	NA	--	--	--			Local Configuration
	vEdge Cloud	c56a10e5-3a13-4ffc-70a4-dd81e914fe18	Token - 9e1bfedd8bb18...	NA	NA	--	--	--			Delete WAN Edge
	vEdge Cloud	1fafac1f-aa46-54a4-cf81-99a5bf04fe91	0233	NA	Dec 26 15:33:04 2030 CET	--	--	--			Copy Configuration
	vEdge 100 B	1920C403182838	100092C5	NA	NA	BRU-SDW-V1CB-02	10.10.10.241	241			Decommission WAN Edge
	vEdge 1000	110G528180107	1001247E	NA	NA	BRU-SDW-V1K-01	10.10.10.234	234			Generate Bootstrap Configuration
	vEdge 100 B	1920C403181450	1000A003	NA	NA	--	--	--			Change Device Values
	vEdge 1000	110G528180076	10012474	NA	NA	BRU-SDW-V1K-04	10.10.10.237	2			Template Log
	vEdge 2000	260E1122180113	10009E65	NA	NA	BRU-SDW-V2K-01	10.10.10.238	238	CLI	--	Device Bring Up
	vEdge 1000	110G528180111	1001249D	NA	NA	BRU-SDW-V1K-02	10.10.10.235	235	CLI	--	...



# Takeaways

# Takeaways

- Replace multiple devices in the branch with VNF Service Chains
- Plan Virtual Branch based on the performance, throughput and solution requirements, treat this task as a regular network segment design.
- Use NFVIS build-in failure detection mechanisms for faster convergence
- Automate your virtual branch deployment

Thank you

CISCO *Live!*

#CiscoLive





# Possibilities

#CiscoLive