SD-WAN on Cisco IOS XE Routers: An End-to-End View

Summary

This white paper presents an overview of the Cisco® Software-Defined WAN (SD-WAN) solution on Cisco IOS® XE routers. It is a good introduction for those who want to run SD-WAN on selected Cisco Integrated Services Routers (ISRs) and, Aggregation Services Routers (ASRs) and Enterprise Network Compute System (ENCS). The paper explains key building blocks of the SD-WAN solution on Cisco IOS XE routers, describes main upgrade steps, and covers different deployment use cases.

This document will not cover basic functionality of Cisco SD-WAN. It is purely focused on SD-WAN on IOS XE.

Many customers have a large Cisco IOS XE installed base and are looking at SD-WAN to address the following needs:

- Reduce costs
- Speed up operation
- Provide a better user experience
- Integrate the latest cloud technologies

The Cisco SD-WAN solution provides all of these benefits, runs now on selected Cisco IOS XE routers, and is the most economical and best technical solution for an existing installed base.

Introduction

The SD-WAN image based on Cisco IOS XE software is not a standard Cisco IOS XE release. It does not just add SD-WAN features on top of all existing Cisco IOS XE capabilities.

Instead, we have kept the existing Viptela SD-WAN framework, in which vManage acts as the central Network Management System (NMS) and now manages also the configuration of the Cisco IOS XE device. Only a selected Cisco IOS XE feature set that makes sense for SD-WAN is used in the SD-WAN image for Cisco IOS XE. New device models—for example, the Cisco 4331 ISR and the Cisco Integrated Services Virtual Router (ISRv)—have been introduced in vManage. The whole workflow, including configuration, provisioning, and troubleshooting, remains the same. vManage simply has additional new devices that will be used in exactly the same way as vEdge routers.

Contents

Requirements for SD-WAN on Cisco IOS XE

This white paper does not replace detailed release notes and the step-by-step configuration guide. Please refer to the online documentation for such details.

The high-level requirements for SD-WAN on Cisco IOS XE can be classified as follows:

Hardware requirements

The first Cisco IOS XE SD-WAN image supports the following hardware platforms:

Cisco ASR 1000 series aggregation services routers

- ASR 1001-HX and ASR 1001-X
- ASR 1002-HX and ASR 1002-X

Cisco ISR 1000 series integrated services routers

- C1111-8P, C1111-8P LTE EA, and C1111-8P LTE LA
- C1117-4P LTE EA and C1117-4P LTE LA

Cisco ISR 4000 Series

- ISR 4221
- ISR 4321
- ISR 4331
- ISR 4351

ENCS 5412 with T1/E1 and 4G NIM modules

- ISRv

Memory requirements

For a 4000 Series ISR, ensure that there is a minimum of 4 GB of DRAM; 8 GB or more is recommended. For an ASR 1000 Series router, ensure that there is a minimum of 8 GB of DRAM. Note that the ASR 1002-HX defaults to a 16 GB DRAM minimum.

Module requirements

Note that the SD-WAN image will not support all modules from day 0. You will need to remove unsupported modules from an existing Cisco IOS XE router to make the boot process smoother.

Please refer to the Migration Guide and online documentation for the full list of supported devices: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/Software_Installation_and_Upgrade_for_IOS_XE_Routers

Software requirements

- All SD-WAN controllers (vManage, vSmart, and vBond) have to be on supported version 18.3.0.
- Existing vEdge routers must run 17.2.1 or a later release to interoperate with the Cisco IOS XE SD-WAN image. This is because of code changes introduced to support Bidirectional Forwarding Detection (BFD) tunnel building between a vEdge and cEdge.
- If needed, perform the ROMMON upgrade before loading the SD-WAN image on the Cisco IOS XE platform. Unlike Cisco IOS XE images, the SD-WAN images will not have a necessary ROMMON image bundled in to automatically initiate an upgrade. Refer to the online documentation for the supported ROMMON versions such as 16.7(3r) for 4300 Series ISRs.

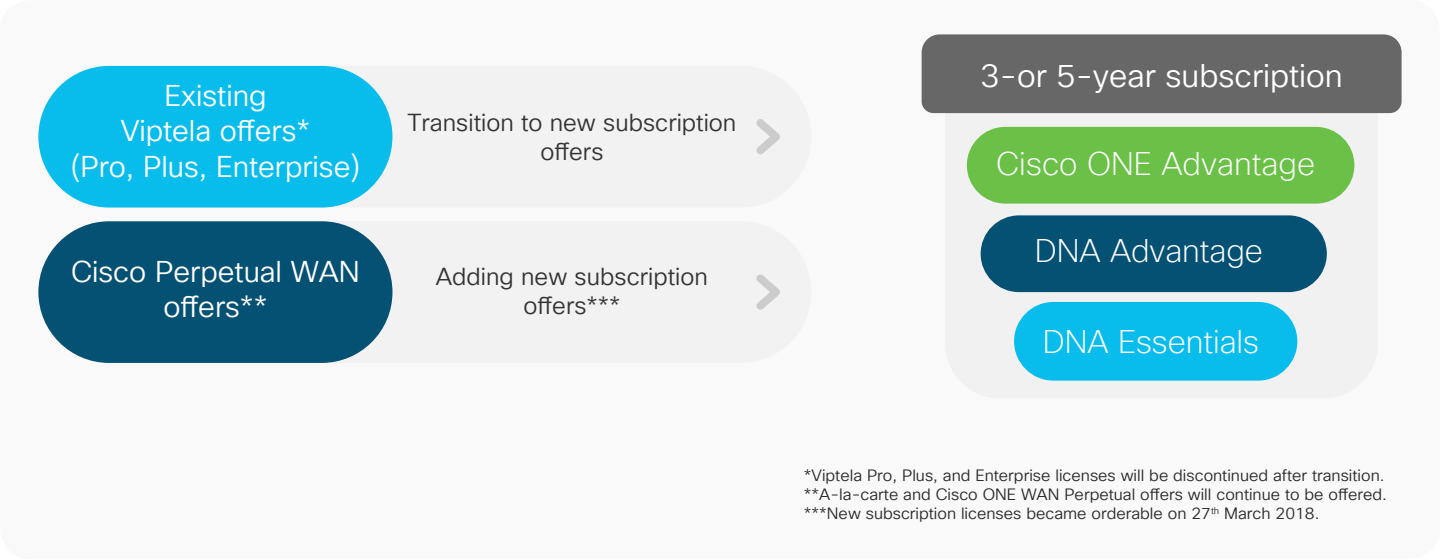
Please refer to the release notes for detailed software support: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/Software_Installation_and_Upgrade_for_IOS_XE_Routers

Infrastructure requirements

You will need Dynamic Host Configuration Protocol (DHCP) with DNS and default gateway for Cisco Network Plug and Play (PnP). An Internet connection should allow communication to devicehelper.cisco.com using ports 80 and 443 for PnP. If there is a firewall, see Firewall Ports for Viptela Deployments: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Viptela_Overlay_Network_Bringup/01Bringup_Sequence_of_Events/Firewall_Ports_for_Viptela_Deployments

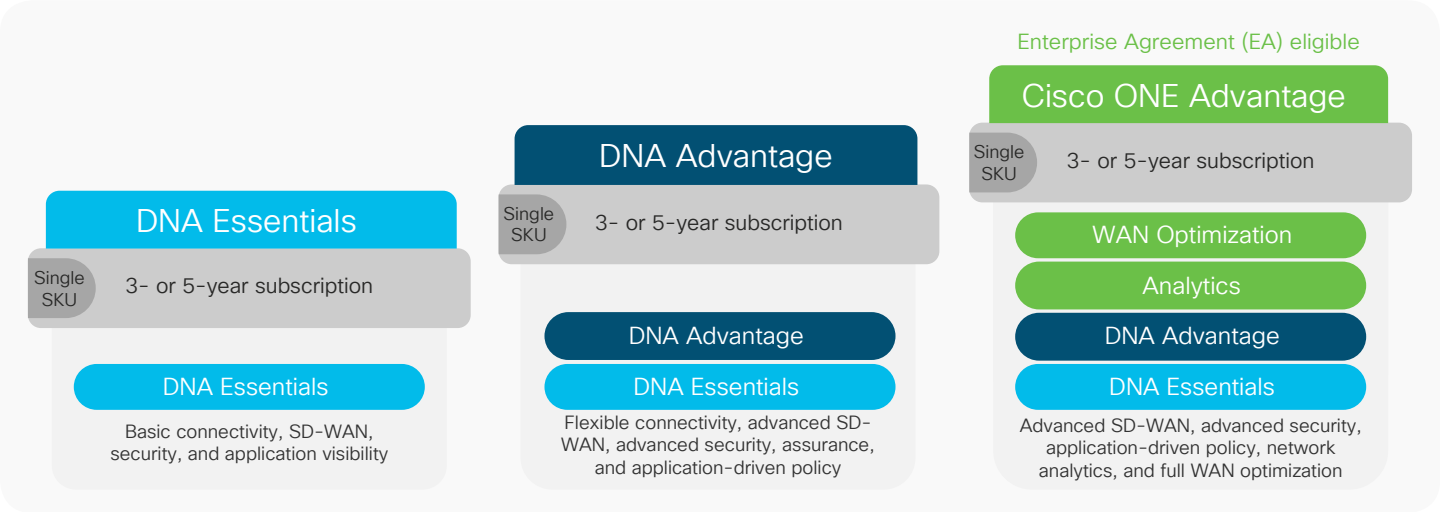
Licensing

One consistent offer applies across all enterprise routing platforms, including software support, as shown in the figure below.



*Viptela Pro, Plus, and Enterprise licenses will be discontinued after transition.
**A-la-carte and Cisco ONE WAN Perpetual offers will continue to be offered.
***New subscription licenses became orderable on 27th March 2018.

There are three options: Cisco DNA™ Essentials, Cisco DNA Advantage, and Cisco ONE™ Advantage, as shown below.

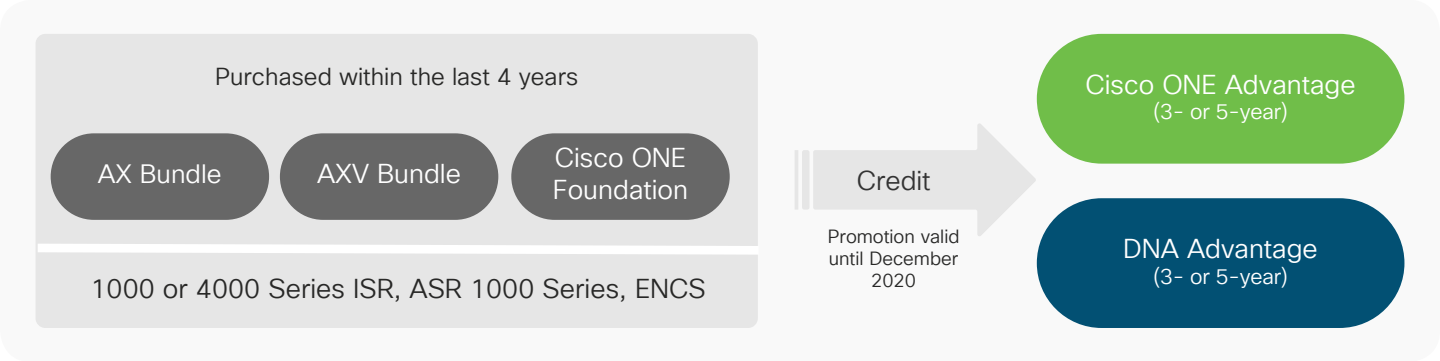


"How to choose" explained in five steps:

1. Identify license tier
2. Select bandwidth
3. Pick license term
4. Choose on-premises or cloud managed
5. Determine platform for future scale

For details, refer to the vEdge ordering guide:
https://www.cisco.com/c/dam/en/us/products/se/2018/4/Sales/Cisco_SD-WAN_OG_v2b.pdf.

The following figure outlines investment protection for existing WAN customers.

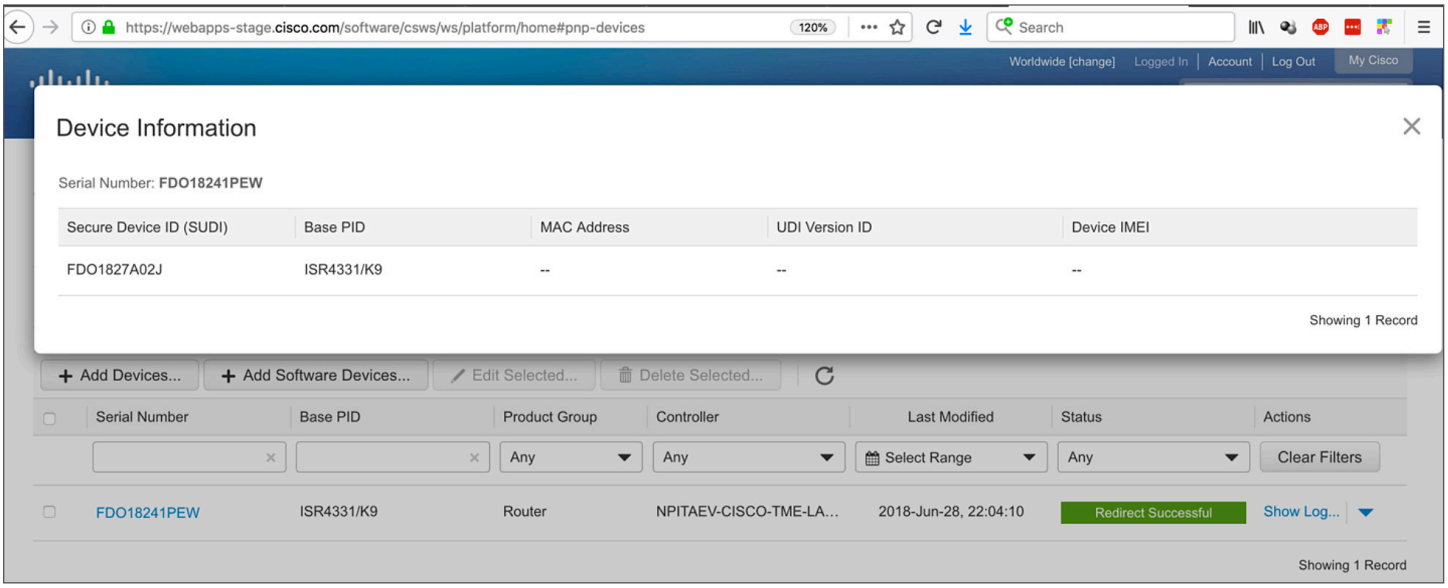


Smart licensing and PnP support guide

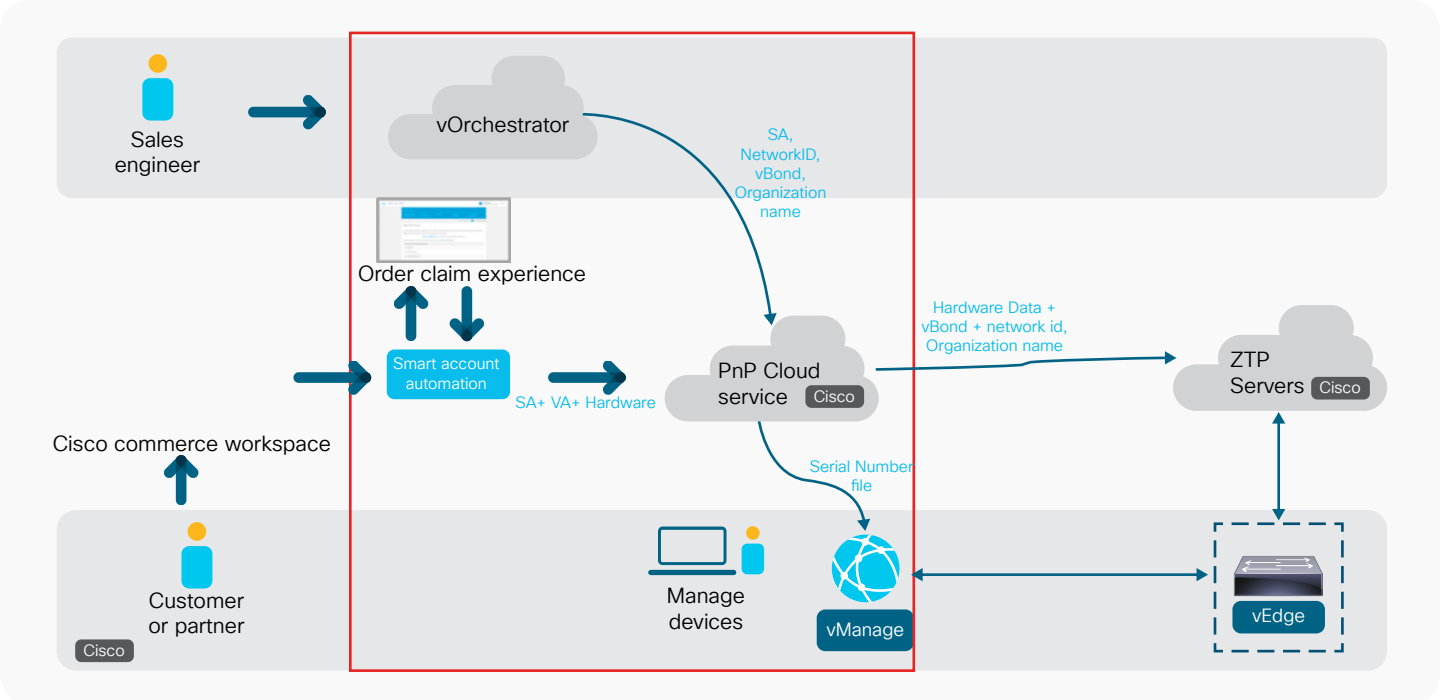
Smart Licensing is required in order to use Cisco Network Plug and Play (PnP) during the software upgrade from standard Cisco IOS XE to the SD-WAN Cisco IOS XE software image.

You will need the router's serial number and Secure Unique Device Identifier (SUDI). Some devices, such as the ASR-1002X and the ISRv virtual router, do not have a SUDI. Note that the serial number displayed with "show license udi" can be different from the SUDI displayed with "show crypto pki certificates." You will need both for PnP.

The following example from the PnP portal shows a serial file, which is different from the SUDI for a 4331 ISR.



The following figure gives an overview of the full Smart Licensing and PnP workflow.



Smart Accounts and Virtual Accounts are essential in the successful onboarding of a SD-WAN router to its corresponding network. This white paper will not cover all Smart Licening and PnP details. In the following we will briefly describe, what is happening under the hood for SD-WAN case.

For cloud-hosted deployments, while spinning up the vBond controller using vOrchestrator, you will select the Smart Account and Virtual Account on vOrchestrator. This will make sure that the vBond information associated with a Virtual Account is passed to the PnP portal. This sync also takes care of assigning an organization name and network ID (known as the overlay ID in Viptela) to the cloud controllers, and the same information is maintained in the PnP Connect portal.

When placing an order in Cisco Commerce Workspace, the customer can assign the same Smart Account and Virtual Account to the order. The customer can log in to vManage (version 18.3 or later) to find the Smart and Virtual Account (Administer -> Setting - > Organization name -> View).

The devices deployed as part of this order would flow into the PnP portal and would be associated with the vBond controller that was pushed by vOrchestrator. Once the association is successful, the data is pushed to Zero-Touch Provisioning (ZTP).

For on-premises deployments, the customer or the sales engineer helping with the customer's deployment would need to enter the vBond profile information into PnP, so that the controller information can be passed to ZTP. Steps for setting up a vBond controller and how to associate devices with it are given later in this guide.

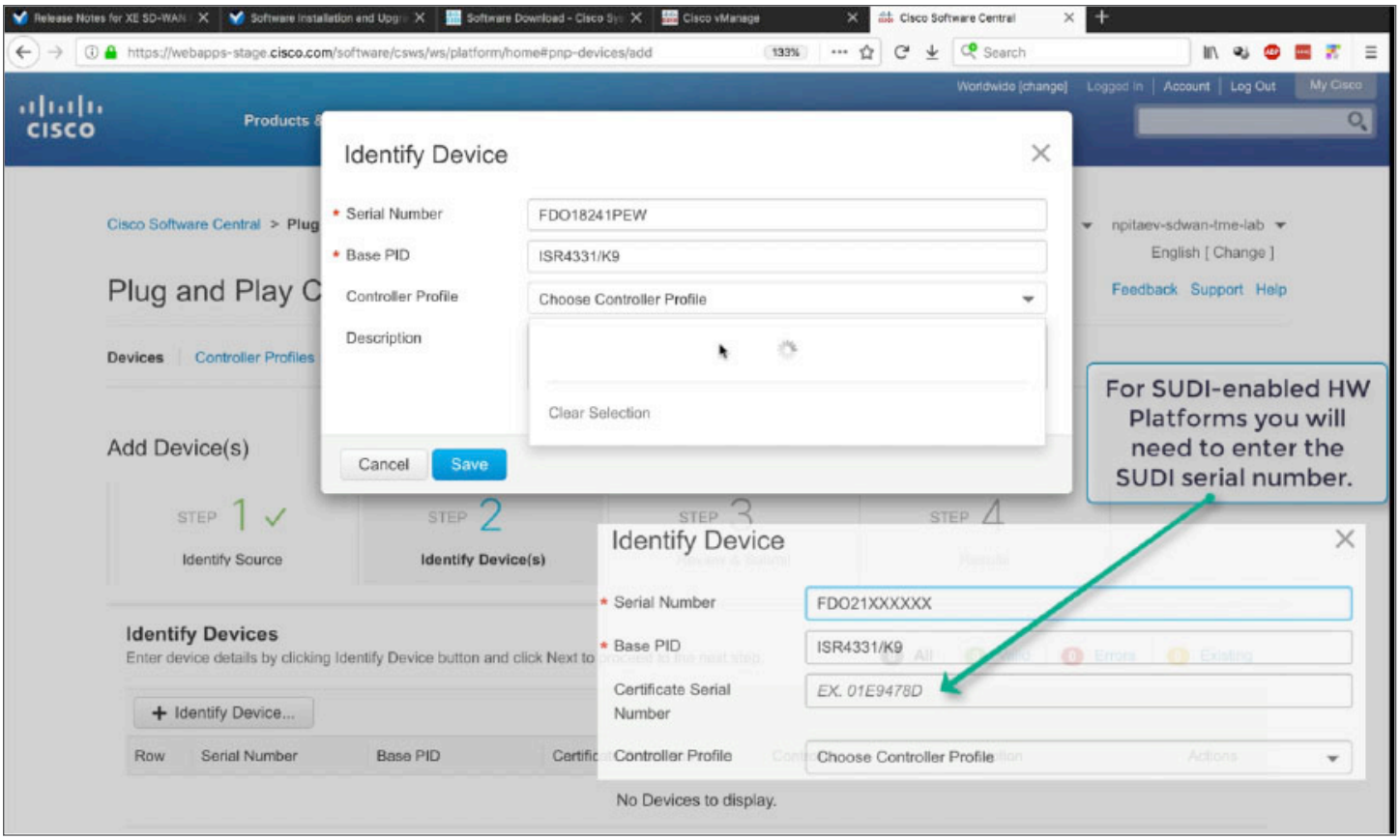
For details, please refer to the PnP for SD-WAN guide and the following YouTube Video "Upgrading Cisco ISR4000 to SD-WAN" https://www.youtube.com/watch?v=qugfllEmSEM

Generating the SD-WAN serial file and installing it into vManage

If you have an existing Cisco IOS XE router and want to integrate it into the SD-WAN fabric using PnP, you will need to determine its serial number by using the "show license udi" command in the Command-Line Interface (CLI):

```
BR1-cEdge-ISR4k#show license udi

SlotID   PID                    SN                     UDI

-------------------------------------------------------------------------------

*        ISR4331/K9             FDO18241PEW     ISR4331/K9:FDO18241PEW

BR1-cEdge-ISR4k#
```

As was mentioned previously, you will also need to provide the SUDI information displayed with the “show crypto pki certificates” command. Please refer to the following screen shot for details:



Customers will need to contact a Cisco presales SE, provide the serial number, and obtain a serial file, which must be uploaded into vManage. This standard SD-WAN step is described in the online documentation: https://sdwan-docs.cisco.com/Product_Documentation/vManage_How-Tos/Security_Certificates/Upload_the_vEdge_Serial_Number_File

Software upgrade process to the SD-WAN image

Software upgrade using PnP

Follow these steps to upgrade to the SD-WAN image using PnP on a Cisco IOS XE based router:

1. Check the prerequisites and supported models in the online documentation
2. Provide Internet access, and use DHCP server with DNS
3. Preprovision the router in vManage: upload the serial file and create a device template
4. Preprovision the device in the PnP Cloud Connect Service
5. Load the SD-WAN image to the Cisco IOS XE router
6. Erase the existing Cisco IOS XE configuration
7. Reboot the router

Note that the dynamic IP address provided by DHCP is needed for PnP. If you need to use static IP, refer to the next section, “Upgrade Without PnP.”

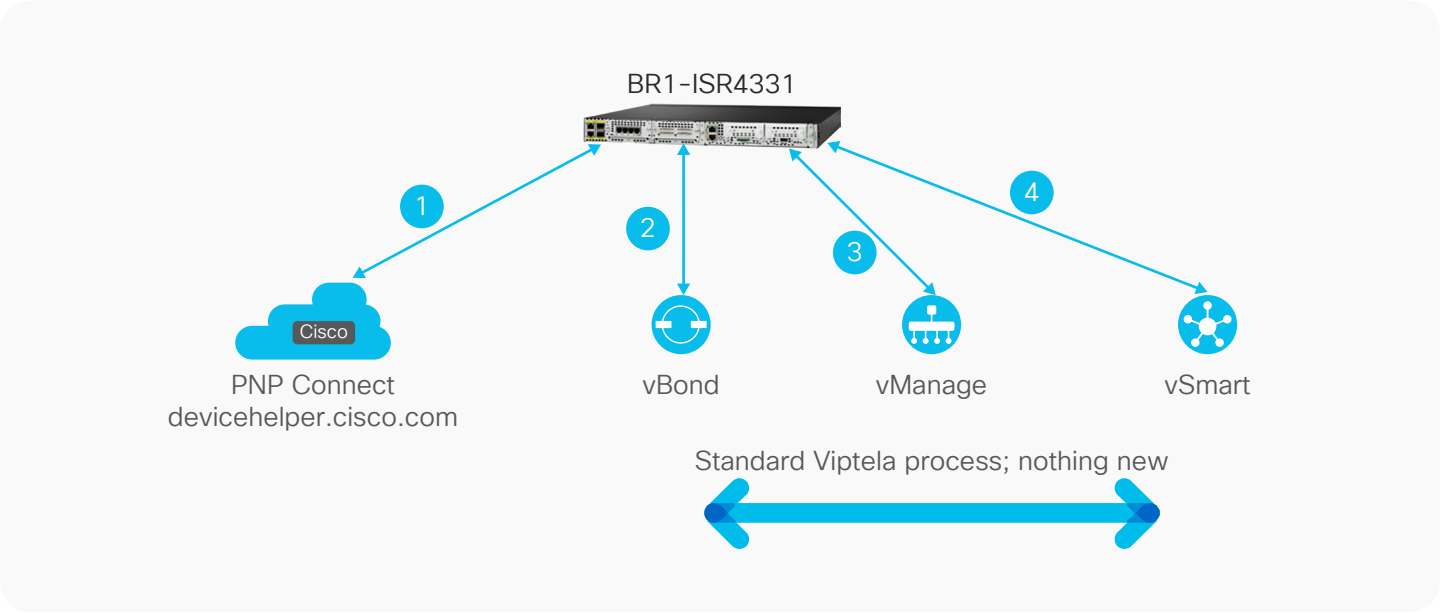
After reboot, the router will have an empty configuration. By default, the Gigabit Ethernet (GE) interface will be enabled and configured for DHCP. The router will obtain an IP address, DNS server IP address, and default getaway via DHCP, will resolve devicehelper.cisco.com, and will connect to it via ports 80 or 443.

The PnP server will check the serial number and push key parameters such as the vBond IP address and organization name to the router.

The router will reach out to vBond and perform standard SD-WAN zero-touch provisioning.

Here is the summary of all 4 steps, which are illustrated in the picture below:

1. IOS XE Router contacts PNP connect under devicehelper.cisco.com presents its serial file and gets SD-WAN related information (vBond IP, organization name, etc.).
2. IOS XE Router contacts vBond over secure tunnel, after authentication vBond sends vManage IP to the IOS XE Router.
3. IOS XE Router contacts vManage over secure tunnel, after authentication, vManage sends full configuration to IOS XE router.
4. IOS XE Router contacts vSmart over secure tunnel and after authentication it will join SD-WAN fabric.



For the step-by-step details, refer to the online documentation “Software Installation for Cisco IOS XE Routers.” https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/Software_Installation_and_Upgrade_for_IOS_XE_Routers

Upgrade without PnP

If PnP cannot be used for the initial SD-WAN upgrade, you will need to upload the SD-WAN image in the same way, as you will do it for the PnP case. The you will need to reboot the router, and apply the SD-WAN configuration manually.

The recommended way to upgrade is to use PnP, which requires dynamic IP address assignment via DHCP.

For the non-PnP option, you will need console access.

The information below is equivalent to the initial configuration, which you will use for vEdge routers.

1. PnP must first be stopped to allow access to the CLI.
2. After PnP is stopped, you will enter configuration mode and define the base SD-WAN system settings.
3. Then you will configure the tunnel interface that will be used for overlay connectivity. The tunnel number must match the WAN interface used. For example, if using Gig0/0/2, the tunnel interface number will be 2. Note that because DHCP is assumed, there is no configuration requirement for the WAN interface, as it will already have an IP address.
4. You have to define the base SD-WAN interface parameters, including the color and encapsulation. It is also assumed that a default route and DNS entry have been obtained via DHCP. If this is not the case, these must also be configured in global configuration mode.
5. If the vBond address was defined as a host name, you also need to configure DNS.
6. At this point, control connections should form.
7. Once control is up, the device can be managed through vManage via standard templates. See the following documentation for information on creating templates: https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates.

Upgrade for ISRv and ASR 1002-X

The upgrade for ISRv and ASR 1002-X, which do not have a SUDI, is done using the SD-WAN .cfg file. It is similar to the cloud-init file, which is used to provide bootstrap options during the first boot of a VM in KVM.

The key upgrade steps are:

1. Upload the SD-WAN image to the router
2. Generate the .cfg file on vManage
3. Upload the .cfg file to the Cisco IOS XE router
4. Erase the configuration and boot the SD-WAN image
5. The router will use the bootstrap configuration from the .cfg file after reboot and will join the SD-WAN fabric

Alternatively, you can use the non-PnP option described earlier to configure non-SUDI devices.

Config migration tool

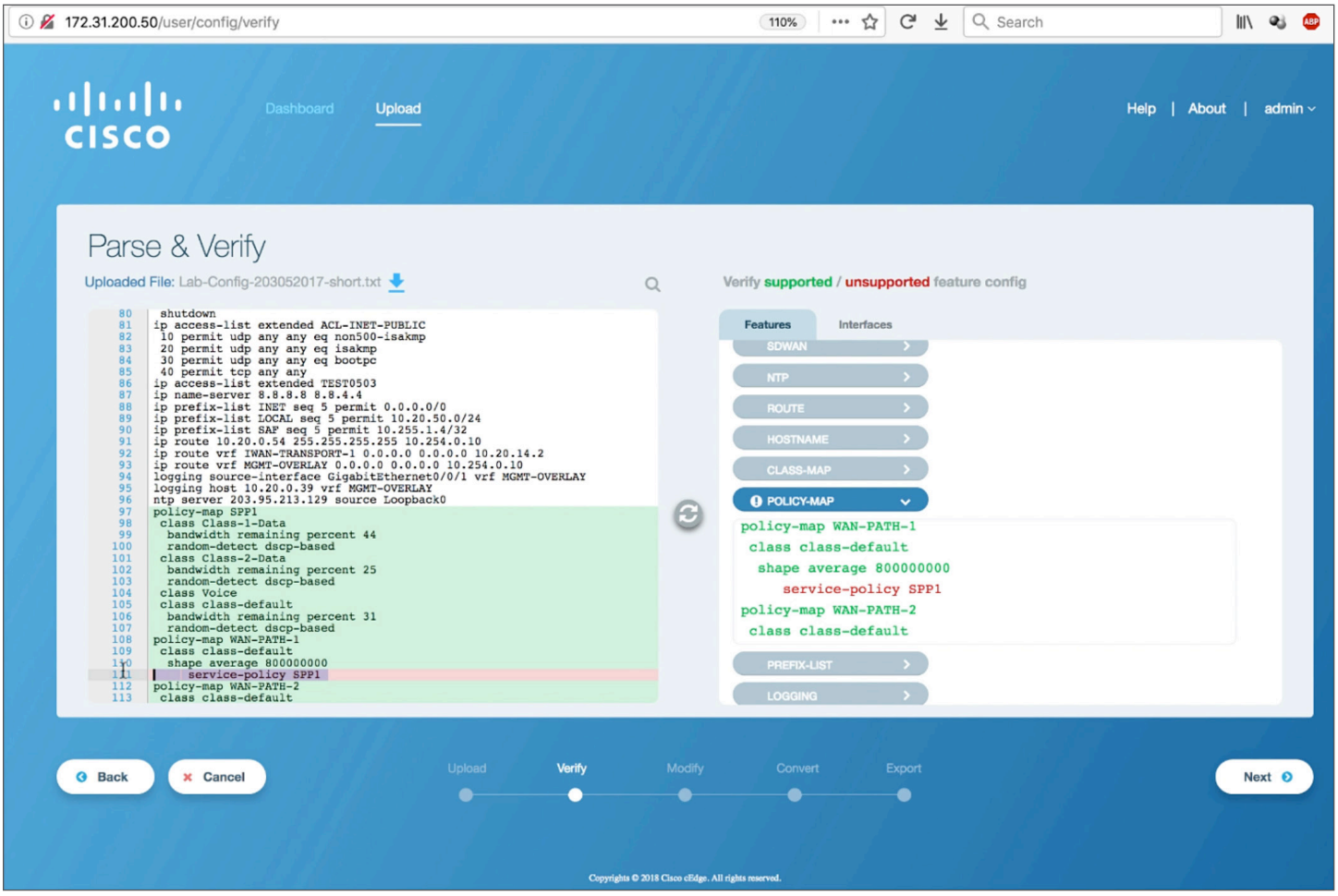
A special tool will help with the Cisco IOS XE router configuration migration.

The workflow is as follows:

1. Upload the existing Cisco IOS XE configuration into the config migration tool.
2. The tool will analyze the configuration and highlight unsupported features.
3. Modify the configuration by removing the unsupported config lines and then click Refresh. The tool will then analyze the modified configuration again.

4. Once all unsupported features are eliminated, the tool will convert the Cisco IOS XE configuration to SD-WAN.
5. You can download the converted file and/or provide the vManage IP address with credentials, and the tool will create appropriate configuration templates in vManage using API calls.

The following screen shot shows the main step of the configuration conversion, where you see in red specific configuration lines, which are not supported on the SD-WAN side and needs to be removed. Please note, that this screen shot is just an example and the list of supported features will vary based on the SD-WAN software release.



Note that in the first release (July 2018), CLI templates are not supported for Cisco IOS XE based routers. You have to use feature templates.

Typical deployment cases

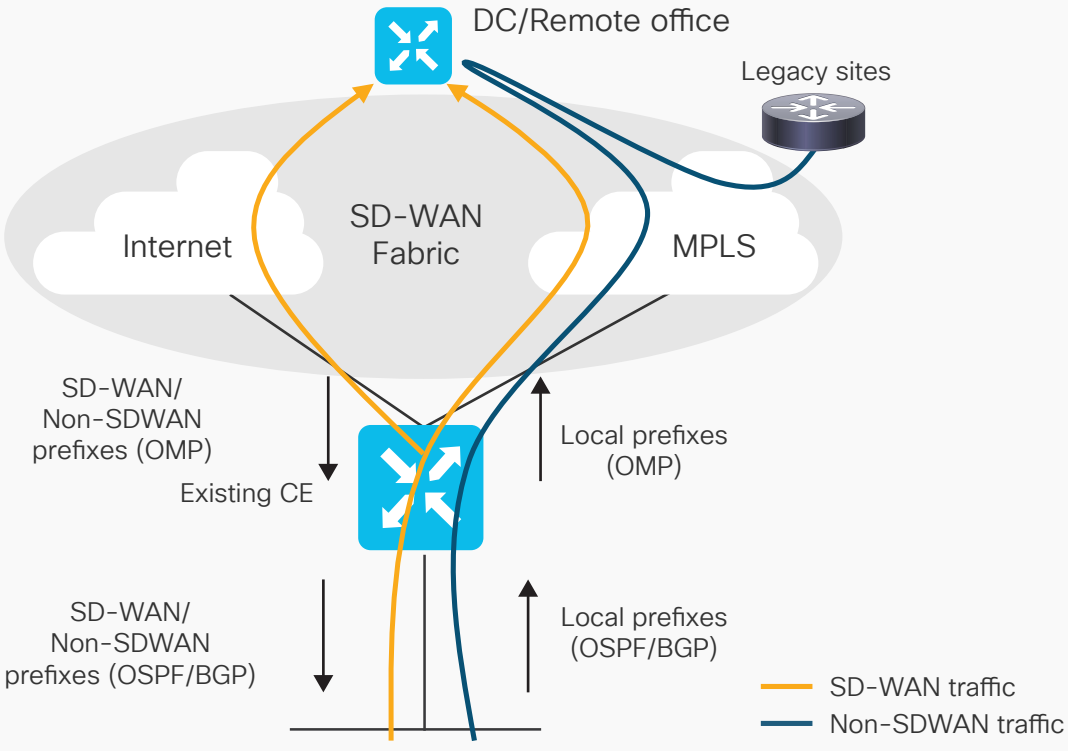
Single Cisco IOS XE SD-WAN router

Most small to medium-sized branch locations have a single router terminating one or more WAN transports. Migrating over to SD-WAN would entail replacing the current third-party router at the site with a Cisco 4000 Series or 1100 ISR or an ASR, depending on the throughput and feature requirements.

If the site already has an SD-WAN-capable ISR or ASR, the migration to SD-WAN just involves a requirements check and a software image upgrade.

Assuming that the SD-WAN controller components have been deployed, and configuration templates and policies have already been defined, follow these steps:

1. Replace the existing router or upgrade the existing router to SD-WAN Cisco IOS XE
2. The router uses PnP to discover its controllers
3. vManage applies the respective configuration template to the router
4. The router peers with vSmart to exchange routing information
5. The router also begins applying policies to achieve traffic engineering, app-aware routing, etc.
6. During the course of migration, migrated SD-WAN sites can talk to other migrated SD-WAN sites directly
7. Migrated SD-WAN sites should leverage the data center or regional hub or aggregation sites or designated migration sites when communicating with legacy or non-SD-WAN sites



Two Cisco IOS XE SD-WAN routers in a redundant configuration

There are differences between some features that are implemented on physical vEdge routers and those on the Cisco IOS XE based SD-WAN image.

That's why we do not recommend to mix physical vEdge Routers together with IOS XE based routers at the same branch location.

One example is Virtual Router Redundancy Protocol (VRRP). The VRRP implementation on a vEdge physical router is as follows: The master router switches to a backup if a peer comes up with the same priority but a higher IP address. The vEdge implementation supports removal and rollback of a GE interface that has VRRP configured.

The Cisco IOS XE VRRP implementation is as follows: The master router remains as master if a peer comes up with the same priority but a higher IP address. The IP address is used only to resolve states between backups of the same priority if the master goes to init (if a failover happens). The Cisco IOS XE implementation does not support removal of a GE interface that has VRRP configured.

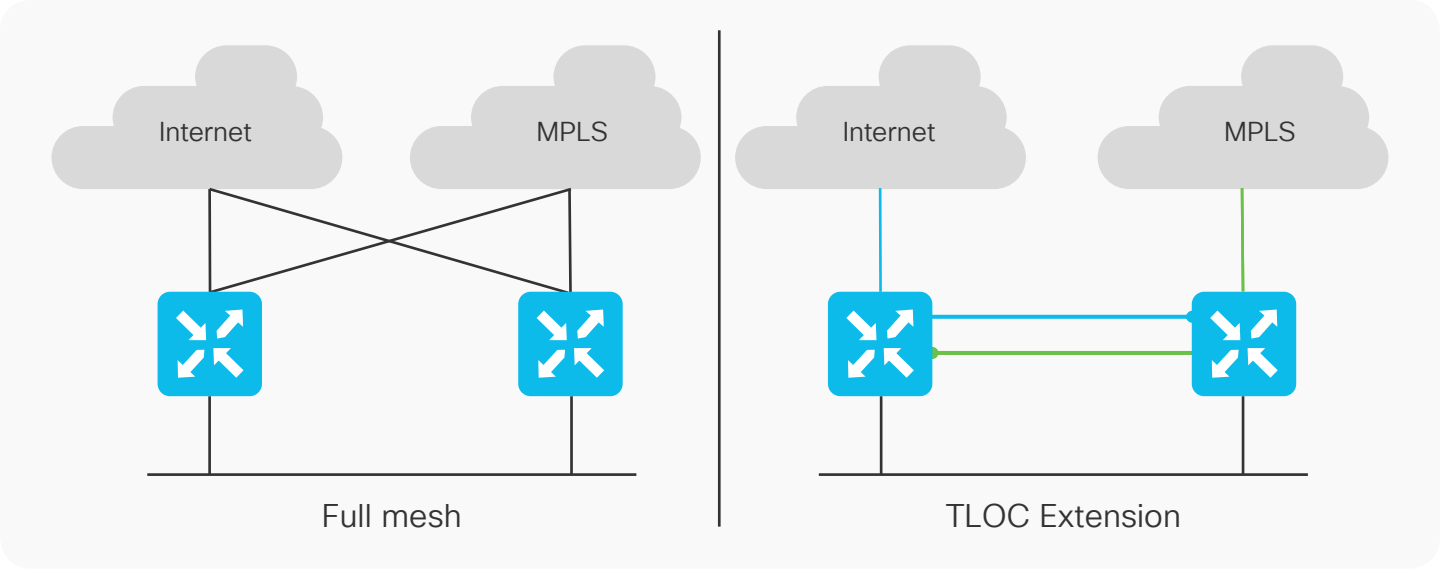
That's why Cisco Engineering implemented VRRP changes for vEdges in 18.3 release and made VRRP implementation on the vEdge side RFC 5798 compliant. This allowed VRRP on vEdge routers interoperate with IOS XE-based SD-WAN routers.

Other differences between physical vEdge routers and the Cisco IOS XE based SD-WAN image are in the following areas:

- Quality of Service (QoS)
- DHCP
- Network Address Translation (NAT)

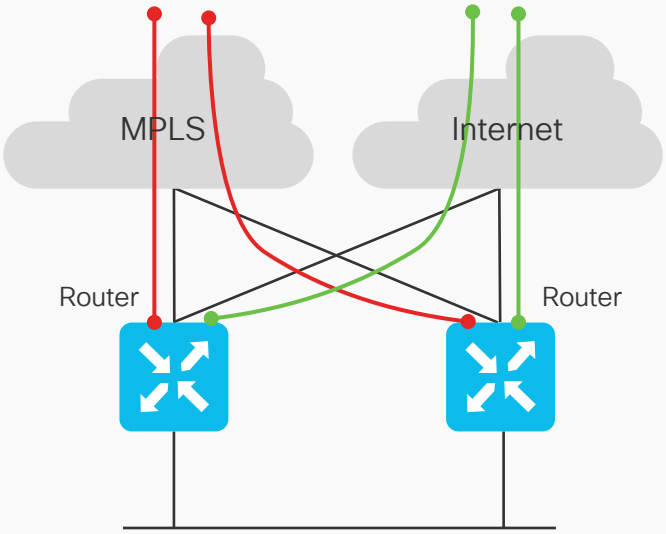
Please refer to the online documentation for details.

Dual router deployments are common for medium- and large-sized branches as well as at data centers. Such a deployment model provides greater throughput, scale, and redundancy.

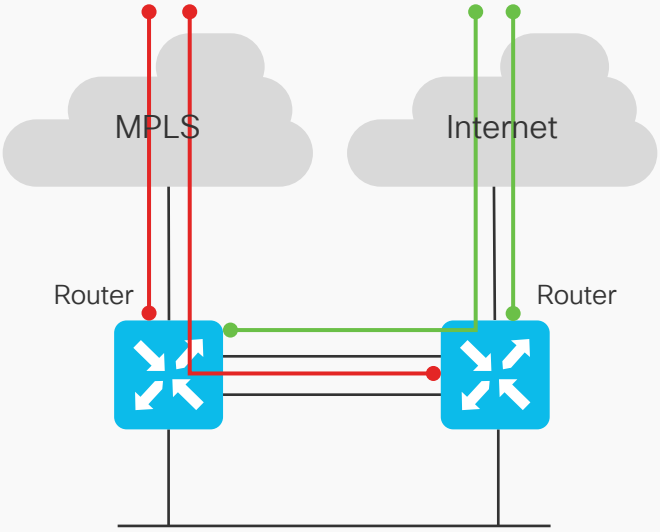


Now let us have a look at redundancy - on the WAN/transport side you have the following.

Transport redundancy (meshed)



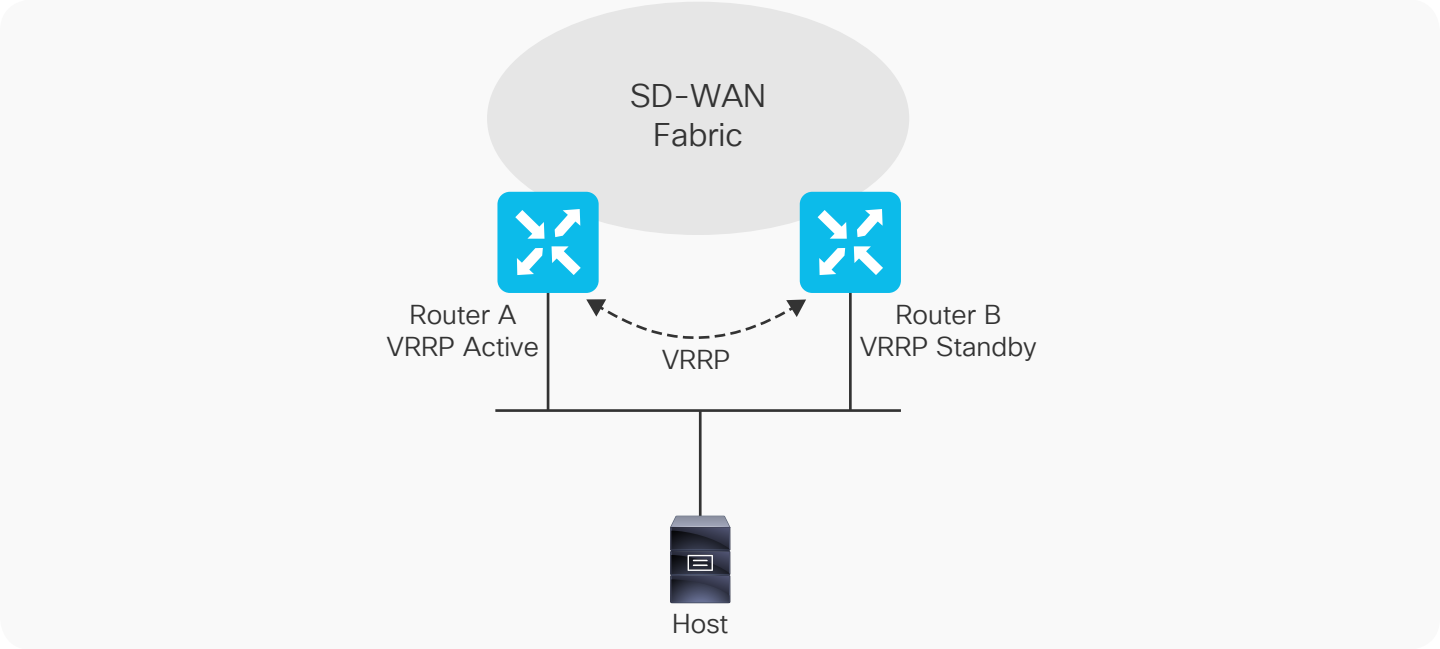
Transport Location (TLOC) extension



- Please refer to the generic description of the TLOC extension in the online documentation.
- TLOC extension is supported on the Cisco IOS XE based image.

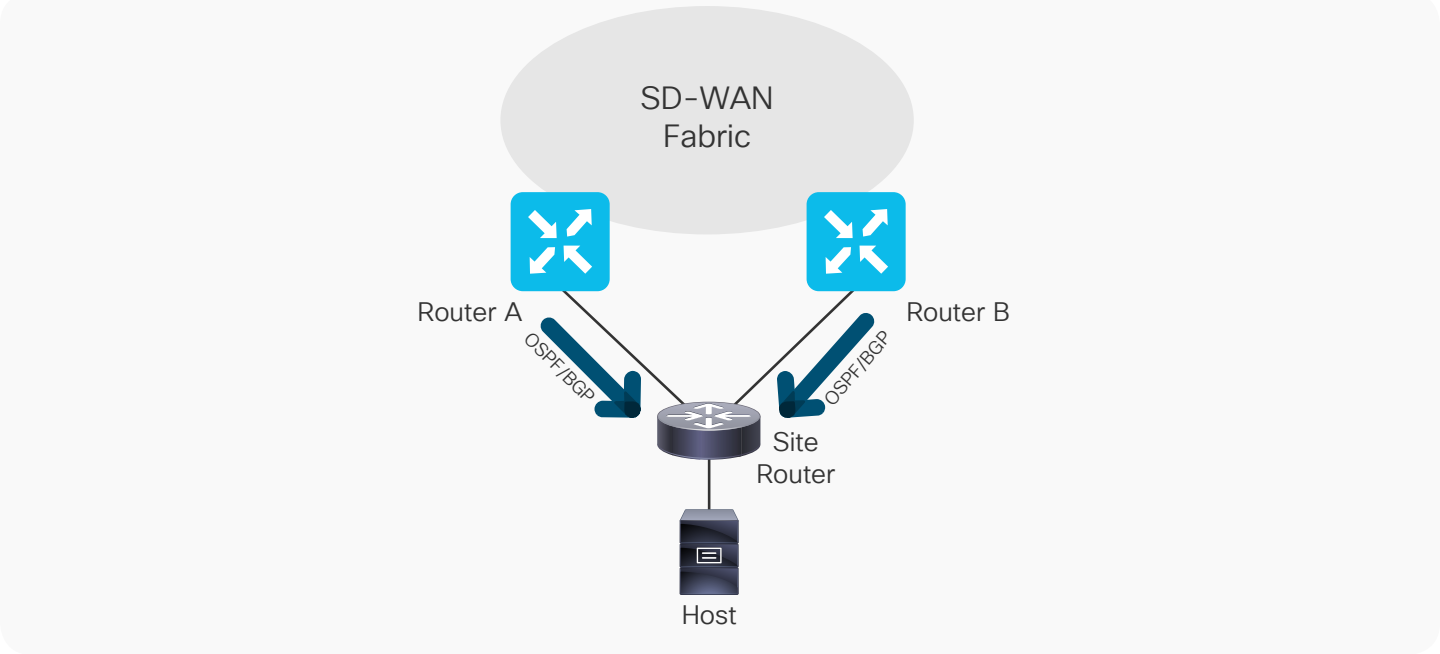
On the LAN side you have the following.

The routers can service one or more Layer 2 domains



VRRP is used to provide redundancy on the LAN side. Because we do not mix IOS XE and physical vEdge routers, you will experience the known IOS XE VRRP feature set.

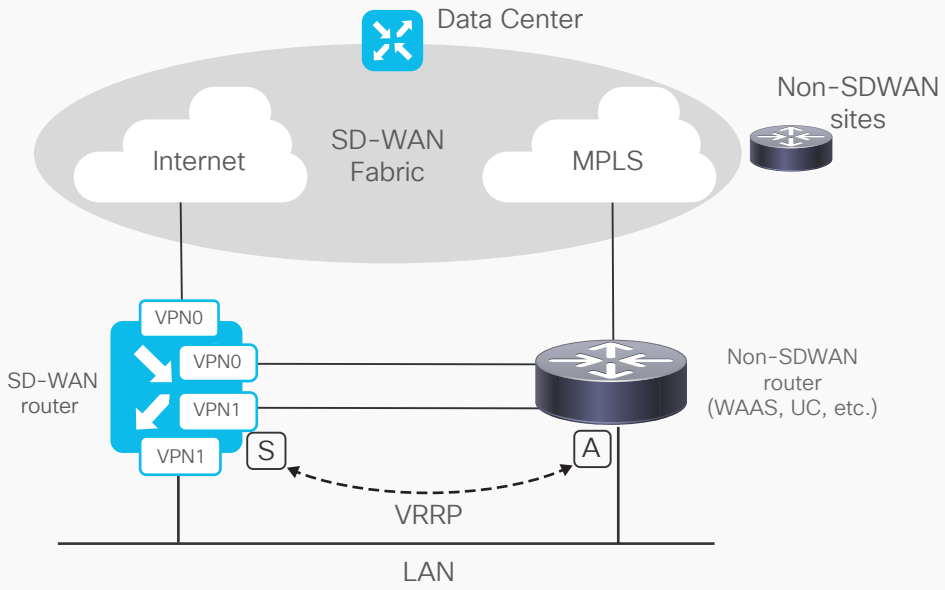
The routers can service one or more Layer 3 domains



SD-WAN Routers can establish OSPF or BGP to the site router, learn local site prefixes from the site router, and advertise overlay prefixes to the site router.

Two physical routers, one of which is non-SD-WAN

The following topology describes a use case involving a non-SD-WAN router that is needed for non-SD-WAN functionality such as Wide Area Application Services (WAAS) or unified communications.



On the WAN side, the WAN transports can be connected directly to the SD-WAN router, or in some cases (such as over the course of a migration to SD-WAN), the SD-WAN router can be connected to one transport and the services router to the other.

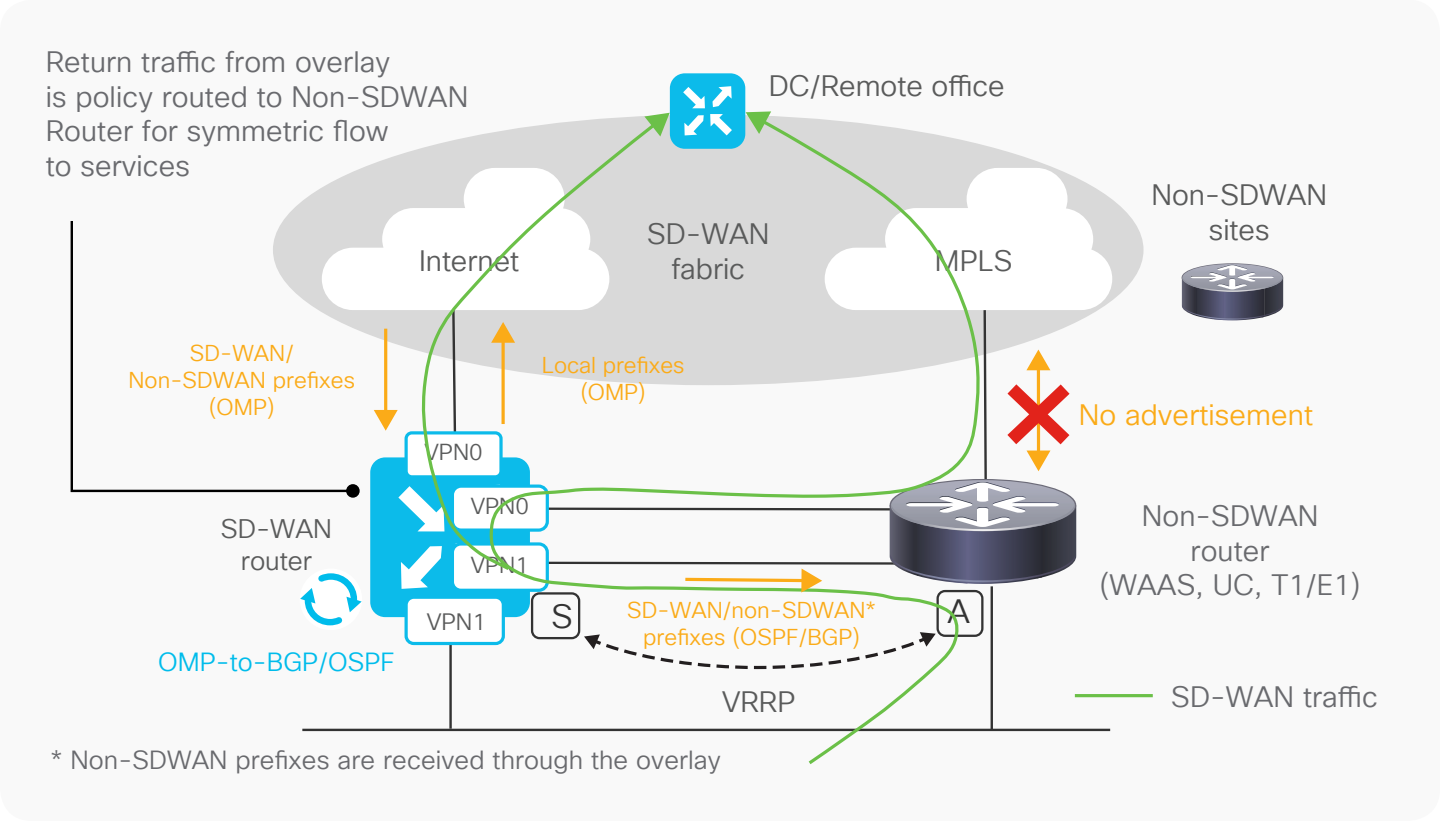
Regardless of the approach, the SD-WAN router will leverage all available WAN transports to build the SD-WAN fabric.

Typically, traffic that needs to be serviced by WAAS, unified communications, or firewalls needs to be consumed by the services device or router prior to encryption on the SD-WAN router. For this purpose, the non-SD-WAN router acts as a VRRP master on the LAN side.

The SD-WAN router then learns all of the SD-WAN-site prefixes over the fabric and advertises them to the non-SD-WAN router and the LAN.

In the event of a non-SD-WAN router failure, the SD-WAN router can become the VRRP master and continue forwarding traffic over the available transport.

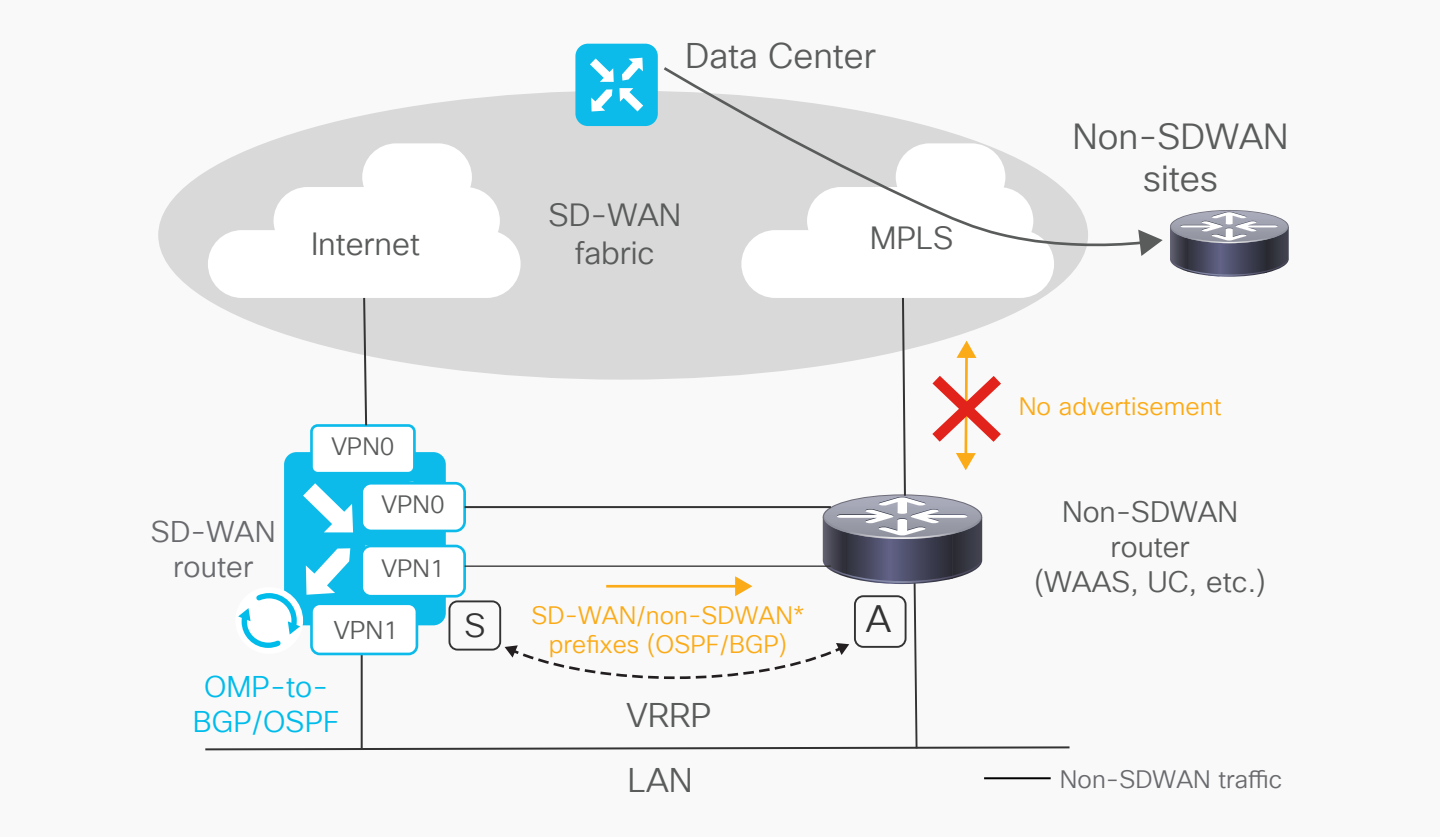
SD-WAN traffic flow



1. Traffic sourced from the LAN and destined to a remote SD-WAN site arrives at the non-SD-WAN or services router first
2. The relevant service or feature is applied to the traffic
3. The router then forwards the traffic to the service-side VPN on the SD-WAN router
4. The SD-WAN router forwards traffic over the SD-WAN fabric
5. Return traffic from the SD-WAN fabric arrives to the SD-WAN router first

Note that if the service or feature that is being used on the services router is stateful in nature (WAAS or firewall, for example), a local route policy can be configured on the SD-WAN router so that it routes the return traffic back to the services router first, instead of sending it directly to the LAN. This helps ensure flow symmetry on the services router.

Non-SD-WAN traffic flow



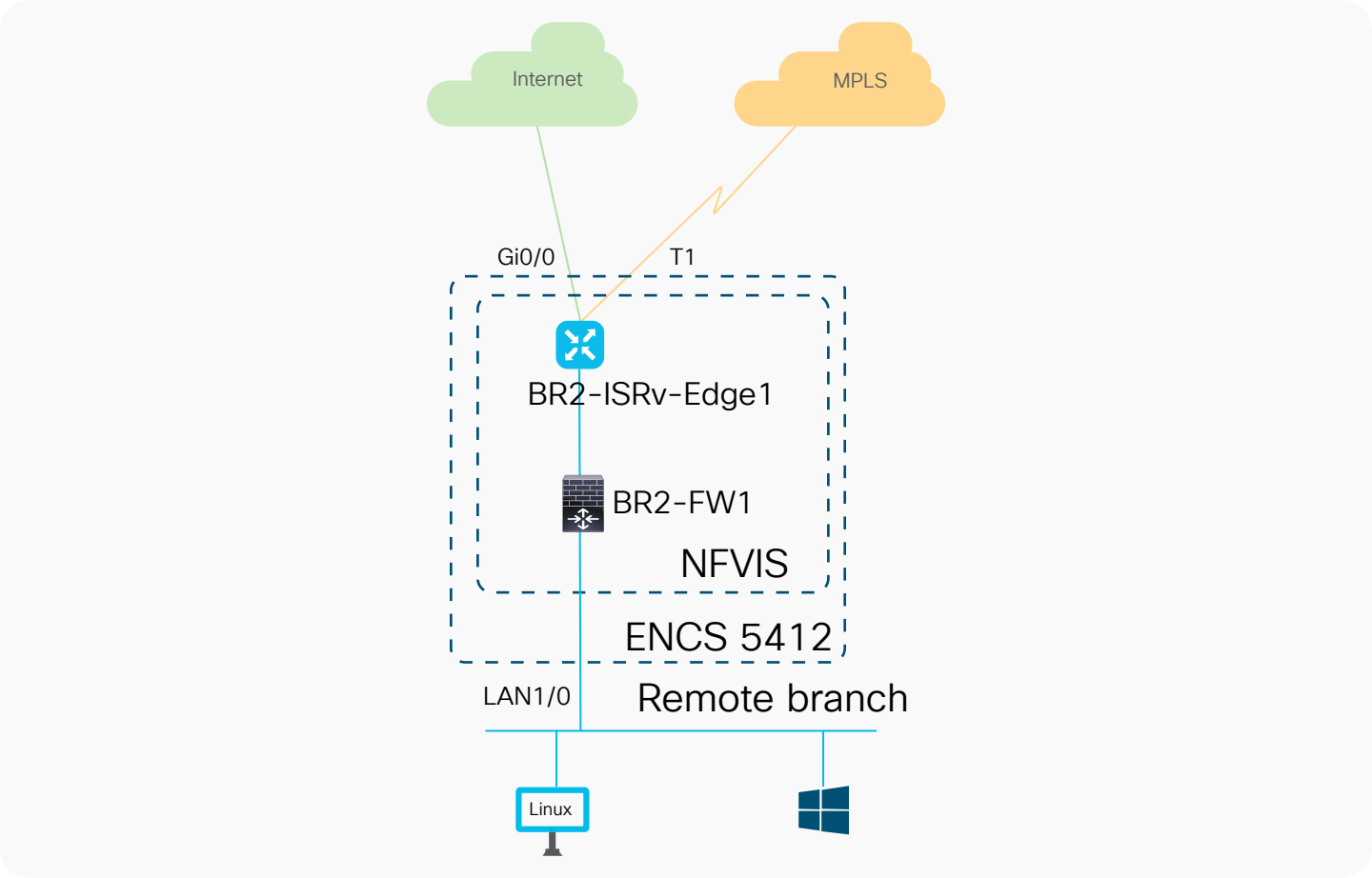
1. Traffic sourced from the LAN and destined to a remote non-SD-WAN site arrives at the non-SD-WAN or services router first
2. The relevant service or feature is applied to the traffic
3. The router then forwards the traffic to the service-side VPN on the SD-WAN router
4. The SD-WAN router forwards traffic over the SD-WAN fabric to the data center, regional hub, aggregation site, or migration site; from there, traffic is sent out the underlay or MPLS transport toward the non-SD-WAN site
5. Return traffic from the non-SD-WAN site will use the underlay or MPLS to route traffic back to the data center, regional hub, aggregation site, or migration site; from there, the SD-WAN fabric is used to forward traffic back to the SD-WAN router at the originating site

Note that if the service or feature being used on the services router is stateful in nature (WAAS or firewall, for example), a local route policy can be configured on the SD-WAN router so that it routes the return traffic back to the services router first, instead of sending it directly to the LAN. This helps ensure flow symmetry on the services router.

Virtual router solution on the ENCS platform

The Cisco 5000 Series Enterprise Network Compute System (ENCS) is a line of x86-based compute appliances designed for the Cisco Enterprise Network Functions Virtualization (ENFV) solution. The 5000 Series ENCS is a hybrid platform that combines the best attributes of a traditional router and a traditional server and offers the same functionality with a smaller infrastructure footprint. Offered with the Cisco ISRv with SD-WAN capabilities and NFV Infrastructure Software (NFVIS) as the hosting layer, the platform offers a complete solution for a simplified deployment.

Here is a simple example of a virtual branch running a virtual router and a virtual firewall on ENCS:



NFVIS is a Linux/KVM-based operating system running on ENCS. It is optimized for Virtual Network Functions (VNF) deployments supporting:

- Zero-Touch Deployment: Automatic connection to PnP, easy day 0 provisioning
- VNF monitoring
- Lifecycle management
- Service chaining
- Open API: Programmable API for service orchestration and REST and NETCONF API
- Monitoring: NETCONF notifications, host and VM statistics, packet capture

ISRv is a virtual-form-factor Cisco IOS XE based router that supports the same SD-WAN functionalities as physical Cisco IOS XE routers such as the 4000 Series ISRs. All use cases that are valid for physical routers are also applicable to virtual routers. Workflow, configuration, and features are exactly the same. Please refer to the ENCS and NFVIS online documentation for more details.

Note that there are some functional differences between ISRv and vEdge Cloud. For example, ISRv supports NIM slot E1/T1, while vEdge Cloud supports Ethernet only. There is no difference in terms of SD-WAN handling in vManage; ISRv has the same “look and feel” as vEdge Cloud.

Operational aspects

Return Materials Authorization (RMA)

Note that in the case of an RMA the new Cisco IOS XE router will not come with an SD-WAN image. A software upgrade will be needed. Please refer to the software upgrade section of this document for details.

Caveats for the first Cisco IOS XE SD-WAN release

Unsupported features

The key unsupported features in the first Cisco IOS XE SD-WAN release (July 2018) are:

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Voice services
- Service chaining with Overlay Management Protocol (OMP)
- CloudExpress (SAAS)
- Cloud OnRamp (IAAS)
- IPv6 transport
- NAT pool-service side
- Reverse proxy

There is a comprehensive roadmap for future SD-WAN software releases, which covers among others the features listed above.

Please refer to the release notes for the details: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/Release_Notes/Release_Notes_for_XE_SD-WAN_Release_16.9.1_and_SD-WAN_Release_18.3

Solutions for use cases in which Cisco IOS XE features are not yet supported

EIGRP

EIGRP is not supported in the first Cisco IOS XE SD-WAN release.

If you need EIGRP on the LAN-facing side, you can simply run BGP or OSPF to a router or virtual router and redistribute EIGRP.

Standard IPsec Internet Key Exchange (IKE) v1 or v2 (service side)

Use ISRv on ENCS to establish standard IP Security (IPsec) tunnels.

Unified communication

To enhance the Voice traffic end-point capability at the branch/Datacenter, the voice gateway and call manager can be hosted for example on ENCS platform as VNF. This can be deployed as a 2-box solution with SDWAN Edge router.

The voice traffic originating from the LAN side needs to be processed by the Cisco Call Manager and SIP gateway router prior to encryption on the SDWAN router. For this purpose, LAN routing should be configured to direct all the LAN originated traffic to UC Service router (ENCS 5400) first. SDWAN Edge router then encrypts and send it over SDWAN fabric.

Traffic flow:

- Voice Traffic sourced from the LAN and destined to a remote SDWAN site arrives at the non-SDWAN/services router (ENCS) first
- Voice Gateway running on the ISRv will intercept the traffic and process it
- Post that the SDWAN router receives the traffic and applies IPSec and forwards traffic over the SDWAN fabric via VPN-0
- Return traffic from the SDWAN fabric arrives to the SDWAN router first
- The SDWAN router then forwards return traffic to the UC Services router first which will process the voice traffic and forward it to the appropriate LAN device.

Conclusion

Cisco SD-WAN enables customers to transition to a next-generation cloud-delivered software-defined WAN infrastructure. It delivers a better application experience by using application-aware routing; secures branch communication through segmentation, zone-based firewall, application firewall, and Cisco Umbrella™; allows seamless cloud adoption with Cloud onRamp for SaaS and IaaS applications; and ultimately provides a transformative operational experience. Selected Cisco ASR and ISR routers can now participate in the Cisco SD-WAN solution.

Custom call to action

The best way to understand and learn about the Cisco SD-WAN solution is to try at dcloud.cisco.com and then run a Proof Of Concept (POC). Cisco presales engineers have a standard POC test plan that covers the most common SD-WAN use cases. A free dCloud lab for SD-WAN is available on dcloud.cisco.com.

Please contact your account team and ask for a POC for SD-WAN on Cisco IOS XE today.

C11-741071-00 08/18