Cisco HyperFlex SD-WAN Deployment Guide

First Published: 2020-02-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

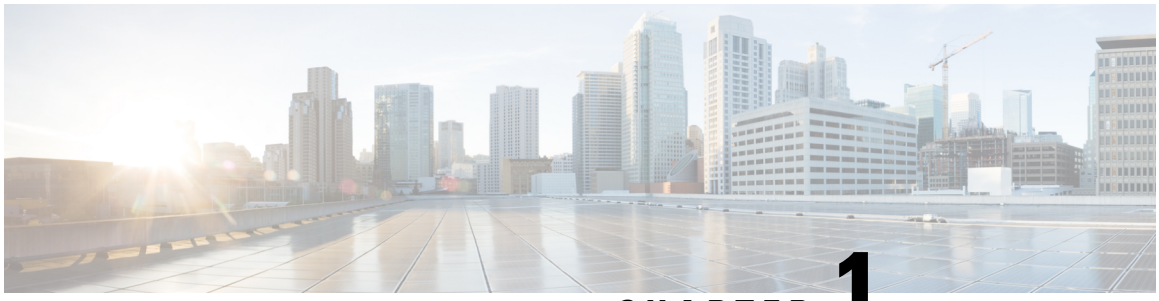
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Overview

Technology Overview

Cisco HyperFlex SD-WAN

The Cisco HyperFlex SD-WAN solution is a major technology inflection which integrates Edge Computing, hyperconverged infrastructure, machine learning, and SD-WAN technologies. Cisco SD-WAN vEdge Routers are routing components of the architecture that deliver the essential WAN, security and multi-cloud capability of the Cisco SD-WAN solution. Cisco HyperFlex Edge brings the simplicity of hyperconvergence to remote and branch office (ROBO) and edge environments.

Powered by Intersight, the solution provides a fully automated, zero touch provisioning of the compute, storage, LAN and WAN networking for lights out branch deployment at a massive scale. It dramatically simplifies the management of WAN networking using Software-Defined WAN and enables new types of connectivity models beyond traditional VPNs.

Cisco Intersight

Cisco Intersight™ is a management platform delivered as a service with embedded analytics for your Cisco and 3rd party IT infrastructure. This platform offers an intelligent level of management that enables IT organizations to analyze, simplify, and automate their environments in more advanced ways than the prior generations of tools. Cisco Intersight provides an integrated and intuitive management experience for resources in the traditional data center as well as at the edge. With flexible deployment options to address complex security needs, getting started with Intersight is quick and easy.

Cisco Intersight has deep integration with Cisco UCS and HyperFlex systems allowing for remote deployment, configuration, and ongoing maintenance. The model-based deployment works for a single system in a remote location or hundreds of systems in a data center and enables rapid, standardized configuration and deployment. It also streamlines maintaining those systems whether you are working with small or very large configurations.

Cisco HyperFlex Edge Systems

Cisco HyperFlex Edge systems are optimized for remote sites, branch offices and edge environments. As a smaller form factor of Cisco HyperFlex, Cisco HyperFlex Edge keeps the full power of a next generation hyperconverged platform without the use of Cisco UCS Fabric Interconnects. Cisco HyperFlex Edge systems

support a variable configuration of 2, 3, or 4 HyperFlex converged nodes and support the scaling of CPU, memory and storage capacity (hot-add additional capacity drives) based on your requirements. Cisco HyperFlex Edge provides scalable and cost-optimized solutions for anywhere deployment.

Cisco SD-WAN

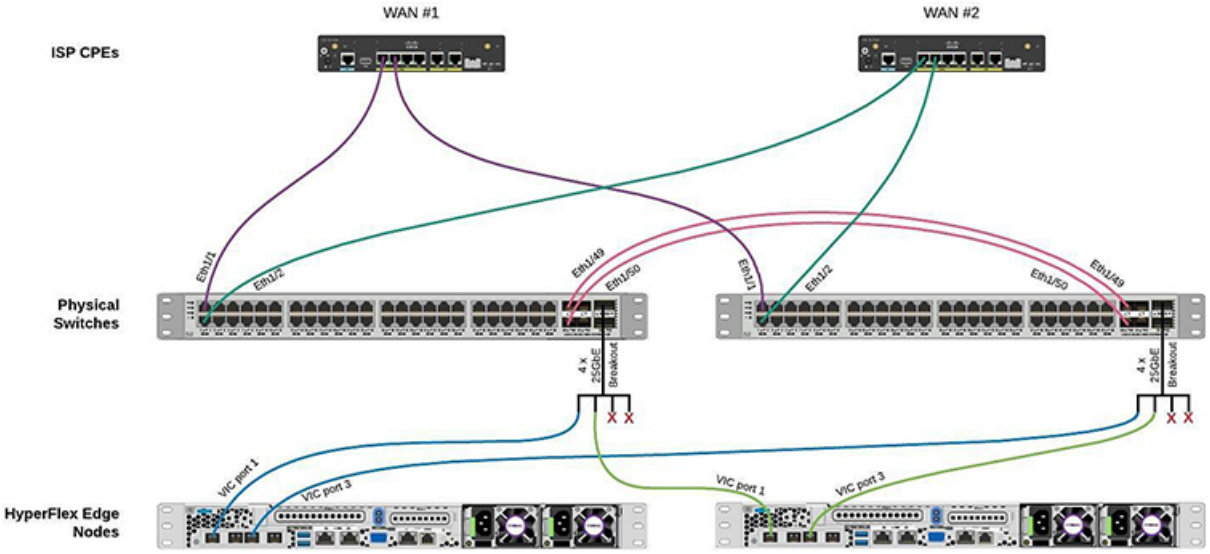
The Software-Defined Wide-Area Network (SD-WAN) is a specific application of software-defined networking (SDN) technology applied to WAN connections such as broadband internet, 4G, LTE, or MPLS. It connects enterprise networks including branch offices and datacenters over large geographic distances. WAN connections often used technology that required special proprietary hardware. SD-WAN, on the other hand, utilizes the internet or cloud-native private network.

Architecture Overview

Physical Architecture

This section provides the detailed physical architecture of the Cisco Catalyst C9300L-48P-4X-A for use in a HyperFlex SD-WAN environment.

The following diagram shows the HyperFlex SD-WAN solution with two nodes. Deploying the SD-WAN solution on HyperFlex clusters is supported on HyperFlex Edge 2, 3, and 4 nodes. The WAN connections are vEdge Routers, which can be either single or dual terminated. Up to 2, 3, or 4 WAN connections are supported. HyperFlex Edge 10 Gigabit Ethernet (GbE) network topology is supported on the Catalyst switches.

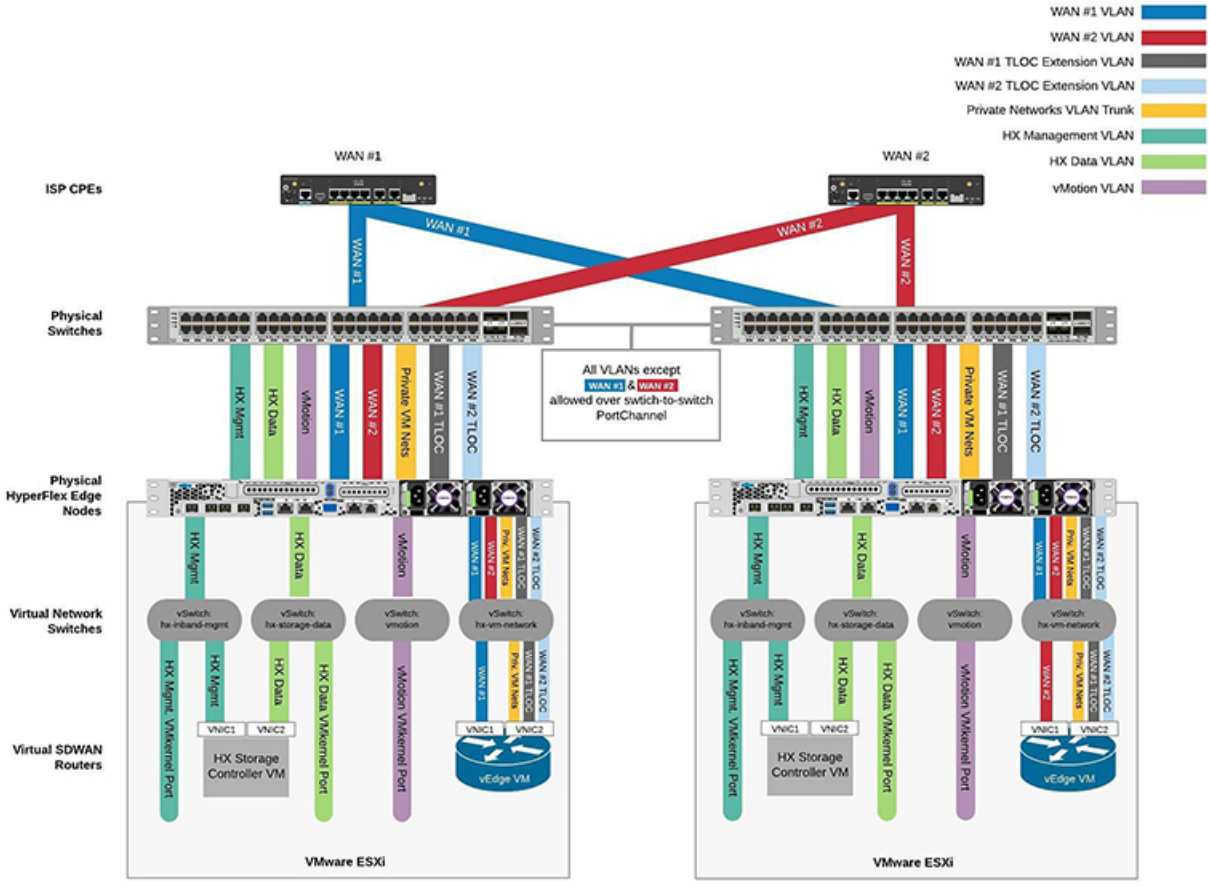


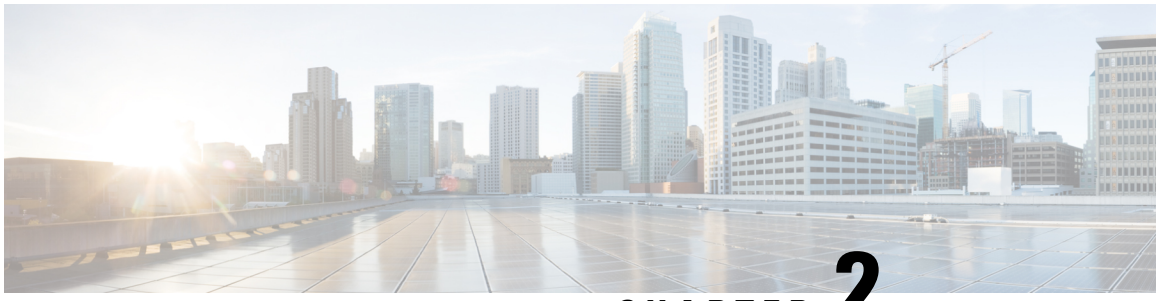
Logical Architecture

This section provides the detailed logical architecture of a HyperFlex SD-WAN environment.

A vEdge Cloud Router is deployed as an SD-WAN Edge Router. The vEdge VM is deployed with 4 vNICs by default. Out of the 4, 3 vNICs are used for WAN facing access connections. One vNIC is used for LAN facing service side (trunk) connections. The HyperFlex SD-WAN installer configures the vSwitches automatically.

Note You have to manually configure the physical switches.





CHAPTER 2

Preinstallation

Installation Prerequisites

Caution This feature is in preview and is not meant for use in your production environment. Cisco recommends that you use this feature on a test network/system.

This feature is currently not supported on Cisco Intersight Virtual Appliance.

You can deploy the SD-WAN solution on a HyperFlex Edge cluster only if the following requirements are met:

- Deployment is supported only from Intersight.
- You must have an Account Administrator role.
- At a minimum, one of the Edge server must be in the Intersight Advantage license tier to view Solutions.
- Only HyperFlex Edge with 10 Gigabit Ethernet (GbE) uplink is supported.
- Cisco HyperFlex HX220c M5 Hybrid and All-Flash nodes are supported.

Complete the following prerequisites before initiating the HyperFlex SD-WAN deployment wizard in Intersight:

1. Ensure that the vManage account has network connectivity to Cisco Intersight. Do the following:
   a. Navigate to Cisco Support Case Manager.
   b. To open a new case, select **New Case** > **Products & Services** > **Open Case**.
   c. Enter the appropriate entitlement information details. Typically, you need to enter the serial of the WAN Edge device. Select **Next**.
   d. Enter the case details.

e. Select **Technology**, search for the appropriate Sub Tech keyword *Technology: Software Defined Wide Area Networking (SDWAN) SubTechnology: SDWAN CloudInfra*.

f. The support team will work to authenticate Cisco Intersight to the vManage account and inform you when the authentication process is done.

2. Configure the switches for use in a HyperFlex Edge Fabric. For an example of how to configure the Cisco Catalyst C9300L-48P-4X-A switches, see Configuring the Cisco Catalyst C9300L-48P-4X-A Switches.
3. Use one of the supported switches as listed in the HyperFlex Edge Deployment Guide. Configure the switches manually with the required and recommended settings before beginning the installation process. See the Cisco HyperFlex Edge Deployment Guide, Release 4.0 for more details.
4. Claim the HyperFlex nodes in Intersight. See Claim Devices, on page 12 for more details.
5. In the Cisco IMC, the **NIC Mode** can be either **Cisco Card** or **Dedicated**. Ensure that the Cisco IMC Switchport VLAN is the same as the VLAN used for HyperFlex management.

Important Cisco Card is the preferred option.

6. Manually configure the required Feature templates for branch routing design in vManage. Manually upload the list of deployable vEdge virtual router chassis UUIDs in vManage. For more information, see the Systems and Interfaces Configuration Guide, Cisco SD-WAN Releases 19.1, 19.2, and 19.3.

Supported Versions and System Requirements

Licensing Requirements

The following table lists the required license requirements for the various components:

Component	Licensing Requirement
Cisco HyperFlex Edge Systems	HyperFlex Data Platform Edge Edition
Cisco Intersight	Intersight Advantage
Cisco SD-WAN	Cisco DNA Essentials

Software Versions

The following table lists the minimum supported software version:

Component	Minimum Supported Software Version
Cisco HyperFlex Data Platform	4.0(1b), 4.0(2a)
Cisco IMC	4.0(2f) **Restriction**4.0(4h) is not supported

Component	Minimum Supported Software Version
Cisco vEdge Cloud	19.2.1
Cisco Catalyst 9000	IOS-XE 17.1
VMware ESXi	6.5 U3, 6.7 U2
VMware vCenter	6.5 U3, 6.7 U2

Hardware Requirements

Deployment of the HyperFlex SD-WAN solution is supported only on Cisco HyperFlex HX220c M5 Hybrid and All-Flash nodes.

Use one of the supported switches as listed in the HyperFlex Edge Deployment Guide. Configure the switches manually with the required and recommended settings before beginning the installation process. See the Cisco HyperFlex Edge Deployment Guide, Release 4.0 for more details.

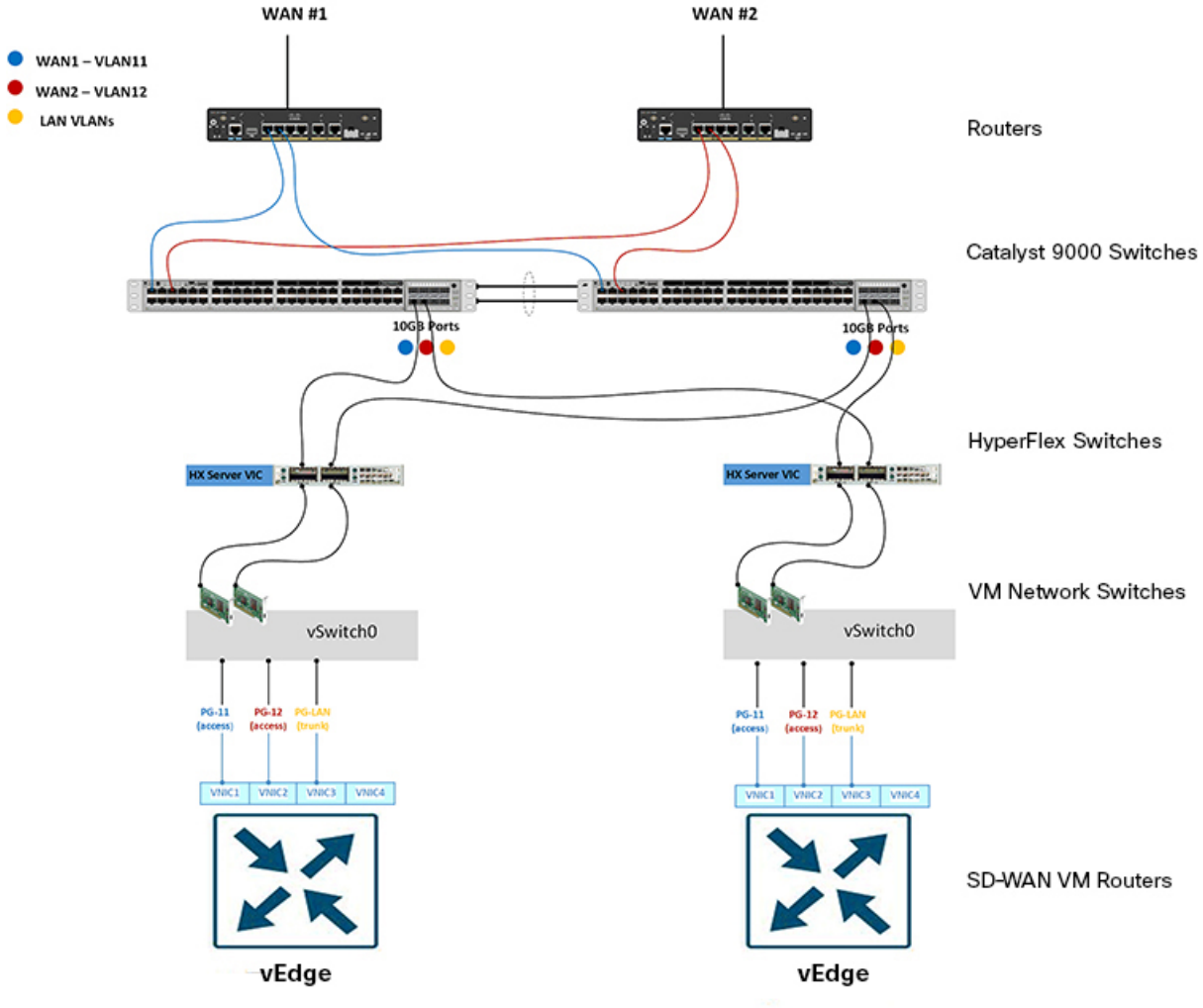
Supported Topologies

The following variants of Physical WAN connectivity and SD-WAN WAN termination topologies are supported for HyperFlex SD-WAN deployment.

HyperFlex SD-WAN Dual Router and Dual WAN Termination Topology

In this topology, separate physical WAN hand-off devices per physical WAN router are connected with dual termination on SD-WAN virtual routers.

- The WAN hand-offs from the different physical routers are connected separately to the customer provided endpoints (CPE). Each CPE has southbound connections that are connected to each switch as an access switch port on a separate L2 VLAN per WAN.
- Each WAN is terminated on both SD-WAN virtual routers as a separate vNIC on the router virtual machine.
- The connectivity of each VNIC is configured through the port group that corresponds to the WAN VLAN configured on the vSwitch in the Hypervisor.
- Each port group directly corresponds to the L2 VLAN which is utilized by the CPE southbound interfaces for each WAN.
- In this topology, there is no need to configure transport location (TLOC) extensions between the two routers to share the WAN connections between the two routers.
- The LAN vNIC configured on the SD-WAN virtual router is used to route traffic on the Service VPNs configured as sub-interfaces on the LAN vNIC. These sub-interfaces are used to route traffic between multiple local Service VPNs and VPNs established across the WANs.

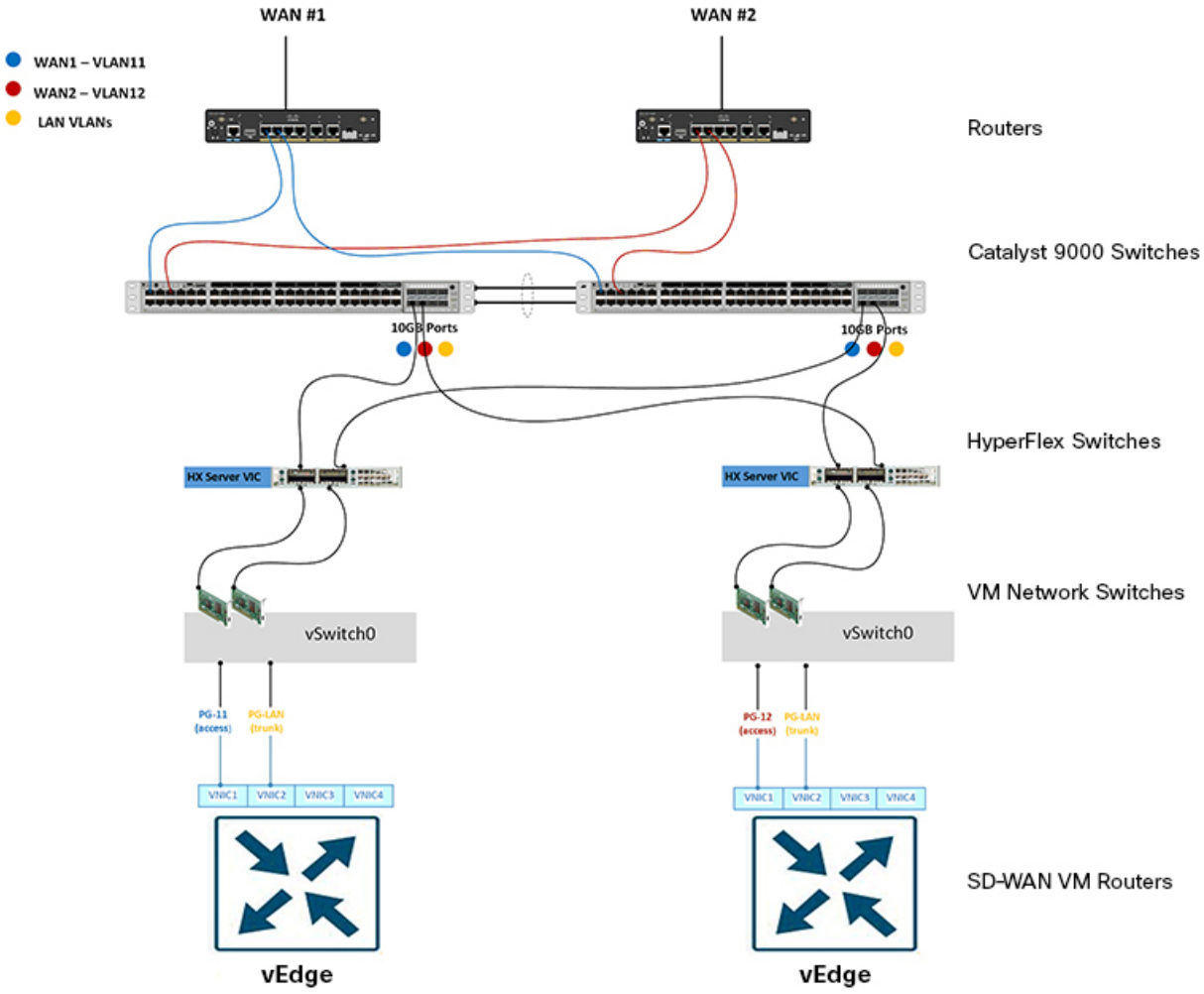


HyperFlex SD-WAN Dual Router and Single WAN Termination Topology

In this topology, separate physical WAN hand-off devices per physical WAN router are connected with single termination on SD-WAN virtual routers.

- The WAN hand-offs from the different physical WAN routers are connected separately to the customer provided endpoints (CPE). Each CPE has southbound connections that are connected to each switch as an access switch port on a separate L2 VLAN per WAN.
- Each WAN is terminated only on a single SD-WAN virtual router as a separate vNIC on the virtual router machine.
- The connectivity of each vNIC is configured through the port group that corresponds to the WAN VLAN configured on the vSwitch in the Hypervisor.
- Each port group directly corresponds to the L2 VLAN which is utilized by the CPE southbound interfaces for each WAN.
- In this topology, transport location (TLOC) extensions must be configured between the two routers to share the WAN connections between the two routers.

- A VLAN per WAN must be defined to allow east-west communication between the routers.
- The LAN vNIC configured on the SD-WAN virtual router is used to route traffic on the Service VPNs configured as sub-interfaces on the vNIC. These sub-interfaces are used to route traffic between multiple local Service VPNs and VPNs established across the WANs.



Limitations

The following list outlines the limitations in deploying the SD-WAN solution on HyperFlex Edge clusters using Intersight:

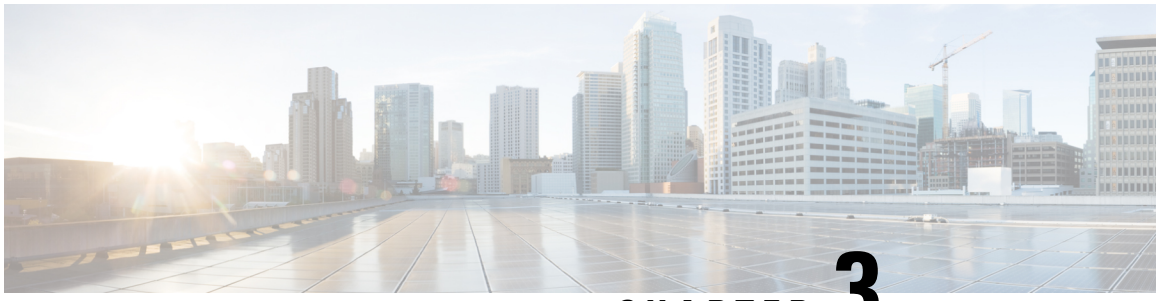
- Deployment of the HyperFlex SD-WAN solution is not supported on HyperFlex clusters with Fabric Interconnects.
- HyperFlex Edge 1 Gigabit Ethernet (GbE) is not supported.
- Deployment of the HyperFlex SD-WAN solution is not supported on HyperFlex M4 nodes.

- Only ESXi deployment is supported. Hyper-V and KVM deployments are not supported.
- Cluster expansion is not supported.

Known Issues

The following list outlines the known issues that may occur when deploying the SD-WAN solution on HyperFlex Edge clusters:

- You cannot terminate a deploy HyperFlex SD-WAN workflow which is in-progress.
- Cisco IMC release 4.0(4h) is not supported.
- Device Templates generated from CLI Template are not supported. Use Feature Templates instead, to create Device Templates.
- You can view Solutions in the left navigation in Intersight only if at least, one Edge server is in the Intersight Advantage license tier.



CHAPTER 3

Installation

Installation Overview

The following table summarizes the installation workflow for deploying the SD-WAN solution on a HyperFlex cluster:

Step	Summary	Reference
Preinstallation Tasks Complete the tasks 1—5 before deploying the SD-WAN solution on a HyperFlex cluster.		
1.	Configure the switches for use in a HyperFlex Edge Fabric.	For an example of how to configure the Cisco Catalyst C9300L-48P-4X-A switches, see Configuring the Cisco Catalyst C9300L-48P-4X-A Switches.
	Use one of the supported switches as listed in the HyperFlex Edge Deployment Guide. Configure the switches manually with the required and recommended settings before beginning the installation process.	See the Cisco HyperFlex Edge Deployment Guide, Release 4.0 for more details.
2.	Log into Cisco Intersight and Claim Devices.	Log In to Cisco Intersight, on page 12 Claim Devices, on page 12
3.	Create a Cisco Smart Account Configuration for HyperFlex SD-WAN.	Cisco Smart Account Configuration for HyperFlex SD-WAN, on page 13

Step	Summary	Reference
4.	Manually configure the required Feature templates for branch routing design in vManage. Manually upload the list of deployable vEdge virtual router chassis UUIDs in vManage.	For more information, see the Systems and Interfaces Configuration Guide, Cisco SD-WAN Releases 19.1, 19.2, and 19.3.
Install, Configure, and Deploy		
5.	Run the Create HyperFlex SD-WAN wizard to deploy the SD-WAN solution on a HyperFlex Cluster.	Deploy SD-WAN Solution on a HyperFlex Cluster, on page 17
Post Installation		
6.	Complete post installation tasks.	Post Installation, on page 25

Log In to Cisco Intersight

Log In using Cisco ID

To login to Cisco Intersight, you must have a valid **Cisco ID** to create a Cisco Intersight account. If you do not have a Cisco ID, create one here.

Important The device connector does not mandate the format of the login credentials, they are passed as is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server.

Log In using Single Sign-On

Single Sign-On (SSO) authentication enables you to use a single set of credentials to log in to multiple applications. With SSO authentication, you can log in to Intersight with your corporate credentials instead of your Cisco ID. Intersight supports SSO through SAML 2.0, and acts as a service provider (SP), and enables integration with Identity Providers (IdPs) for SSO authentication. You can configure your account to sign in to Intersight with your Cisco ID and SSO. Learn more about SSO with Intersight here.

Claim Devices

Complete the following steps to claim one or more devices to be managed by Cisco Intersight:

Before you begin

This procedure assumes that you are an existing user with a Cisco account. If not, see Log In to Cisco Intersight, on page 12. Only Intersight users with Account Administrator, Device Administrator, or Device Technician privileges can claim a new device.

Step 1 In the Cisco Intersight, left navigation pane, select **Administration** > **Devices**.

Step 2 In the **Devices** details page, click **Claim a New Device**.

Step 3 In the **Claim a New Device** page, select **Direct Claim** and complete the following fields:

Note You can locate the **Device ID** and the **Claim Code** information in:

a. Cisco IMC by navigating to **Admin** > **Device Connector**.

b. Cisco HyperFlex by navigating to **HyperFlex Connect UI** > **Settings** > **Device Connector**.

UI Element	Essential Information
Device ID	Enter the applicable Device ID. • For a Cisco UCS C-Series Standalone server, use serial number. Example: NGTR12345 • For HyperFlex, use Cluster UUID. Example: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Claim Code	Enter device claim code. You can find this code in the Device Connector for the device type. **Note** Before you gather the Claim Code, ensure that the Device Connector has outbound network access to Cisco Intersight, and is in the "Not Claimed" state.

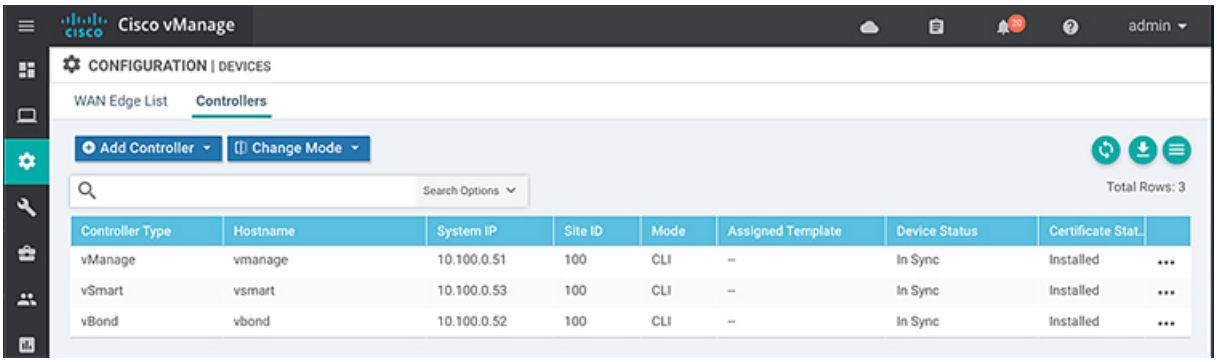
Step 4 Click **Claim**.

Note Refresh the Devices page to view the newly claimed device.

Cisco Smart Account Configuration for HyperFlex SD-WAN

Before completing the operations listed in this section, consider the following prerequisites:

- You must have a Cisco Smart Account.
- You must have a Virtual Account within the Cisco Smart Account.
- Cisco vManage add Deployed and configured controllers like vBond, vSmart, and vManage controllers. Ensure that the **Device Status** is *In Sync* as shown in the following figure.



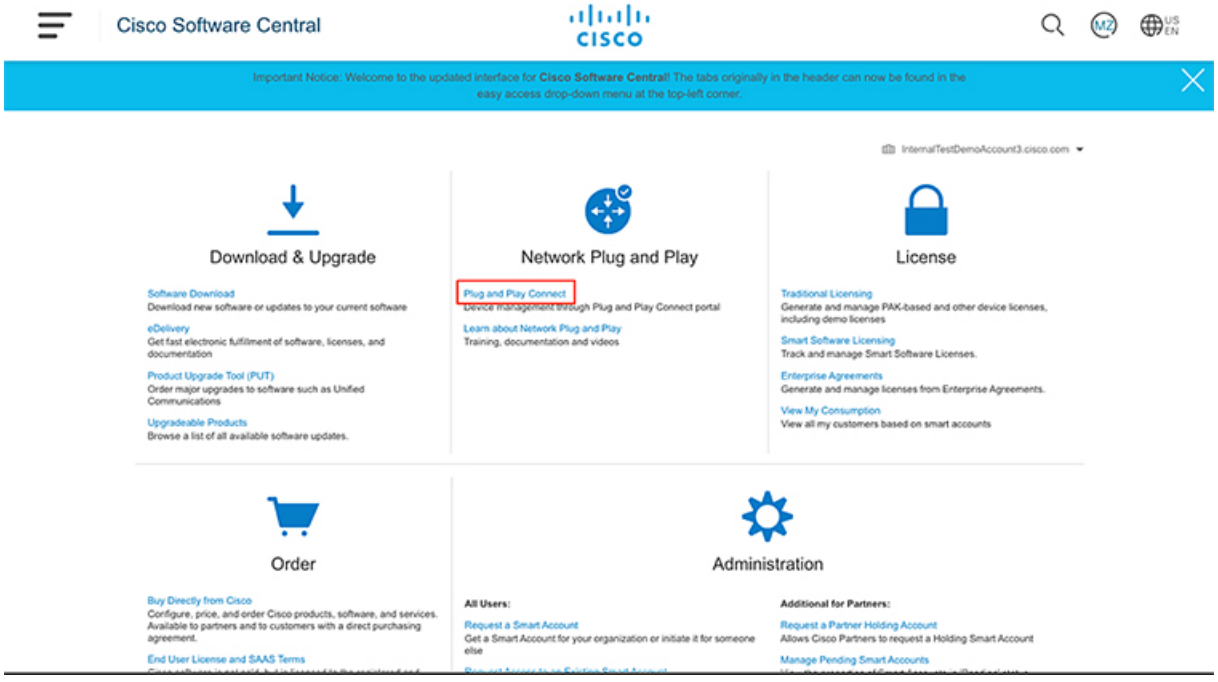
To create a Cisco Smart Account Configuration for HyperFlex SD-WAN, do the following:

1. Create Plug and Play Controller Policies in Smart Account, on page 14.
2. Create Plug and Play Software Devices in Smart Account, on page 15.
3. Sync vManage to Smart Account, on page 16.

Create Plug and Play Controller Policies in Smart Account

Step 1 Navigate to https://software.cisco.com and log in with your credentials.

Step 2 Click on **Plug and Play Connect** under the **Network Plug and Play** section.



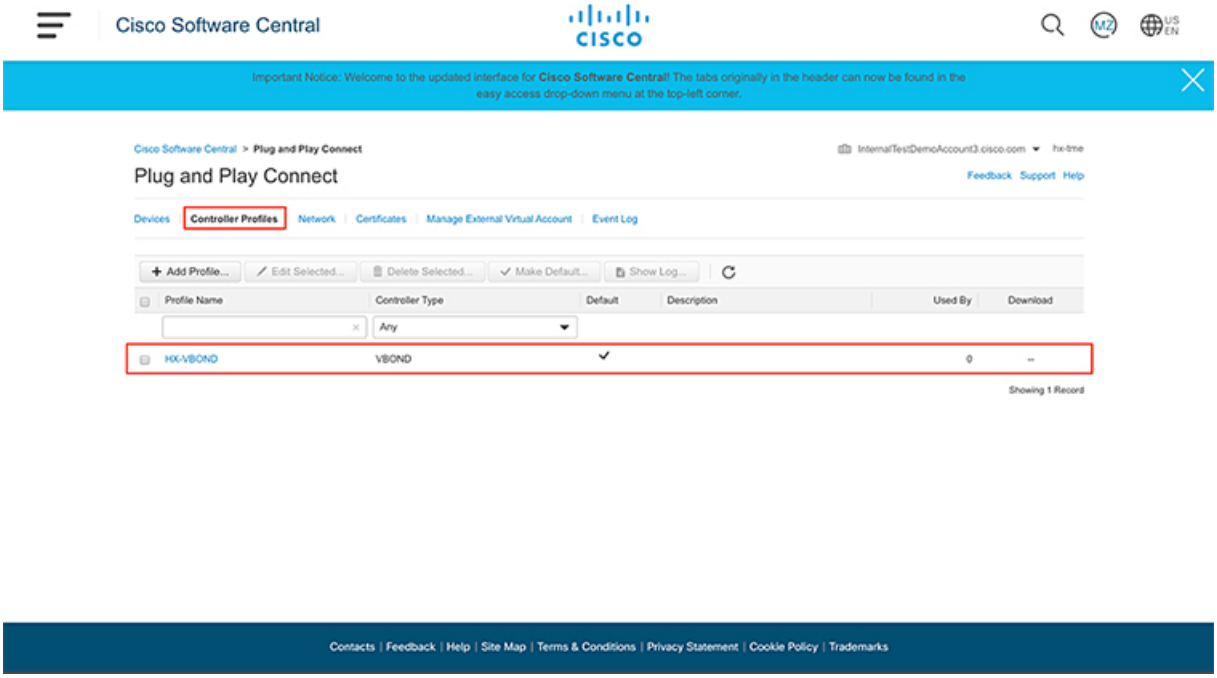
Step 3 Click on **Controller Profiles**.

Step 4 Click **Add Profile**.

a) In the **Profile Type** step, select **VBOND** from the **Controller Type** drop-down. Click **Next**.

b) In the **Profile Settings** step, enter a **Profile Name**, set **Default Profile** to **Yes**, enter an **Organization Name**, and enter the vBond information for the **Primary Controller**. Also, upload the **Server Root CA**. Click **Next**.
c) In the **Review** step, review the details and click **Submit**.
d) In the **Confirmation** step, click **Done**.

Step 5 The newly created Controller Profile will show up under the **Controller Profiles** section of **Plug and Play Connect**.



What to do next

Create plug and play software devices in Smart Account.

Create Plug and Play Software Devices in Smart Account

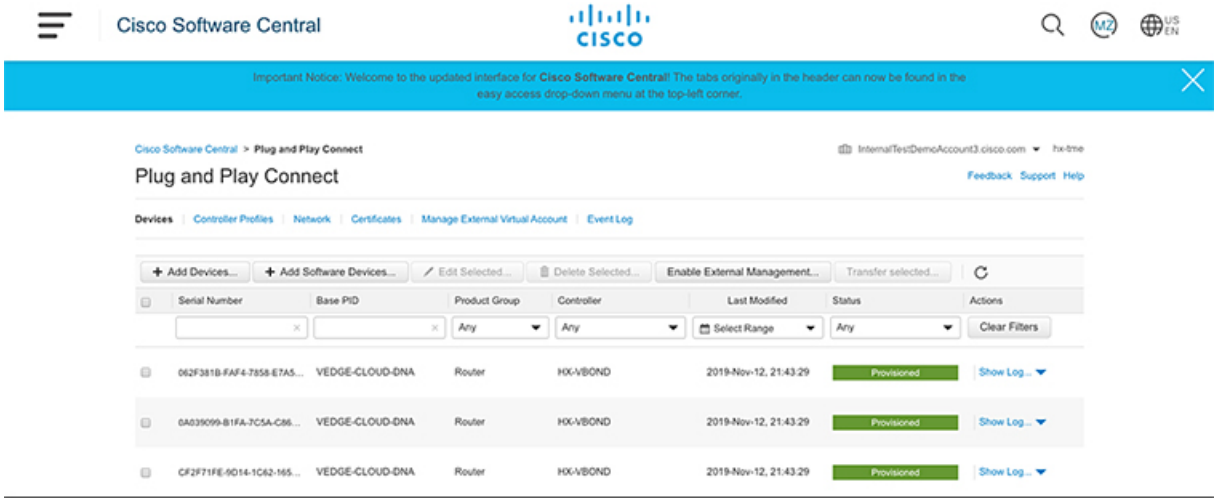
Before you begin

Create a Controller Profile in Smart Account.

Step 1 Navigate to https://software.cisco.com and log in with your credentials.
Step 2 Click on **Plug and Play Connect** under the **Network Plug and Play** section.
Step 3 Click on **Devices**.
Step 4 Click on **Add Software Devices**.
a) In the **Identify Devices** step, click **Add Software Device**. In the **Identify Device** popup window, set the **Base PID** to ***VEDGE-CLOuD-DNA***, enter a **Quantity**, and select the **Controller Profile** created earlier. Click **Save**. The Devices will now show up under the **Identify Devices** section. Click **Next**.
b) In the **Review & Submit** step, review the device information provided and click **Submit**.

c) In the **Results** step, click **Done**.

Step 5 In the **Devices** page, based on the **Quantity** entered, a number of devices will show up. When a device is created, initially it will show a **Status** of Pending for Publish. After sometime, the status will change to **Provisioned**.



What to do next

Sync vManage to Smart Account.

Sync vManage to Smart Account

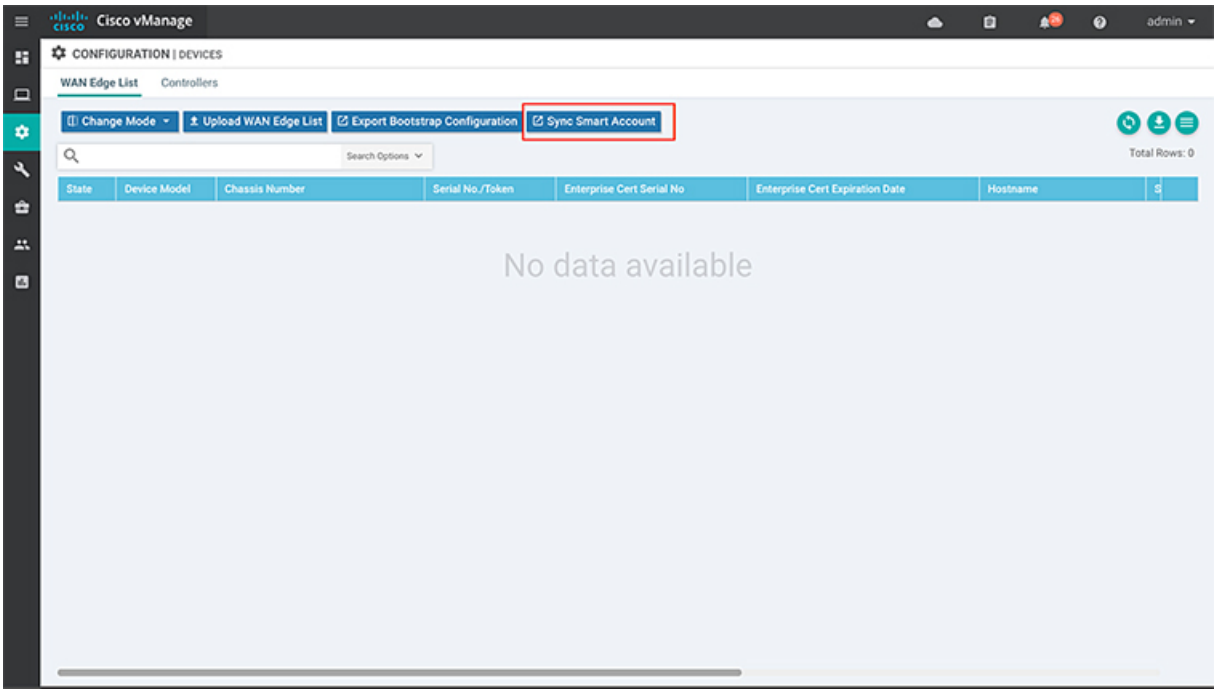
Before you begin

Create plug and play software devices in Smart Account.

Step 1 In your web browser, log into Cisco vManage.

Step 2 Navigate to **Configuration** > **Devices**.

Step 3 Click on **Sync Smart Account**.

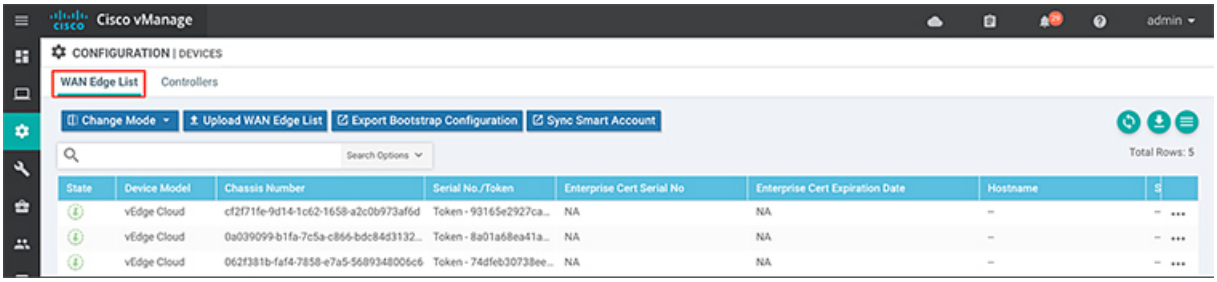


Step 4 In the **Sync Smart Account** popup, enter the **Username** and **Password** associated with the Smart Account where the Controller Profile and Software Devices were created earlier. Leave the **Validate the uploaded WAN Edge List and send to controllers** option checked. Click **Sync**.

Step 5 In the **Task View** page, the status of the **Smart Account Device Sync** shows as *In Progress* for a couple of minutes and then becomes *Success*.

Step 6 Navigate back to the **Configuration** > **Devices** page.

Step 7 Verify if the **Software Devices** created in the associated Smart Account show up in the **WAN Edge List** table as shown in the following image.



Deploy SD-WAN Solution on a HyperFlex Cluster

In the Deploy HyperFlex SD-WAN wizard, complete the following details to deploy the SD-WAN solution on a HyperFlex cluster using Intersight.

Step 1 Navigate to **Solutions**.

Step 2 Select the **Deploy HyperFlex SD-WAN** solution, and click **Initiate**.

Note In the **Executions** column, click on the number to navigate to the Requests page. Here you can view recent executions of the Deploy HyperFlex SD-WAN solution.

To view existing partially complete solutions, in the ellipsis (…) click Drafts. To edit an existing draft, select a draft from the Drafts table view, in the ellipsis (…) click **Edit**.

Step 3 Click **Start** to begin the Deploy HyperFlex SD-WAN wizard.

Step 4 In the **General** page, complete the following details:

Field	Description
Organization drop-down list	You can make the HyperFlex SD-WAN cluster belong to either the default organization or a specific organization: • Default organization—Choose default to make the HyperFlex SD-WAN cluster belong to the default organization. All policies that belong to the default organization are in the Create HyperFlex SD-WAN wizard. • Specific organization—To make the HyperFlex SD-WAN cluster belong to a specific organization, select the desired organization from the drop-down. Only policies that belong to the selected organization are in the Create HyperFlex SD-WAN wizard.
Name field	Enter a name for the SD-WAN profile. The name entered here is displayed on the Requests page, after the SD-WAN solution is deployed on the HyperFlex cluster.
(Optional) **Description** field	Add a description for the SD-WAN profile.
(Optional) **Add Tag** field	Add a tag key.

Step 5 In the **vManage Connection** page, complete the following details to connect to your vManage account:

Field	Description
vManage Account	
vManage Server field	Enter the vManage URL that the account holds information for.
Port field	Default is 8443. Enter the vManage port number on which the application is running.
User field	Enter the local username for authenticating with the vManage server.

Field	Description
Password field	Enter the local password for authenticating with the vManager server.
Virtual Router Deployment Configuration	
Deployment Size drop-down list	Select the scale of the SD-WAN router virtual machine deployment. This can be: • **Typical**—4vCPU / 4GB memory • **Minimal**—2vCPU / 4GB memory
Version drop-down list	Select the version depending on the relationship to the solution distributable object.
Number of WANs field	Select the number of WAN connections required across the SD-WAN site. The number of WANs can be: • Single WAN—1 to 4 • Dual WAN—2
WAN Termination Type drop-down list	Defines if the WAN networks are singly or dually terminated. • **Single**—Singly terminated WANs are configured only on one of the SD-WAN routers. One single WAN terminator is configured on each vEdge router. For example, WAN 1 is configured on vEdge node 1 and WAN 2 is configured on vEdge node 2. • **Dual**—Dually terminated WANs are configured on all the SD-WAN routers.

Step 6 In the **Virtual Router Configuration** page, configure the virtual routers by providing Chassis UUID and Device Template using information from vManage.

Field	Description
Virtual Router 1 and **Virtual Router 2**	
Chassis UUID field	Enter the chassis ID number of the vEdge router.
Device Template field	Enter the name of the Cisco vManage device template that the current device should be attached to. A device template consists of many feature templates and has the SD-WAN router configuration. For more information, see the Systems and Interfaces Configuration Guide, Cisco SD-WAN Release 19.1, 19.2, and 19.3.

Step 7 The fields in the **Virtual Router Device Specific Configuration** page, are dynamically generated based on the Device Template created in vManage. The fields displayed on this page will vary depending on the device specific Feature Template.

Attention **The names of the fields displayed are based on the default names of the vManage Feature Template**.

The following table is an example of single WAN termination:

Field	Description
Virtual Router 1 and **Virtual Router 2**	
vpn-vedge-interface	
Interface Name(vpn_if_name_DualWanTermination_ge0/2.X) field	The name of the Interface.
IPv4 Address(vpn_if_ipv4_address) field	The IPv4 address can either be static or set to receive the IP address from a DHCP server.
Group ID(vpn_if_vrrp_grpid) field	The virtual router ID, which is a numeric identifier of the virtual router.
Priority(vpn_if_vrrp_priority) field	The priority level of the router. The router with the highest priority is elected as master.
IP Address(vpn_if_vrrp_vrrp_ipaddress) field	The IP address of the virtual router.
Interface Name(vpn_if_name_Tunnel_Interface_TLOC_Extn) field	The name of the interface.
IPv4 Address(vpn_if_ipv4_address) field	The IPv4 address can either be static or set to receive the IP address from a DHCP server.
TLOC Extension(vpn_if_tloc_extension) field	The name of the physical interface which is on the same router that connects to the WAN transport.
IPv4 Address(vpn_if_ipv4_address) field	The IPv4 address for the TLOC.
Color(vpn_if_tunnel_color_value) field	The color selected for the TLOC.
vpn-vedge	
Address(vpn_next_hop_ip_address_0) field	The IP address of the next-hop router.
Address(vpn_next_hop_ip_address_0) field	
Address(vpn_next_hop_ip_address_1) field	
system-vedge	
Hostname(system_host_name)	Hostname of the vEdge router.
System IP(system_system_ip)	System IP address of the vEdge router.

Field	Description
Site ID(system_site_id)	The site ID.

Step 8 In the **Hypervisors Network Configuration** page, you can configure the SD-WAN port groups. The number of WANs listed on this page depend on the number of WANs selected in the *Virtual Router Deployment Configuration* policy in the vManage Connection page.

Field	Description
WAN 1 Port Group Name	Enter the name of the WAN port group.
VLAN ID	Enter the VLAN ID to be added to the port group.
WAN 2 Port Group Name	Enter the name of the WAN port group.
VLAN ID	Enter the VLAN ID to be added to the port group.
LAN Port Group Name	Enter the name of the LAN port group.

Step 9 In the **HyperFlex Cluster Profile**, you can use an existing HyperFlex Cluster Profile or create a new one for SD-WAN deployment.

- Click **Select Pre-Created** to use an existing HyperFlex Cluster Profile.
- To create a new HyperFlex Cluster profile, click **Create New**.

You also have the option to **Skip HyperFlex Edge Cluster Profile** creation for now and create it later before SD-WAN deployment.

Step 10 In the **HyperFlex Edge Cluster Configuration** page, if you are creating a new HyperFlex Edge Cluster Profile, enter the appropriate values. For detailed instructions on how to configure a HyperFlex Edge Cluster using Intersight, see the *Deploying HyperFlex Edge Clusters* chapter in the Cisco HyperFlex Systems Installation Guide for Cisco Intersight.

If you are using an existing HyperFlex Cluster Profile, review the HyperFlex Edge Cluster configuration details and click **Next**.

Step 11 On the **Nodes Assignment** page, you can assign nodes now or optionally, you can choose to assign the nodes later. To Assign nodes, click the **Assign nodes** check box and select the node you want to assign. Click **Next**.

Attention
- You can assign a minimum of 2 and a maximum of 4 nodes to a Cisco HyperFlex Edge cluster.
- Only nodes that are have Intersight Advantage license are displayed here.

Step 12 In the **Nodes Configuration** page, you can view the IP and Hostname settings that were automatically assigned. Optionally, you can change the following configurations manually:

Field	Description
Cluster Management IP Address	This IP address must belong to the management subnet.
MAC Prefix Address	Enter a single prefix which is within the prefix range specified in the Network Configuration policy.
Nodes	

Field	Description
Hostname	The hostname of the server.
Hypervisor IP	IP address for the Hypervisor Management network.
Storage Controller IP	IP address for the HyperFlex Management network.

Click **Next**.

Step 13 On the **Summary** page, you can view the following details:

- General—Name of the SD-WAN profile, organization SD-WAN belongs to, tags used.
- Targets—Name, Status, Model, and Serial number of the HyperFlex Edge nodes
- HyperFlex Cluster—HyperFlex cluster configuration and node configuration details, and Errors/Warnings if any. Organization the HyperFlex cluster belongs to, name of the HyperFlex cluster and tags used.
- SD-WAN—Policy configuration, virtual router configuration, and Hypervisors network configuration. Details like organization the SD-WAN belongs to, name of the SD-WAN profile, and tags used.

Step 14 Click **Validate** to validate the configuration and **Execute** to begin the deployment. Optionally, click **Validate**, and then **Close** to complete deployment later.

Results:

On the **Requests** page, you can view the progress of the various configuration tasks and do one of the following:

- **Edit**—You can edit the desired inputs in the HyperFlex SD-WAN deployment wizard.
- **Retry Execution from Failure**—You can retry the execution from the failure point.
- **Retry Execution**—You can retry the execution from the beginning.

When the deployment fails due to incorrect data, you can reenter the input data in the HyperFlex SD-WAN deployment wizard. You may choose to retry the execution from the failure point or rerun the execution from the beginning.

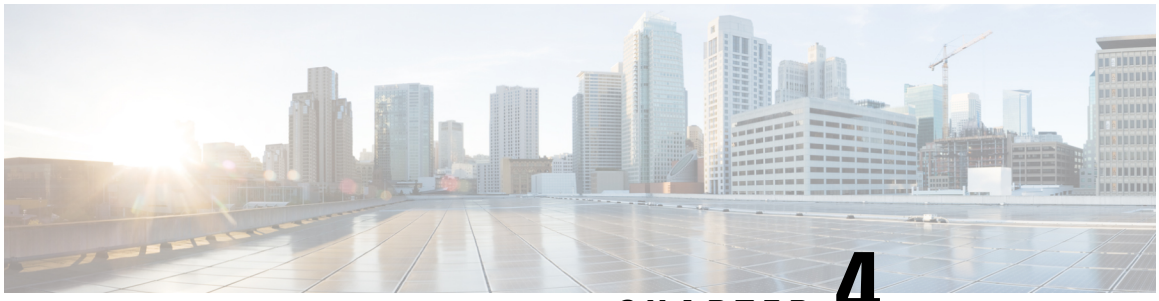
Only the following input changes will take effect when you **Retry Execution from Failure**:

- HyperFlex Cluster Profile:
  - DNS, NTP, and Timezone Policy—When the installation fails due to incorrect DNS, you must correct the DNS manually in all ESXi hosts, in addition to changing it in Intersight.
  - Security Policy
  - vCenter Policy
- SD-WAN Profile:
  - UUID and Template

Note When you edit the Template you will see one of the following changes in the Template inputs, depending on the state of the deployment:

- If the solution is not submitted yet, changing the template will change the Template values in the HyperFlex SD-WAN deployment wizard based on the values from the new template.
- If the solution is already executed and failed after deployment of vEdge Routers, editing the template requires a clean-up and reexecute the HyperFlex SD-WAN deployment.

When you **Retry Execution**, all other inputs like HyperFlex Network Configuration, Storage Network, and IP & Hostname policies, and vEdge Router settings will take effect.



CHAPTER 4

Post Installation

Post Installation

To verify if the TLOC and VRRP configuration is set on the HyperFlex Cluster, do one of the following in vManage:

- Single WAN Termination Deployment—Verify if the Transport Location (TLOC) and Virtual Router Redundancy Protocol (VRRP) is set correctly.
- Dual WAN Termination Deployment—Verify if the VRRP is set correctly.

Single WAN Termination Deployment

To view the TLOC configuration details, do the following:

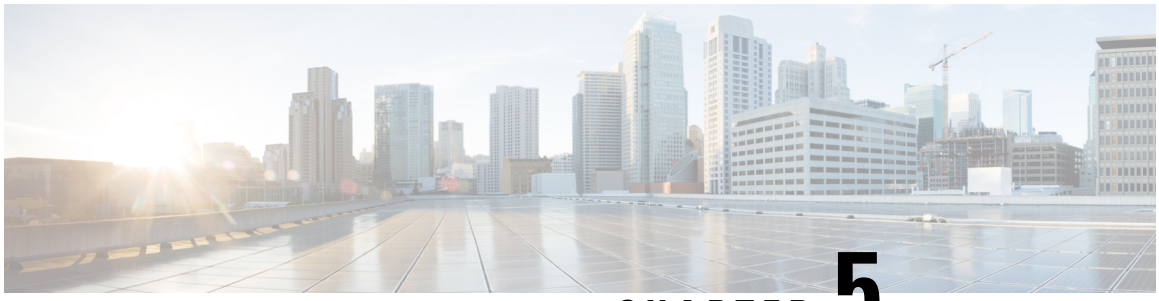
1. Log in to vManage in your web browser.
2. Navigate to **Monitor** > **Network**.
3. Under **WAN-Edge**, select the vEdge Router.
4. Navigate to **WAN** > **TLOC**.

Dual WAN Termination Deployment

To view the VRRP configuration details, do the following:

1. Log in to vManage in your web browser.
2. Navigate to **Monitor** > **Network**.
3. Under **WAN-Edge**, select the vEdge Router.
4. Select **Real Time**.
5. From the command drop-down located in the right pane, select **VRRP Information**.

   Verify the **Priority**, **State**, and **OMP State** details.



CHAPTER 5

Upgrade

Upgrade ESXi Hypervisor

Upgrade Guidelines

Before you upgrade the ESXi Hypervisor on a HyperFlex cluster with vEdge Router deployed on it, consider the following requirements and guidelines:

- Ensure that at the least one node with an vEdge router is always up and available.
- vSphere standard and above license is required to perform vMotion on vEdge routers.
- All nodes in the HyperFlex cluster must be in a maintenance mode.
- If deployment was made on Single WAN termination, ensure that Transport Locator (TLOC) and Virtual Router Redundancy Protocol (VRRP) are available and configured.

Attention VRRP must be configured.

- If deployment was made on Dual WAN termination, ensure that VRRP is available and configured.

Upgrade Prerequisites

Before you upgrade the ESXi Hypervisor on a HyperFlex cluster with SD-WAN deployed on it, consider the following prerequisites:

- Migrate the vEdge router to a different VMware ESXi node.

Upgrade Procedure

To upgrade the ESXi Hypervisor on a HyperFlex cluster with SD-WAN deployed on it, do the following:

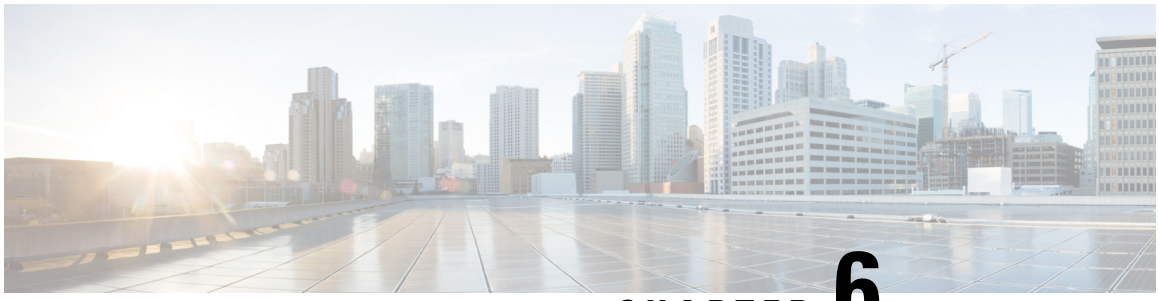
1. Log in to VMware vSphere Web Client, navigate to the HyperFlex cluster.
2. Migrate the vEdge router to a different VMware ESXi node:

Right-click on the vEdge Router, and select **Migrate** and select **Change both host and datastore**. Click **Next**.

3. On the **Configure** tab, expand **Networking** > **Virtual Switches**, and select **Standard Switch:vmotion**.
4. Click **Add Networking**.
5. In the **Add Networking** wizard, do the following:
   a. In **Select Connection Type**, select **VMkernel Network Adapter**.
   b. In **Select Target Device**, click **Select an existing standard switch**.
   c. In **Port Properties**, specify the VMkernel port settings.

Attention Use the same VLAN ID that you entered in the Hypervisors Network Configuration page from the Deploy HyperFlex SD-WAN Wizard.

6. Upgrade the ESXi Hypervisor. For more details, see the *VMware ESXi Upgrade* section in *VMware vSphere Documentation*.



CHAPTER 6

Troubleshooting

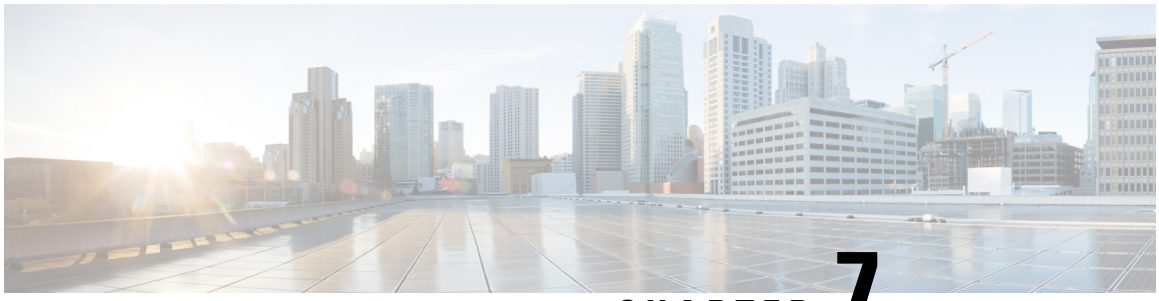
Troubleshooting

vEdge Deployment Failures

In case of vEdge deployment failures, verify the following:

- Chassis ID provided is available in vManage and ensure it is not assigned to any other device.
- The values in the *Virtual Router Device Specific Configuration* page are accurate including the following information:
  - There must be no duplicate entry for the System-IP, site-id, or Host name which is already there in the vManage inventory.
  - Verify if the vBond IP is configured correctly, and verify that the vBond Controller is added to vManage.
  - To establish overlay path, vpn-0 configuration is important. Check if all configuration is complete in vpn-0.
  - Verify if the CA certificates pushed from vManage to vEdge are correct.
  - Verify if all the Certificates are in Valid state in vManage and sent to vBond Controllers.
  - The Device Status of the vBond controller must be In-Sync with the status in vManage.
  - Ensure that the WAN port group is created with the correct WAN VLAN.

Troubleshooting



CHAPTER 7

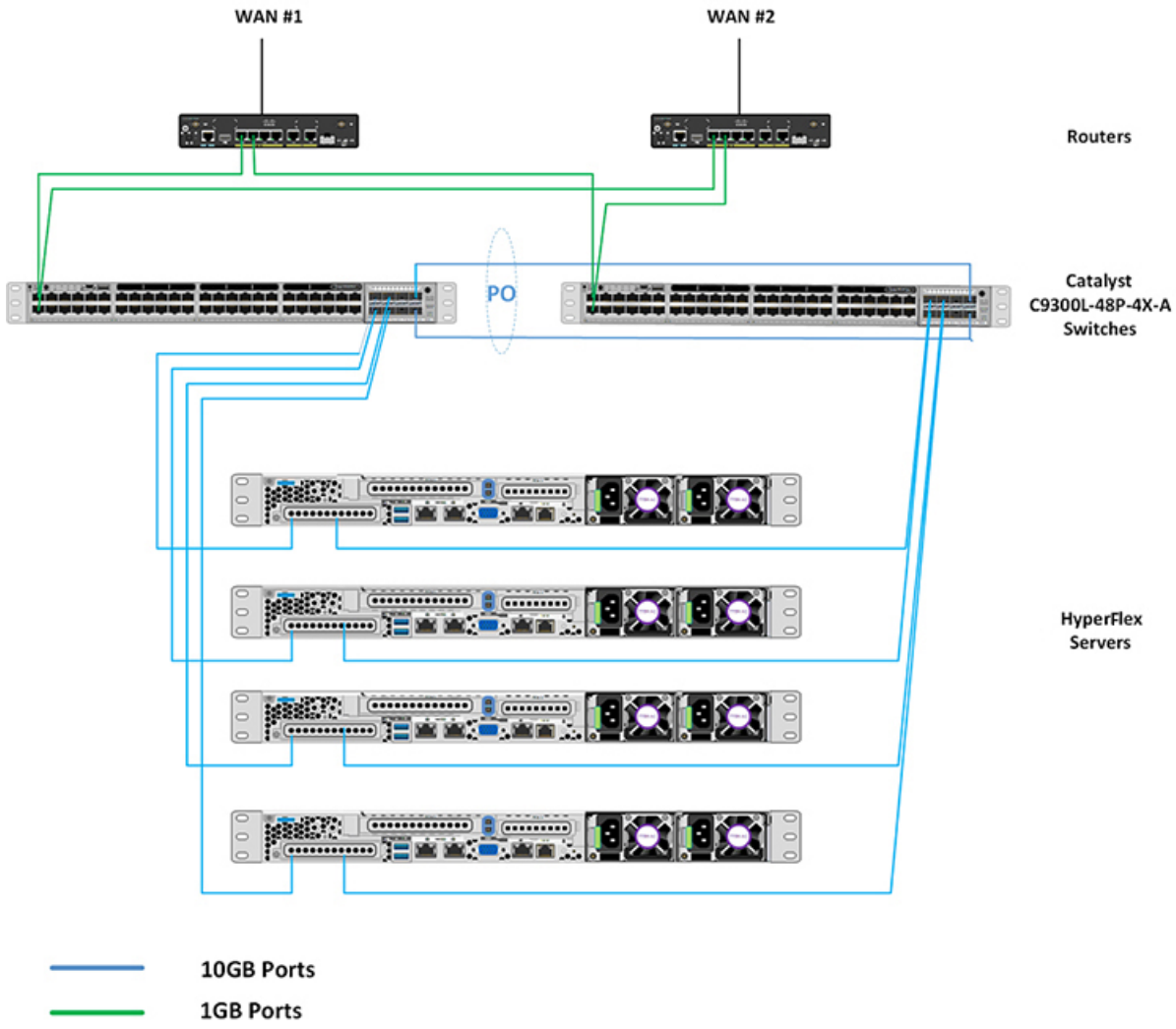
Appendix

Configuring the Cisco Catalyst C9300L-48P-4X-A Switches

This section provides a detailed procedure for configuring the Cisco Catalyst C9300L-48P-4X-A for use in a HyperFlex SD-WAN environment. Follow these steps precisely because failure to do so could result in an improper configuration. The deployment of the switches is in standalone mode.

Network Switch Configuration

No switch stacking is used in this configuration. The 10GbE connections on the server are connected to port 1 (to switch A) and port 3 (to switch B) of the Cisco VIC 1457 mLOM on each server.



Physical Connectivity

HyperFlex SD-WAN Catalyst Cabling

The following tables provide the details of all the physical connections used by HyperFlex and the networking requirements for the SD-WAN solution.

Cisco Catalyst C9300L-48P-4X-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Catalyst 9300-A	TenGig1/1/1	10 GbE	UCSM5-Edge-Node1	VIC1
Cisco Catalyst 9300-A	TenGig1/1/2	10 GbE	UCSM5-Edge-Node2	VIC1
Cisco Catalyst 9300-A	TenGig1/1/3	10 GbE	UCSM5-Edge-Node3	VIC1

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Catalyst 9300-A	TenGig1/1/4	10 GbE	UCSM5-Edge-Node4	VIC1
Cross Link 1	TenGig1/1/7	10 GbE	Cisco Catalyst 9300-B	TenGig 1/1/7
Cross Link 2	TenGig1/1/8	10 GbE	Cisco Catalyst 9300-B	TenGig 1/1/8
ISP #1 Link 1	GigEth1/0/1	1 GbE	Physical Router A	N/A
ISP #2 Link 1	GigEth1/0/2	1 GbE	Physical Router B	N/A
	MGMT0	SVI	Management IP	SVI

Cisco Catalyst C9300L-48P-4X-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Catalyst 9300-B	TenGig1/1/1	10 GbE	UCSM5-Edge-Node1	VIC2
Cisco Catalyst 9300-B	TenGig1/1/2	10 GbE	UCSM5-Edge-Node2	VIC2
Cisco Catalyst 9300-B	TenGig1/1/3	10 GbE	UCSM5-Edge-Node3	VIC2
Cisco Catalyst 9300-B	TenGig1/1/4	10 GbE	UCSM5-Edge-Node4	VIC2
Cross Link 1	TenGig1/1/7	10 GbE	Cisco Catalyst 9300-A	TenGig 1/1/7
Cross Link 2	TenGig1/1/8	10 GbE	Cisco Catalyst 9300-A	TenGig 1/1/8
ISP #1 Link 2	GigEth1/0/1	1 GbE	Physical Router A	N/A
ISP #2 Link 2	GigEth1/0/2	1 GbE	Physical Router B	N/A
	MGMT0	SVI	Management IP	SVI

HyperFlex SD-WAN Necessary VLANs

The following table shows an example of how to define the VLAN IDs. You can define the VLAN IDs depending on your network requirements.

VLAN Name	VLAN Purpose	Example ID
Intranet-MGMT	Management traffic among CIMC In-Band IP address, ESXi management IP address, HyperFlex management IP address. CIMC VLAN (Can be same or different from the Management VLAN).	100
HyperFlex Storage	VLAN to serve storage traffic, requires only L2 connectivity.	31
HyperFlex vMotion	VLAN for vMotion VLAN, if applicable.	32
VM-Network	VLAN/VLANs for VM/application network.	33
WAN #1	VLAN for ISP1	11
WAN #2	VLAN for ISP2	12

Initial Setup For Cisco Catalyst C9300L-48P-4X-A Switches

The following sections provide an initial setup procedure for Cisco Catalyst C9300L-48P-4X-A/B Switches.

Attention This procedure assumes the use of a pair of Cisco Catalyst C9300L-48P-4X-A switches running vEdge version 17.1 or higher.

To set up the initial configuration for the Cisco Catalyst C9300L-48P-4X-A switches, complete the following steps on both switch A and Switch B:

Cisco Catalyst 9300L Switch A/B Initial Configuration

```
show running-config
!
hostname Selvan-Cat9k-A
!
!
vrf definition HX-MGMT
!
!
ip routing
!
ip name-server vrf HX-MGMT 8.8.8.8
ip domain name cat9k
!
!
system mtu 9000
license boot level network-advantage addon dna-advantage
!
interface Port-channel1
description " cross-link-to-SDWAN-A/B-switch"
switchport trunk allowed vlan 11-12,31,100,200
switchport mode trunk
!
```

```
interface GigabitEthernet0/0
description “Mgmt interface for switch”
vrf forwarding Mgmt-vrf
ip address 10.193.232.83 255.255.255.0
negotiation auto
!
interface GigabitEthernet1/0/1
description “ISP #1 Link 1/2”
switchport access vlan 11
switchport mode access
!
interface GigabitEthernet1/0/2
description “ISP #2 Link 1/2”
switchport access vlan 12
switchport mode access
!
interface GigabitEthernet1/0/7
description “Member of port channel 1”
switchport trunk allowed vlan 11-12,31,100,200
switchport mode trunk
mtu 9000
channel-group 1 mode active
!
interface GigabitEthernet1/0/8
description “Member of port channel 1”
switchport trunk allowed vlan 11-12,31,100,200
switchport mode trunk
mtu 9000
channel-group 1 mode active
!
interface TenGigabitEthernet1/1/1
description “CIMC port for node-1”
switchport trunk allowed vlan 11,12 ,31,100,200
switchport mode trunk
mtu 9000
!
interface TenGigabitEthernet1/1/2
description “CIMC port for node-2”
switchport trunk allowed vlan 11,12,31,100,200
switchport mode trunk
mtu 9000
!
interface Vlan11
description VLAN for WAN1
vrf forwarding HX-MGMT
ip address 192.168.11.252 255.255.255.0
ip nat outside
!
interface Vlan12
description VLAN for WAN2
vrf forwarding HX-MGMT
ip address 192.168.12.252 255.255.255.0
ip nat outside
!
interface Vlan100
description "Default GW for DC & Cimc"
vrf forwarding HX-MGMT
ip address 192.168.100.252 255.255.255.0
ip nat inside
standby version 2
standby 10 ip 192.168.100.254
standby 10 priority 110
standby 10 preempt
!
```

```
interface Vlan200
description vlan for vedge
vrf forwarding HX-MGMT
ip address 192.168.200.252 255.255.255.0
standby version 2
standby 10 ip 192.168.200.254
standby 10 priority 110
standby 10 preempt
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip nat pool nat-232 10.193.232.111 10.193.232.114 netmask 255.255.255.0
ip nat inside source route-map ViaVlan11 interface Vlan11 vrf HX-MGMT overload
ip nat inside source route-map ViaVlan12 interface Vlan12 vrf HX-MGMT overload
ip nat inside source list 1 pool nat-232
ip route vrf HX-MGMT 0.0.0.0 0.0.0.0 192.168.11.254
ip route vrf HX-MGMT 192.168.61.0 255.255.255.0 192.168.200.1

!
ip access-list standard 1
20 permit 192.168.100.0 0.0.0.255
!
route-map ViaVlan12 permit 10
match ip address 1
match interface Vlan12
!
route-map ViaVlan11 permit 10
match ip address 1
match interface Vlan11
!
```

Attention **Post-deployment remove *ip route vrf HX-MGMT 0.0.0.00.0.0.0192.168.11.254* and *ip route vrf HX-MGMT 192.168.61.0255.255.255.0192.168.200.1*. Replace it with *ip route vrf HX-MGMT 0.0.0.00.0.0.0192.168.200.1*.**