

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

# Cross-Domain Integration

Troubleshooting Cisco SD-Access - SD-WAN Integration

Mariusz Kaźmierski  
Principal Engineer, EMEAR CX Centers  
BRKTRS-3457

CISCO *Live!*

#CiscoLive

# Cisco Webex App

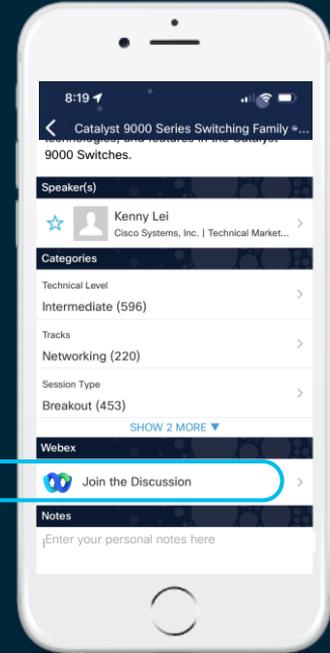
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://cicolive.ciscoevents.com/cicolivebot/#BRKTRS-3457>



# Agenda

- 1) SD-Access / SD-WAN: Basics
- 2) Cross-Domain: Supported Designs
- 3) SD-Access / SD-WAN: Integration Principles

# 1. SD-Access / SD-WAN

## Basics



# ■ SD-Access (SDA) - basics

Software



## Cisco DNA Center

Orchestrator responsible for intent-based automation and assurance in Campus Network.

## Cisco Identity Services Engine (ISE)

Engine that provides a dynamic end-point to SGT group mapping and policy definition.

# SD-Access (SDA) - basics

Software



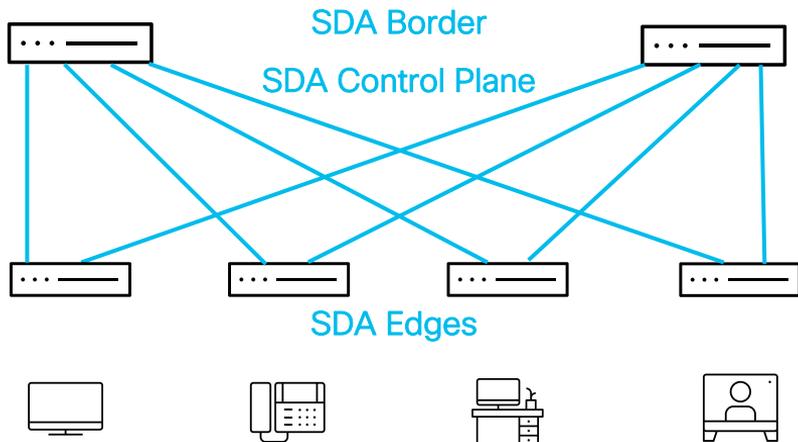
## Cisco DNA Center

Orchestrator responsible for intent-based automation and assurance in Campus Network.

## Cisco Identity Services Engine (ISE)

Engine that provides a dynamic end-point to SGT group mapping and policy definition.

SDA Fabric  
VXLAN / LISP



## SDA Border

Fabric device that connects SDA Fabric with the external network.

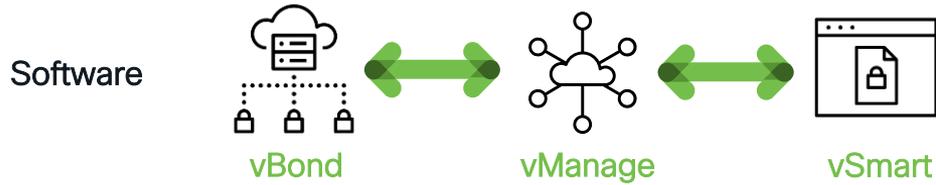
## SDA Control Plane

Fabric device that governs control-plane operations in the fabric.

## SDA Edge

Fabric device to which end-points are connected to.

# SD-WAN - basics



## vManage

**management-plane** and single pane of glass for day0, day1 and day2 operations in SD-WAN.

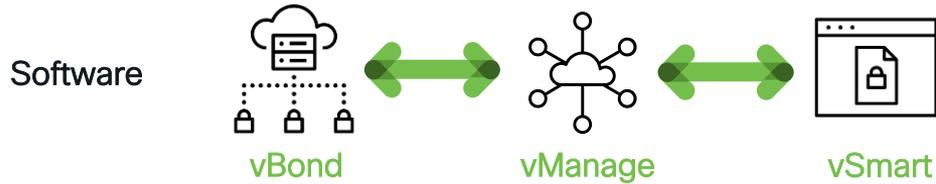
## vBond

**orchestration-plane** responsible for on-boarding (Zero Touch Provisioning) new devices into SD-WAN fabric.

## vSmart

**control-plane** responsible for applying and enforcing configured policies in SD-WAN fabric.

# SD-WAN - basics



## vManage

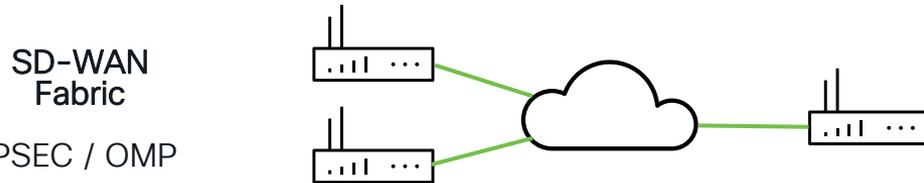
**management-plane** and single pane of glass for day0, day1 and day2 operations in SD-WAN.

## vBond

**orchestration-plane** responsible for on-boarding (Zero Touch Provisioning) new devices into SD-WAN fabric.

## vSmart

**control-plane** responsible for applying and enforcing configured policies in SD-WAN fabric.



## cEdge

**data plane** device that forwards packets based on decisions received from the control plane (vSmarts).

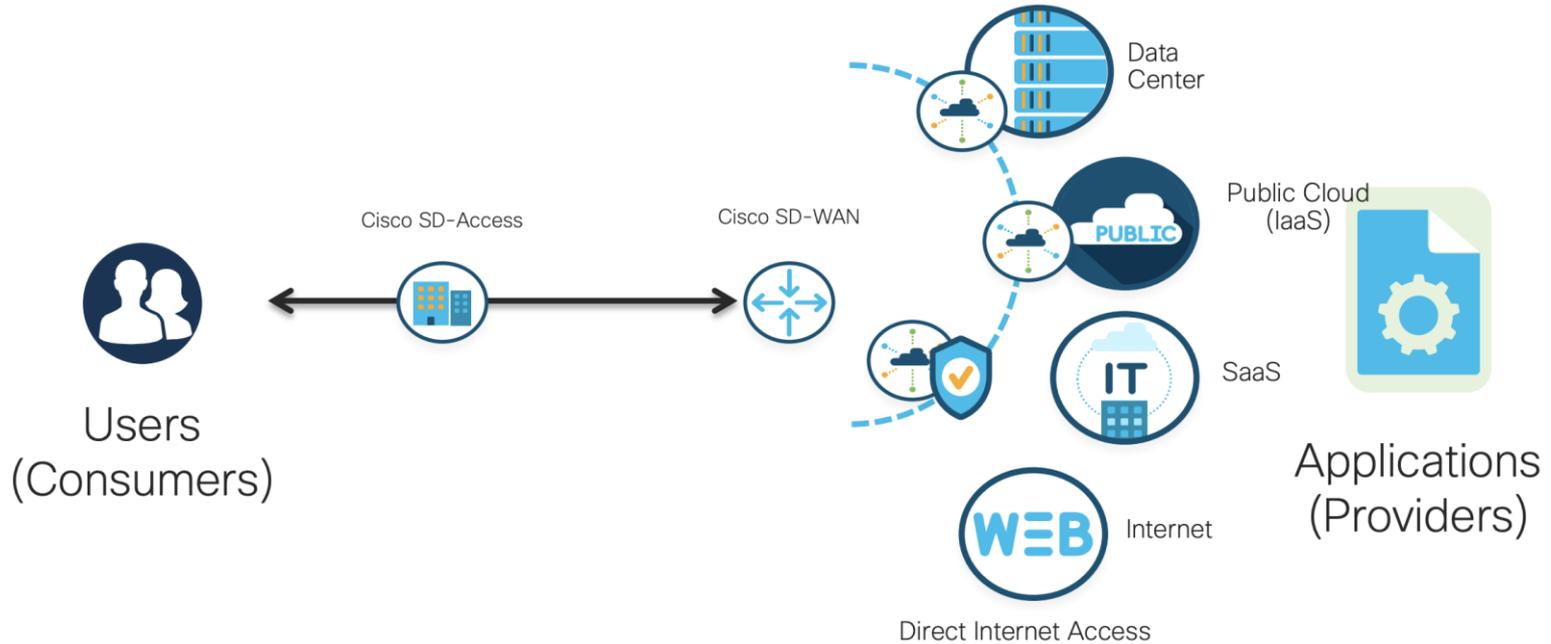
# SD-Access – SD-WAN: Comparison

Function	SD-Access	SD-WAN
Management	Cisco DNA Center	vBond – UI vManage – NMS
Control Plane	LISP	vSmart (OMP)
Data Plane Underlay	Based on RLOC	Based in TLOC
Data Plane Overlay	VXLAN	IPSec

# 2. Cross-Domain Supported Designs



# Integration Goals – WHY?



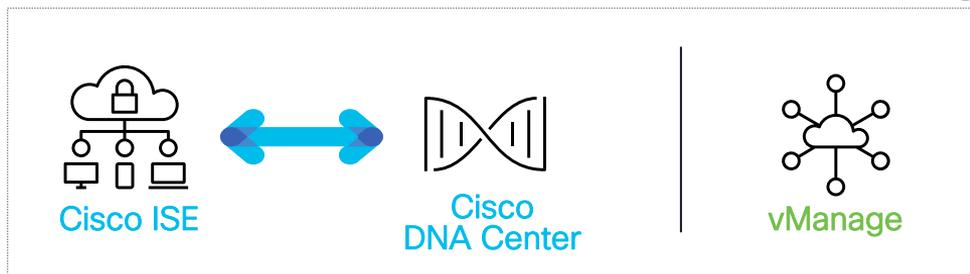
# Integration Goals – WHY?

- 1) **Ensure** micro- and macro-segmentation across the whole enterprise.
- 2) **Use** consistent end-to-end group-based policies.
- 3) **Leverage** intelligent routing between different branch offices.
- 4) **Automate** new site deployments.
- 5) **Monitor** network via single pane of glass.

- SDA
- SD-WAN
- manual TrustSec (VRF-lite)

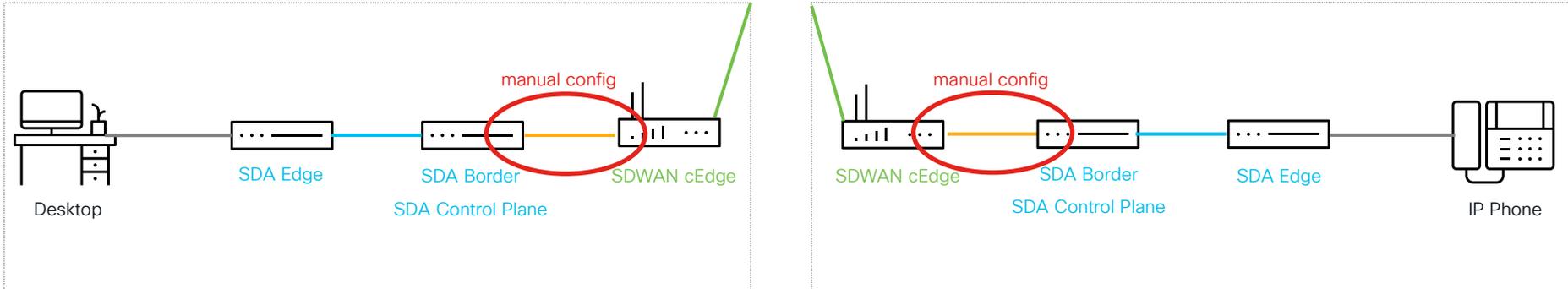
# SDA - SD-WAN: Independent Domain

HQ

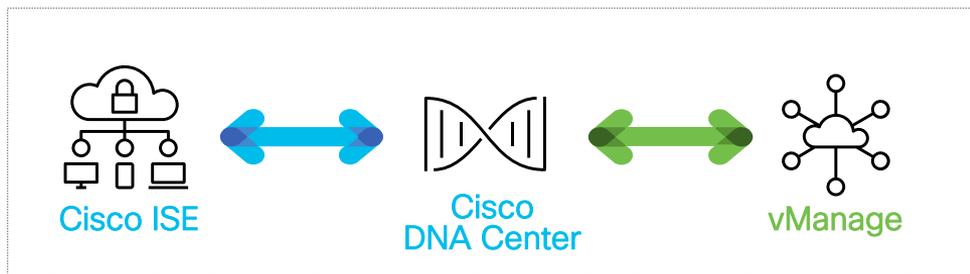


Branch 1

Branch 2

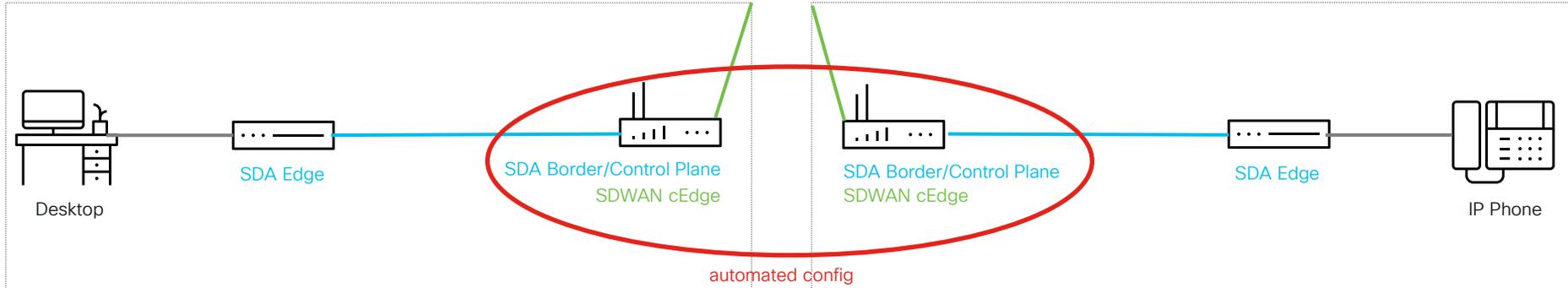


# SDA - SD-WAN: Integrated Domain



Branch 1

Branch 2



# Compatibility Matrix

make sure that compatible software is used!

## SD-Access Compatibility Matrix for Cisco DNA Center 2.2.2.8

Device Role	Device Series	Device Model	Recommended Release	Supported Release
Collocated SD-Access Border, Control Plane and SD-WAN WAN Edge	Cisco 4000 Series Integrated Services Routers	ISR4331 ISR4351 ISR4451 ISR4461 ISR4431	IOS XE 17.3.4	IOS XE 17.3.4
	Cisco ASR 1000 Series Aggregation Services Routers	ASR1001-X ASR1001-HX ASR1002-X ASR1002-HX	IOS XE 17.3.4	IOS XE 17.3.4
	Cisco Catalyst 8300 Series Edge Platforms	C8300-1N1S-4T2X C8300-1N1S-6T C8300-2N2S-4T2X C8300-2N2S-6T	IOS XE 17.3.4	IOS XE 17.3.4
SD-WAN Controller	SD-WAN Controller Software	vManage vSmart vBond	20.4.2.2	20.4.2.2

## SDA-SDWAN Compatibility Matrix

# 3. SDA - SD-WAN Integration Principles



# SD Access – SD-WAN: integration principles

## Orchestrator Layer

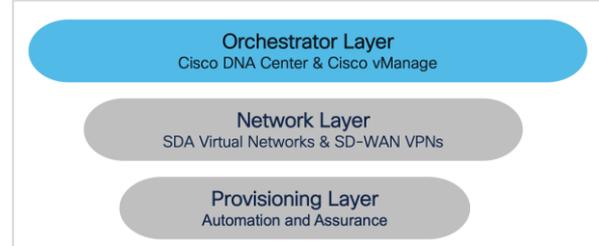
Cisco DNA Center & Cisco vManage

## Network Layer

SDA Virtual Networks & SD-WAN VPNs

## Provisioning Layer

Automation and Assurance



# SDA / SD-WAN Integration

Orchestrator Layer: Cisco DNA Center & Cisco vManage



# Integrate Cisco DNA Center with Cisco vManage

- Integration workflow is initiated from Cisco DNA Center.
- Cisco DNA Center has a ‘superior’ role over Cisco vManage:
  - Cisco DNA Center sends (HTTPS APIs) requests to push SDA-related configuration to cEdges.
  - Cisco DNA Center syncs regularly with vManage (new VPNs, attached devices, etc.).
  - Cisco vManage does not query / initiate communication with Cisco DNA Center!
- SD-WAN devices (cEdges) are going to be known and co-managed by both orchestrators:
  - **vManage** for SD-WAN configuration,
  - **Cisco DNA Center** for SD-Access configuration (configuration push via vManage).

# Cisco DNA Center - System 360: initial state

The screenshot displays the Cisco DNA Center interface for System 360. The top navigation bar includes the Cisco DNA Center logo, a search icon, a help icon, a refresh icon, and a notification bell. The main content area is divided into two primary sections: System Management and Externally Connected Systems.

**System Management**

- Software Updates** (As of Apr 20, 2022 10:22 PM):
  - Connected to Cisco's software server.
  - System Package is up to date.
- Backups** (As of Apr 20, 2022 10:22 PM):
  - No backups server configured. [Configure](#)
- Application Health** (As of Apr 20, 2022 10:22 PM):
  - Automation
  - Assurance

**Externally Connected Systems**

- Identity Services Engine (ISE)** (As of Apr 19, 2022 10:22 PM):

Primary	100.64.0.102 <a href="#">↗</a>	Available <span>✔</span>
Pxgrid	100.64.0.102 <a href="#">↗</a>	Available <span>✔</span>

[Update](#)
- IP Address Manager (IPAM)** (As of Apr 20, 2022 10:22 PM):
  - No IPAM server configured. [Configure](#)
- vManage** (As of Apr 19, 2022 10:22 PM):
  - No vManage server configured. [Configure](#)

A blue callout box with white text is positioned over the vManage section, stating: "vManage integration needs to be explicitly configured".

# Cisco DNA Center – SD-WAN Integration

Settings / External Services

## vManage

Use this form to configure the vManage server and credentials. These settings enable communication with the vManage server to manage SD-WAN devices from Cisco DNA Center.

A certificate is required if vManage is authenticated via a root CA. This certificate is installed in vEdge during the onboarding process in NFVIS provisioning.  
Note: Only Privacy-Enhanced Mail (PEM) standard files can be uploaded to Cisco DNA Center.

Host Name/IP Address*	100.67.0.1	The hostname or IP address of vManage
Username*	admin	The user ID of vManage
Password*	.....	The password of vManage
Port Number*	8443	The vManage port number

Certificate is not trusted for this IP. [Click here to add in trustpool.](#)

vManage needs to be reachable through provided IP / port and accessible via provided credentials (net-admin)

Cisco DNA Center must import vManage certificate for successful HTTPS API communication

# Cisco DNA Center – System 360: final state

The screenshot displays the Cisco DNA Center interface for System 360. The top navigation bar includes the Cisco DNA Center logo, the system name 'System 360', and utility icons for search, refresh, status, and notifications. The main content area is divided into two primary sections: 'System Management' and 'Externally Connected Systems'.

**System Management** (As of Apr 20, 2022 10:47 PM):

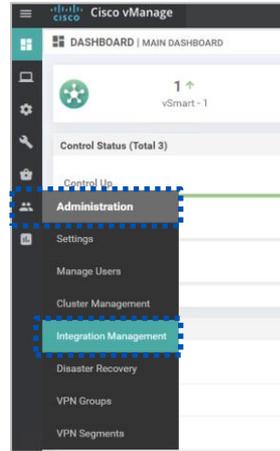
- Software Updates:** Two green status indicators: 'Connected to Cisco's software server.' and 'System Package is up to date.'
- Backups:** One orange status indicator: 'No backups server configured.' with a 'Configure' link.
- Application Health:** Two green status indicators: 'Automation' and 'Assurance'.

**Externally Connected Systems** (As of Apr 19, 2022 10:47 PM):

- Identity Services Engine (ISE):** Two entries, both with green status indicators: 'Primary' (100.64.0.102) and 'Pxgrid' (100.64.0.102), both marked 'Available'. An 'Update' link is at the bottom.
- IP Address Manager (IPAM):** One orange status indicator: 'No IPAM server configured.' with a 'Configure' link.
- vManage:** Two entries, both with green status indicators: 'Server URL' (100.67.0.1) and 'Username' (admin), both marked 'Available'. An 'Update' link is at the bottom. A blue dashed box highlights the vManage configuration area, and a blue callout box above it states 'vManage integration enabled and available'.

# Cisco vManage - Integration status

To check the status, go to:  
Administration →  
Integration Management



# Troubleshooting integration issues

## Cisco DNA Center: Audit Logs

The screenshot shows the Cisco DNA Center interface for Audit Logs. At the top, there's a navigation bar with 'Cisco DNA Center' and 'Activities - Audit Logs'. Below that, there are tabs for 'Audit Logs', 'Tasks', and 'Work Items'. A filter icon is on the left, and a date range 'By Date: Apr 20, 2021 11:30 pm - Apr 20, 2022 11:30 pm' is on the right, along with 'Subscribe' and 'Refresh' buttons. A timeline at the top shows dates from 5/1 to 4/1. The main content area is titled 'Today' and shows 11 of 11 events. The selected event is 'Apr 20, 2022 14:57:18.632 (CEST) BAD\_USER\_CREDENTIAL\_EVENT: Authentication has failed for user "admin". Please provide valid credentials...'. A detailed view of this event is shown on the right, with fields for Description, User, Interface, Destination, and Source. A search bar at the bottom of the detailed view shows '0 out of 0' results.

**Today** 11 of 11

- Apr 20, 2022 22:47:42.747 (CEST) Sent notification for SDWAN transit.
- Apr 20, 2022 22:47:41.894 (CEST) Successfully saved vManagement properties.
- Apr 20, 2022 22:47:41.099 (CEST) The request to add vManagement credentials was received.
- Apr 20, 2022 22:47:36.113 (CEST) Request received to upload a trustpool certificate to Trust Anchor
- Apr 20, 2022 22:47:23.348 (CEST) Unable to add/update vManagement properties.
- Apr 20, 2022 22:47:22.639 (CEST) The request to add vManagement credentials was received.
- Apr 20, 2022 22:22:05.354 (CEST) LOGIN\_USER\_EVENT: 'admin' logged in successfully.
- Apr 20, 2022 14:57:21.744 (CEST) LOGIN\_USER\_EVENT: 'admin' logged in successfully.
- Apr 20, 2022 14:57:18.632 (CEST) BAD\_USER\_CREDENTIAL\_EVENT: Authentication has failed for user "admin". Please provide valid...

**Apr 20, 2022 14:57:18.632 (CEST) Log Id**

Description	BAD_USER_CREDENTIAL_EVENT: Authentication has failed for user "admin". Please provide valid credentials		
User	system	Interface	SYSTEM
Destination	SYSTEM	Source	10.61.98.140

0 out of 0

Use Cisco DNA Center Audit Logs to better track potential integration issues

TROUBLESHOOTING TIP

# Troubleshooting integration issues

## Cisco DNA Center: Log Explorer

The screenshot displays the Cisco DNA Center interface for 'System 360'. The breadcrumb path is 'System > System 360'. The main content area is titled 'System 360' and includes an 'Actions' dropdown menu. Below this, there is a 'Cluster' section with three panels:

- Hosts (1)**: As of Apr 20, 2022 11:00 PM. Shows a single host '100.64.0.101' with a 'View 137 Services' link.
- High Availability**: As of Apr 20, 2022 11:00 PM. Contains a warning: 'Enabling High Availability requires installing a minimum of 3 Cisco DNA Center hosts.' with a 'View Guide' link.
- Cluster Tools**: As of Apr 20, 2022 10:47 PM. Lists 'Monitoring', 'Log Explorer', and 'Workflow', each with an external link icon. The 'Log Explorer' item is highlighted with a dashed blue box.

Use Cisco DNA Center Log Explorer to further explore possible integration issues

TROUBLESHOOTING TIP

# Troubleshooting integration issues

## Cisco DNA Center: Log Explorer

The screenshot displays the Cisco DNA Center Log Explorer interface. A search filter is applied to 'kubernetes.container\_name:nfv-provisioning-service'. The log message is from 'logstash-\*' and shows an error: 'I/O error on GET request for "https://100.67.0.1:8443/dataservice/client/token": PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target; nested exception is javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target'. The log is from the 'nfv-provisioning-service' container in the 'fusion' namespace.

Filter messages to see logs only from a specific container: `nfv-provisioning-service`

Narrow down logs to specific time range

Look for any error or warning message

```
kubernetes.container_name: nfv-provisioning-service log: Wrapped by: org.springframework.web.client.ResourceAccessException: I/O error on GET request for "https://100.67.0.1:8443/dataservice/client/token": PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target; nested exception is javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target stream: stdout
docker.container_id: 7570b02fee383c7155101d9a4600d7359876331f7688c3d73280a66c67a911e0 kubernetes.namespace_name: fusion kubernetes.pod_name: nfv-provisioning-
```

# Troubleshooting integration issues

## vManage: Audit Logs

The screenshot shows the Cisco vManage interface with the 'MONITOR | AUDIT LOG' section active. A search filter 'partner' is applied to the log entries. A blue callout box points to the search filter with the text: 'Use filtering option to see only logs from specific module (partner)'. The log table shows a single entry with the following details:

Timestamp	User	User IP	Message	Module	Feature	Device	Task ID
20 Apr 2022 12:47:19 PM CEST	admin	100.64.0.101	Registered a new dnac partner DNAC_622a31b308d2e35e...	partner	partner-configuration	-	-

Additional UI elements include a 'Filter' dropdown, a 'Search Options' dropdown, and a 'Total Rows: 1 of 7' indicator.

Look for activities initiated from Cisco DNA Center IP address

# SD-WAN: Attach cEdges into Integration

Showing list of third-party controllers registered on vManage. Associate Sites for each controller from the 'Actions' menu icon in the table.

Controller Name	Description	Partner Id	Platform	Updated By	Date Registered	Devices	
DNAC_622a31b308d2e35ec0479aaa	DNAC deployment for 622a31b308d2e35ec04...	622a31b308d2e35ec0479aaa	dnac	admin	20 Apr 2022	0	...

Attach Devices  
Detach Devices

Select „Attach Devices”  
from sub-menu

Attach device from the list below

Available Devices

Name	Device IP
CSR1K-MAIN	100.67.0.10

Selected Devices (2 Items Selected)

Name	Device IP
ISR-BRANCH-01	172.26.0.1
ISR-BRANCH-02	172.27.0.1

Attach Cancel

Select all cEdges that will be part  
of SDA - SD-WAN integration

# Cisco DNA Center & vManage: Audit Logs

Audit log added in vManage

Timestamp	User	User ID	Message	Module	Feature	Device	Task ID
20 Apr 2022 2:05:23 PM CEST	admin	100.65.0.1	Updated device mapping for dnac partner 738e178f-a20...	partner	partner-configuration	-	--

Audit logs added in Cisco DNA Center

Activities - Audit Logs

Filter

By Date: Apr 21, 2021 12:30 am - Apr 21, 2022 12:30 am | Subscribe Refresh

Today 2 of 2

- Apr 21, 2022 00:05:47.731 (CEST) Adding a device with id: null, deviceIp: null, serialNumber: null
- Apr 21, 2022 00:05:47.701 (CEST) Adding a device with id: null, deviceIp: null, serialNumber: null

# Cisco DNA Center: Inventory

The screenshot shows the Cisco DNA Center interface. The breadcrumb navigation is "Provision · Network Devices · Inventory". The left sidebar shows a hierarchy: Global > Krakow > Site-01 and Site-02. The main content area shows a table of 2 devices. A blue callout box at the top right of the table states: "After devices are automatically added to Cisco DNA Center they need to be manually assigned to a specific site/building". A dashed blue box highlights the "Reachability" and "Manageability" columns for both devices. The table data is as follows:

Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site
ISR-BRANCH-01	172.26.0.1	Unsupported Cisco Device	Unreachable	Managed Device Connec...	N/A	NA	.../Krakow/Site-01
ISR-BRANCH-02	172.27.0.1	Unsupported Cisco Device	Unreachable	Managed Device Connec...	N/A	NA	.../Krakow/Site-02

It is perfectly fine to have a device in the **Unreachable** state (as underlay might still not be provisioned from SDA perspective & there is no Loopback0 configured). The device **MUST** be in 'Managed' state

TROUBLESHOOTING TIP

# Orchestrator Layer:

## Cisco DNA Center & Cisco vManage: Summary

At the end of this stage the status will be as follows:

- Cisco DNA Center is fully integrated with Cisco vManage:

vManage		
As of Apr 19, 2022 10:47 PM		
Server URL	100.67.0.1 <a href="#">↗</a>	Available
Username	admin	

- cEdges devices from Cisco vManage are added into Cisco DNA Center inventory.

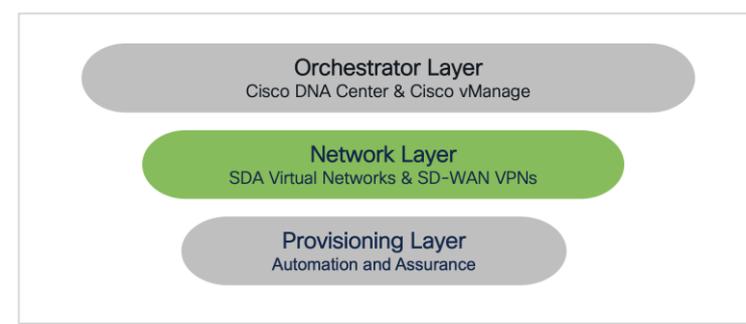
The screenshot shows the Cisco DNA Center interface for the 'Inventory' section. The breadcrumb path is 'Global > Krakow'. The page title is 'Provision · Network Devices · Inventory'. The left sidebar shows a hierarchy with 'Global' and 'Krakow' (containing 'Site-01' and 'Site-02'). The main content area shows a table of devices. Two devices are listed: 'ISR-BRANCH-01' and 'ISR-BRANCH-02'. Both are marked as 'Unreachable' with a red circle icon. The 'Manageability' column shows a yellow triangle icon and the text 'Managed Device Conne...'. The 'Compliance' column shows 'N/A' and the 'Health Score' column shows 'NA'. The 'Site' column shows '.../Krakow/Site-01' and '.../Krakow/Site-02'.

Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site
ISR-BRANCH-01	172.26.0.1	Unsupported Cisco Device	Unreachable	Managed Device Conne...	N/A	NA	.../Krakow/Site-01
ISR-BRANCH-02	172.27.0.1	Unsupported Cisco Device	Unreachable	Managed Device Conne...	N/A	NA	.../Krakow/Site-02



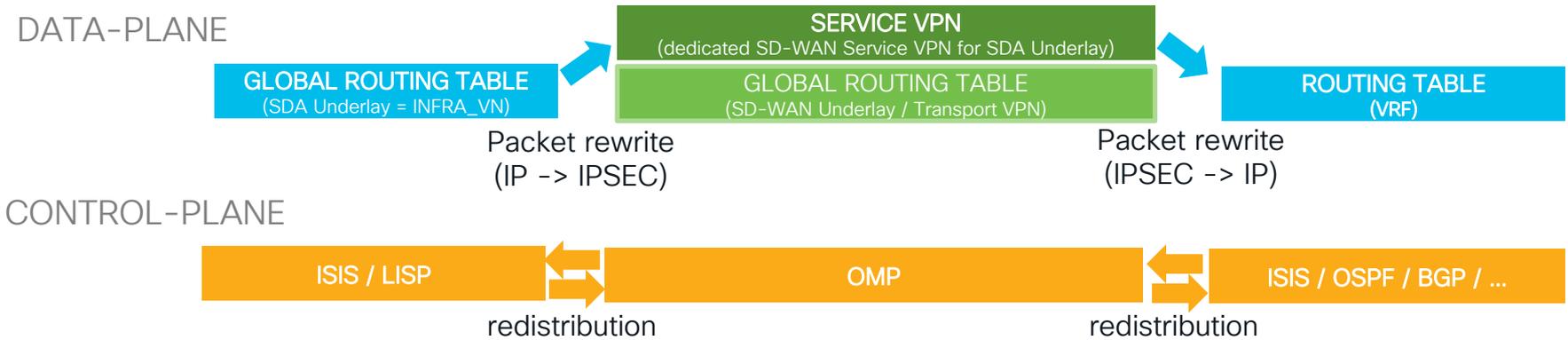
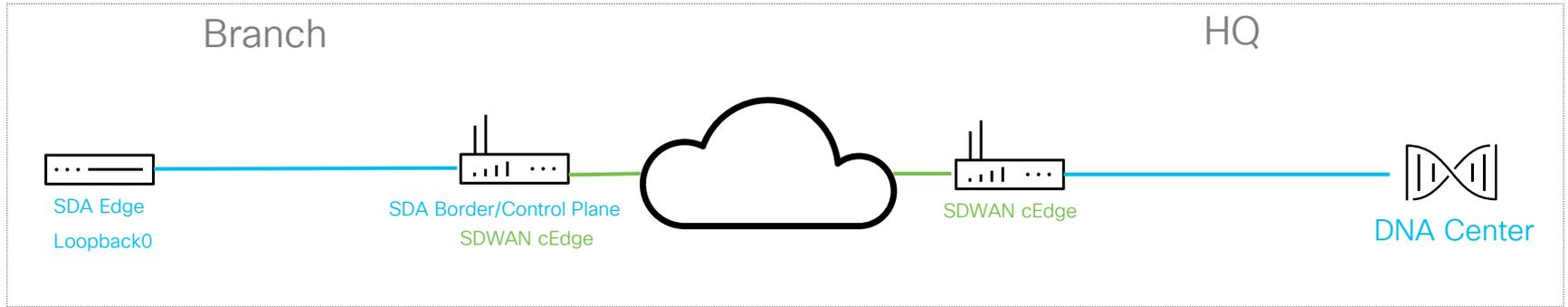
# SDA / SD-WAN Integration

Network Layer: SDA Virtual Networks & SD-WAN VPNs



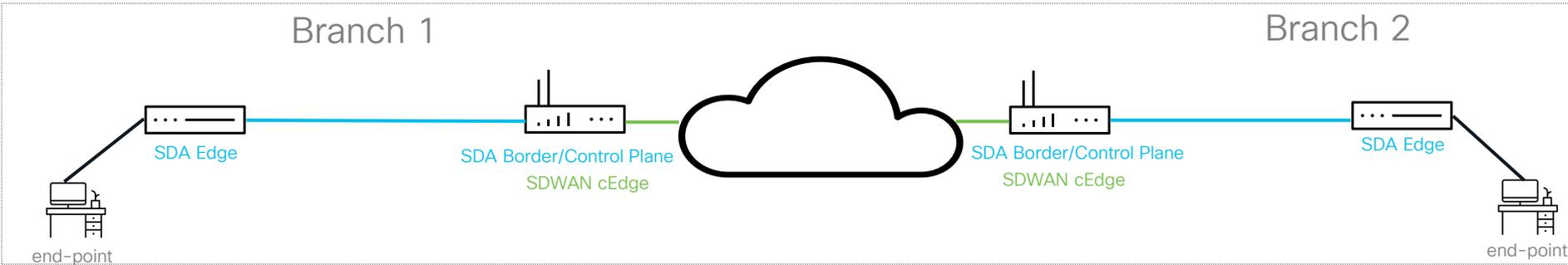
# Integrate SDA Virtual Networks with SD-WAN VPNs

## SDA Underlay: end to end connectivity

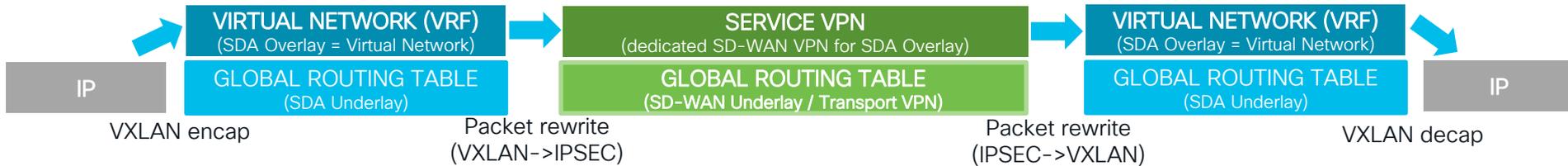


# Integrate SDA Virtual Networks with SD-WAN VPNs

## SDA Overlay: end to end connectivity & security



### DATA-PLANE



### CONTROL-PLANE

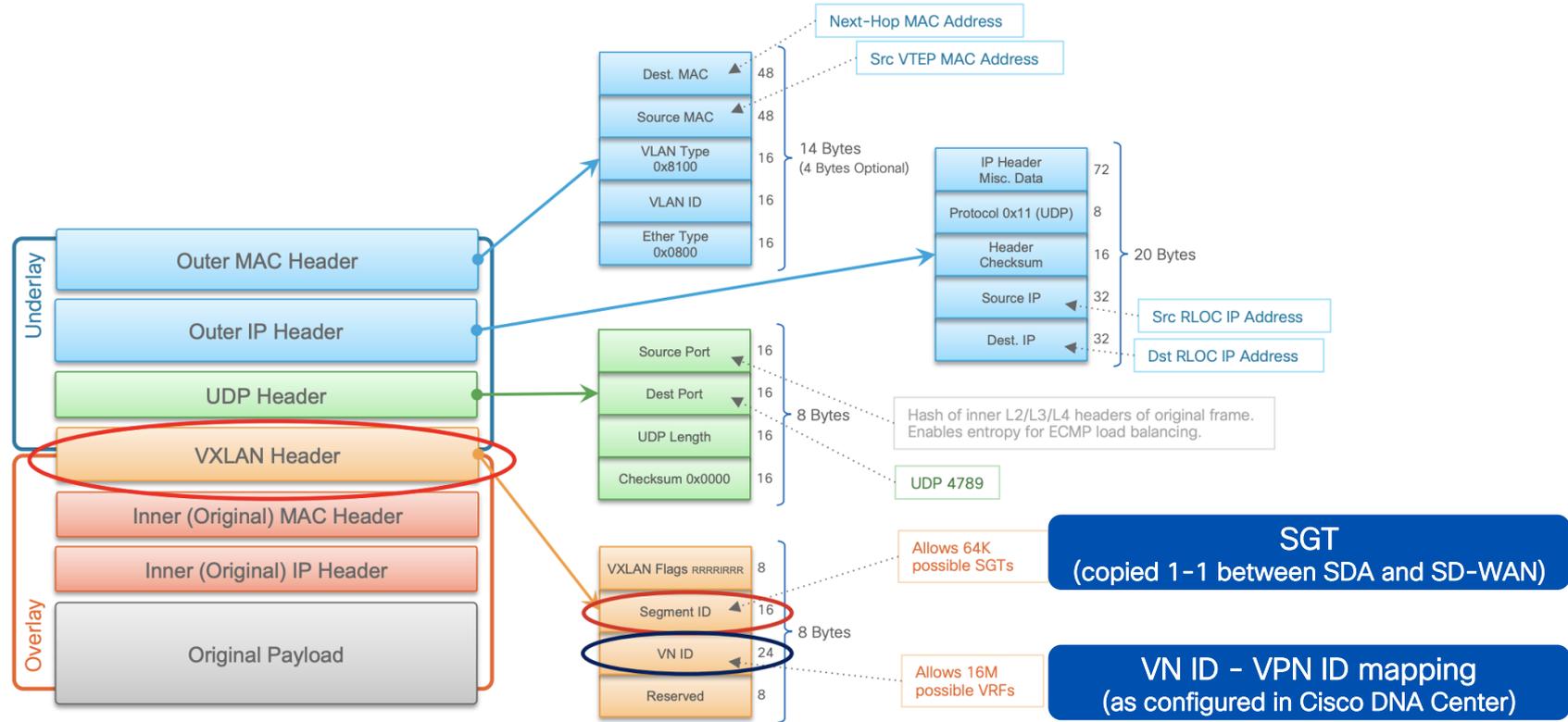


### SECURITY-PLANE



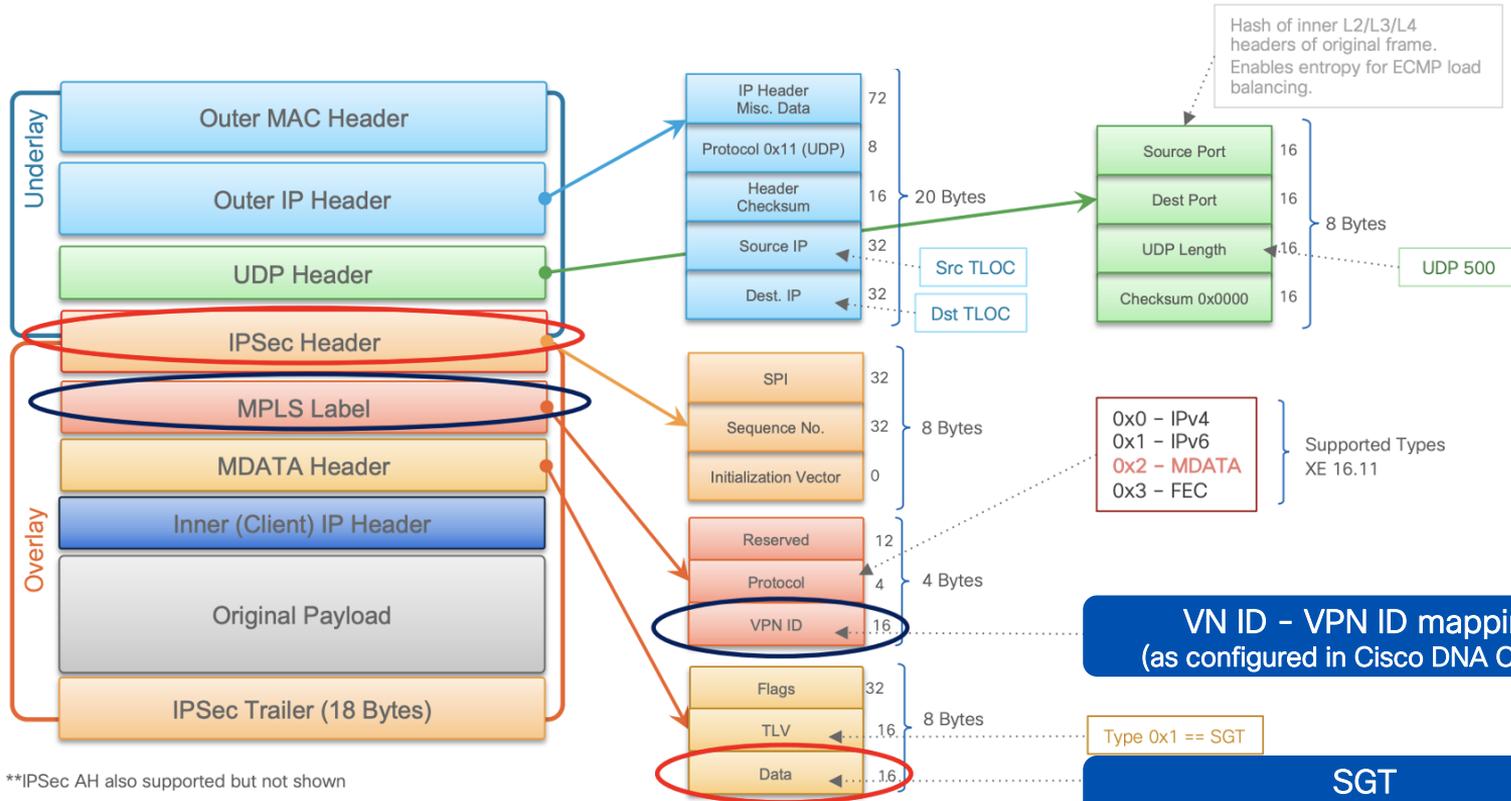
# SDA Virtual Networks with SD-WAN VPNs

## SDA (VXLAN) Encapsulation



# SDA Virtual Networks with SD-WAN VPNs

## SDWAN (IPSec) Encapsulation



\*\*IPSec AH also supported but not shown

# vManage: Service VPN mapping

Device Feature **Create VPNs that will be mapped to SDA Underlay & SDA Overlay VNs.**

+ Add Template

Template Type Non-Default  Search Options

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By
VPN_SDA_UNDERLAY	VPN definition for SD-Access un...	Cisco VPN	CSR1000v   ISR4431	3	3	admin
VPN_SDA_OVERLAY_DEVICE_VN	VPN definition for SD-Access ov...	Cisco VPN	CSR1000v   ISR4431	3	3	dnacadmin
VPN_SDA_OVERLAY_USER_VN	VPN definition for SD-Access ov...	Cisco VPN	CSR1000v   ISR4431	3	3	dnacadmin

Generally, there is no need to add physical / logical interfaces to Service VPNs as they will be created automatically by Cisco DNA Center during:

- LAN Automation (for SDA underlay)
- Provisioning (for SDA overlay)

Associating Service VPN to the WAN Edge devices ensures these VPNs are shared with Cisco DNA Center

# vManage - Service VPNs

SD-WAN VPN100 = SDA Underlay (Global Routing Table)

Cisco vManage

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN > VPN\_SDA\_UNDERLAY

Device Type: CSR1000v,ISR4431

Template Name: VPN\_SDA\_UNDERLAY

Description: VPN definition for SD-Access underlay

Basic Configuration | DNS | Advertise OMP | IPv4 Route | IPv6 Route

BASIC CONFIGURATION

VPN: 100

Name: VPN underlay for SDA

Enhance ECMP Keying: On Off

Create Service VPN that will be associated to SDA Underlay

Assign VPN ID that will be associated to SDA Underlay in Cisco DNA Center

# vManage – Service VPNs

SD-WAN VPN10 = SDA Overlay (VN: DEVICE\_VN)

Device Type: CSR1000v,ISR4431

Template Name: VPN\_SDA\_OVERLAY\_DEVICE\_VN

Description: VPN definition for SD-Access overlay (DEVICE\_VN)

VPN ID: 10

Name: VPN overlay for SDA (DEVICE\_VN)

Enhance ECMP Keying: On

Create Service VPN that will be associated to SDA Overlay.

Assign VPN ID that will be associated to SDA Overlay (specific VN) in Cisco DNA Center

# vManage – Service VPNs

SD-WAN VPN20 = SDA Overlay (VN: USER\_VN)

Device Type: CSR1000v,ISR4431

Template Name: VPN\_SDA\_OVERLAY\_USER\_VN

Description: VPN definition for SD-Access overlay (USER\_VN)

Basic Configuration | DNS | Advertise OMP | IPv4 Route | IPv6 Route

**BASIC CONFIGURATION**

VPN: 20

Name: VPN overlay for SDA (USER\_VN)

Enhance ECMP Keying:  On  Off

Create Service VPN that will be associated to SDA Overlay

Assign VPN ID that will be associated to SDA Overlay (specific VN) in Cisco DNA Center

# vManage - Service VPNs

Advertise OMP

IPv4

BGP (IPv4)	<input type="checkbox"/>	<input type="radio"/> On	<input checked="" type="radio"/> Off
Static (IPv4)	<input type="checkbox"/>	<input type="radio"/> On	<input checked="" type="radio"/> Off
Connected (IPv4)	<input type="checkbox"/>	<input checked="" type="radio"/> On	<input type="radio"/> Off
OSPF External	<input type="checkbox"/>	<input type="radio"/> On	<input checked="" type="radio"/> Off
OSPFV3	<input type="checkbox"/>	<input type="radio"/> On	<input checked="" type="radio"/> Off
EIGRP	<input type="checkbox"/>	<input type="radio"/> On	<input checked="" type="radio"/> Off
LISP	<input type="checkbox"/>	<input checked="" type="radio"/> On	<input type="radio"/> Off
ISIS	<input type="checkbox"/>	<input checked="" type="radio"/> On	<input type="radio"/> Off

**Redistribute „BGP” to OMP**  
enable if IP Transit/shared services is used on site

**Redistribute „Connected” to OMP**  
mandatory for underlay VPN & overlay VPN

**Redistribute „LISP” to OMP**  
mandatory for underlay VPN (APs and ENs)  
& overlay VPNs

**Redistribute „ISIS” to OMP**  
mandatory for underlay VPN (LAN Automation)

# Cisco DNA Center

## SDA Virtual Networks & SD-WAN VPNs - mapping

☰ Cisco DNA Center

Policy · Virtual Network



Virtual Networks (4)

- Filter | Actions ▾
- DEFAULT\_VN
  - DEVICE\_VN
  - INFRA\_VN
  - USER\_VN

By associating Service VPN to the WAN Edge devices in vManage, you ensure that VPNs IDs are shared with Cisco DNA Center

vManage VPN

Guest VN

Edit Virtual Network

Name  
INFRA\_VN

vManage VPN  
100

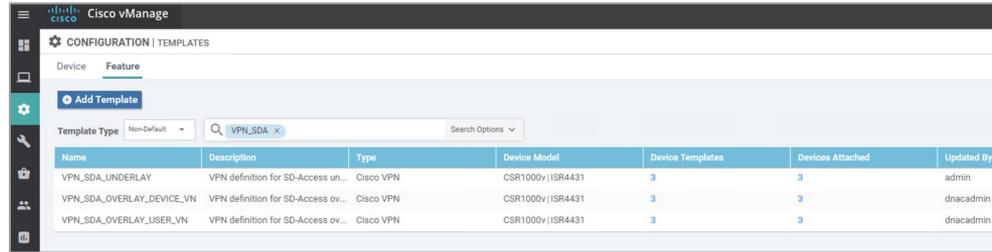
Add a mapping between:  
SDA Virtual Network (VN)  
and SD-WAN VPN ID

# Network Layer:

## SDA Virtual Networks & SD-WAN VPNs: Summary

At the end of this stage the status will be as follows:

- Service VPNs are created in vManage that will correspond to SDA Underlay & SDA Overlay VNs.



The screenshot shows the Cisco vManage interface for configuring templates. The 'CONFIGURATION | TEMPLATES' page is active, with the 'Feature' tab selected. A search filter 'VPN\_SDA' is applied. The table below lists the configured templates.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By
VPN_SDA_UNDERLAY	VPN definition for SD-Access un...	Cisco VPN	CSR1000v ISR4431	3	3	admin
VPN_SDA_OVERLAY_DEVICE_VN	VPN definition for SD-Access ov...	Cisco VPN	CSR1000v ISR4431	3	3	dnacadmin
VPN_SDA_OVERLAY_USER_VN	VPN definition for SD-Access ov...	Cisco VPN	CSR1000v ISR4431	3	3	dnacadmin

- Proper redistribution rules are added between SDA Control Plane protocols used in SDA Underlay and SDA Overlay and SD-WAN OMP.
- “VN-ID to VPN-ID” mappings are configured in Cisco DNA Center:



The screenshot shows the Cisco DNA Center interface for configuring virtual networks. The 'Policy - Virtual Network' page is active, showing a table of virtual networks.

Name	vManage VPN	Guest VN	Scalable Group(s)
DEFAULT_VN			18
DEVICE_VN	10		3
INFRA_VN	100		Add
USER_VN	20		2



# SDA / SD-WAN Integration

## Provisioning Layer: Automation and Assurance

Orchestrator Layer  
Cisco DNA Center & Cisco vManage

Network Layer  
SDA Virtual Networks & SD-WAN VPNs

Provisioning Layer  
Automation and Assurance



# LAN Automation - concept

- LAN Automation is the Plug-n-Play (PnP) **zero-touch provisioning** of the **underlay network** in the SD-Access solution,
- As part of LAN Automation, Cisco DNA Center will configure (through vManage) cEdges as Seed Devices to discover and configure other SD-Access devices,
- LAN Automation will provision IS-IS routing protocol to provide end-to-end routed underlay connectivity in SDA fabric.

# LAN Automation - diagram

## Step 1: Configuration of Seed Device (configuration - part 1)



Configuration push

### SEED DEVICE (cEdge)

```
vrf forwarding 100
no ip address
service instance 1 ethernet
 encapsulation untagged
 bridge-domain 1
exit
```

```
interface Loopback0
no shutdown
clns mtu 1400
vrf forwarding 100
ip address 172.26.100.65 255.255.255.255
ip router isis 100
exit
```



cEdge  
=  
Seed Device



LAN-automated  
device  
=  
SDA Edge

### SEED DEVICE (cEdge)

```
router isis 100
vrf 100
metric-style wide
redistribute omp
default-information originate
bfd all-interfaces
domain-password "Cisco!123"
log-adjacency-changes
net 49.0000.1720.2610.0065.00
nsf ietf
```

### Actions:

- 1) Configure Service VPN that corresponds to SDA Underlay.
- 2) Configure Loopback0 in SDA Underlay Service VPN (/32 address assigned from provided IP Pool)
- 3) Configure ISIS routing protocol in SDA Underlay Service VPN.

# LAN Automation - diagram

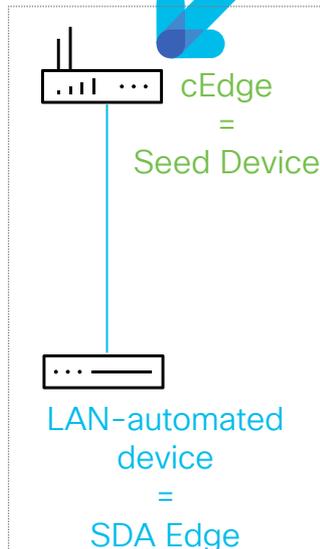
## Step 1: Configuration of Seed Device (configuration - part 2)



Configuration push

### SEED DEVICE (cEdge)

```
interface GigabitEthernet0/0/2
vrf forwarding 100
no ip address
negotiation auto
service instance 1 ethernet
 encapsulation untagged
 bridge-domain 1
```



### SEED DEVICE (eEdge)

```
interface BDI1
no shutdown
clns mtu 1400
bfd interval 500 min_rx 500 multiplier 3
vrf forwarding 100
ip address 172.26.100.1 255.255.255.192
ip router isis 100
exit
```

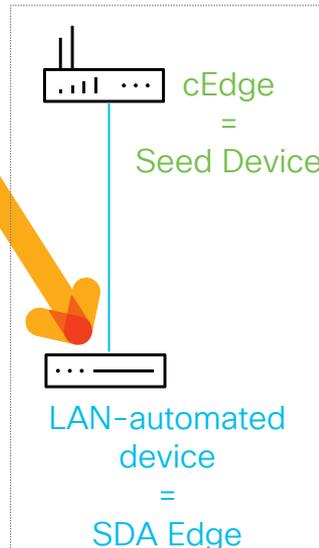
```
ip dhcp excluded-address 172.26.100.1
ip dhcp pool nw_orchestration_pool
 option 43 ascii
 "5A1D;B2;K4;I100.64.0.101;J80;"
 vrf 100
 default-router 172.26.100.1
 network 172.26.100.0 255.255.255.192
exit
```

### Actions:

- 4) Configure BDI interface for IP communication between Seed Device and LAN-automated device.
- 5) Configure DHCP Pool with Option43 pointing to Cisco DNA Center (PnP Server).
- 6) Configure interface towards LAN-automated device.

# LAN Automation – diagram

## Step 2: PnP process



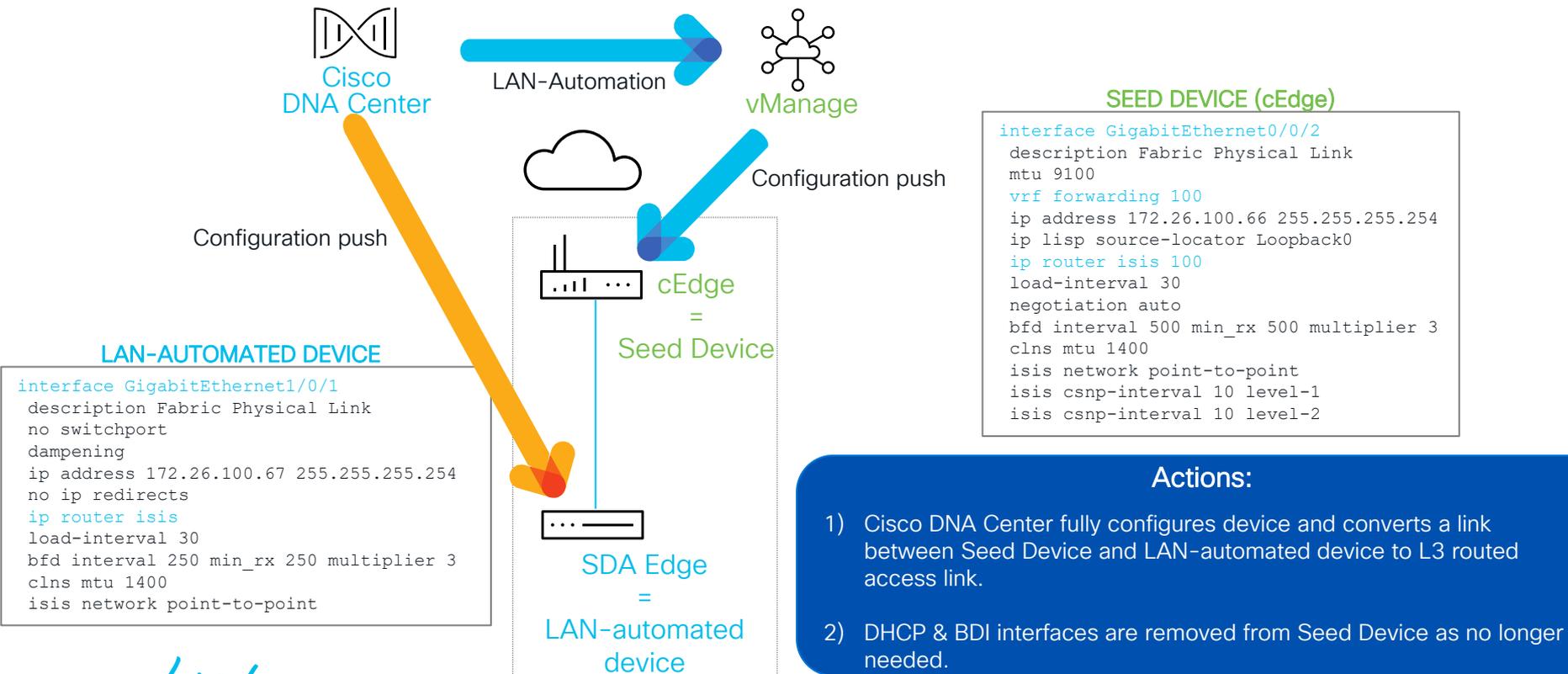
### Actions:

- 1) LAN-automated device receives IP address from DHCP and start communication with PnP Server (Cisco DNA Center)
- 2) Cisco DNA Center fully configures device.

IP REACHABILITY (UNDERLAY)  
(redistribution: connected/IS-IS → OMP)

# LAN Automation – diagram

## Step 3: LAN Automation – routed access



# Cisco DNA Center: LAN Automation

The screenshot displays the Cisco DNA Center interface for managing network devices. The breadcrumb navigation shows 'Provision · Network Devices · Inventory'. The left sidebar shows a hierarchy: 'Global' > 'Unassigned Devices' > 'Krakow' > 'Site-01' > 'Site-02'. The main content area shows a table of devices under the 'Provision' focus. The 'Inventory' action menu is open, highlighting 'LAN Automation'. A blue callout box at the bottom right contains the text: 'Start LAN Automation process on each site to on-board a new device connected to cEdge'.

Inventory

Plug and Play Inventory Insights

Global > Krakow

DEVICES (2)  
FOCUS: Provision

Filter | Add Device Tag Device Actions | Take a Tour | 1 Selected

Device Name	IP Address	Reachability	Provisioning Status
ISR-BRANCH-01	172.26.0.1	Unreachable	Not Provisioned
ISR-BRANCH-02	172.27.0.1		Not Provisioned

Inventory >  
Software Image >  
Provision >  
Telemetry >  
Device Replacement >  
Others >

Assign Device to Site  
Provision Device  
LAN Automation  
LAN Automation Status

Start LAN Automation process on each site to on-board a new device connected to cEdge

# Cisco DNA Center: LAN Automation

Provision · Network Devices · Inventory Preview New Page  🔍 ?

## LAN Automation

Devices will be auto-upgraded to the Golden Image tagged for the device(s). You can modify the Golden Image selection from [Image Repository](#).

Before starting LAN automation, see the [Cisco DNA Center SD-Access LAN Automation Deployment Guide](#)

Primary Site\*  
Global/Krakow/Site-01

Primary Device\*  
ISR-BRANCH-01

Peer Site

Peer Device

SELECTED PORTS OF PRIMARY DEVICE (1)\* [Modify Selections](#)

Gigabi... ernet0/0/2 x

Clear All

Discovered Device Configuration

Discovered Device Site\*  
Global/Krakow/Site-01

Main IP Pool\*  
SITE01-LAN-AUTO

Use traditional LAN Automation workflow to fully provision Underlay on cEdges (including Loopback0 interface)

Select interfaces to which LAN Automated devices will be connected to.

Assign IP Pool dedicated for given site (created in Design tab in Cisco DNA Center)

# Cisco DNA Center: LAN Automation

LAN Automation Status ✕

Last updated Apr 22, 2022 9:11 PM [Refresh](#)

Summary **Devices** Logs

Q Search Table ⌵

Message

Starting Seed Device Configuration phase.

Reserved IP Address 172.26.100.65 for interface Loopback0 on device FCZ2401M056 role PrimarySeedDevice.	Apr 23, 2022 09:08 PM
Reserved Subnet 172.26.100.0/26 for interface BDI1 on device FCZ2401M056.	Apr 23, 2022 09:08 PM
Added hostname mapping FOC2340X0DV for CAT9K-BRANCH-01.	
Started the Network Orchestration Session with primary device: ISR-BRANCH-01.	
Starting LAN Automation by user: admin.	

Cisco DNA Center allocates a new IP address and create Loopback0 in previously associated Service VPN

Cisco DNA Center creates a BDI interface on cEdge for LAN Automation purposes (next hop for on-boarded devices)

TROUBLESHOOTING TIP



# vManage - Configuration Push

The screenshot shows the Cisco vManage interface with the 'MONITOR | AUDIT LOG' section. A search filter '172.26.0.1' is applied to the 'Device' column. The table below shows the resulting audit log entries.

Timestamp	User	User IP	Message	Module	Feature	Device	Task ID
19 Mar 2022 7:28:20 PM CET	admin	100.64.0.101	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_template_configuration-d7c...
19 Mar 2022 7:27:32 PM CET	admin	100.64.0.101	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_template_configuration-884...
19 Mar 2022 7:26:05 PM CET	admin	100.64.0.101	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_template_configuration-388...
19 Mar 2022 7:25:21 PM CET	admin	100.64.0.101	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_template_configuration-c3d...
19 Mar 2022 7:03:15 PM CET	admin	100.64.0.101	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_template_configuration-0fab...
19 Mar 2022 7:02:17 PM CET	admin	100.64.0.101	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_template_configuration-9f99...
19 Mar 2022 6:04:28 PM CET	admin	100.65.0.1	Template SITE01-ISR successfully attached to device 172.26.0...	template	template-device...	172.26.0.1	push_feature_template_configurat...

Filter by specific cEdge device

Look at User IP (should match IP Address of Cisco DNA Center)

Select "CLI Diff" to see what has been pushed to cEdge

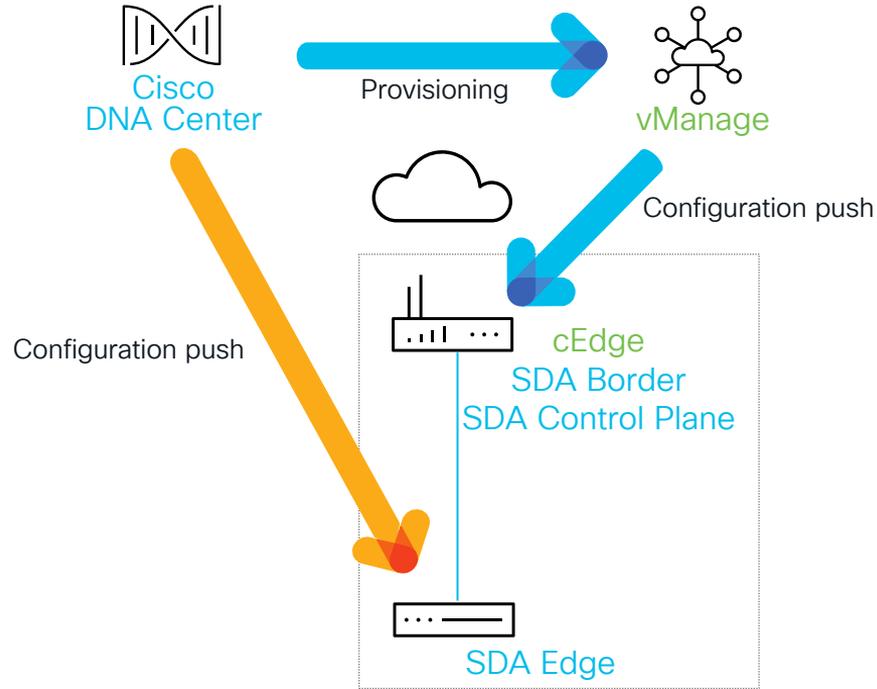
TROUBLESHOOTING TIP

# vManage - Configuration Push

The screenshot shows the Cisco vManage interface with a 'Config Diff' window open. The window displays a comparison of configuration lines between two states. The right-hand column shows the updated configuration, where the 'interface BDI' section is highlighted in green. A blue callout box with white text is overlaid on the right side of the diff window, stating: 'Interface BDI pushed as part of LAN Automation workflow'. The background shows the vManage 'MONITOR | AUDIT LOG' page with a search filter for '172.26.0.1' and a list of audit log entries.

Line	Left Column	Right Column
192	no ip dhcp use class	no ip dhcp use class
193	ip name-server 100.65.0.2	ip name-server 100.65.0.2
194	ip route 0.0.0.0 0.0.0.0 172.26.5.250	ip route 0.0.0.0 0.0.0.0 172.26.5.250
195	ip bootp server	ip bootp server
196	no ip source-route	no ip source-route
197	no ip http server	no ip http server
198	no ip http secure-server	no ip http secure-server
199	no ip http ctc authentication	no ip http ctc authentication
200	no ip igmp ssm-map query dns	no ip igmp ssm-map query dns
201	ip nat settings central-policy	ip nat settings central-policy
202	interface GigabitEthernet0	interface BDI
203	shutdown	no shutdown
204	arp timeout 1200	cls mtu 1400
205	vrf forwarding Mgmt-intf	bfd interval 500 min_rx 500 multiplier 3
206	ip address dhcp client-id GigabitEthernet0	vrf forwarding 100
207	no ip redirects	ip address 172.26.100.1 255.255.255.192
		ip router isis 100
		exit
210	interface GigabitEthernet0	interface GigabitEthernet0
211	shutdown	shutdown
212	arp timeout 1200	arp timeout 1200
213	vrf forwarding Mgmt-intf	vrf forwarding Mgmt-intf
214	ip address dhcp client-id GigabitEthernet0	ip address dhcp client-id GigabitEthernet0
215	no ip redirects	no ip redirects

# Configuration Push – provisioning workflows



TROUBLESHOOTING TIP

# Telemetry - assurance workflows

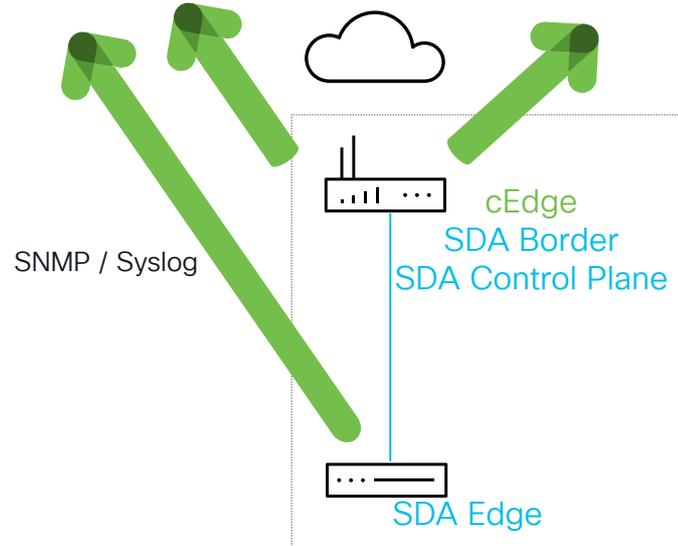
## SITE-LEVEL VISIBILITY:

- Network level Issues and Events
- Network health
- Device 360



## DEVICE-LEVEL VISIBILITY:

- SD-WAN Edge device health
- WAN transport health
- Application statistics



TROUBLESHOOTING TIP

# Provisioning Layer

## Automation and Assurance: summary

At the end of this stage the status will be as follows:

- All SDA devices added to Cisco DNA Center in reachable/state:

Global

DEVICES (4)  
FOCUS: Inventory

Filter | Add Device | Tag Device | Actions | Take a Tour

Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Site
ISR-BRANCH-01	172.26.100.65	Routers	Reachable	Managed	Compliant	.../Krakow/Site-01
ISR-BRANCH-02	172.27.100.65	Routers	Reachable	Managed	Compliant	.../Krakow/Site-02
Switch-172-26-100-68.krk-dna.local	172.26.100.68	Switches and Hubs (WLC Capable)	Reachable	Managed	Compliant	.../Krakow/Site-01
Switch-172-27-100-68.krk-dna.local	172.27.100.68	Switches and Hubs (WLC Capable)	Reachable	Managed	Compliant	.../Krakow/Site-02

c-edges

LAN Automated devices for SDA

devices assigned to proper site



# SDA / SD-WAN Integration

Provisioning Layer: Automation and Assurance

Orchestrator Layer  
Cisco DNA Center & Cisco vManage

Network Layer  
SDA Virtual Networks & SD-WAN VPNs

Provisioning Layer  
Automation and Assurance



# SD-WAN Transit - concept

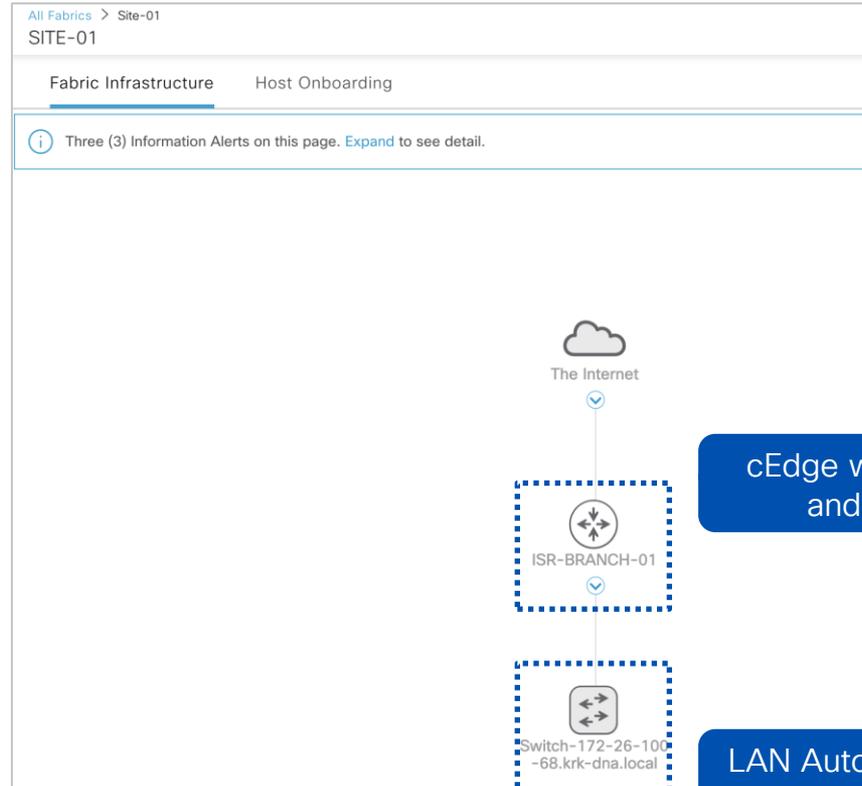
- SD-WAN Transit option is another available transit option (IP Transit, SDA Transit) that could be used to connect SDA sites.
- SD-WAN Transit allows to leverage SD-WAN advanced features and its intelligence to route packets on the most optimal path.
- SD-WAN Transit allows to carry SGT tags end-to-end in the data-plane.

# SD-WAN Transit in Cisco DNA Center

The screenshot shows the Cisco DNA Center interface. At the top, it says "Cisco DNA Center" and "Provision - Fabric". The main heading is "SD-Access Fabrics and Transit/Peer Networks". Below this, there is a sub-heading "Fabrics" and a card for "Default LAN Fabric" with statistics: "0 Site, 0 Fabric Device, 0 Control Plane, 0 Border". Below that is the "Transit/Peer Networks" section, where a card for "SDWAN 100.67.0.1" is highlighted with a dashed blue border. The card also shows "Transit: SDWAN".

SD-WAN Transit is created during Cisco DNA Center and vManage integration

# SD-Access Fabric - configuration



cEdge will act as a Border Node and Control Plane Node

LAN Automated switch will act as an Edge Node

# SD-Access Fabric

## Border and Control Plane configuration

ISR-BRANCH-01 (172.26.100.65)

🔄 Reachable Uptime: 12 days 14 hrs 39 mins

[Run Commands](#) | [View 360](#)

Details **Fabric** Port Channel Advisories Configuration Power Fans User Defined Fields

[Remove From Fabric](#)

Fabric

- E** Edge ⓘ
- B** Border ⓘ
- C** Control Plane ⓘ

**SD-WAN cEdge must be configured as SDA Border Node and Control Plane Node**

# SD-Access Fabric

## Border configuration

The screenshot shows the configuration page for 'ISR-BRANCH-01' under 'SITE-01'. The 'Layer 3 Handoff' tab is selected. The configuration includes:

- Enable Layer-3 Handoff
- Local Autonomous Number: \_\_\_\_\_ (i)
- Default to all virtual networks (i)
- Do not import external routes (i)
- + Add Transit/Peer Site
- SDWAN 100.67.0.1 (highlighted with a dashed blue box)
  - 100.67.0.1 - SDWAN Transit
- This site provides internet access to other sites through SDA Transit. (i)

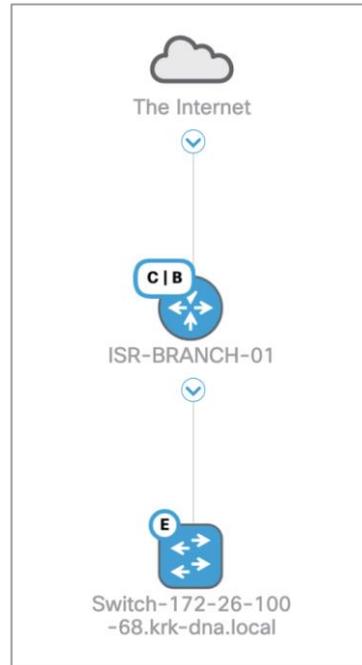
SD-WAN Transit is automatically added to all cEdges during Border configuration

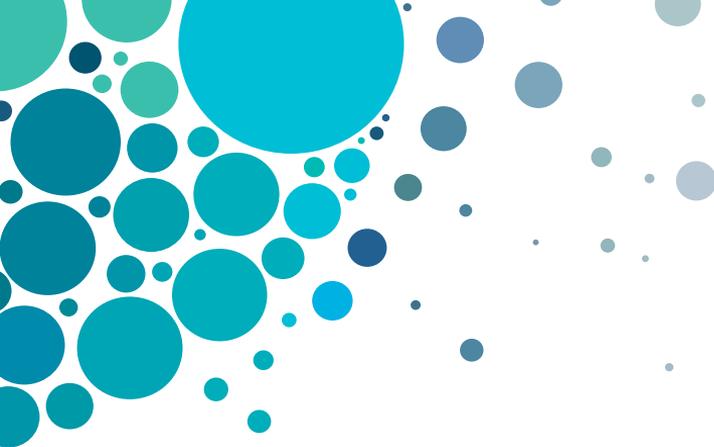
# SD-WAN Transit

## Summary

At the end of this stage the status will be as follows:

- SD-WAN Transit added to all Borders.





# Agenda

Covered so far...

- 1) SD-Access / SD-WAN: Basics
- 2) Cross-Domain: Supported Designs
- 3) SD-Access / SD-WAN: Integration Principles

**Orchestrator Layer**  
Cisco DNA Center & Cisco vManage

**Network Layer**  
SDA Virtual Networks & SD-WAN VPNs

**Provisioning Layer**  
Automation and Assurance

# Prescriptive Deployment Guides

## 1) Cisco SD-Access - SD-WAN Integrated Domain Pairwise Integration

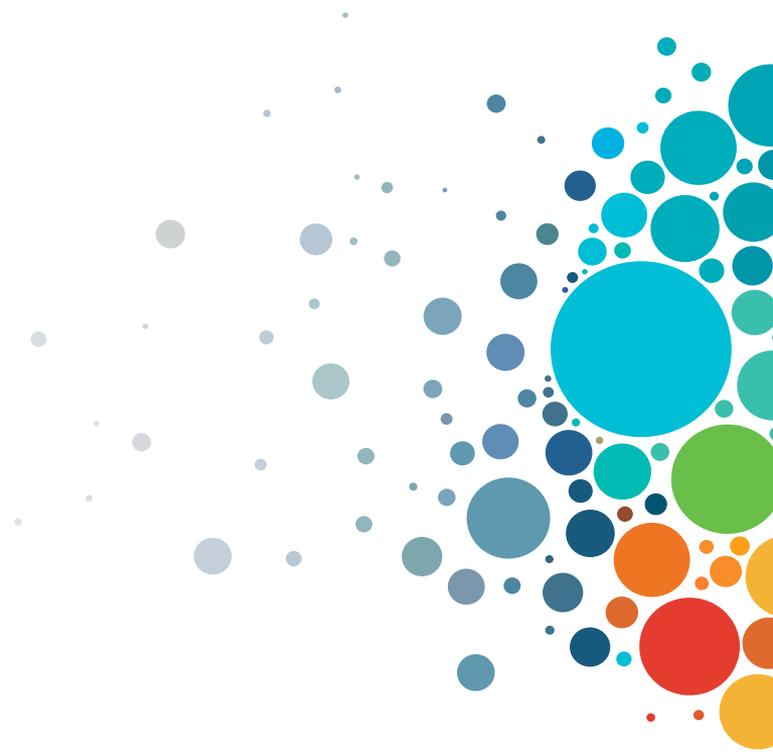
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Cisco-SD-Access-SD-WAN-Integrated-Domain-Guide.pdf>

## 2) Cisco SD-Access - SD-WAN Independent Domain Pairwise Integration

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Cisco-SD-Access-SD-WAN-Independent-Domain-Guide.pdf>

# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](http://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

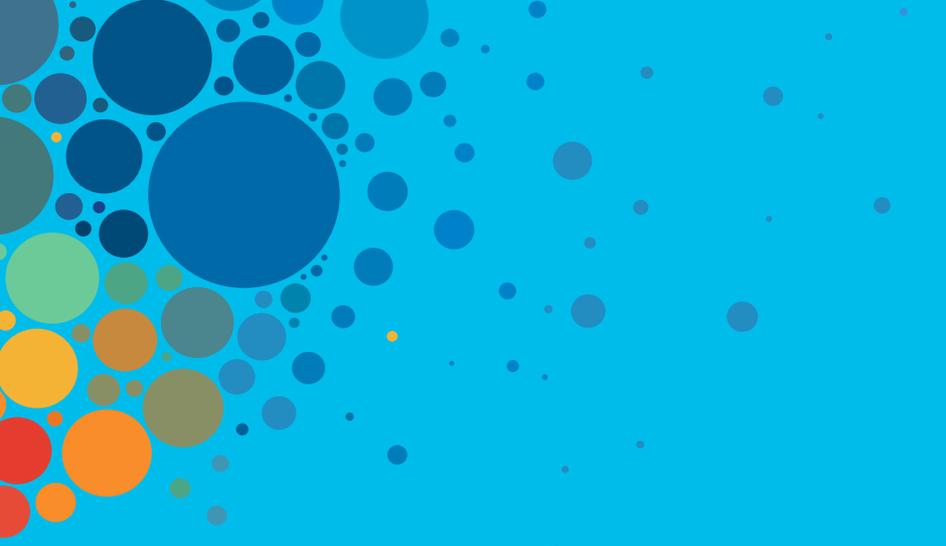
### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

ALL IN

#CiscoLive