
cisco Live!
ALL IN

The bridge to possible

Cross-Domain Integration

Troubleshooting Cisco SD-Access - SD-WAN Integration

Mariusz Kaźmierski
Principal Engineer, EMEAR CX Centers

BRKTRS-3457

Cisco Webex App

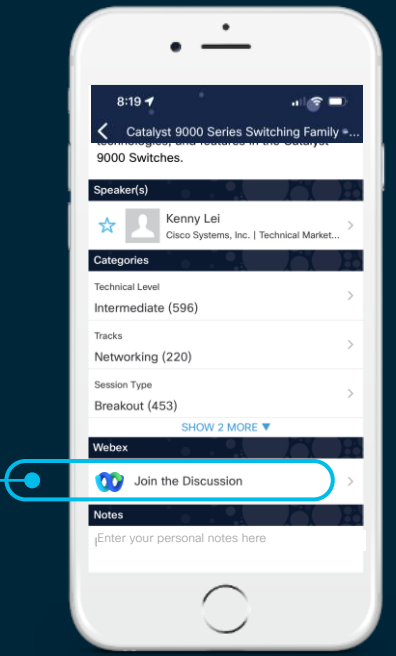
Questions?

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://ciscolive.ciscoevents.com/ciscolivebot/#BRKTRS-3457

Agenda

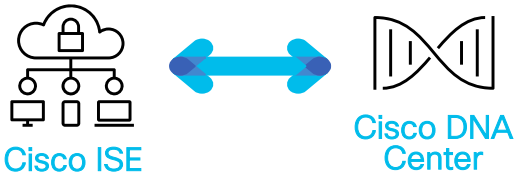
1) **SD-Access / SD-WAN**: Basics
2) **Cross-Domain**: Supported Designs
3) **SD-Access / SD-WAN:** Integration Principles

1. SD-Access / SD-WAN

Basics

SD-Access (SDA) - basics

Software



Cisco DNA Center

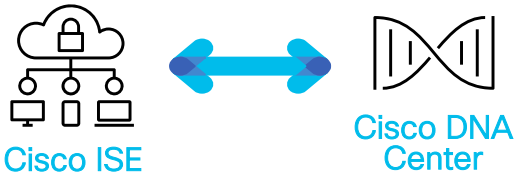
Orchestrator responsible for intent-based automation and assurance in Campus Network.

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

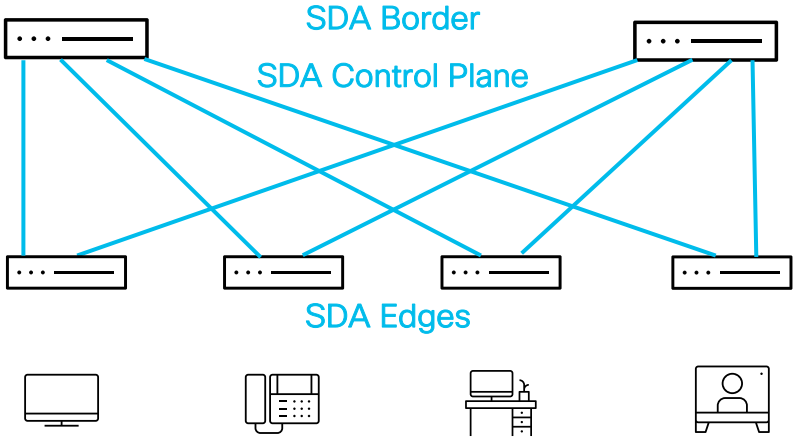
Orchestrator responsible for intent-based automation and assurance in Campus Network.

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

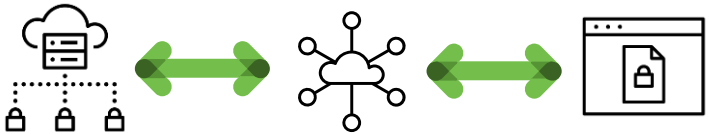
Fabric device that governs control-plane operations in the fabric.

SDA Edge

Fabric device to which end-points are connected to.

SD-WAN - basics

Software



vManage

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

vBond

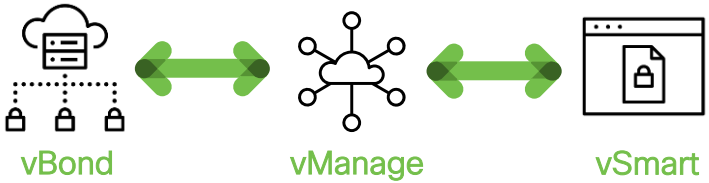
orchestration-plane responsible for on-boarding (Zero Touch Provisioning) new devices into SD-WAN fabric.

vSmart

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

SD-WAN - basics

Software



vManage

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

vBond

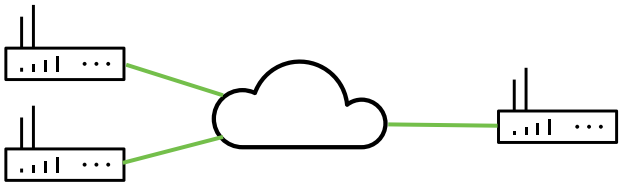
orchestration-plane responsible for on-boarding (Zero Touch Provisioning) new devices into SD-WAN fabric.

vSmart

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

SD-WAN Fabric

IPSEC / OMP



cEdge

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

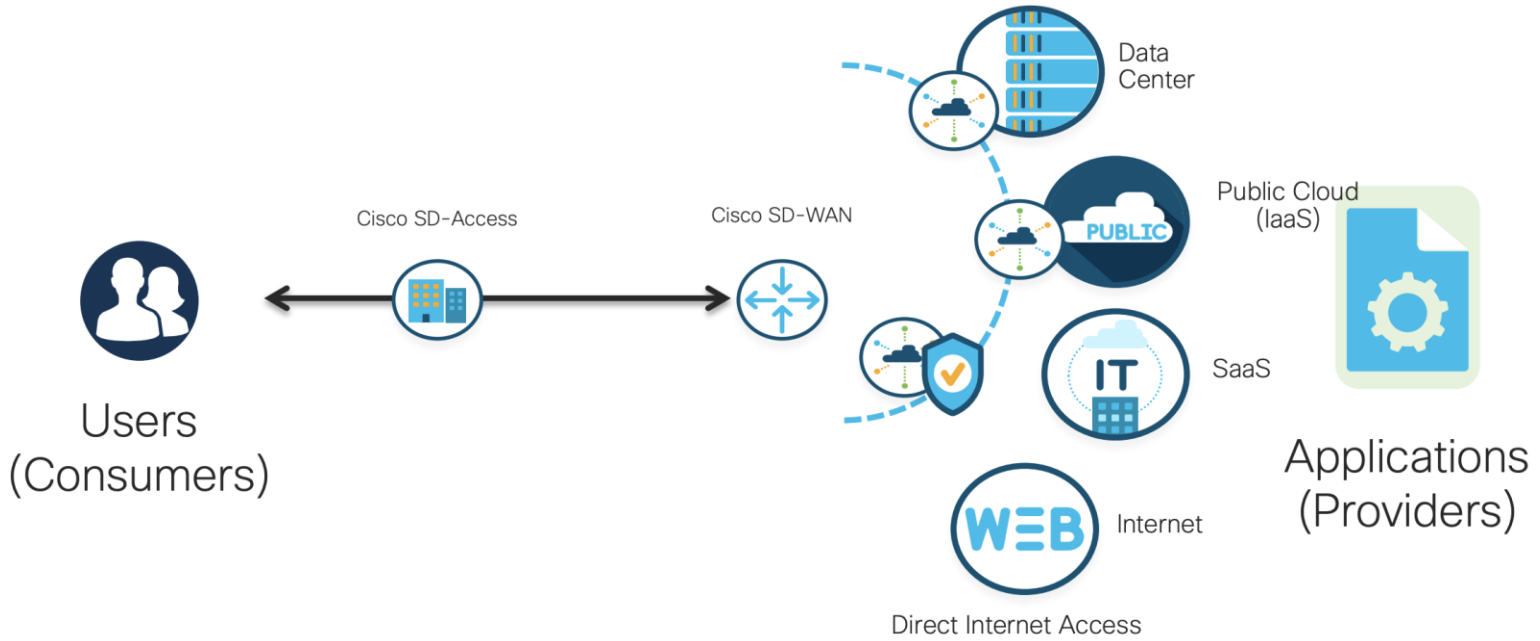
SD-Access – SD-WAN: Comparison

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.

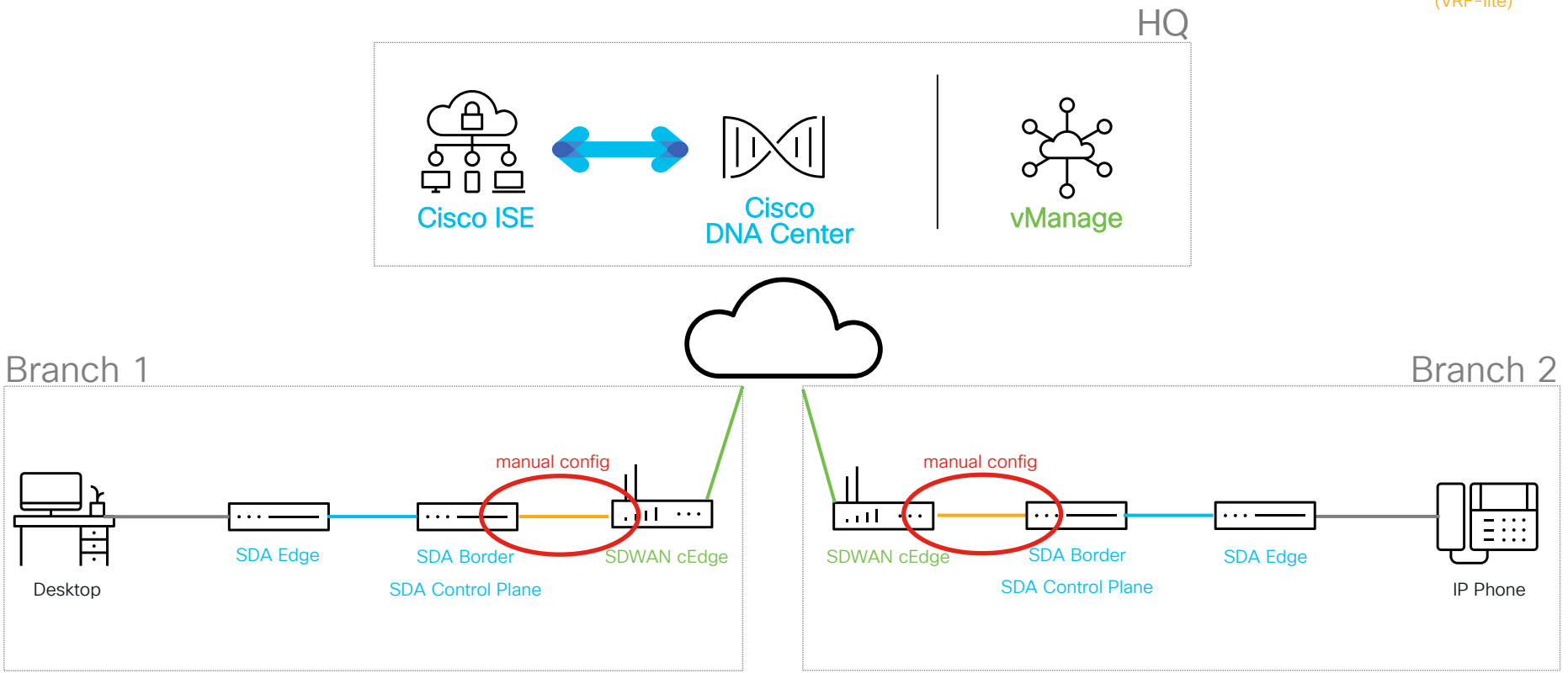
3) **Leverage** intelligent routing between different branch offices.

4) **Automate** new site deployments.

5) **Monitor** network via single pane of glass.

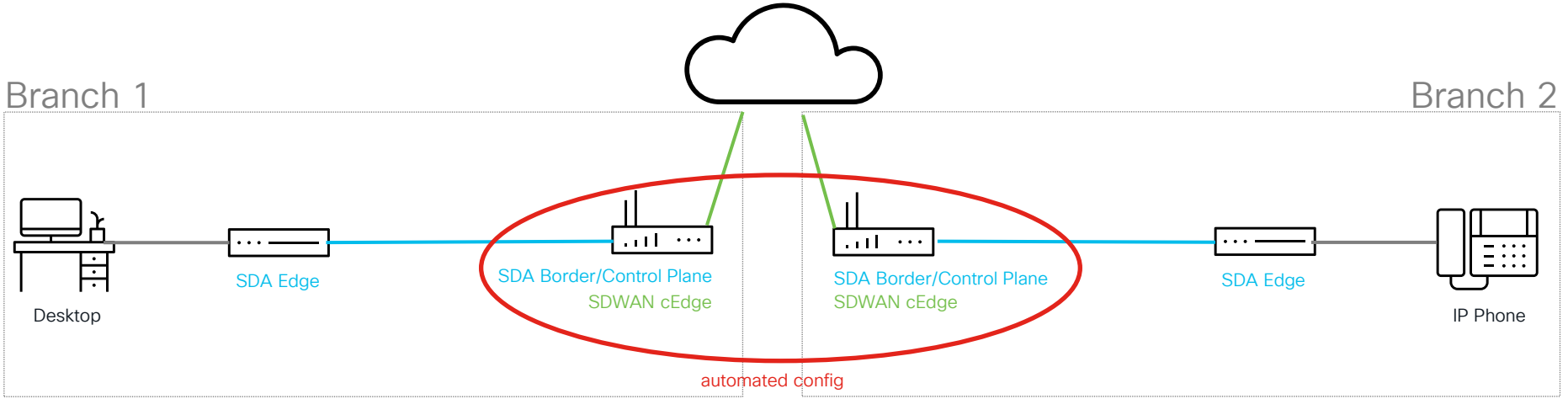
SDA – SD-WAN: Independent Domain

SDA
SD-WAN
manual TrustSec (VRF-lite)



SDA
SD-WAN

SDA – SD-WAN: Integrated Domain



Compatibility Matrix

Cisco Software-Defined Access Compatibility Matrix

make sure that compatible software is used!

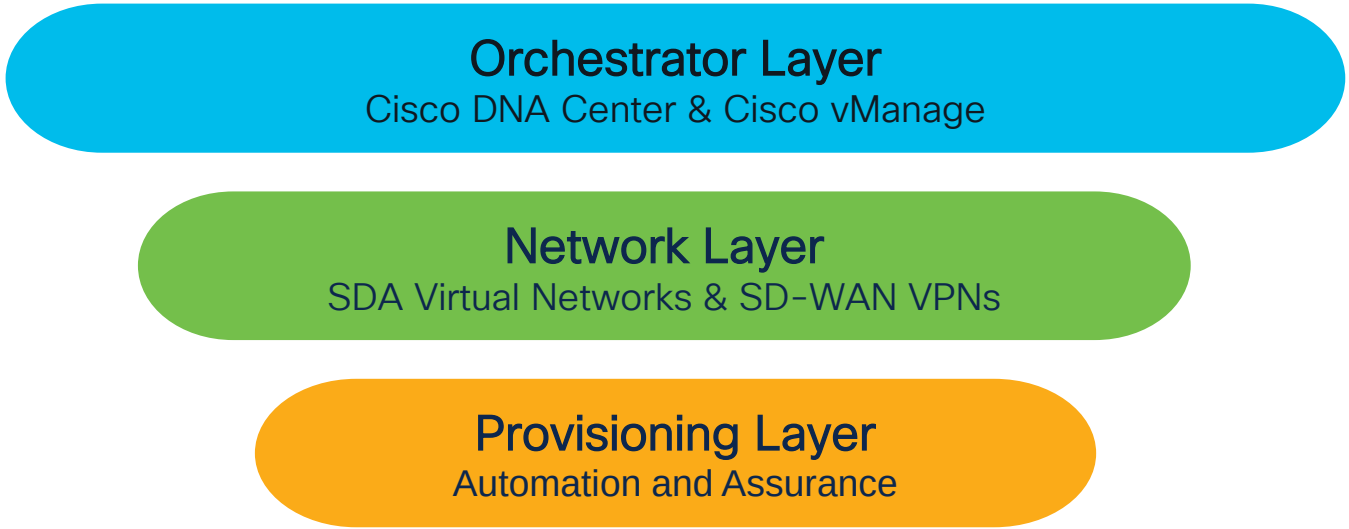
SD-Access Compatibility Matrix for Cisco DNA Center 2.2.2.8

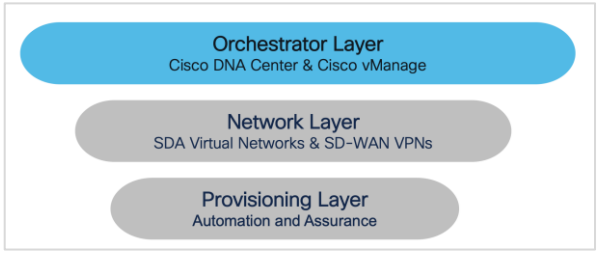
Device Role	Device Series	Device Model	Recommended Release	Supported Release
Collocated SD-Access Border, Control Plane and SD-WAN WAN Edge	Cisco 4000 Series Integrated Services Routers	ISR4331 ISR4351 ISR4451 ISR4461 ISR4431	IOS XE 17.3.4	IOS XE 17.3.4
	Cisco ASR 1000 Series Aggregation Services Routers	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





NEW

SDA / SD-WAN Integration

Orchestrator Layer: Cisco DNA Center & Cisco vManage

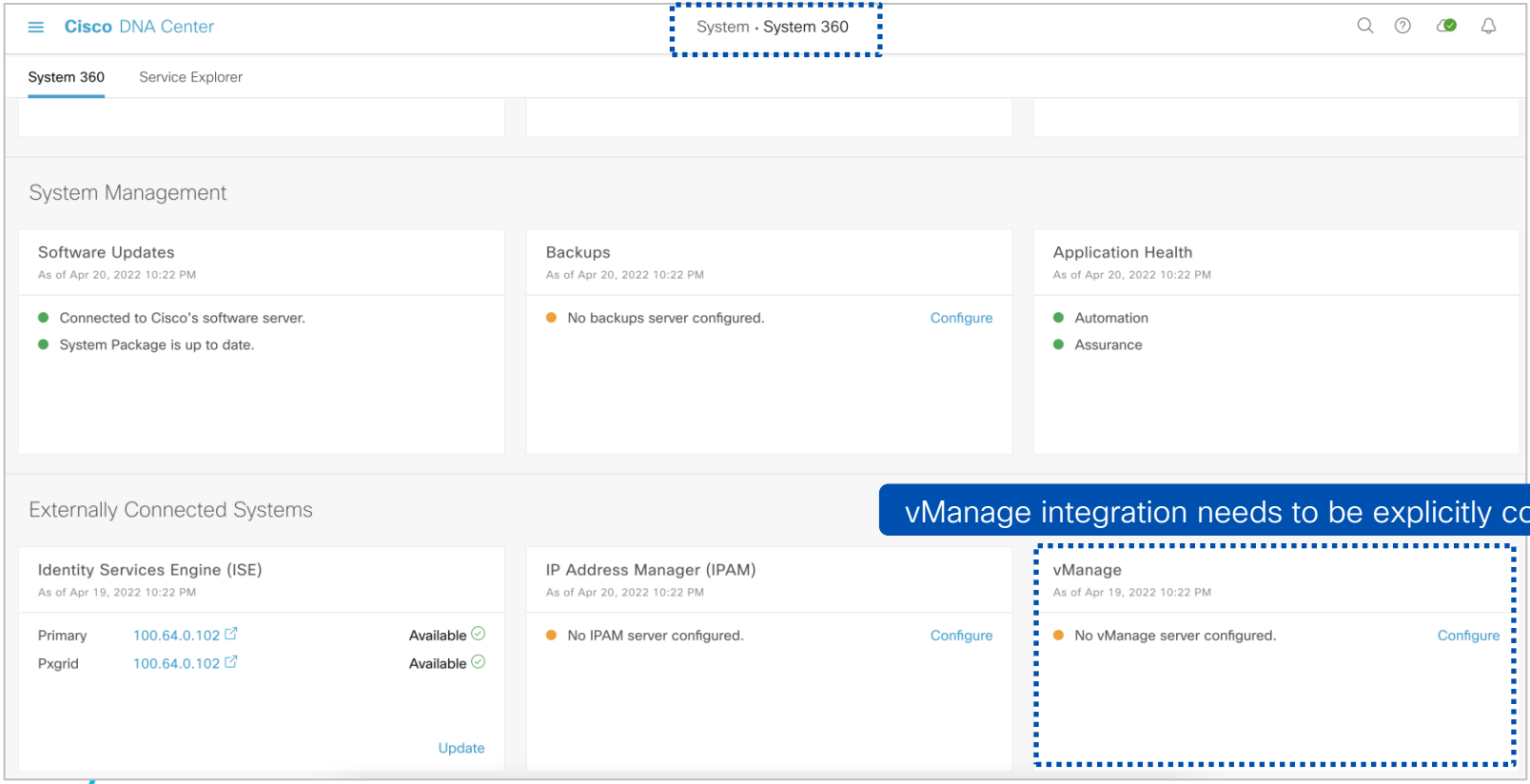
cisco Live!

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!

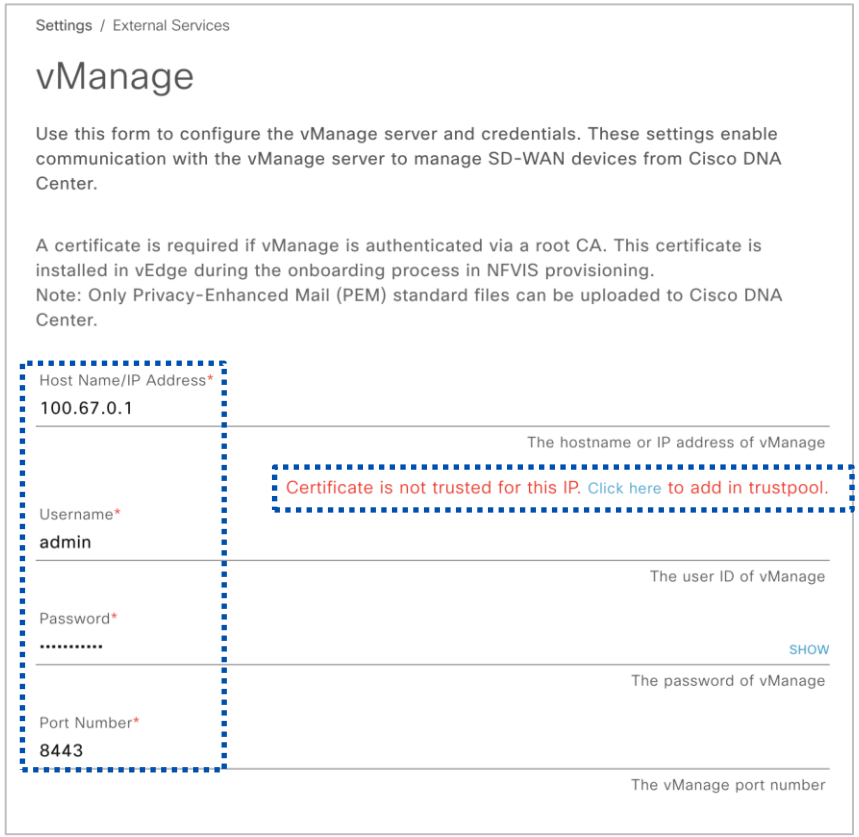
- SD-WAN devices (cEdges) are going to be known and co-managed by both orchestrators:
  - **vManage** for SD-WAN configuration,
  - **Cisco DNA Center** for SD-Access configuration (configuration push via vManage).

Cisco DNA Center – System 360: initial state



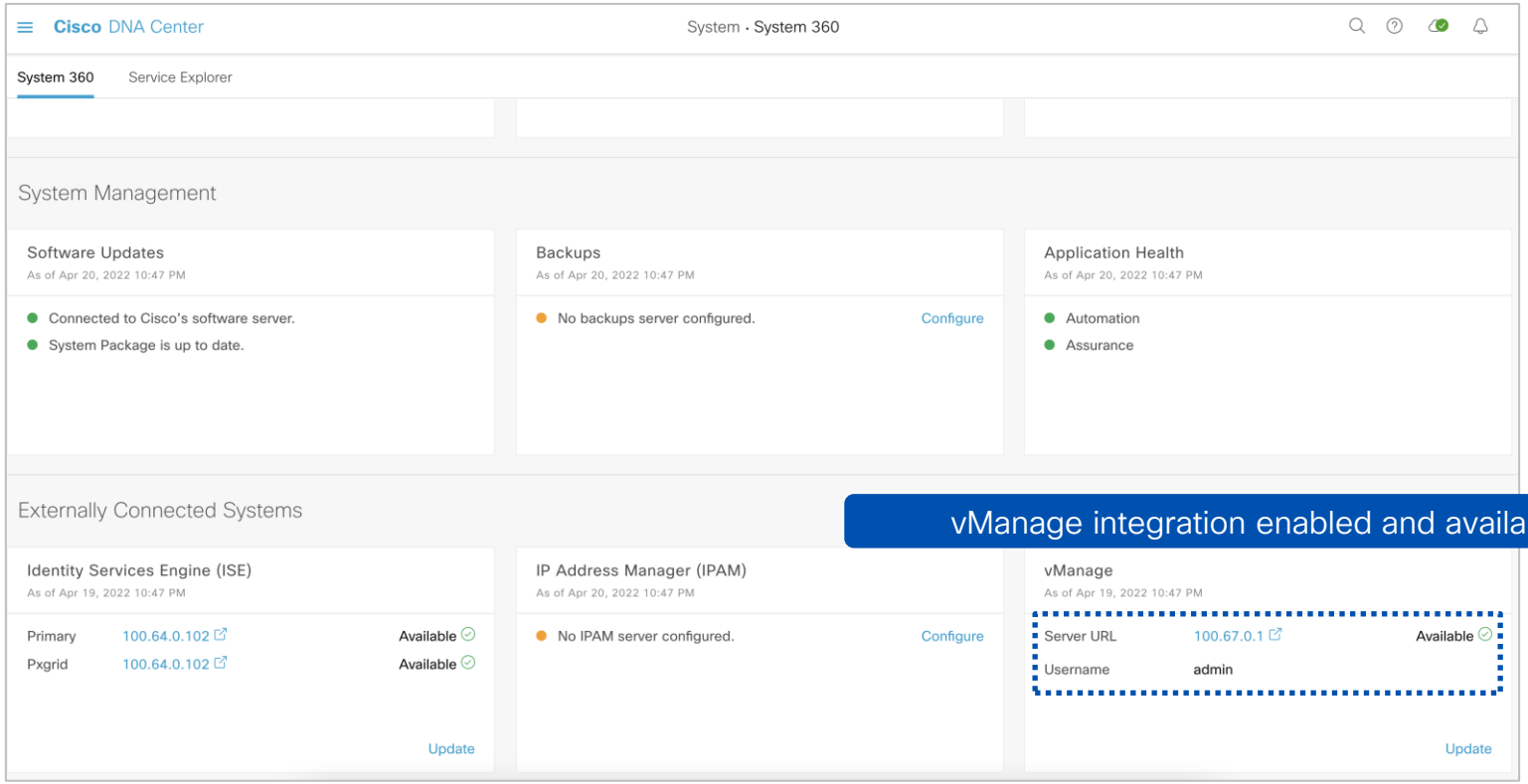
Cisco DNA Center – SD-WAN Integration

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



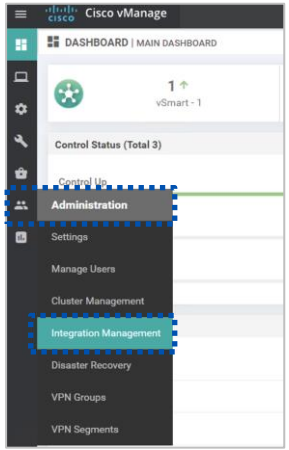
Cisco DNA Center must import vManage certificate for successful HTTPS API communication

Cisco DNA Center – System 360: final state



Cisco vManage – Integration status

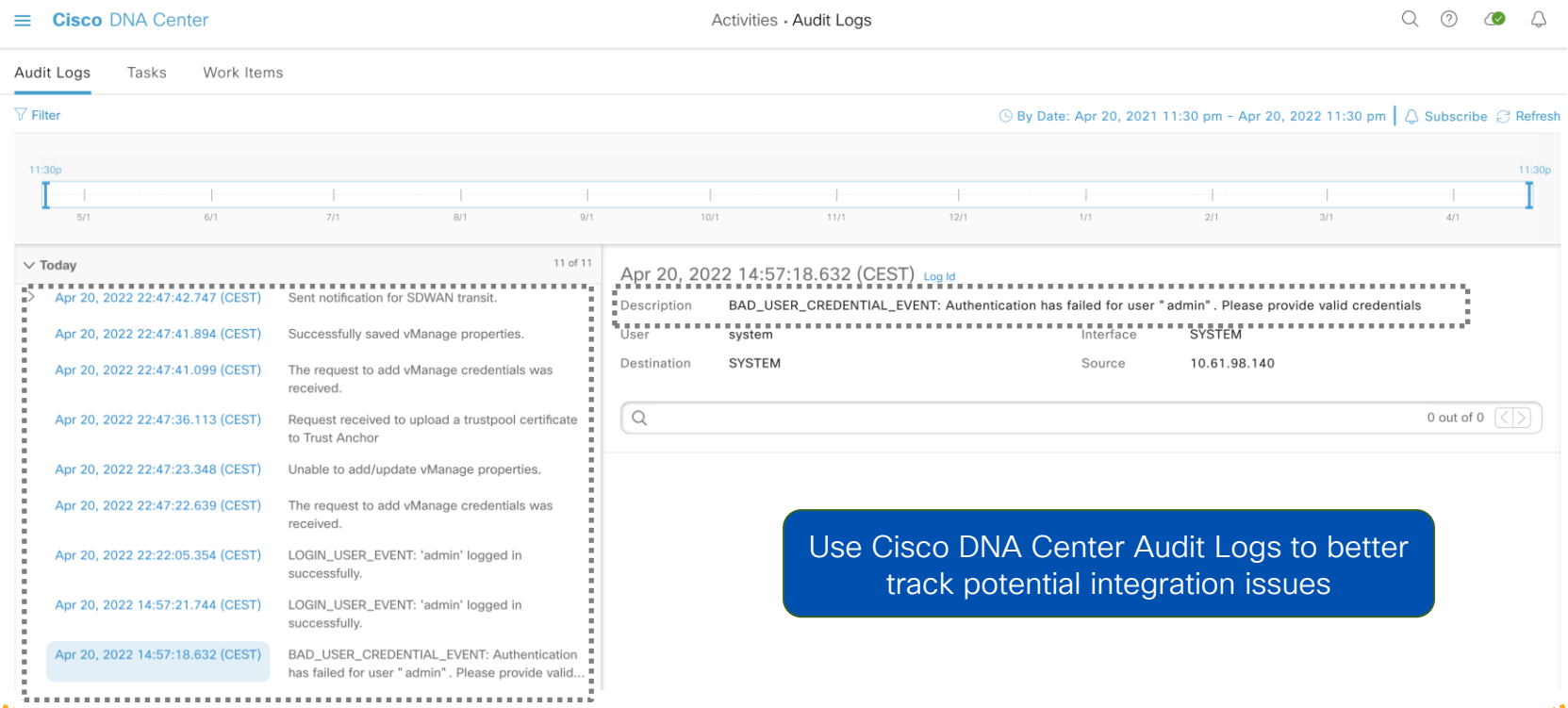
To check the status, go to:
Administration → Integration Management



Cisco DNA Center is added in vManage Integration Management tab

Troubleshooting integration issues

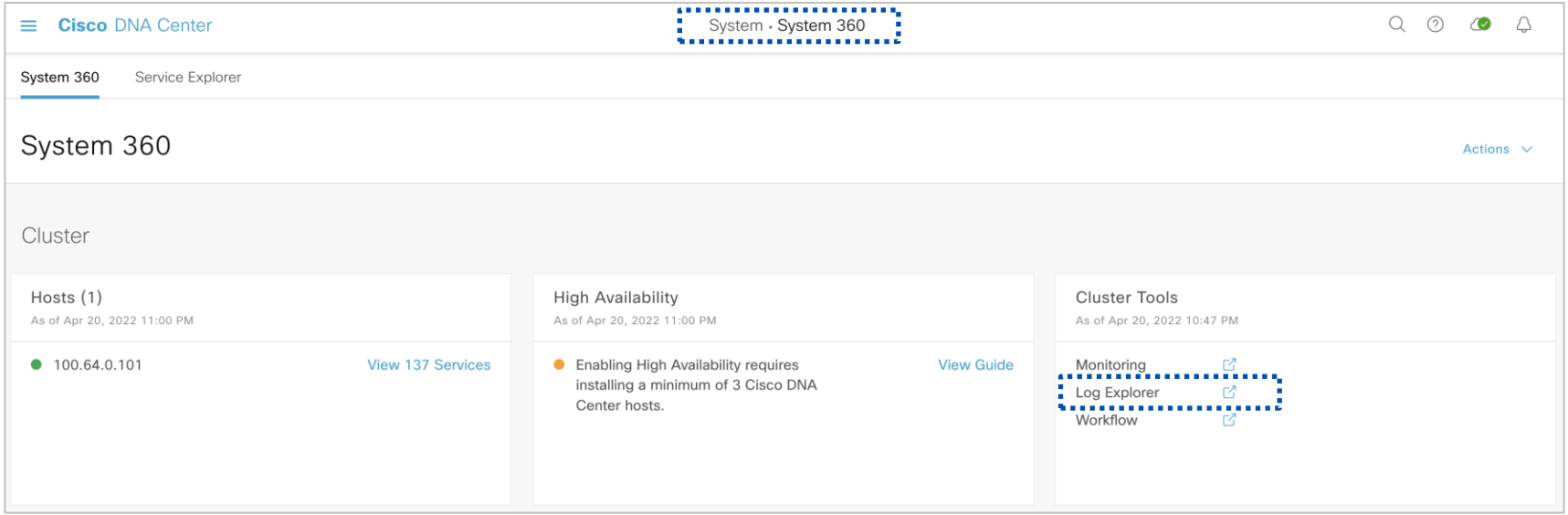
Cisco DNA Center: Audit Logs



TROUBLESHOOTING TIP

Troubleshooting integration issues

Cisco DNA Center: Log Explorer

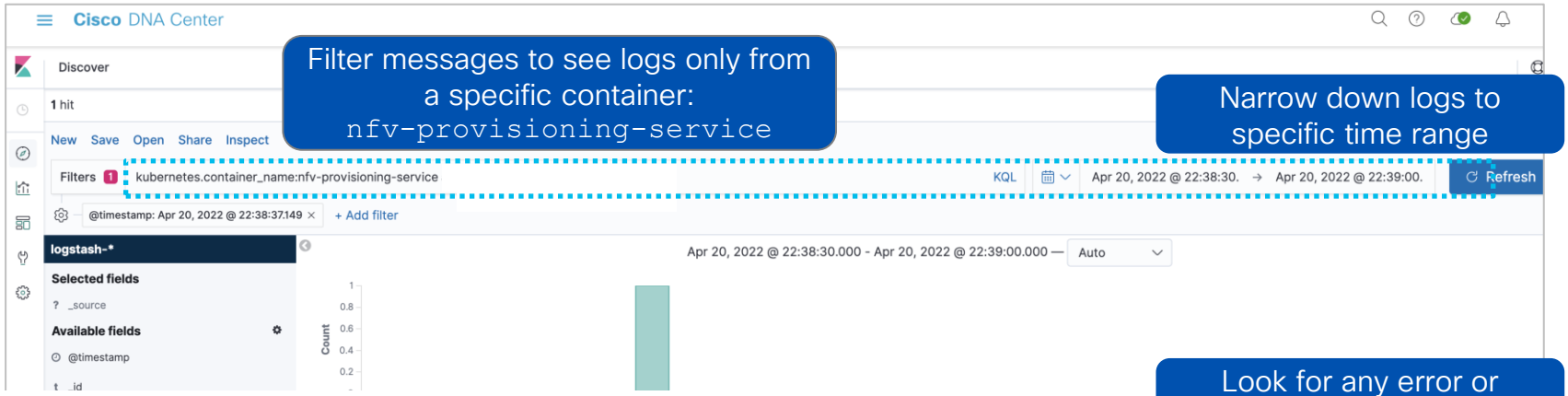


Use Cisco DNA Center Log Explorer to further explore possible integration issues

TROUBLESHOOTING TIP

Troubleshooting integration issues

Cisco DNA Center: Log Explorer



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

Narrow down logs to specific time range

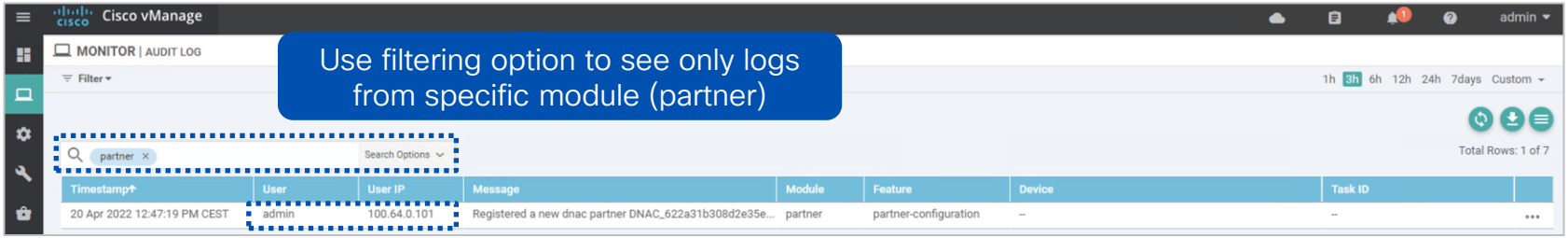
Look for any error or warning message

_source

`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 TIP

Troubleshooting integration issues
vManage: Audit Logs

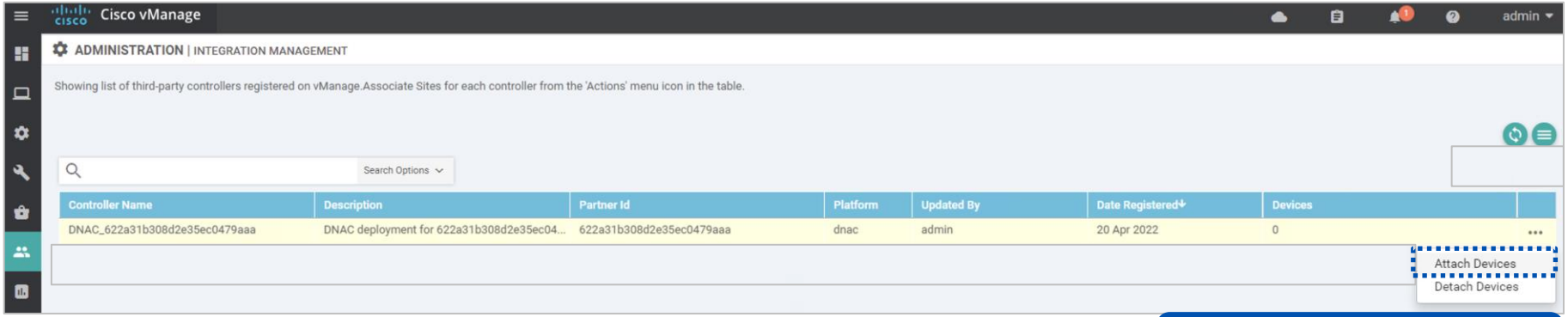


Use filtering option to see only logs from specific module (partner)

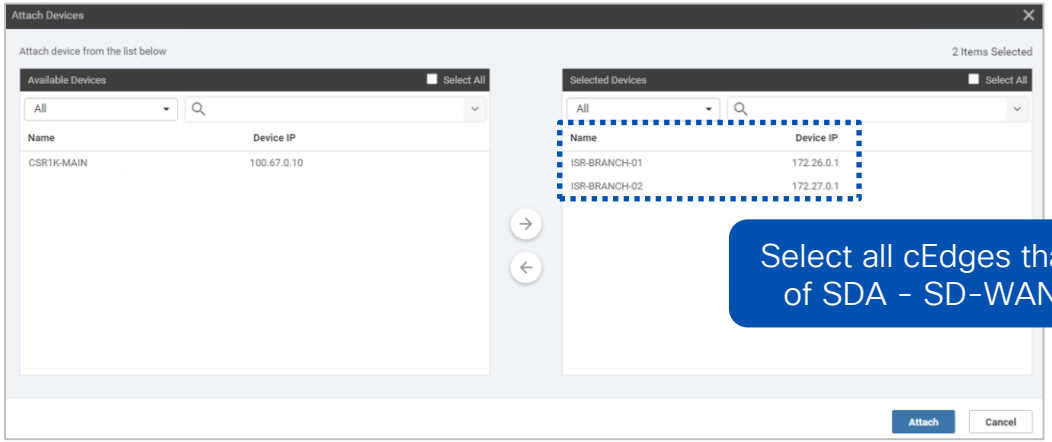
Look for activities initiated from Cisco DNA Center IP address

TROUBLESHOOTING TIP

SD-WAN: Attach cEdges into Integration

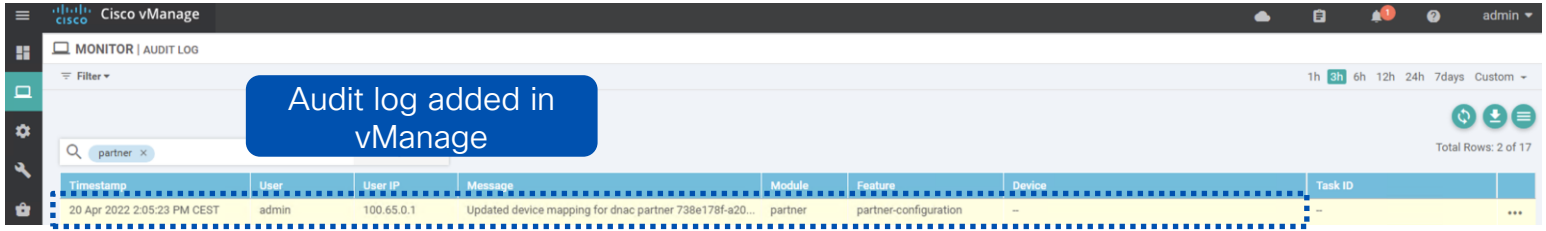


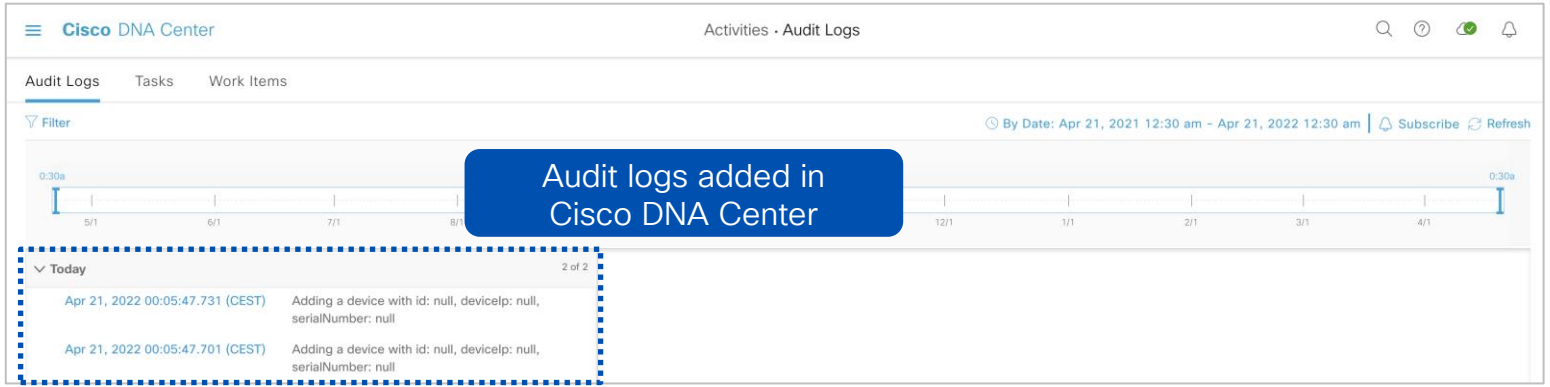
Select „Attach Devices" from sub-menu



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

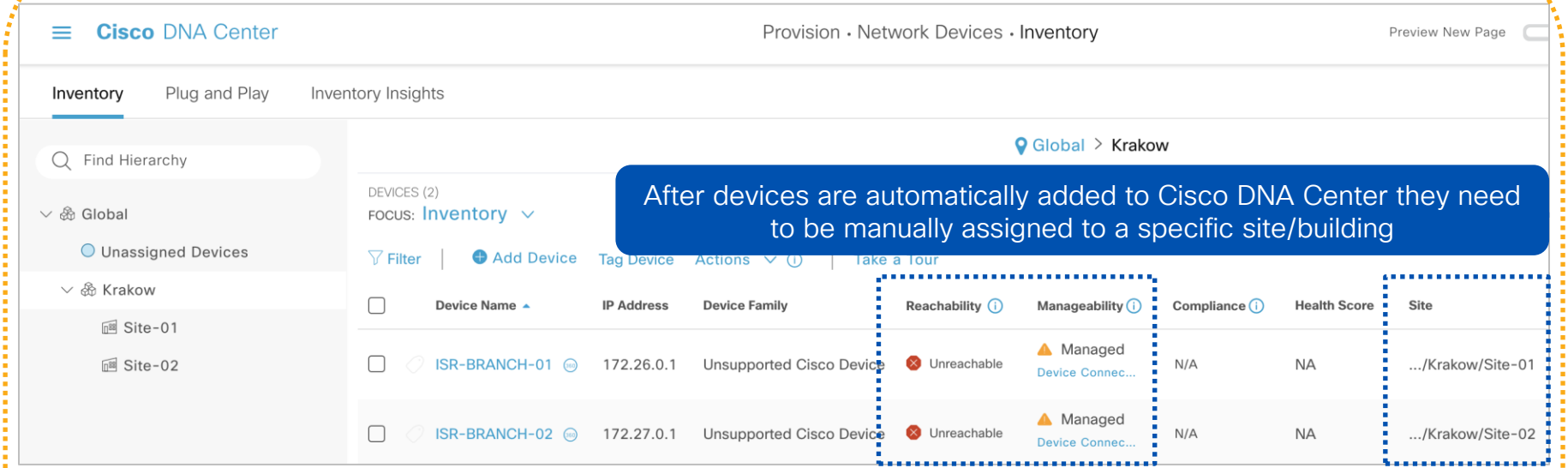
Cisco DNA Center & vManage: Audit Logs





TROUBLESHOOTING TIP

Cisco DNA Center: Inventory



After devices are automatically added to Cisco DNA Center they need to be manually assigned to a specific site/building

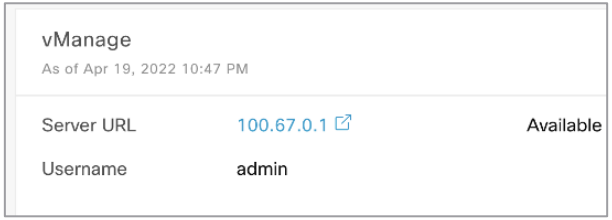
It is perfectly fine to have a device in the **Unreachable** state (as underlay might still not be provisioned from SDA perspective & there is no Loopback0 configured). The device MUST be in 'Managed' state

TROUBLESHOOTING TIP

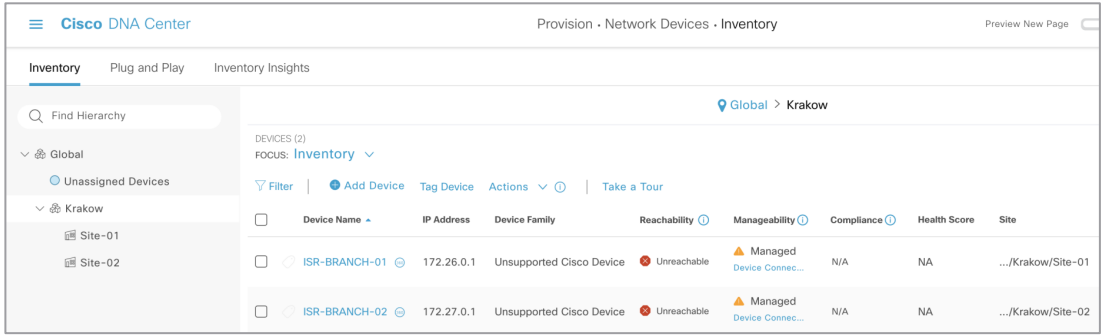
Orchestrator Layer:
Cisco DNA Center & Cisco vManage: Summary

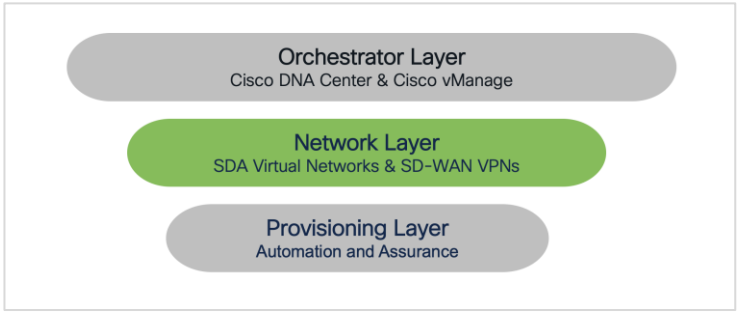
At the end of this stage the status will be as follows:

- Cisco DNA Center is fully integrated with Cisco vManage:



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





NEW

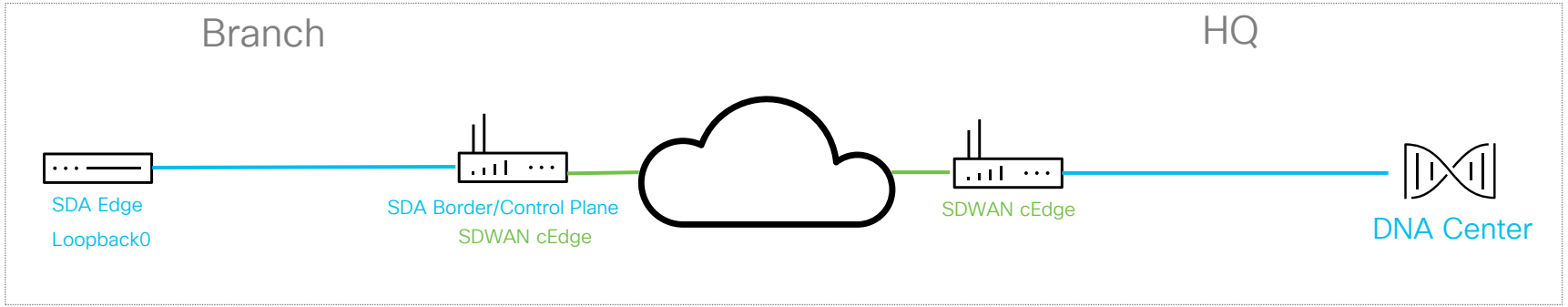
SDA / SD-WAN Integration

Network Layer: SDA Virtual Networks & SD-WAN VPNs

cisco Live!

Integrate SDA Virtual Networks with SD-WAN VPNs

SDA Underlay: end to end connectivity



DATA-PLANE

GLOBAL ROUTING TABLE
(SDA Underlay = INFRA_VN)

SERVICE VPN
(dedicated SD-WAN Service VPN for SDA Underlay)

GLOBAL ROUTING TABLE
(SD-WAN Underlay / Transport VPN)

ROUTING TABLE
(VRF)

Packet rewrite
(IP -> IPSEC)

Packet rewrite
(IPSEC -> IP)

CONTROL-PLANE

ISIS / LISP

OMP

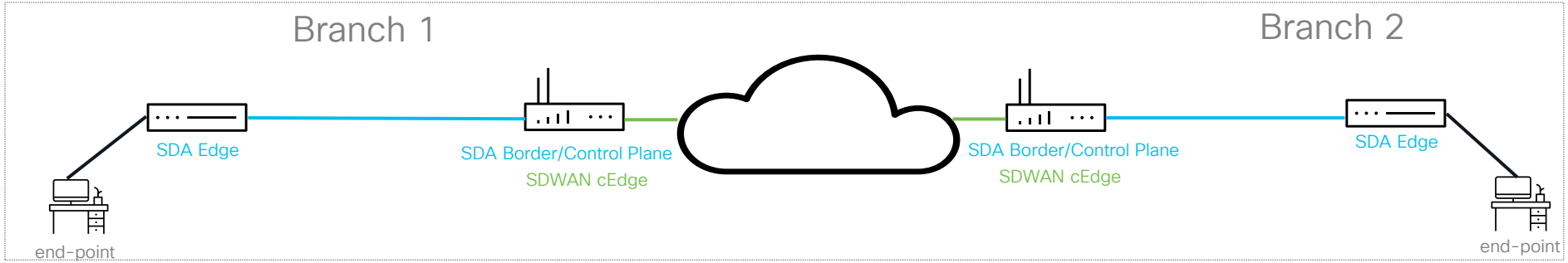
ISIS / OSPF / BGP / ...

redistribution

redistribution

Integrate SDA Virtual Networks with SD-WAN VPNs

SDA Overlay: end to end connectivity & security

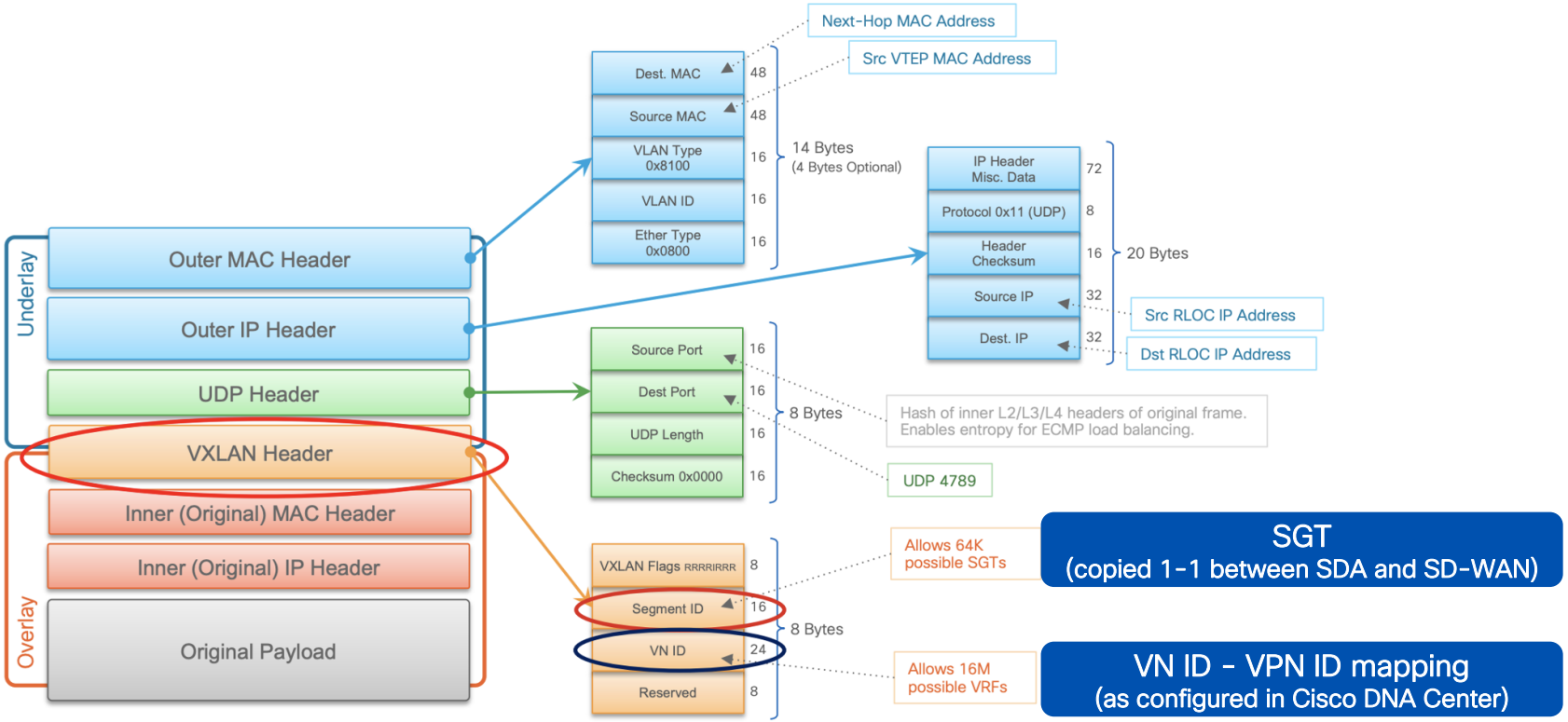


DATA-PLANE

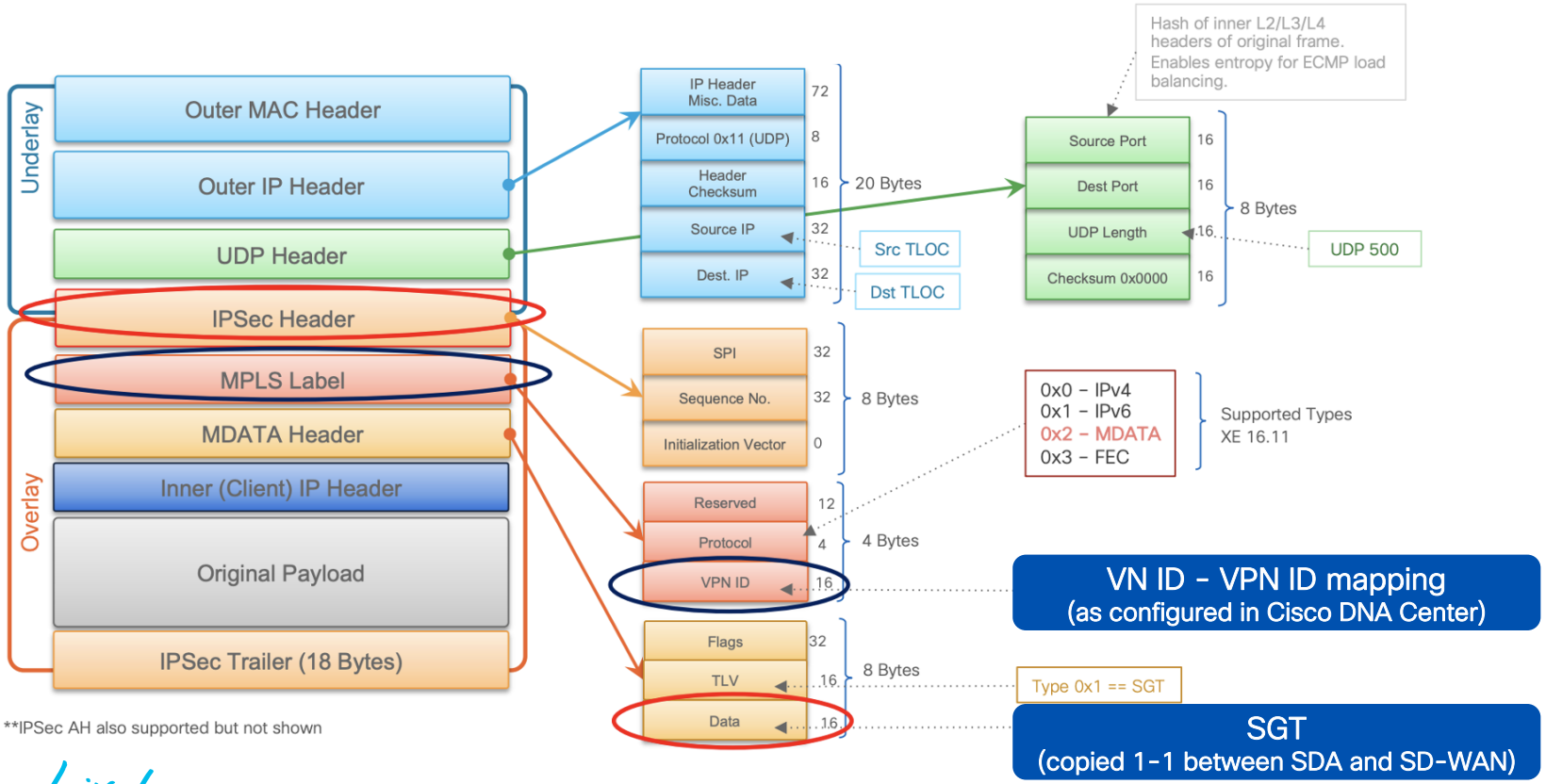
CONTROL-PLANE

SECURITY-PLANE

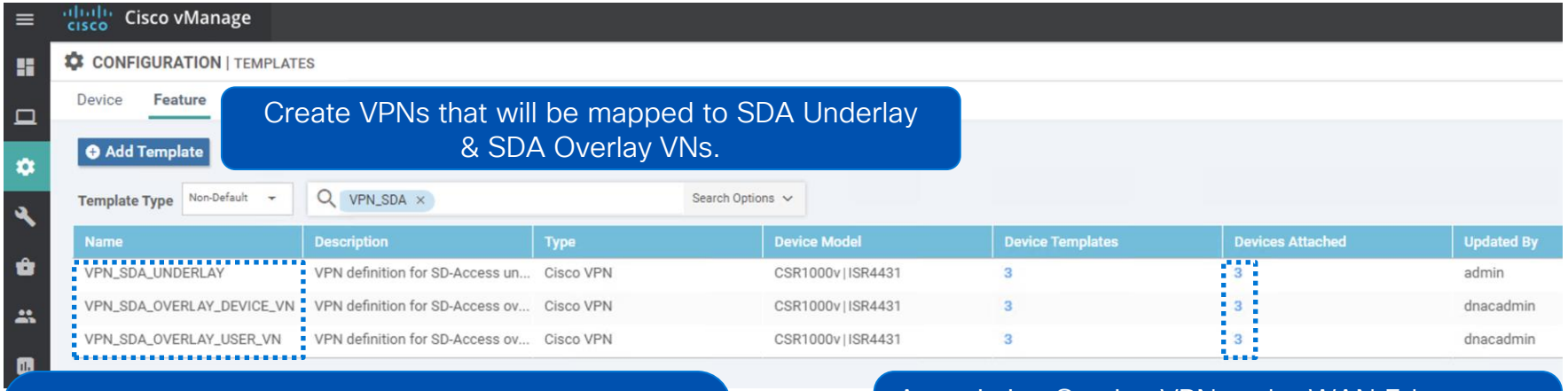
SDA Virtual Networks with SD-WAN VPNs
SDA (VXLAN) Encapsulation



SDA Virtual Networks with SD-WAN VPNs
SDWAN (IPSec) Encapsulation



vManage: Service VPN mapping

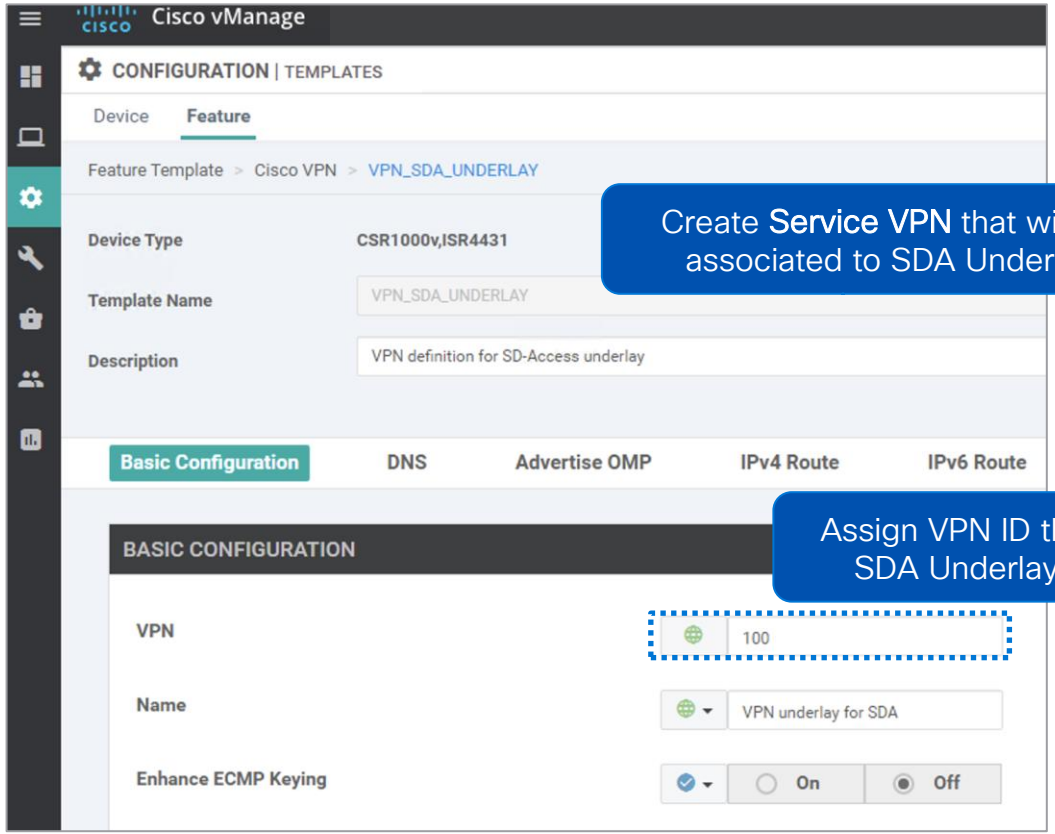


Generally, there is no need to add physical / logical interfaces to Service VPNs as they will be created automatically by Cisco DNA Center during:
- LAN Automation (for SDA underlay)
- Provisioning (for SDA overlay)

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)

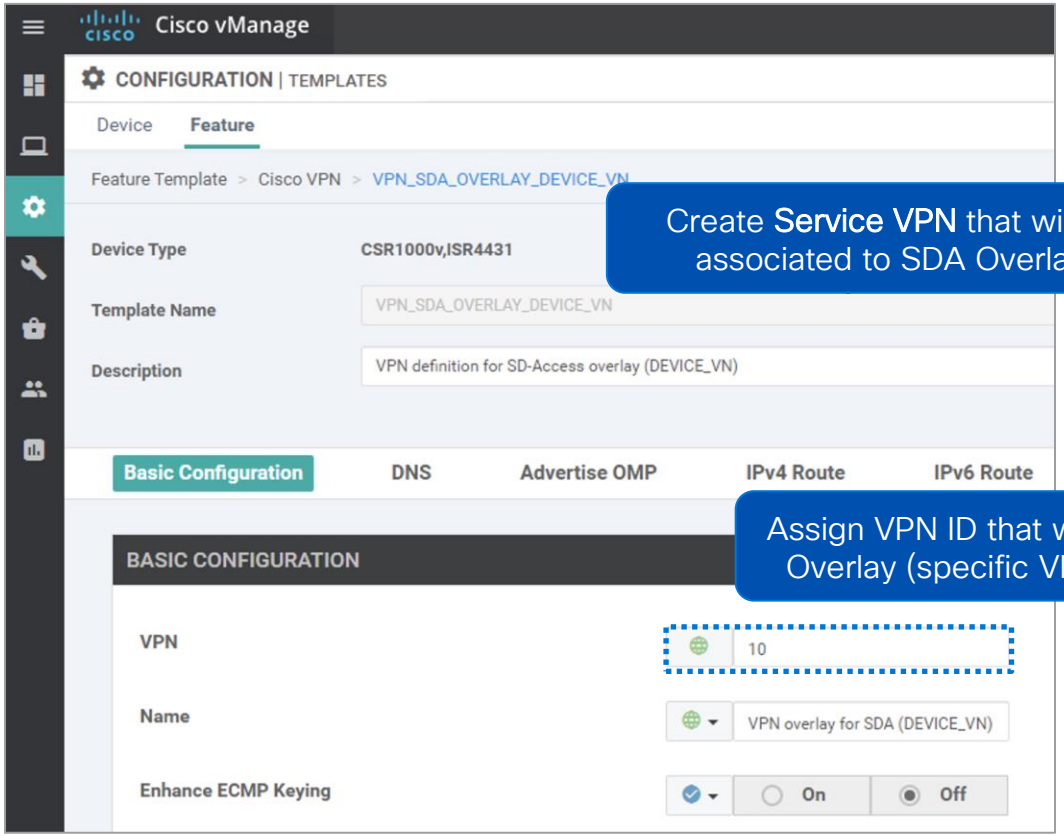


Create **Service VPN** that will be associated to SDA Underlay

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)

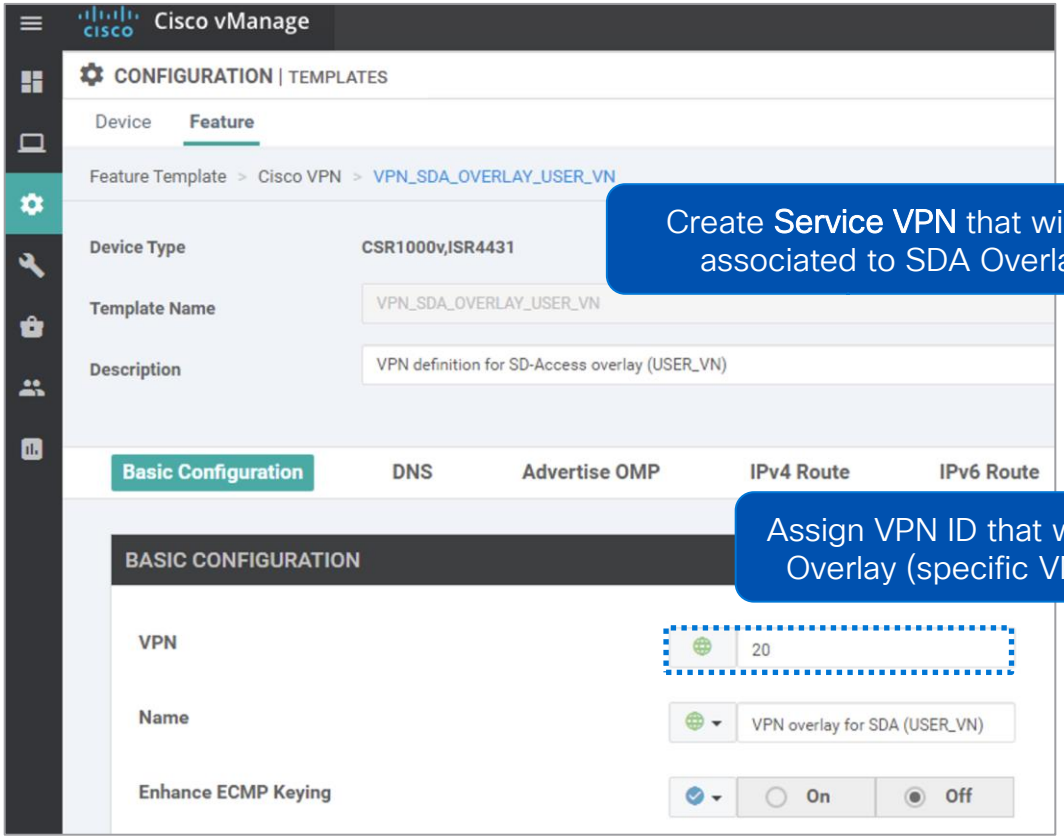


Create **Service VPN** that will be associated to SDA Overlay.

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

vManage – Service VPNs

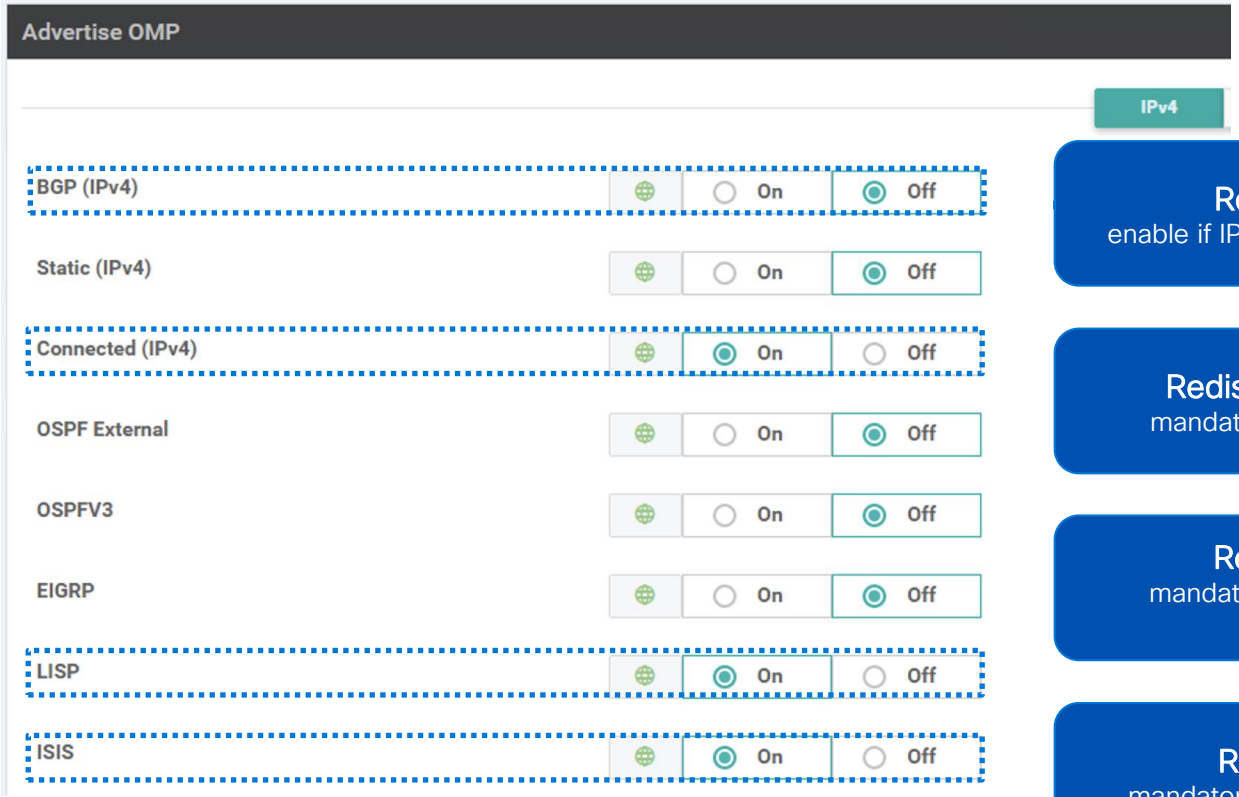
SD-WAN VPN20 = SDA Overlay (VN: USER_VN)



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



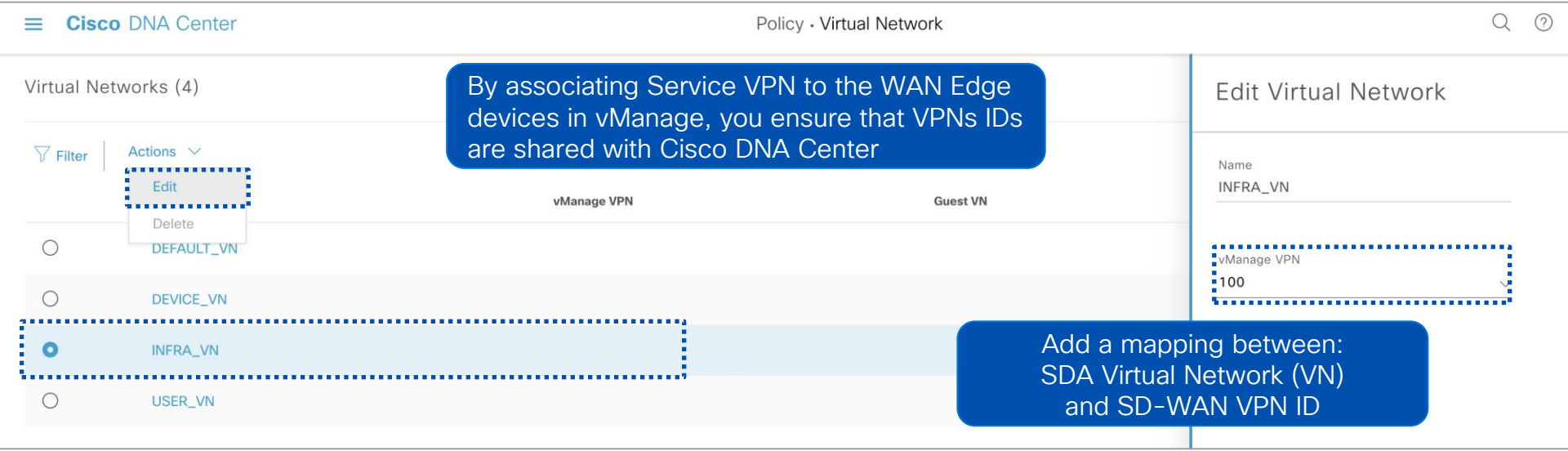
Redistribute „BGP” to OMP
enable if IP Transit/shared services is used on site

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)

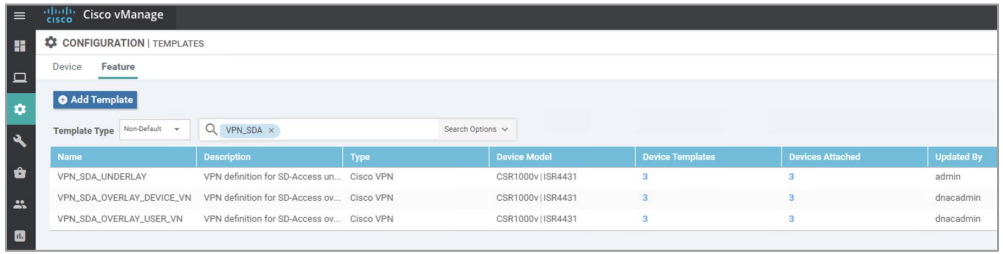
Cisco DNA Center
SDA Virtual Networks & SD-WAN VPNs - mapping



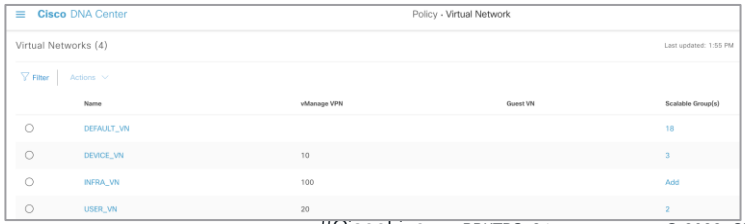
Network Layer:
SDA Virtual Networks & SD-WAN VPNs: Summary

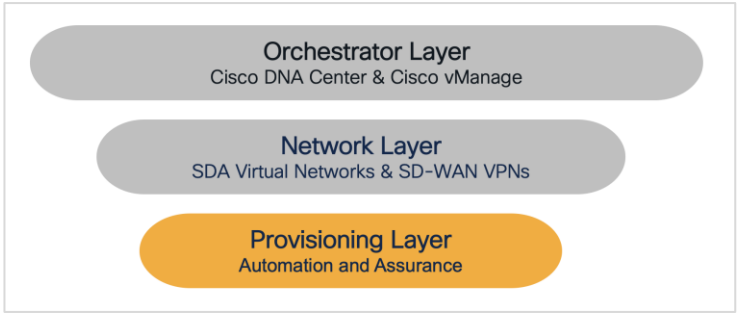
At the end of this stage the status will be as follows:

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



- 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:





NEW

SDA / SD-WAN Integration

Provisioning Layer: Automation and Assurance

LAN Automation - concept

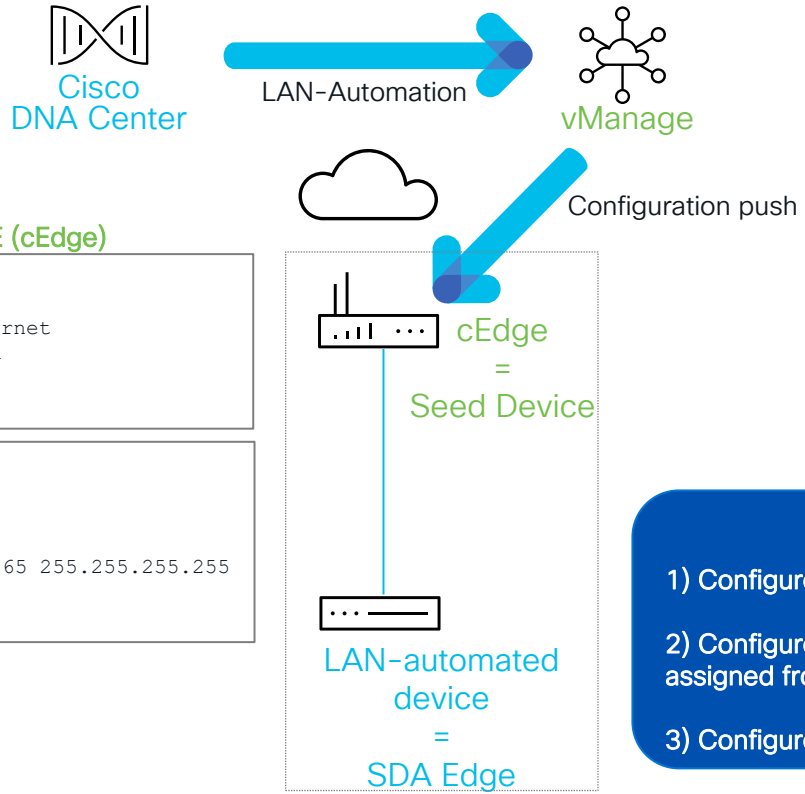
- LAN Automation is the Plug-n-Play (PnP) **zero-touch provisioning** of the **underlay network** in the SD-Access solution,

- 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)



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
```

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:

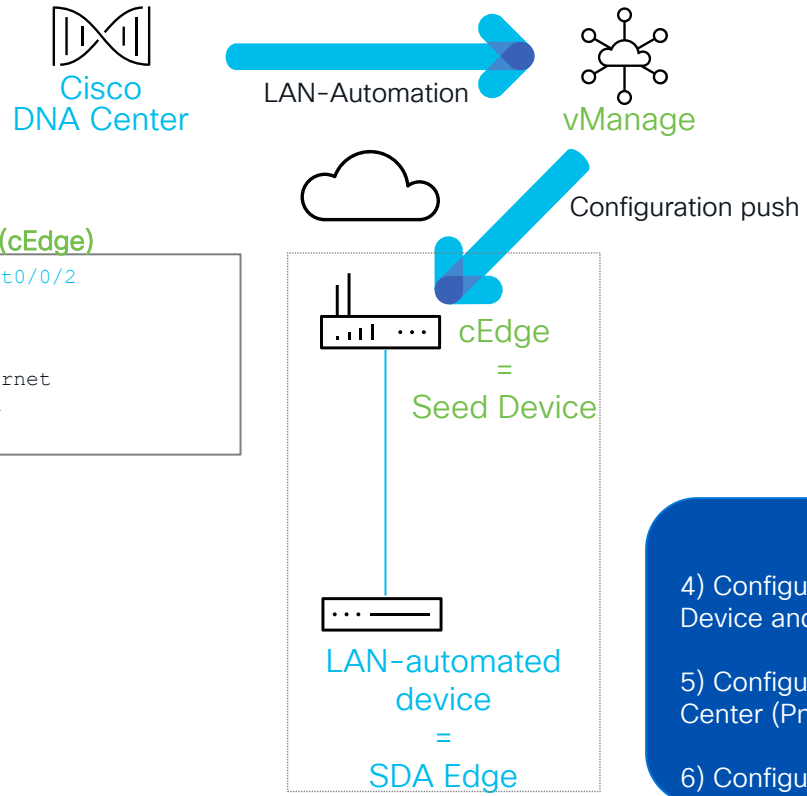
1) Configure Service VPN that corresponds to SDA Underlay.

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)



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
```

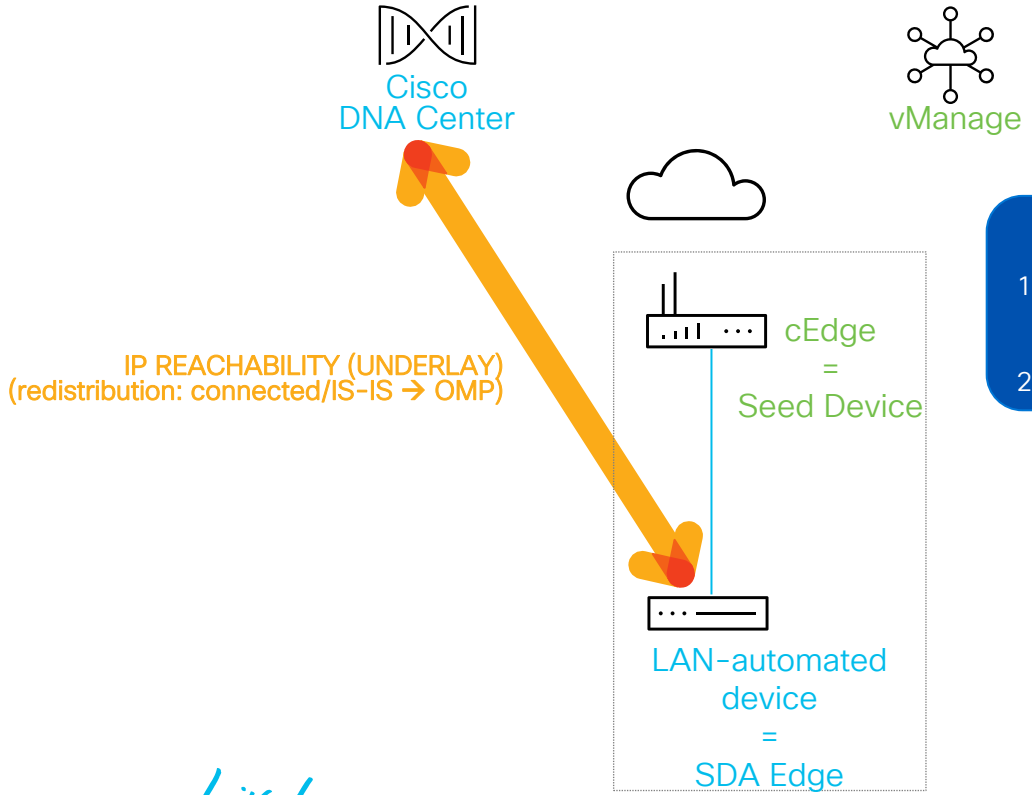
Actions:

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



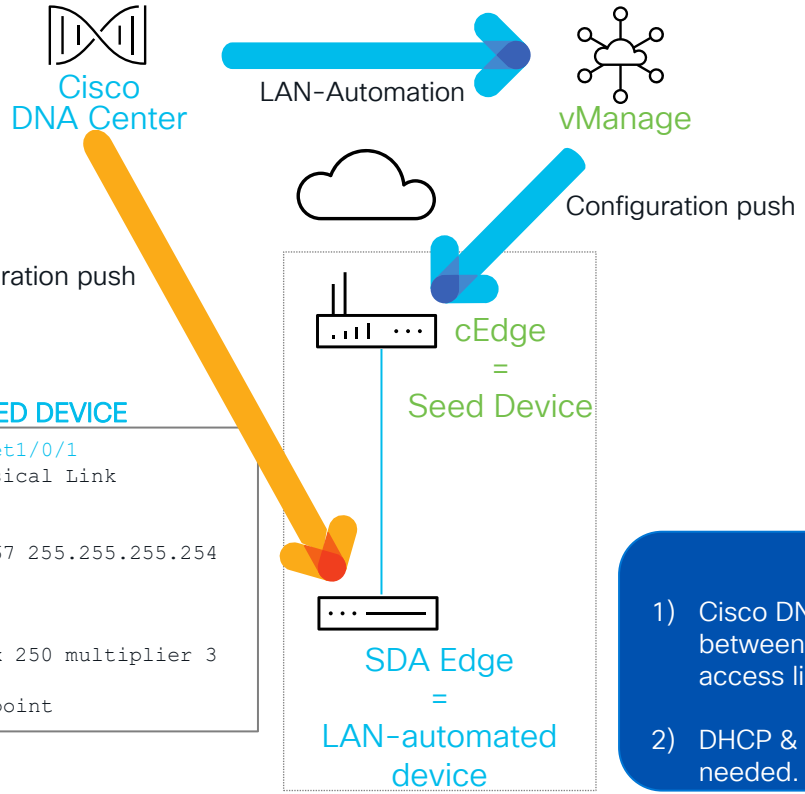
Actions:

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.

LAN Automation – diagram

Step 3: LAN Automation – routed access



LAN-AUTOMATED DEVICE

```
interface GigabitEthernet1/0/1
 description Fabric Physical Link
 no switchport
 dampening
 ip address 172.26.100.67 255.255.255.254
 no ip redirects
 ip router isis
 load-interval 30
 bfd interval 250 min_rx 250 multiplier 3
 clns mtu 1400
 isis network point-to-point
```

SEED DEVICE (cEdge)

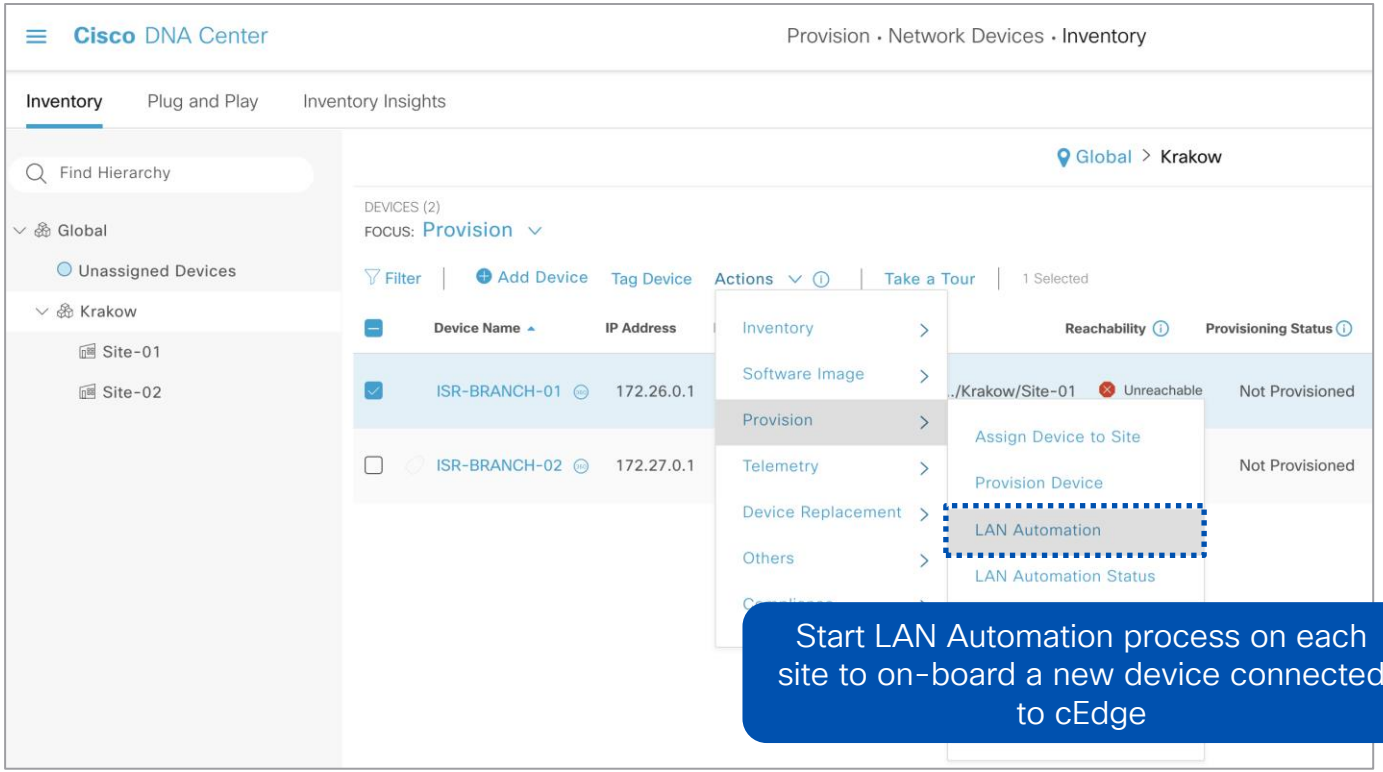
```
interface GigabitEthernet0/0/2
 description Fabric Physical Link
 mtu 9100
 vrf forwarding 100
 ip address 172.26.100.66 255.255.255.254
 ip lisp source-locator Loopback0
 ip router isis 100
 load-interval 30
 negotiation auto
 bfd interval 500 min_rx 500 multiplier 3
 clns mtu 1400
 isis network point-to-point
 isis csnp-interval 10 level-1
 isis csnp-interval 10 level-2
```

Actions:

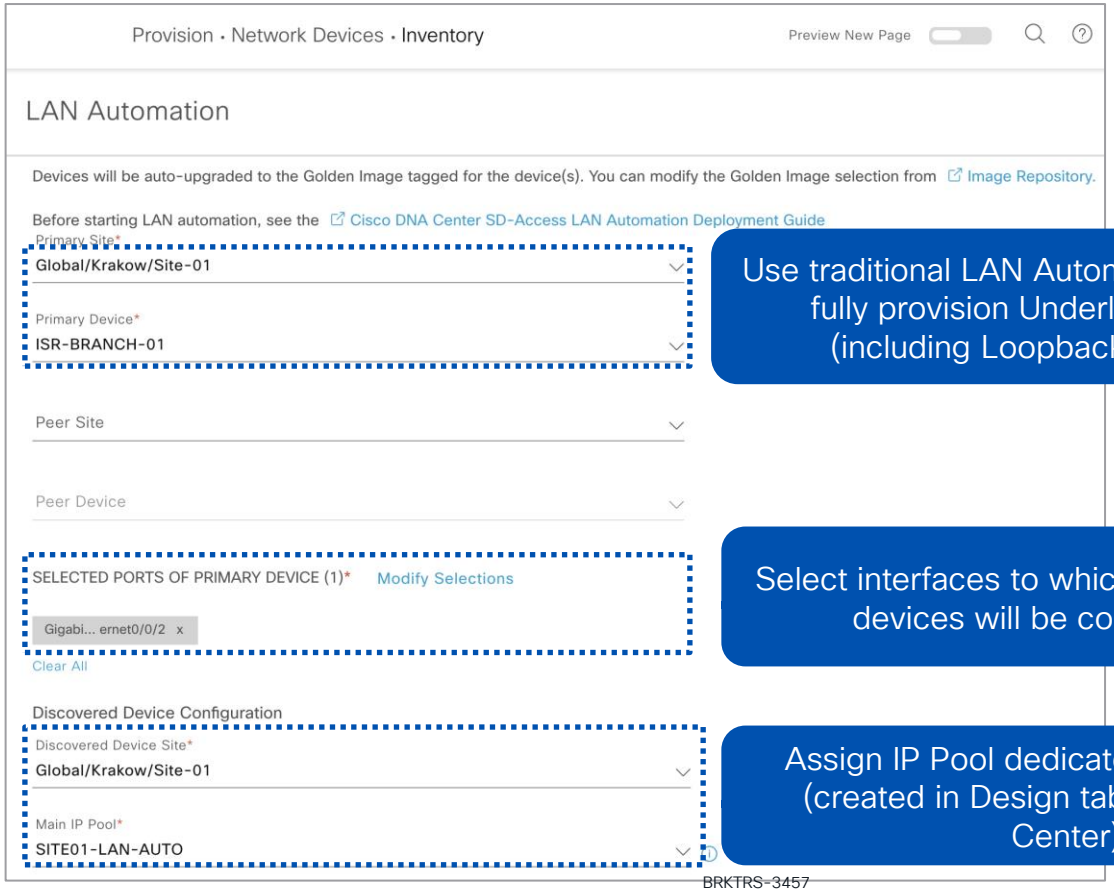
1) Cisco DNA Center fully configures device and converts a link between Seed Device and LAN-automated device to L3 routed access link.

2) DHCP & BDI interfaces are removed from Seed Device as no longer needed.

Cisco DNA Center: LAN Automation



Cisco DNA Center: LAN Automation

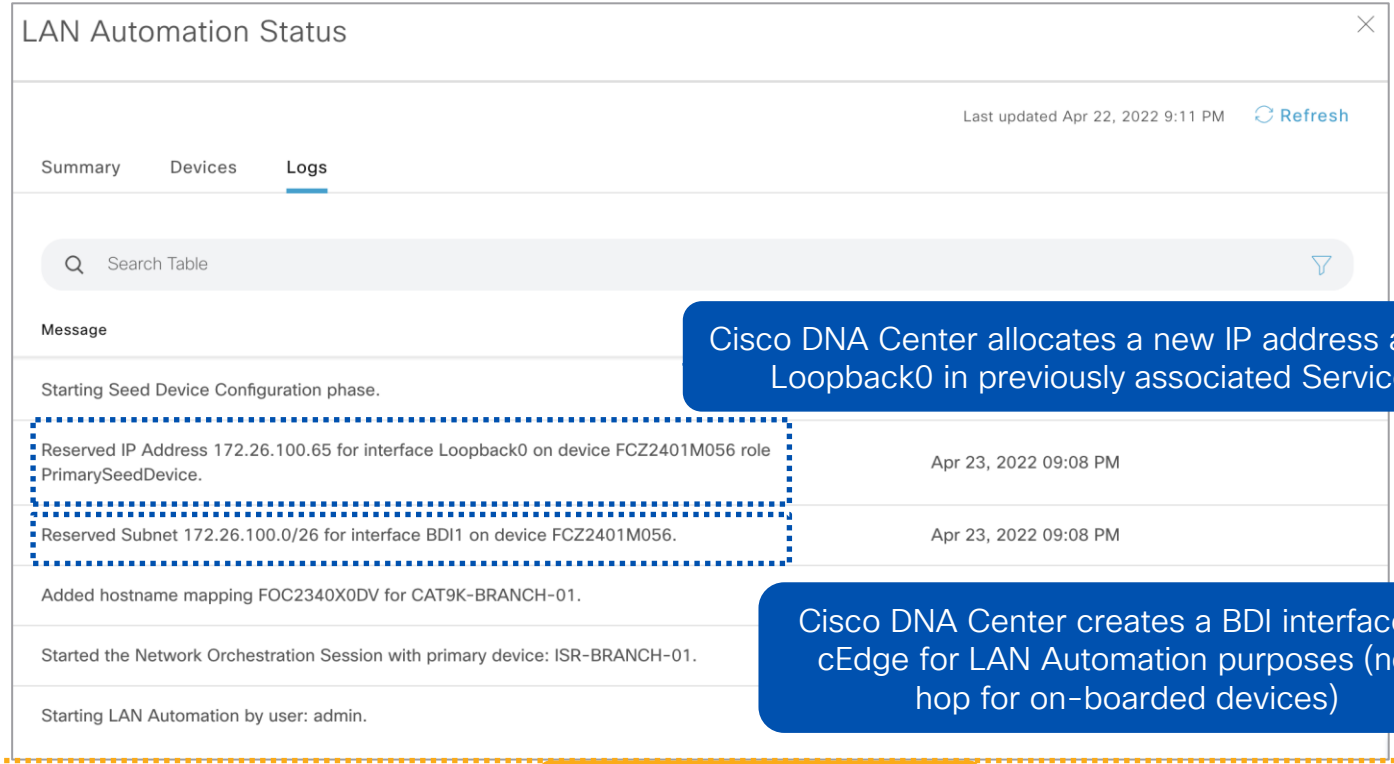


Use traditional LAN Automation workflow to fully provision Underlay on cEdges (including Loopback0 interface)

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



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

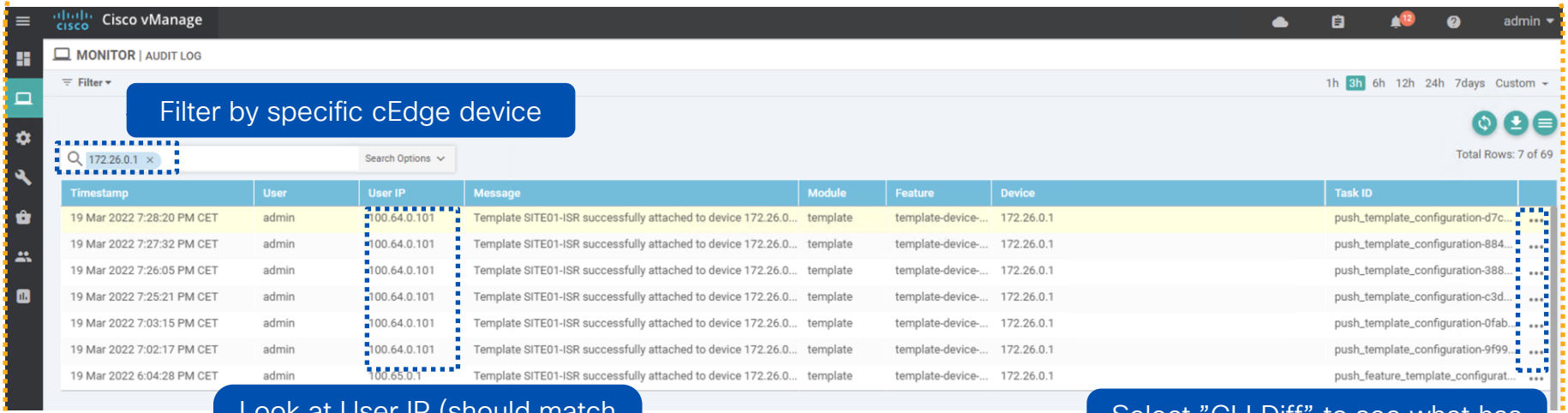
Cisco DNA Center creates a BDI interface on cEdge for LAN Automation purposes (next hop for on-boarded devices)

TROUBLESHOOTING TIP

Audit logs - Configuration Push

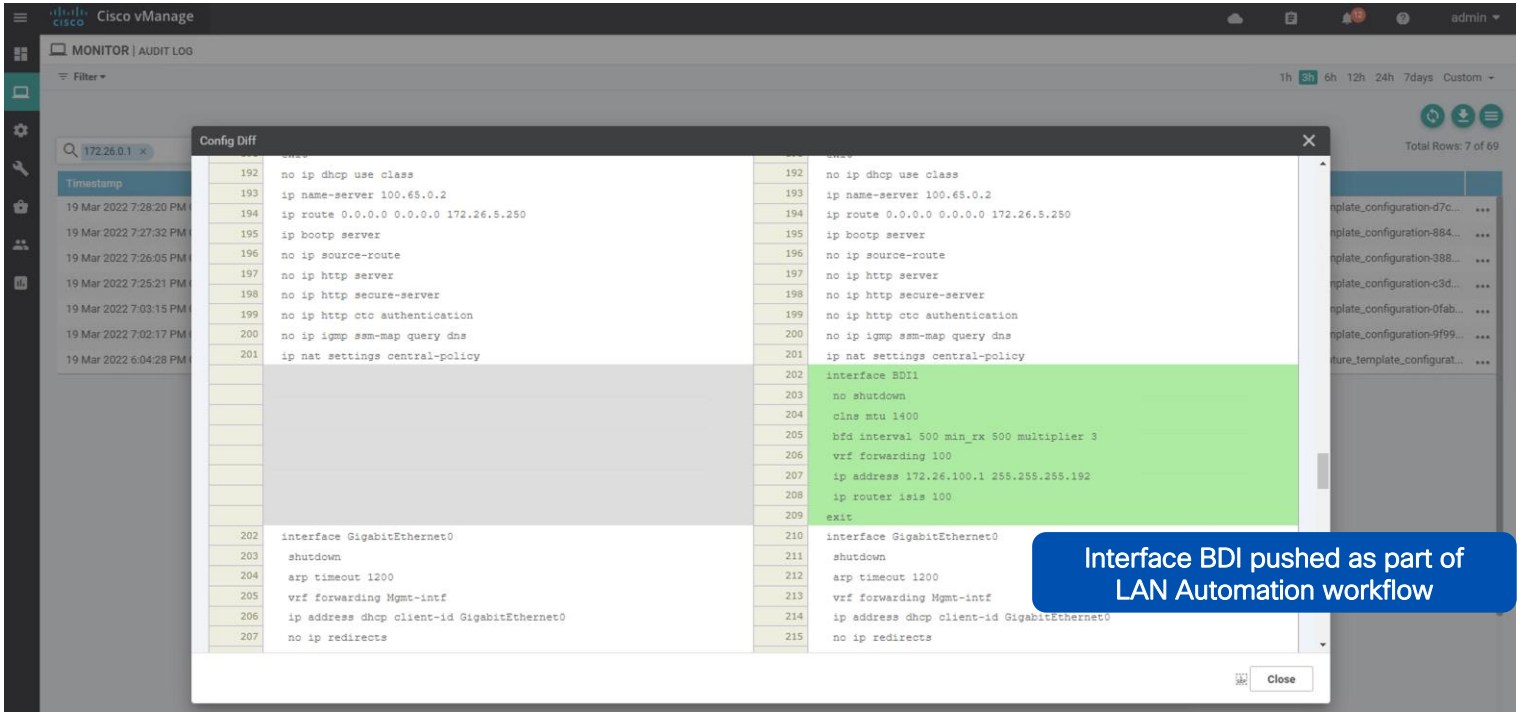
TROUBLESHOOTING TIP

vManage – Configuration Push



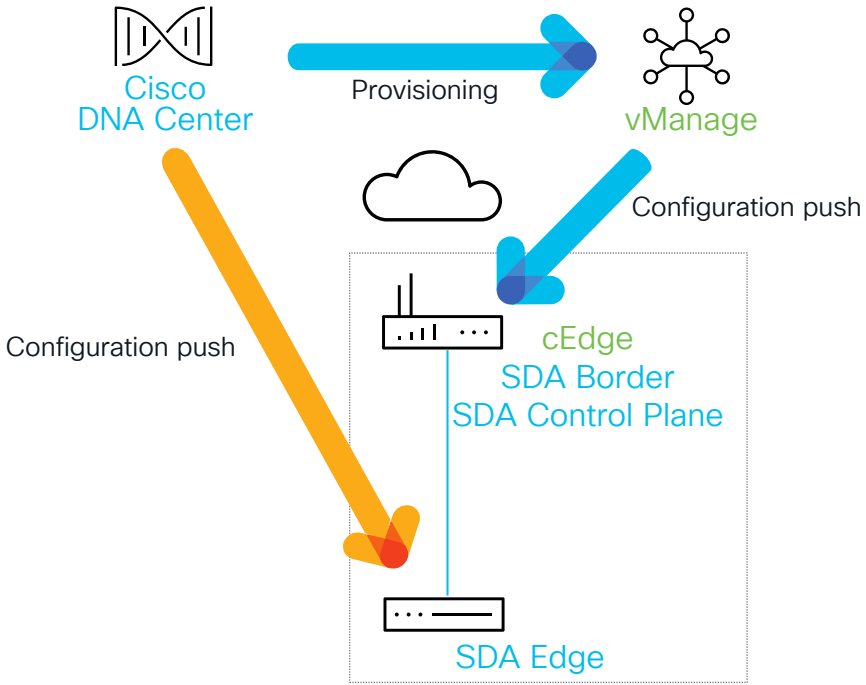
TROUBLESHOOTING TIP

vManage – Configuration Push



TROUBLESHOOTING TIP

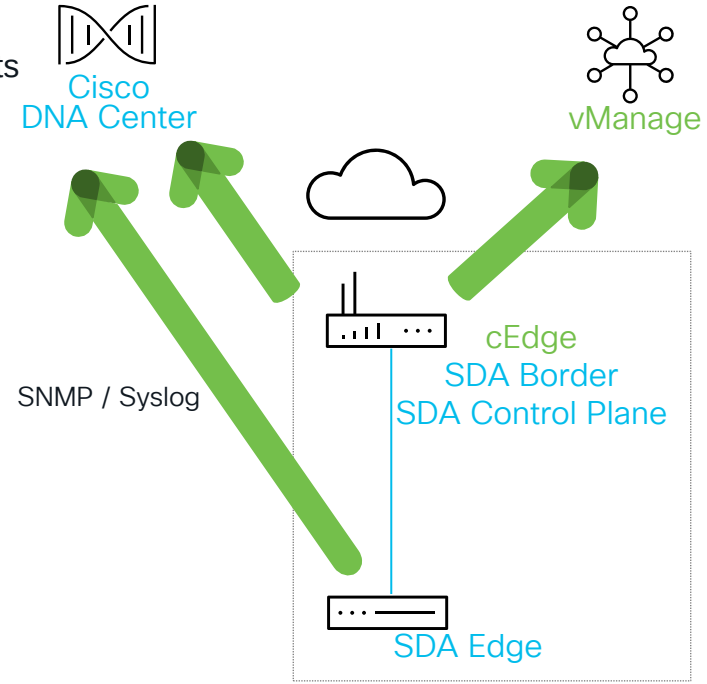
Configuration Push – provisioning workflows



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

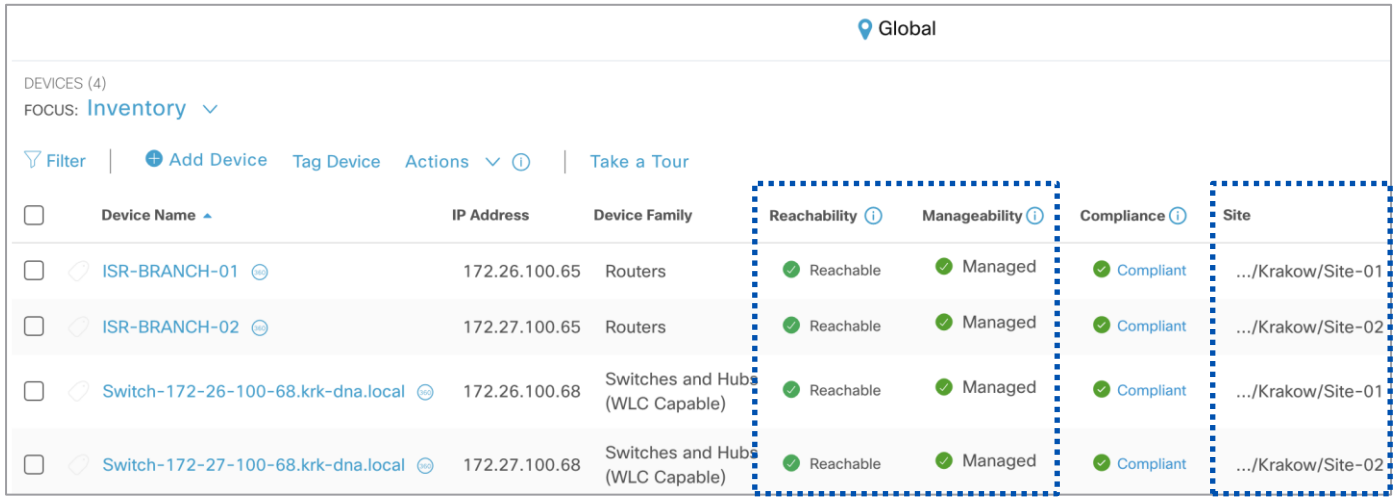
TROUBLESHOOTING TIP

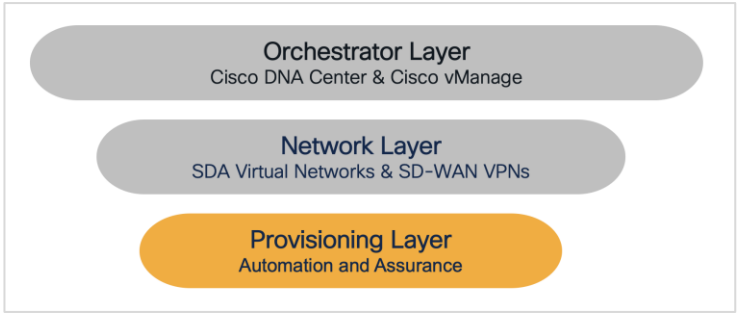
Provisioning Layer

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:





NEW

SDA / SD-WAN Integration

Provisioning Layer: Automation and Assurance

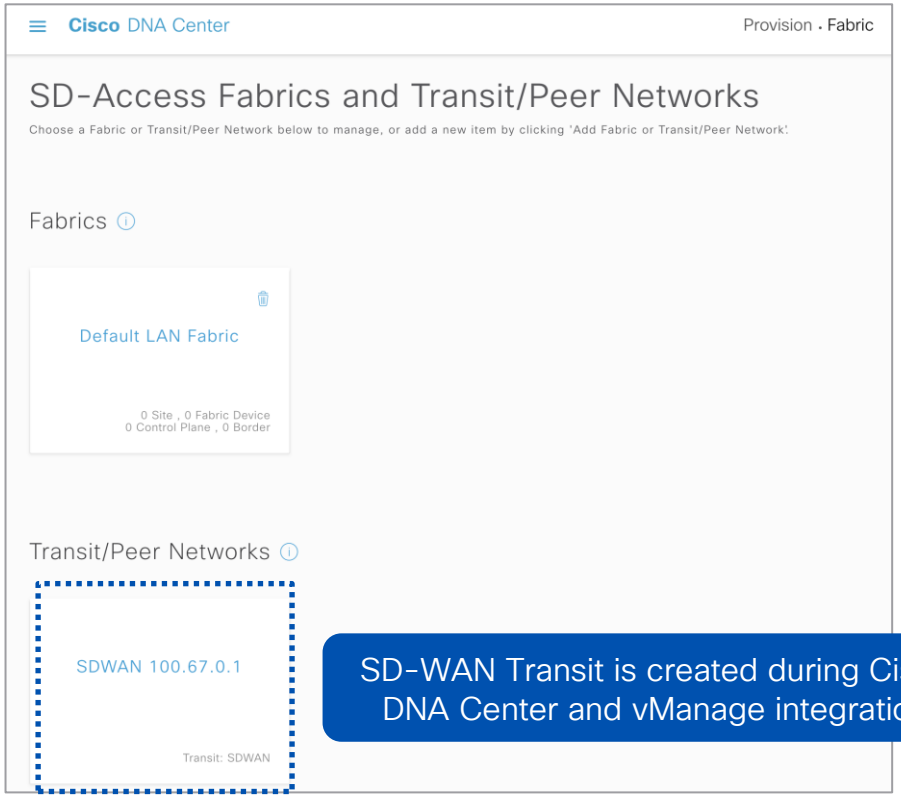
SD-WAN Transit - concept

- 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.

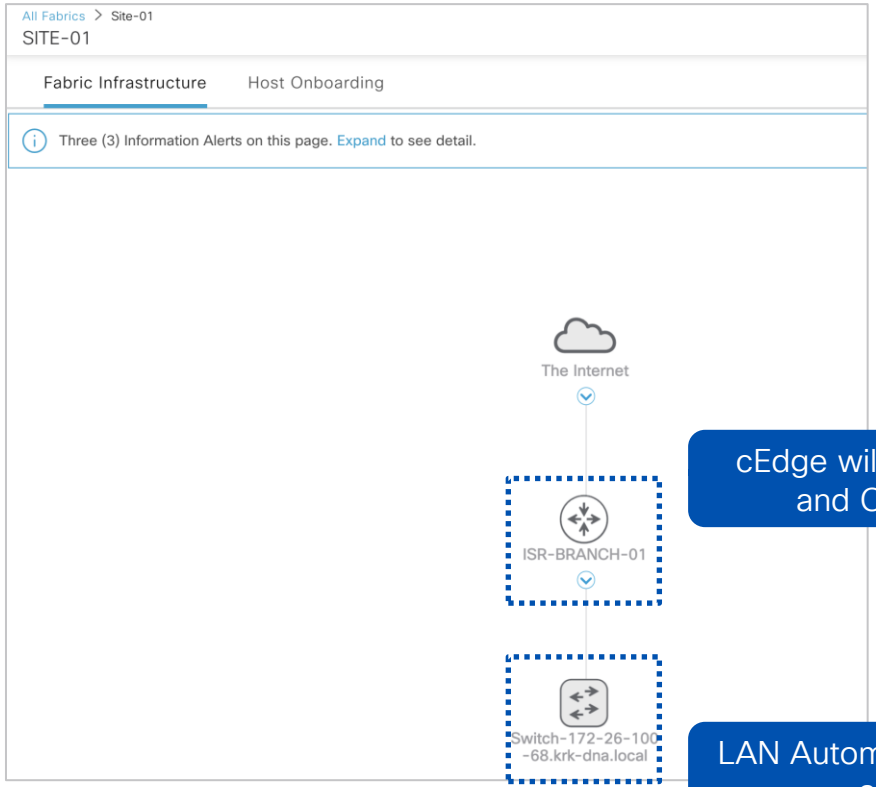
- SD-WAN Transit allows to carry SGT tags end-to-end in the data-plane.

SD-WAN Transit in Cisco DNA Center



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

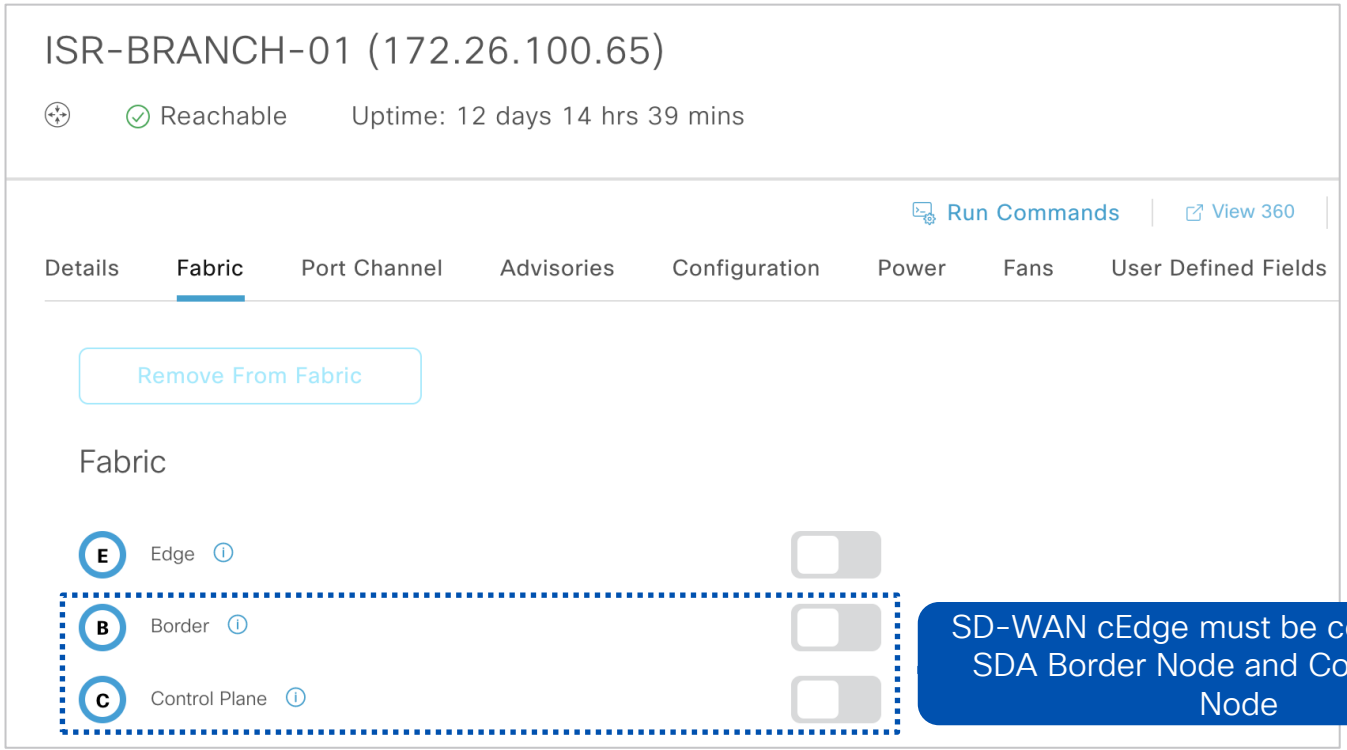
SD-Access Fabric - configuration



cEdge will act as a Border Node and Control Plane Node

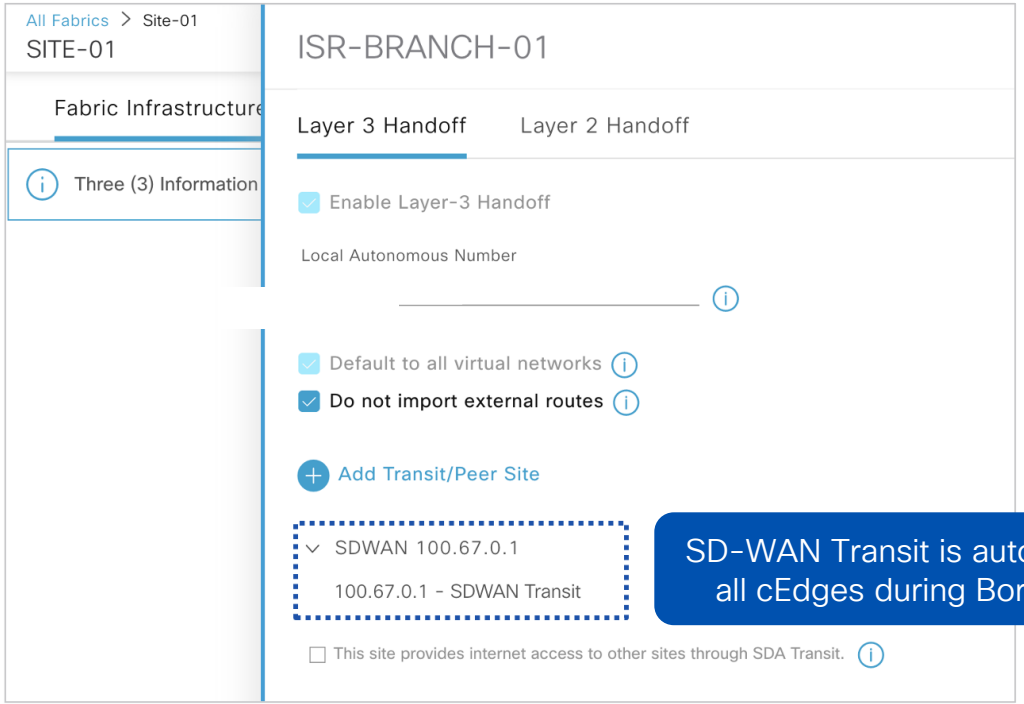
LAN Automated switch will act as an Edge Node

SD-Access Fabric
Border and Control Plane configuration



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

SD-Access Fabric
Border configuration



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

SD-WAN Transit
Summary

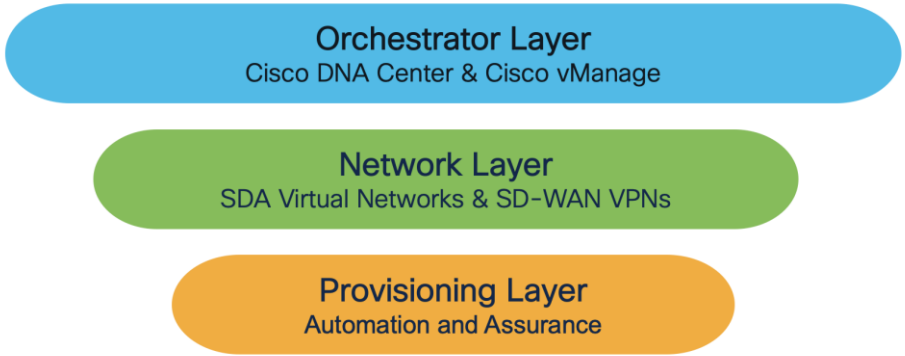
At the end of this stage the status will be as follows:

- 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



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

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

cisco Live!

Thank you


cisco Live!
ALL IN