

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, and then various shades of blue and green. Overlaid on this are large, soft, wavy shapes in similar colors, giving the impression of clouds or liquid waves. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Extending Network Beyond Enterprise Walls

SD-Access and non-SD-Access Approaches

Vinay Saini , Principal Architect , Cisco CX
BRKENS-2832

CISCO *Live!*

#CiscoLive

Cisco Webex App

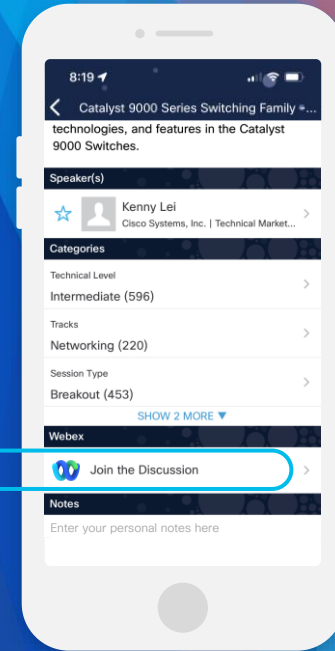
Questions?

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 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2832>

Session Expectations

What is covered

- Cisco SD-Access Network Extensions using IE Switches
- Policy Extension using EN/PEN/SBEN
- Design Architecture SDA OT design
- Design Architecture Non-SDA OT design

What is NOT covered

- Cisco SDA Solution Detail
- Fabric Configuration
- Protocol Details of VXLAN/LISP/CTS

Agenda

SDA-Access Extended Enterprise

- Need and use-cases
- Fabric design with Extended Nodes and Policy Extended Nodes
- Packet Flows and use-cases
- REP Ring Automation using DNA-C

Design and Architecture

- SDA Design adoption for OT environment
- CPwE and SDA extension for OT
- Non-SDA OT design and network extension

Your Presenter Today



Vinay Saini 

Principal Architect – Cisco CX

CCIE Wireless#38448, CWNE#69



Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

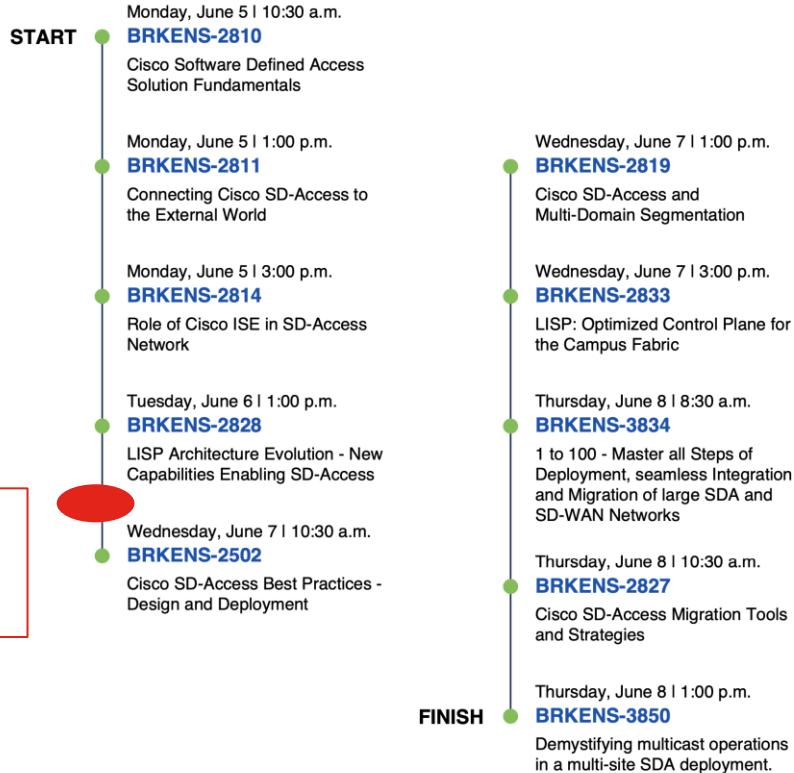


Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

SDA Learning Map



What is Extended SDA Network

Need and Use-cases

Extended Enterprise

Extended Enterprise

Ruggedized Industrial
Networking Products



Non-carpeted/ Outdoor Spaces



Industrial Ethernet and Wireless Devices

Enterprise Fabric



Roadways



Parking Lot



Distribution Center



Airport



Manufacturing

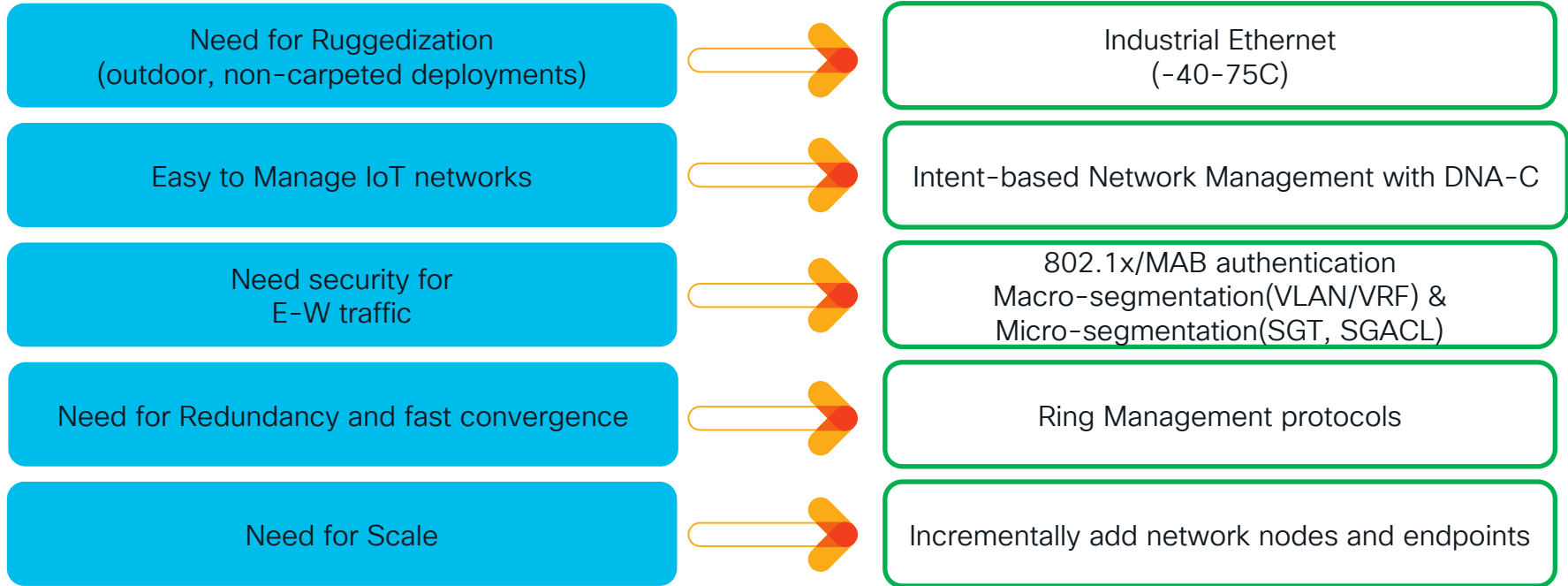


Port/Terminal

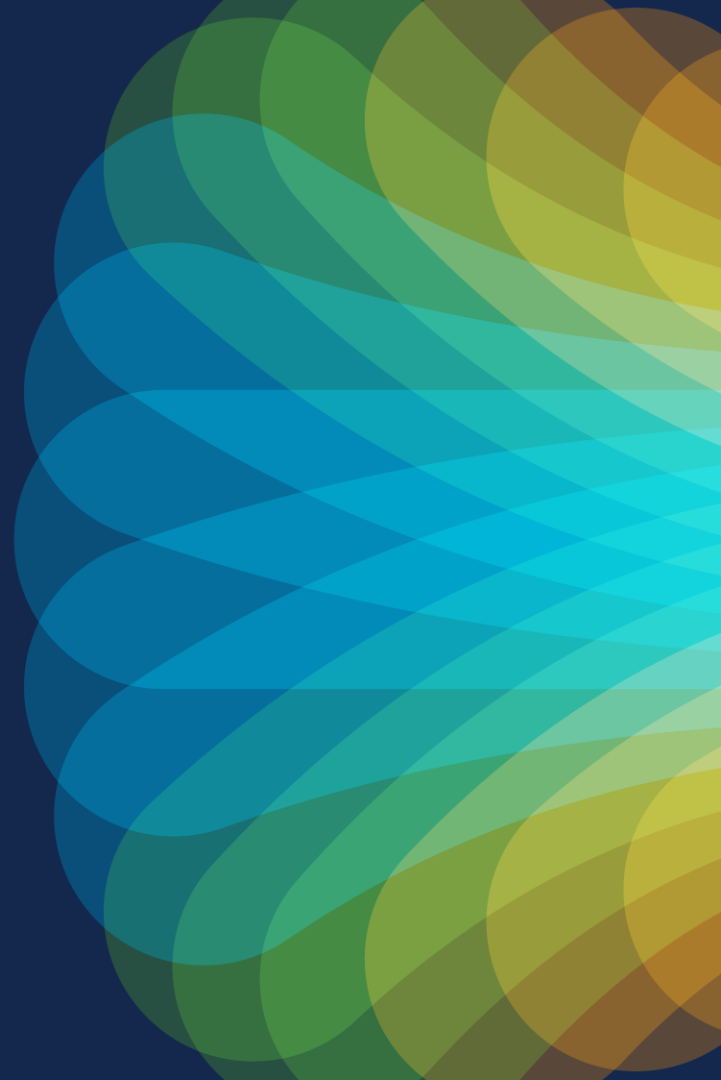


Warehouse

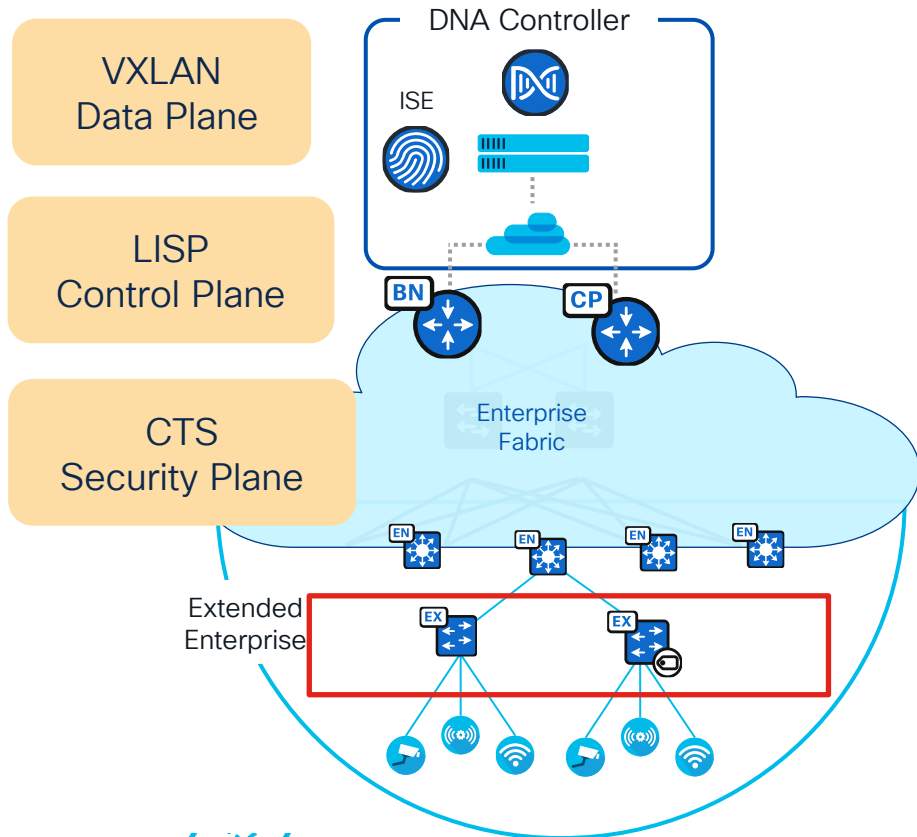
Expectations from this extended network?



Local Extension With Cisco SD-Access

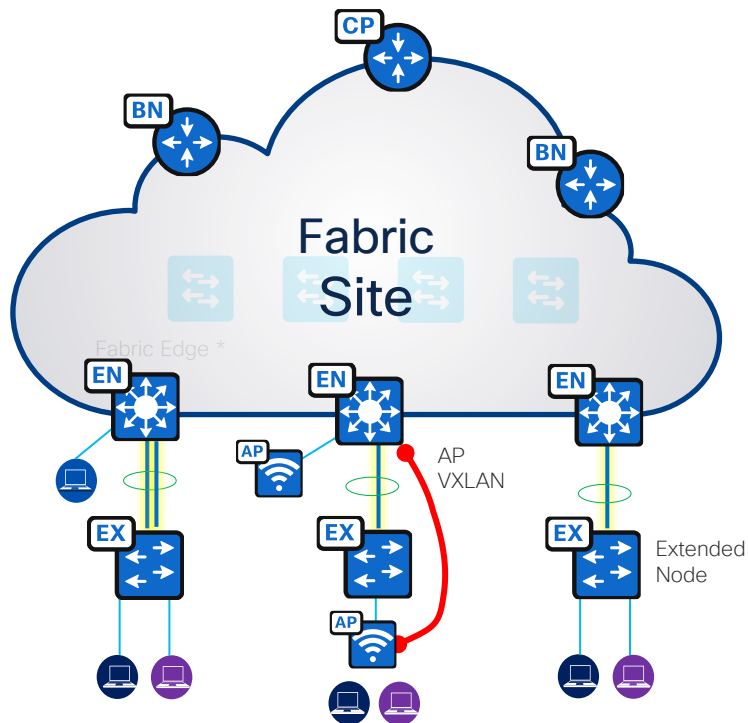


SD – Access Architecture for Extended Networks



- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context.
- **Identity Services Engine** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Control Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Extended Nodes/Policy Extended Nodes** – A Edge access device that connects Wired IoT Endpoints to the SDA Fabric via a Fabric Edge Node

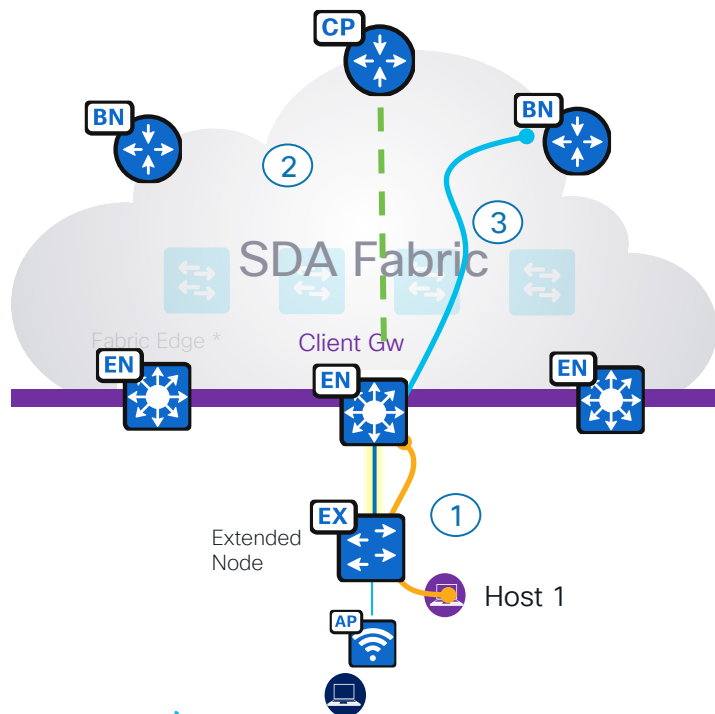
SD-Access Extended Node



- Extended node connects to a single Edge node using an 802.1Q Trunk port and port channel interface.
- The port channel can be over single or multiple links between Extended node and single Edge node.
- Extended node is connected to fabric edge nodes using zero touch plug & play (PNP).

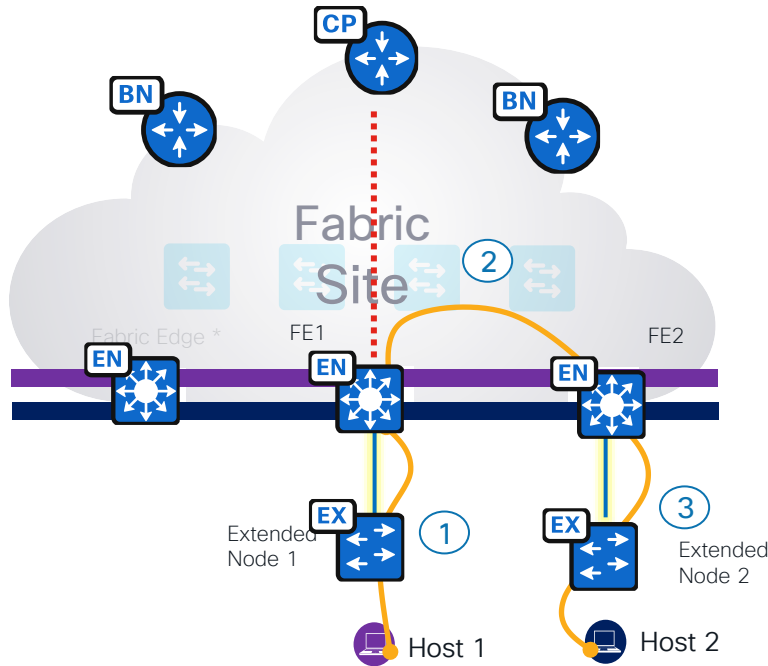
*Separate extended IP Pool needs to be created at DNAC for Extended nodes.

Client External Communication



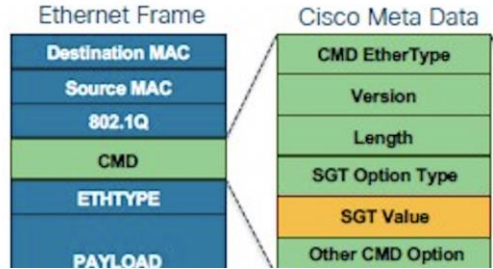
- ① The host connecting to the extended node sends traffic to fabric Edge Node as the default gateway exists on the fabric edge node.
- ② The fabric Edge Node will consult the control plane on where to send traffic.
- ③ Control Plane node tells clients to go via Border node.

Extended Nodes- Host To Host communication



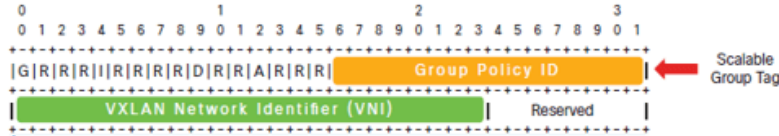
- 1 The host connecting to the extended node sends traffic to fabric edge node as the default gateway exists on the fabric edge node.
- 2 The fabric Edge Node will consult the control plane on where to send traffic and ensures the traffic reaches to the destination (VXLAN encap). In this case it is sent to the other edge node.
- 3 The destination fabric edge sends traffic to the destination host via FE2 and Extended Node 2

SGT – Inline vs VXLAN

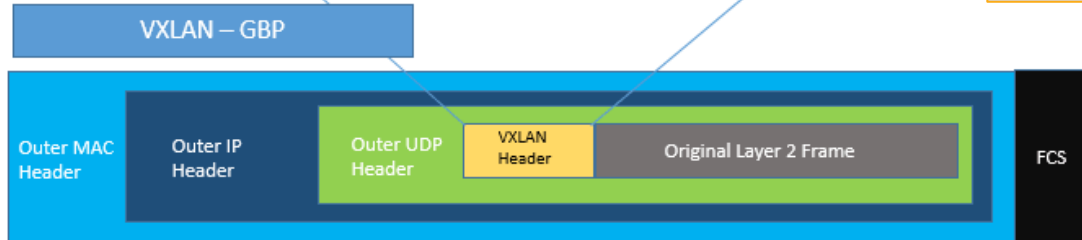


Inline Tagging

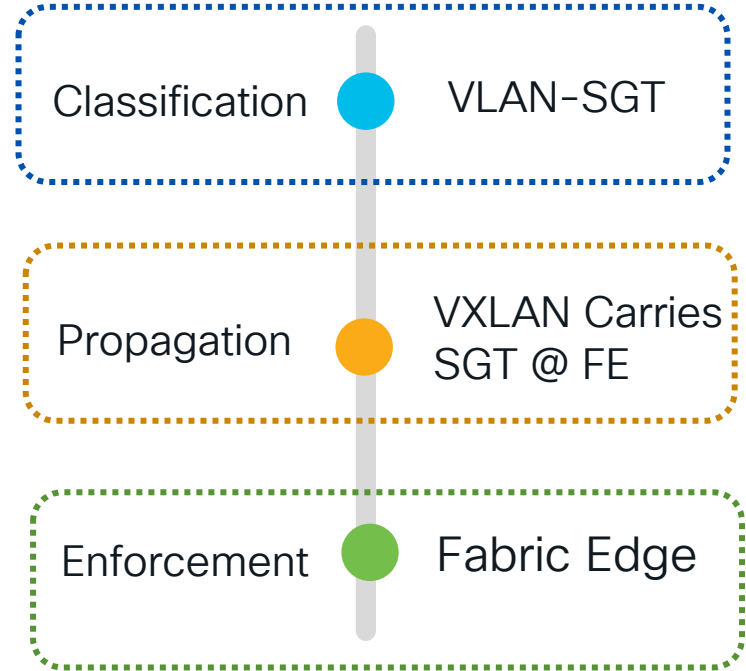
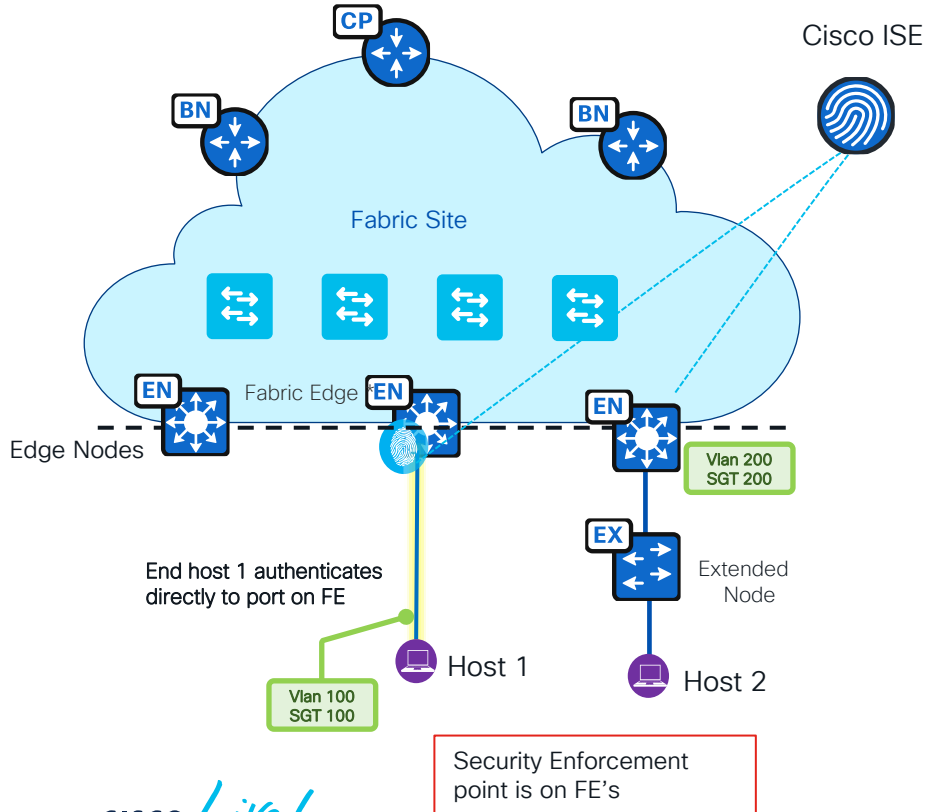
Ethernet frame with the Ethertype set to 0x8909 which indicates a CiscoMetaData header is present.



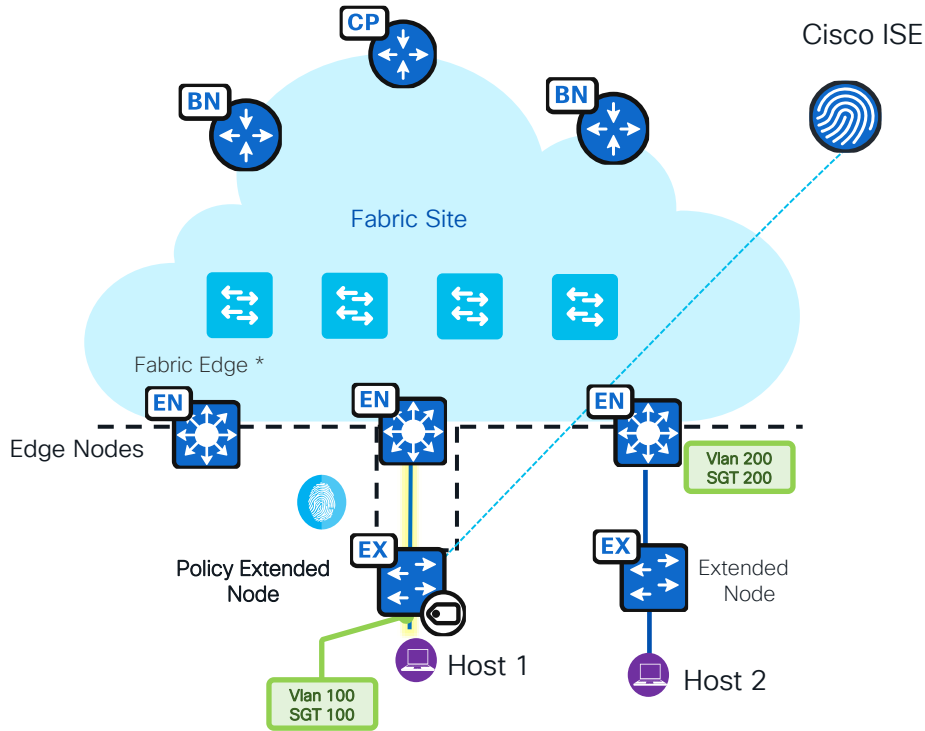
VXLAN Header carrying SGT



Extended Node - Policy Application



Policy Extended Node (PEN)

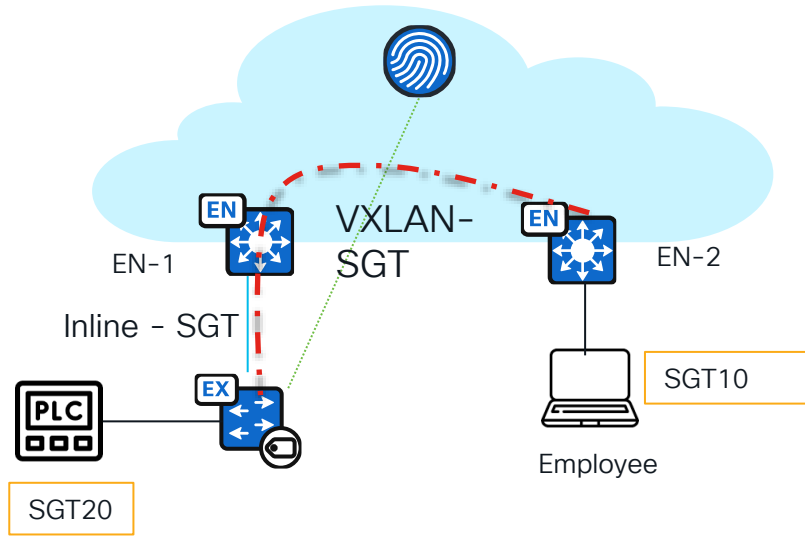


Classification ● SGT @ Port

Propagation ● Inline tagging

Enforcement ● SGACL at PEN

Example SGT and PEN Nodes



Block Employee – PLC Communication

1. Create a policy to block SGT10 to SGT 20 communication
2. PLC authorizes and assigned SGT20
3. Employee Authorizes and assigned SGT10
4. As soon PEN learns about PLC SGT , it downloads policies from ISE.

```
PEN# sh cts role-based permissions
IPv4 Role-based permissions default:
  Permit IP-00
IPv4 Role-based permissions from group 20:Employees to group 10:PLC:
  Deny_IP_Log-00
```

PEN

```
cts role-based enforcement vlan-list 1021-1024
SN-FOC2338V2C6> show cdp neig
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
SN-FOC2338V2CE Gig 1/6          169        R S I      IE-3400-8 Gig 1/6
IE-9K_Fab-Edge Gig 1/7          128        R S I      IE-9310-2 Gig 1/0/17

Total cdp entries displayed : 2
SN-FOC2338V2C6> show runn int gig1/7
Building configuration...

Current configuration : 166 bytes
!
interface GigabitEthernet1/7
 description PNP STARTUP VLAN
 switchport mode trunk
 cts manual
  policy static sgt 8000 trusted
 channel-group 1 mode desirable
end

SN-FOC2338V2C6> show cts pac
AID: 09A36B6CC5A29B316392861C48BB8335
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 09A36B6CC5A29B316392861C48BB8335
  I-ID: FOC2338V2C6
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 17:32:15 UTC Fri Aug 26 2022
PAC-Opaque: 000200B8000300010004001009A36B6CC5A29B316392861C48BB83350006009C0003010099C6F4B234D1E5786564661DB99FCCB5
5B7BA68D1E077DF92008C6DD757EAF5FB821D4CE73FA9031AC67537E741D29081E23E6BC0566C8DB64C2B307B780B553CB0063A3DAEFC9C4EF72
73BF7A389F1F46000FC6582D4A95B30FBE44CB236827A9A05E57B7B1D688B8689FA964A6F36DD58EECD97EDBBE0E
Refresh timer is set for 12w2d
```

EN

```
SN-FDO1931T05Y> show run | inc cts
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authorization network dnac-cts-list group dnac-client-radius-group
SN-FDO1931T05Y> show cts pac
Error occurred while executing command : show cts pac
show cts pac
^
% Invalid input detected at '^' marker.

SN-FDO1931T05Y#
SN-FDO1931T05Y> show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
Cat-9K_Fab_Edge Gig 1/12          163        R S I      C9300-24P Gig 1/0/12
SN-FDO2133U18Y Gig 1/11          129        S I        IE-4000-8 Gig 1/1

Total cdp entries displayed : 2
SN-FDO1931T05Y> show runn inter gi 1/12
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet1/12
 description PNP STARTUP VLAN
 switchport mode trunk
 channel-group 1 mode desirable
end
```

Show CTS PAC
Show CTS Env
Show CTS role-based permission

IE Extended Node, Policy extended node platforms

Extended Node

Industrial Ethernet
IE5000



Catalyst IE3300
Rugged Series



Industrial Ethernet
IE4010



Catalyst IE3400 (H)
Rugged Series



Industrial Ethernet
IE4000



Cisco 3560-CX



Policy Extended Node

Catalyst IE3400
Rugged Series



Catalyst IE3400H
Heavy Duty Series



IE/Cat 9300



IE/Cat 9300 Can act
as EN/PEN/EX
Release: 2.3.3
onwards

DNA Licensing – Extended Node

2 DNA license (Advantage, Essentials)

- Essentials is for pure networking buyers
- Advantage required for SDA Extended Node

License Type	IE2000	IE3000	IE4000	IE4010	IE5000	IE3200	IE3300	IE3400/I E3400H	C3560-CX	CDB
DNA Essentials	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNA Advantage	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

PEN or EN	Switch License	DNAC license
Ext Node	Network Essentials	DNA Advantage
Policy Extended Node	Network Advantage	DNA Advantage

Extended to PEN Node conversion

Cisco DNA Center

Fabric Sites / bgl11

Find Hierarchy

Global

bgl11

Fabric Infrastructure Host O

There are configuration updates available

SN-FCW2507P02R (35.35.35.163)

Reachable Uptime: 20 hrs 53 mins Device Role: ACCESS

Details Fabric Port Channel REP Rings Advisories Configuration

Remove From Fabric

Fabric

Extended Node

Extended Node Attributes

Policy Extended Node

Technology Package License Information:

If you require further assistance please contact us by sending email to export@cisco.com.

Technology-package	Type	Technology-package
Current		Next reboot
network-advantage	Smart License	None
dna-advantage	Subscription Smart License	None

Smart Licensing Status: Smart Licensing Using Policy

EN to PEN Node – Upgrade license , Toggle button

PEN to EN node – Downtime , Remove from fabric

Migrating PEN to Extended Node

- For scenarios customer may have already installed an IE3400/IE3400H as an Extended Node.
 - Remove the Policy Extended Node from the fabric
 - Delete the Policy Extended Node from Inventory
 - Under Provision > Devices > Plug and Play, the device should have been removed.
 - 'Write erase' , Enable the right license and reload the IE3400/IE3400H and it should enter the PNP process and come up as an Extended Node.

Plan Change Window – As devices will be out of operation during migration

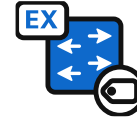
Use-cases



Controlled Inter VLAN access



Controlled Intra-VLAN Access



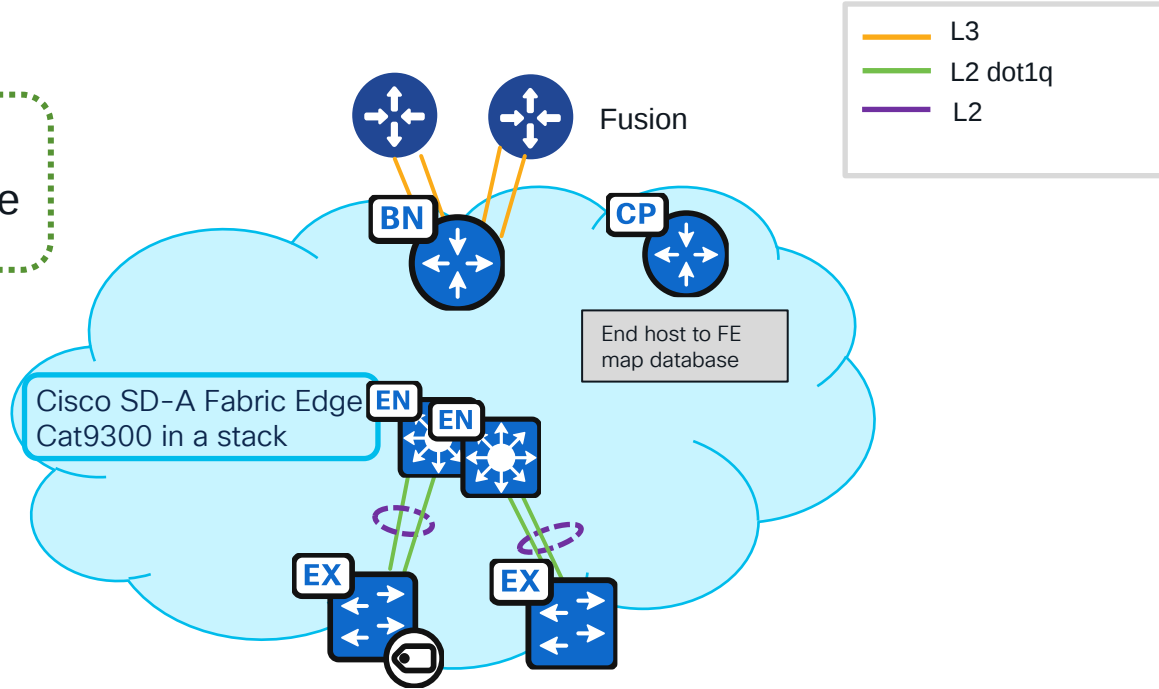
Peer to Peer Blocking within VLAN



Same SGT deny Policy

Supported: Extended node to Stacked FE's

EN/PEN uses Port-channel to connect with Stacked Fabric Edge



REP Rings and Extended Nodes



Network Resiliency Protocols

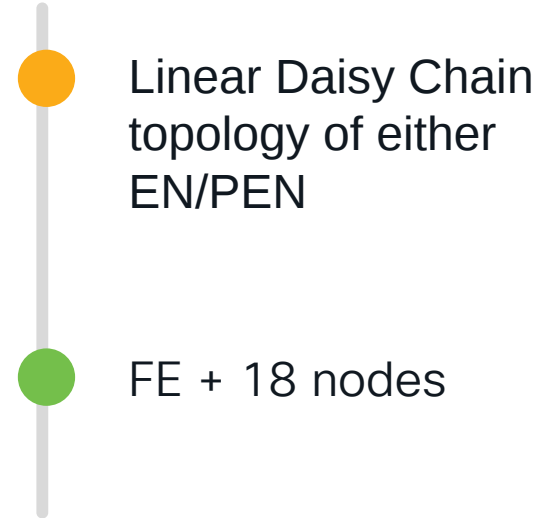
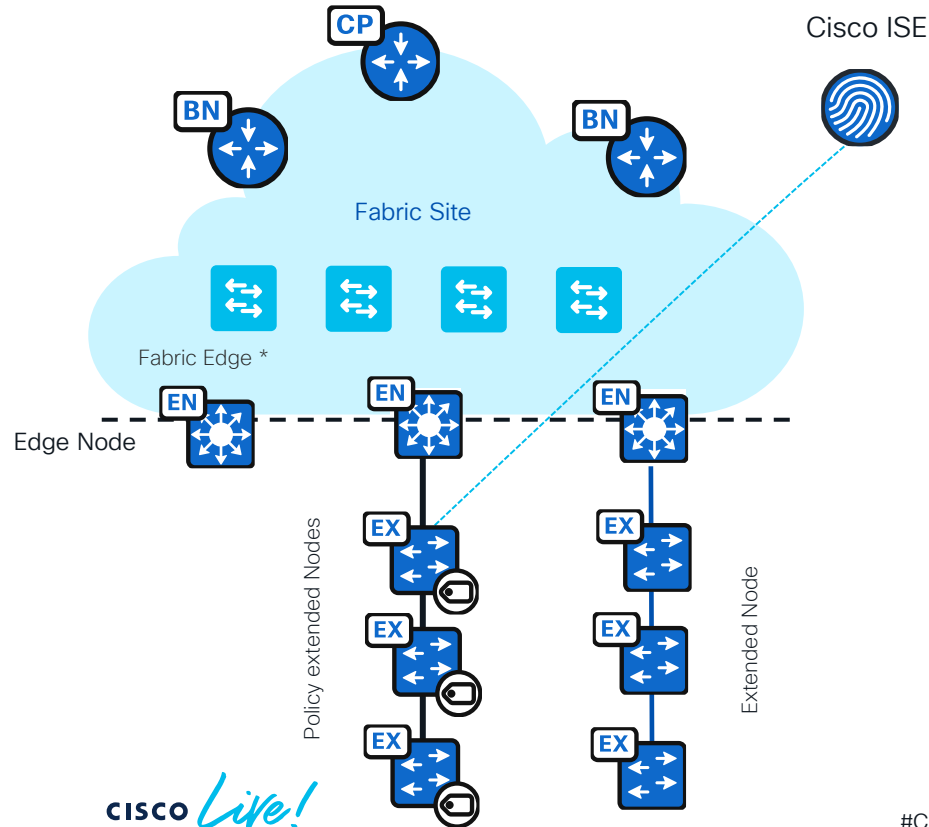
Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Net Conv >250 ms	Net Conv 50-100 ms	Net Conv < 0-10 ms	Layer 3	Layer 2
STP (802.1D)	●	●	●					●
RSTP (802.1w)	●	●	●	●				●
MSTP (802.1s)	●	●	●	●				●
PVST+		●	●	●				●
REP		●			●			●
EtherChannel (LACP 802.3ad)	●		●		●			●
MRP (IEC 62439-2)*	●	●		●	●			●
Flex Links			●		●			
PRP/HSR (IEC 62439)*	●	●	●			●		●
DLR (IEC & ODVA)	●	●				●		●
StackWise		●	●	●			●	●
HSRP		●	●	●			●	
VRRP (IETF RFC 3768)	●	●	●	●			●	

Process and Information

Time Critical

Loss Critical

Daisy Chain- Extended Node

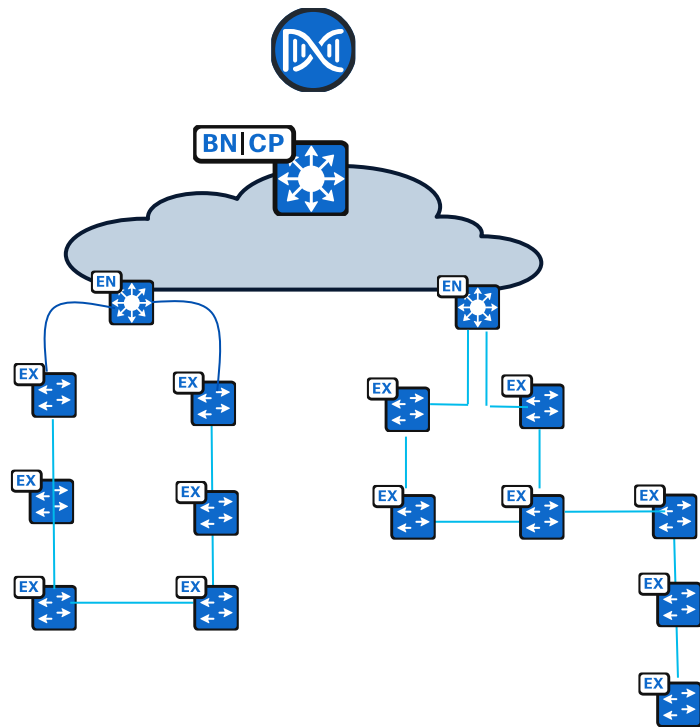


Available from DNA-C Release : 2.2.x (GA)

Supported Topologies

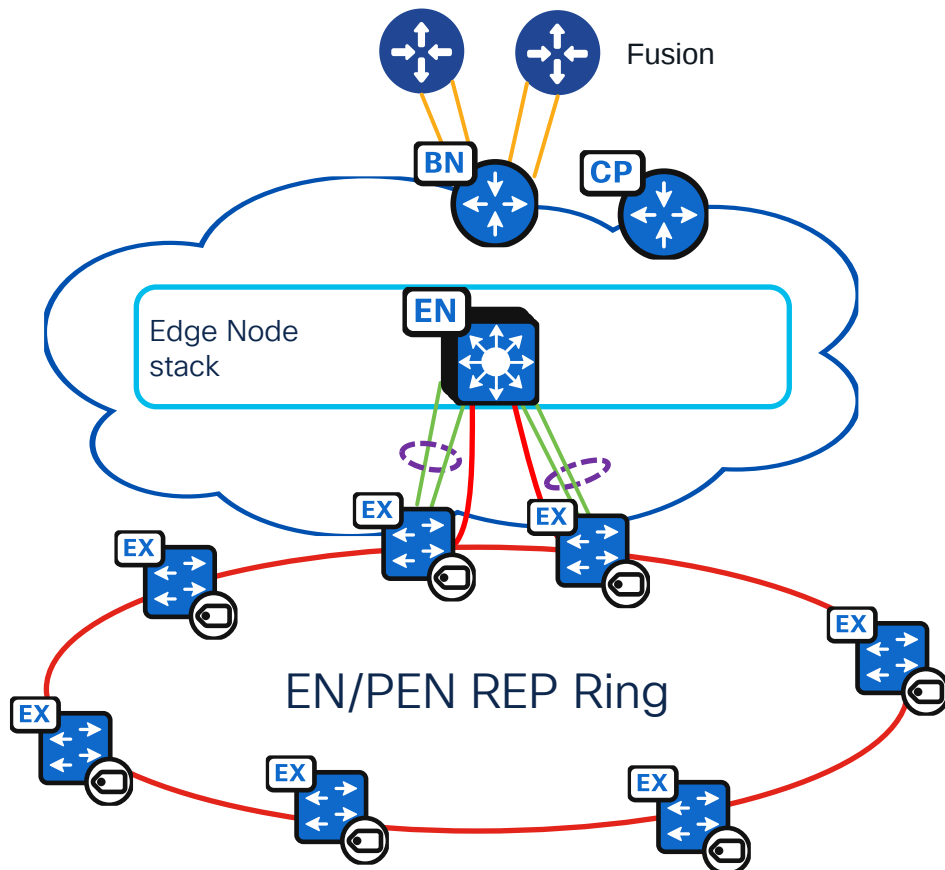
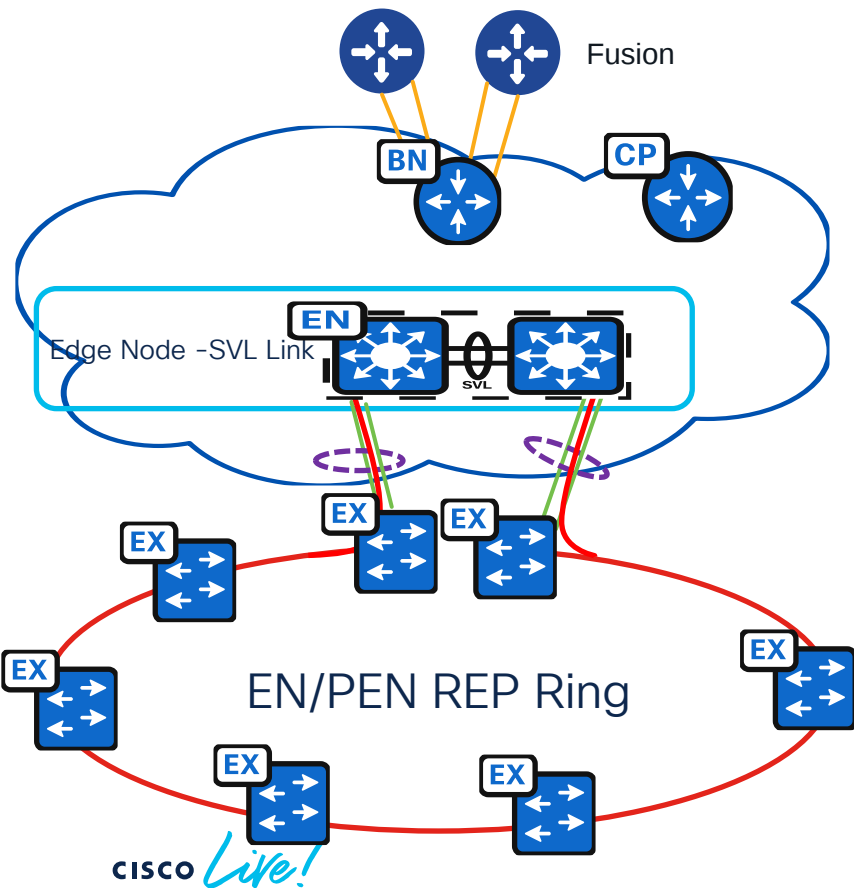
- A simple ring with all Ext-Nodes or all Policy Ext-Nodes is only supported.
- An EN Daisy chain can be attached to a EN REP ring.
- PEN Daisy chain can be attached to a PEN REP ring.

Do not mix PEN and Extended nodes in ring

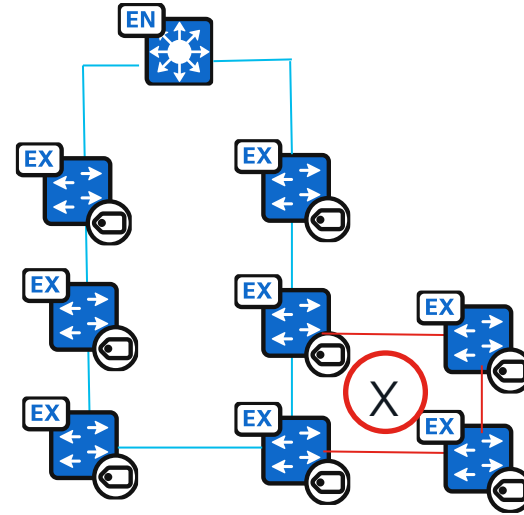
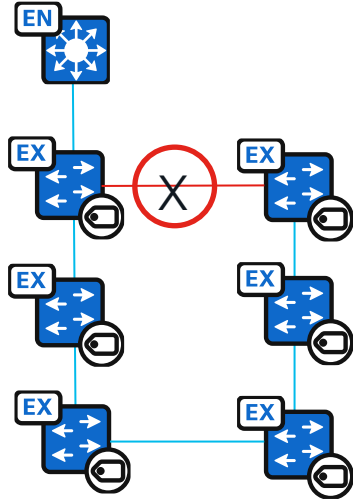


Supported Topologies

Available from DNA-C Release : 2.2.3

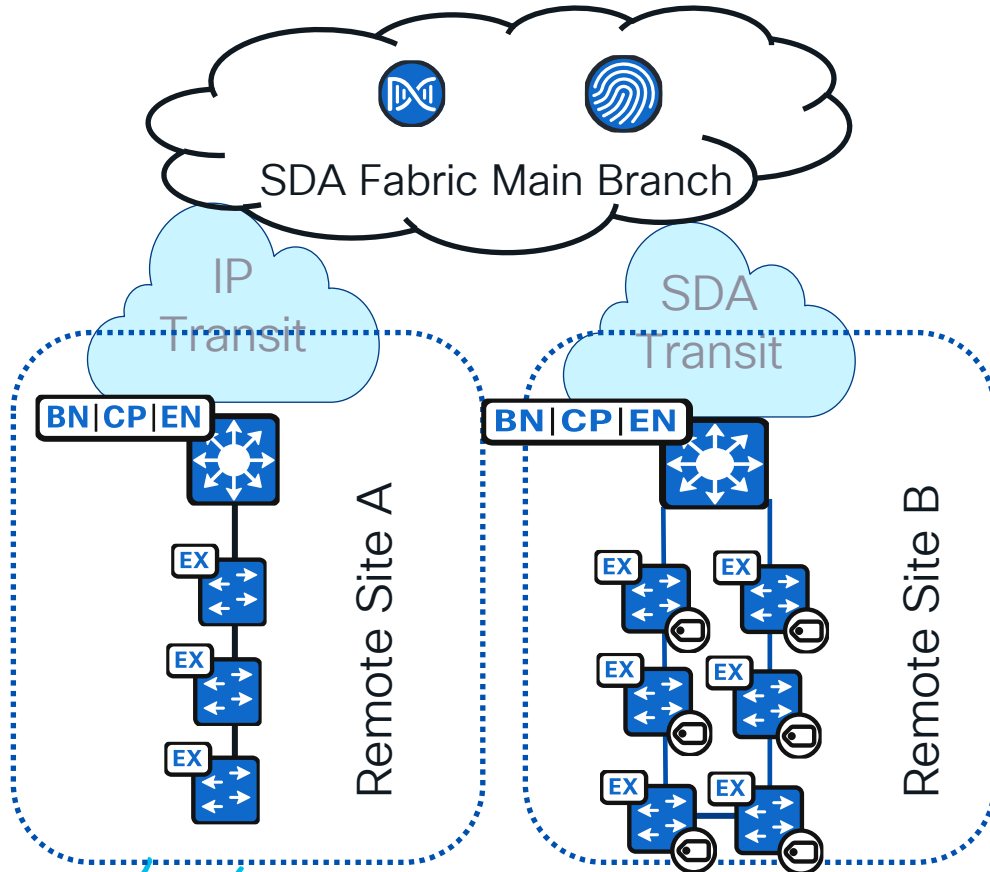


Un-Supported Topologies



- A closed ring connected to a Fabric Edge
- Ring of rings, ring attached to a ring and multiple rings within a given ring are not supported

Fabric in a Box (FIAB) – Network Extensions



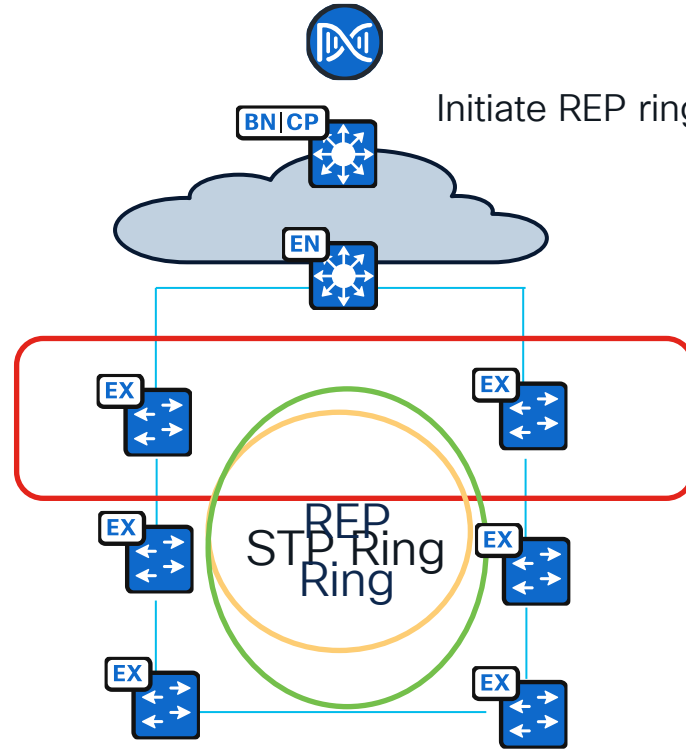
- Border , Control and Edge all in one device
Supports EN/PEN topologies
- Ring and Daisy Chain support
- Allows remote Extension

REP automation

How it works

REP Automation – How it works.

- Onboard STP Ring
- Initiate REP workflow from DNAC
- REP ring ready



Available from DNA-C Release : 2.2.3 onwards

DNA-C REP Configuration

IE-9K__Fab-Edge (42.1.2.36)

  Reachable Uptime: 3 days 23 hrs 13 mins

REP Rings / BGL_18_Parking - Workflow steps

- >  Start Ring Discovery
- >  Discover Ring Members
- >  Configure Devices

- Started shutdown of port interface Port-channel4 on IE-9K__Fab-Edge at May 30, 2022, 9:50:57 AM.
- Completed shutdown of port interface Port-channel4 on IE-9K__Fab-Edge successfully at May 30, 2022, 9:51:07 AM.
- Started configuration of REP segmentation in Port-channel1 on SN-FOC2312V0KL at May 30, 2022, 9:51:07 AM.
- Completed configuration of REP segmentation in Port-channel1 on SN-FOC2312V0KL successfully at May 30, 2022, 9:51:28 AM.
- Started EEM script configuration for Ping on SN-FOC2312V0KL at May 30, 2022, 9:51:28 AM.
- Completed EEM script configuration for Ping on SN-FOC2312V0KL at May 30, 2022, 9:51:38 AM.
- Started configuration of REP segmentation in Port-channel2 on SN-FD01944U0UU at May 30, 2022, 9:51:38 AM.
- Completed configuration of REP segmentation in Port-channel2 on SN-FD01944U0UU successfully at May 30, 2022, 9:51:49 AM.
- Started EEM script configuration for Ping on SN-FD01944U0UU at May 30, 2022, 9:51:49 AM.
- Completed EEM script configuration for Ping on SN-FD01944U0UU at May 30, 2022, 9:51:59 AM.
- Started configuration of REP segmentation in Port-channel2 on SN-FOC2320V08S at May 30, 2022, 9:51:59 AM.
- Completed configuration of REP segmentation in Port-channel2 on SN-FOC2320V08S successfully at May 30, 2022, 9:52:20 AM.
- Started EEM script configuration for Ping on SN-FOC2320V08S at May 30, 2022, 9:52:20 AM.
- Completed EEM script configuration for Ping on SN-FOC2320V08S at May 30, 2022, 9:52:30 AM.
- Started configuration of REP segmentation in Port-channel2 on SN-FOC2301V3TJ at May 30, 2022, 9:52:30 AM.
- Completed configuration of REP segmentation in Port-channel2 on SN-FOC2301V3TJ successfully at May 30, 2022, 9:52:53 AM.
- Started EEM script configuration for Ping on SN-FOC2301V3TJ at May 30, 2022, 9:52:53 AM.
- Completed EEM script configuration for Ping on SN-FOC2301V3TJ at May 30, 2022, 9:53:26 AM.
- Started configuration of REP segmentation in Port-channel2 on SN-FCW24110H0A at May 30, 2022, 9:53:26 AM.
- Completed configuration of REP segmentation in Port-channel2 on SN-FCW24110H0A successfully at May 30, 2022, 9:53:48 AM.
- Started EEM script configuration for Ping on SN-FCW24110H0A at May 30, 2022, 9:53:48 AM.

IE-9K__Fab-Edge (42.1.2.36)

  Reachable Uptime: 3 days 23 hrs 7 mins

REP Rings / BGL_18_Parking

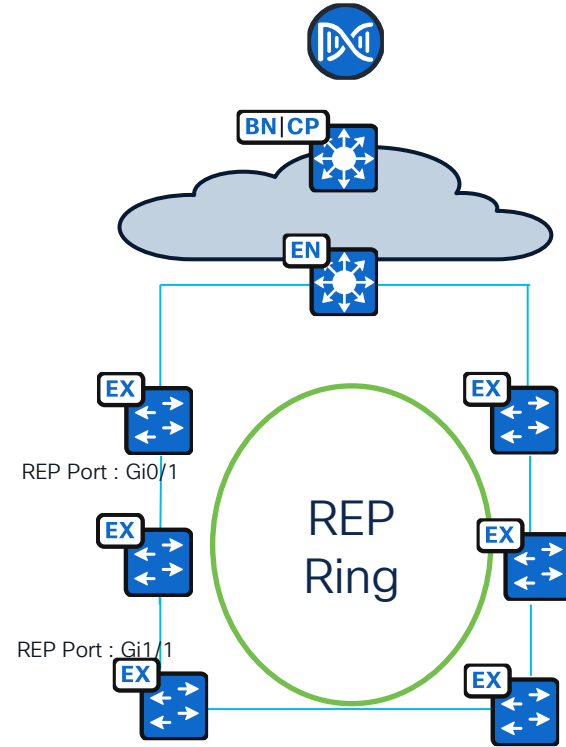
REP Topology Status:

REP Segment 1 BridgeName	PortName	Edge	Role
IE-9K__Fab-Edge	Po3	Pri	Open
SN-FCW24110H0A	Po1		Open
SN-FCW24110H0A	Po2		Open
SN-FOC2301V3TJ	Po1		Open
SN-FOC2301V3TJ	Po2		Alt
SN-FOC2320V08S	Po1		Open
SN-FOC2320V08S	Po2		Open
SN-FD01944U0UU	Po1		Open
SN-FD01944U0UU	Po2		Open
SN-FOC2312V0KL	Po2		Open
SN-FOC2312V0KL	Po1		Open
IE-9K__Fab-Edge	Po4	Sec	Open

Ring Operations : Deleting the node

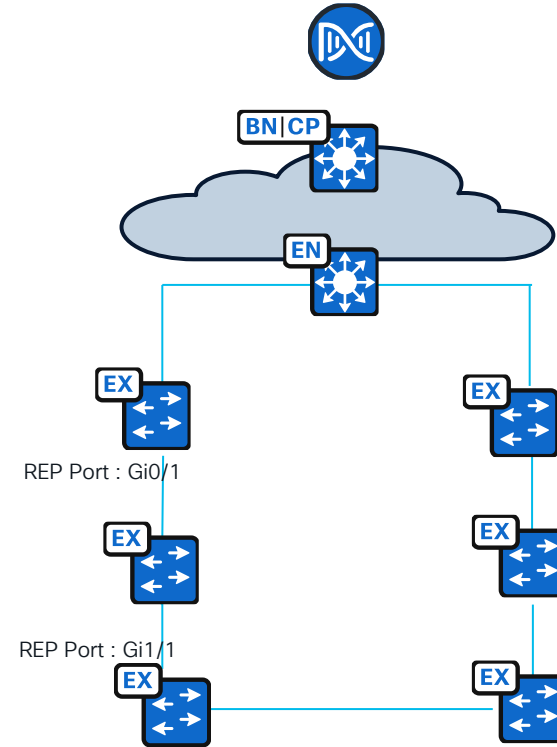
- Remove faulty EN/PEN Node
- Connect REP ports back
- Node part of REP ring

Available from 2.3.2.x



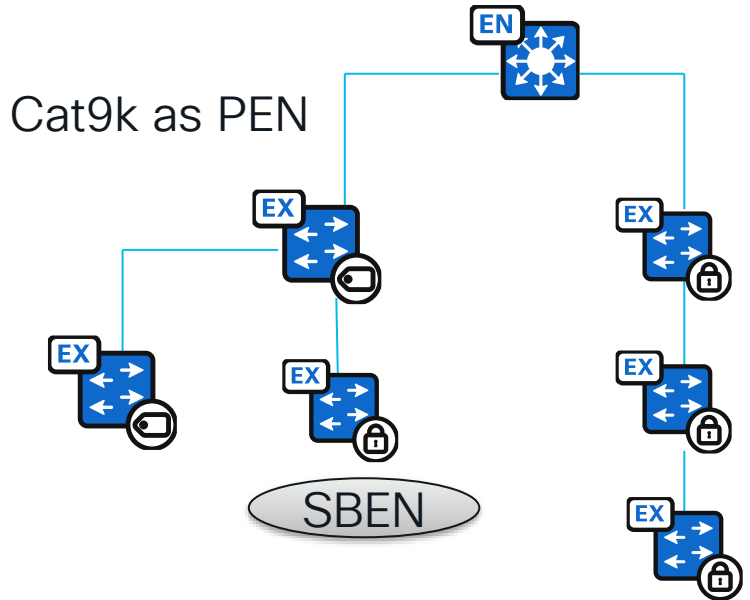
Ring Operations : Adding a node

- Delete REP Ring
- Insert new EN/PEN
- STP Discovery and REP Workflow
- Ring ready



Deletion and re-creation of REP is required

Supplicant Based EN – CAT9k only

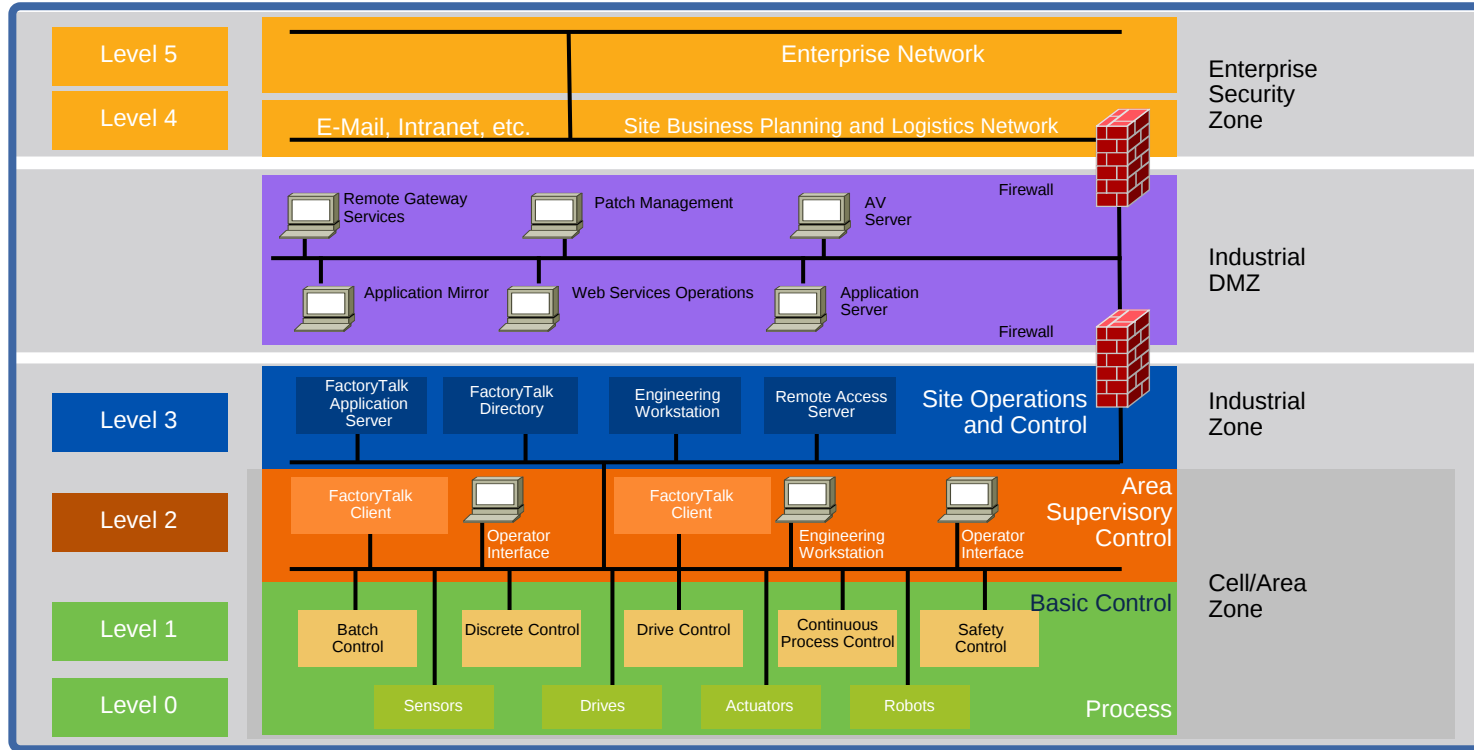


- 802.1x for SBEN
- onboarding
- Max 3 node Daisy Chain
- No REP ring
- PEN/SBEN mix

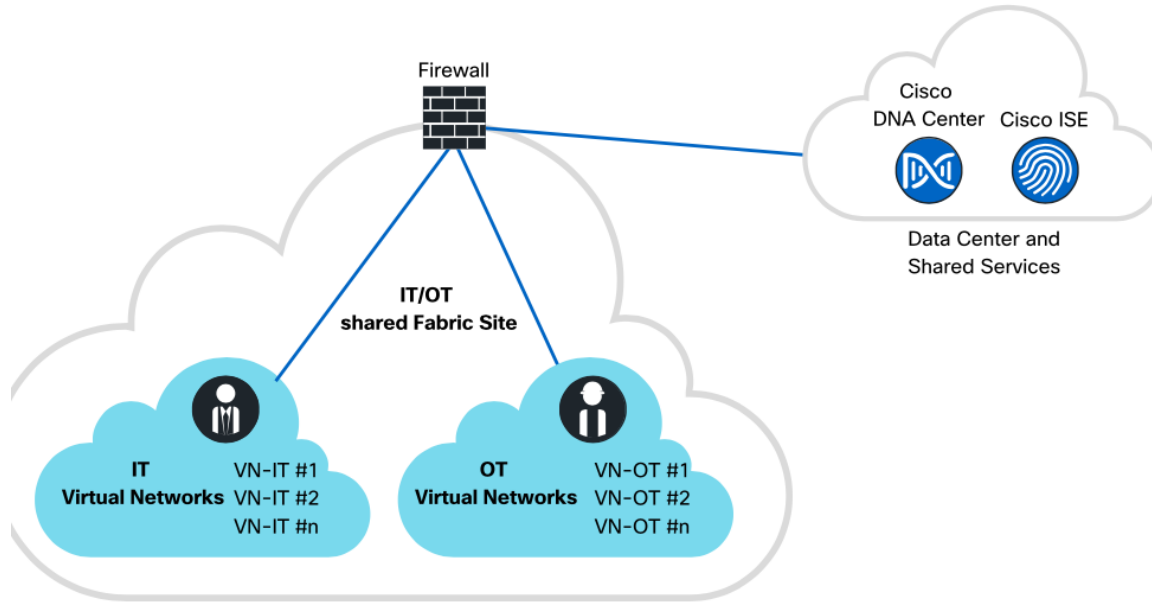
Available from DNAC 2.3.3 onwards

Built on Industry Standards

Purdue/IE62443 Reference Model

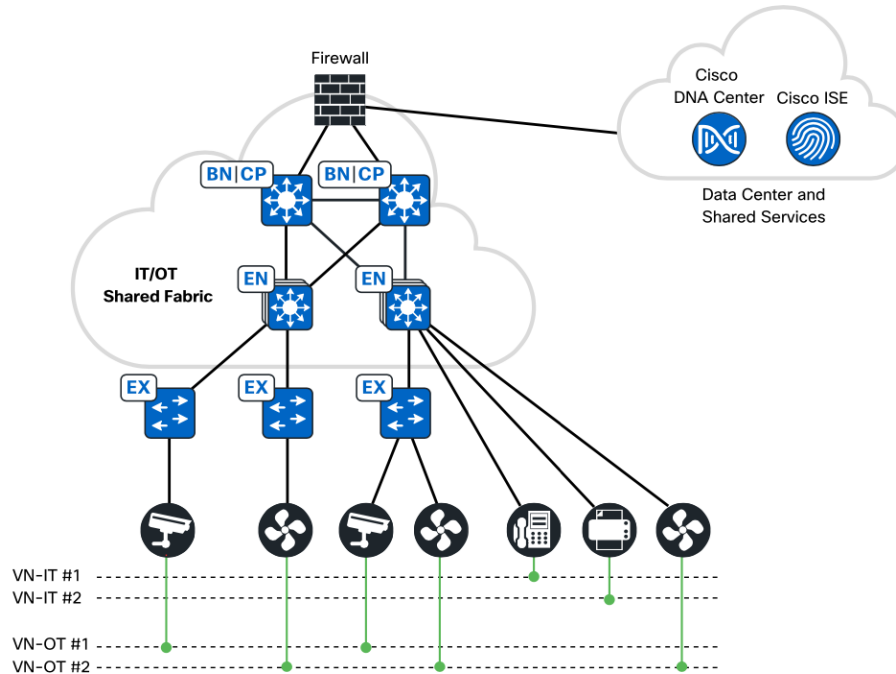


Shared IT and OT SD-Access Fabric



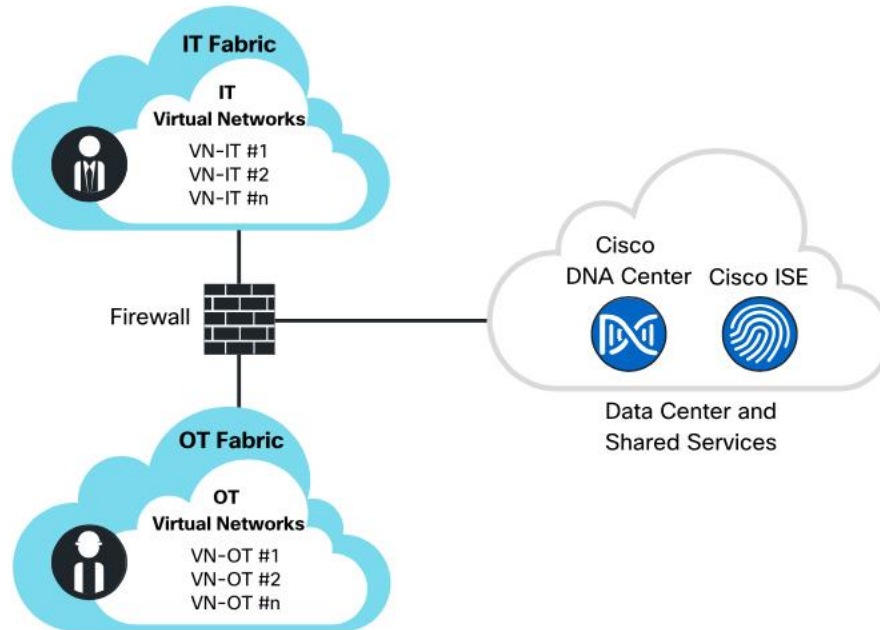
- Simplest Design approach.
- Re-use same H/w
- Not compliant with Purdue model

Shared IT-OT Physical Topology



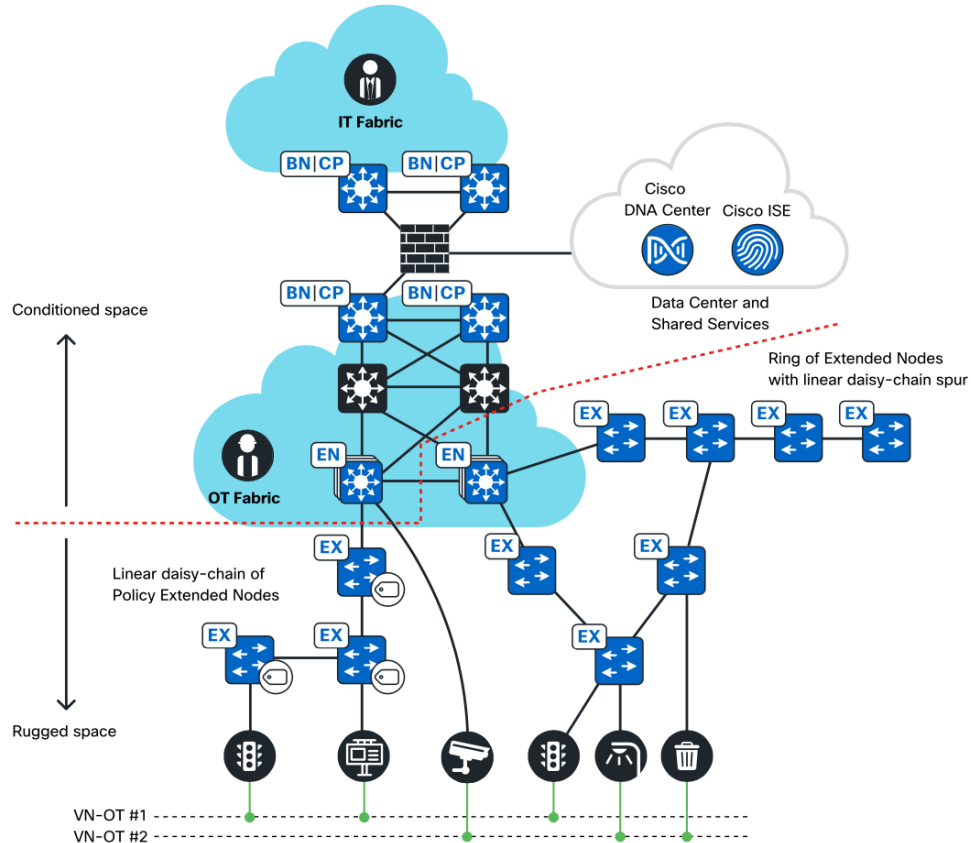
- Edge and Ex nodes Static or Dynamic VN/VLAN Provisioning.
- Inter VN Traffic IT/OT is controlled by Firewall

Dedicated IT and OT Access Sites



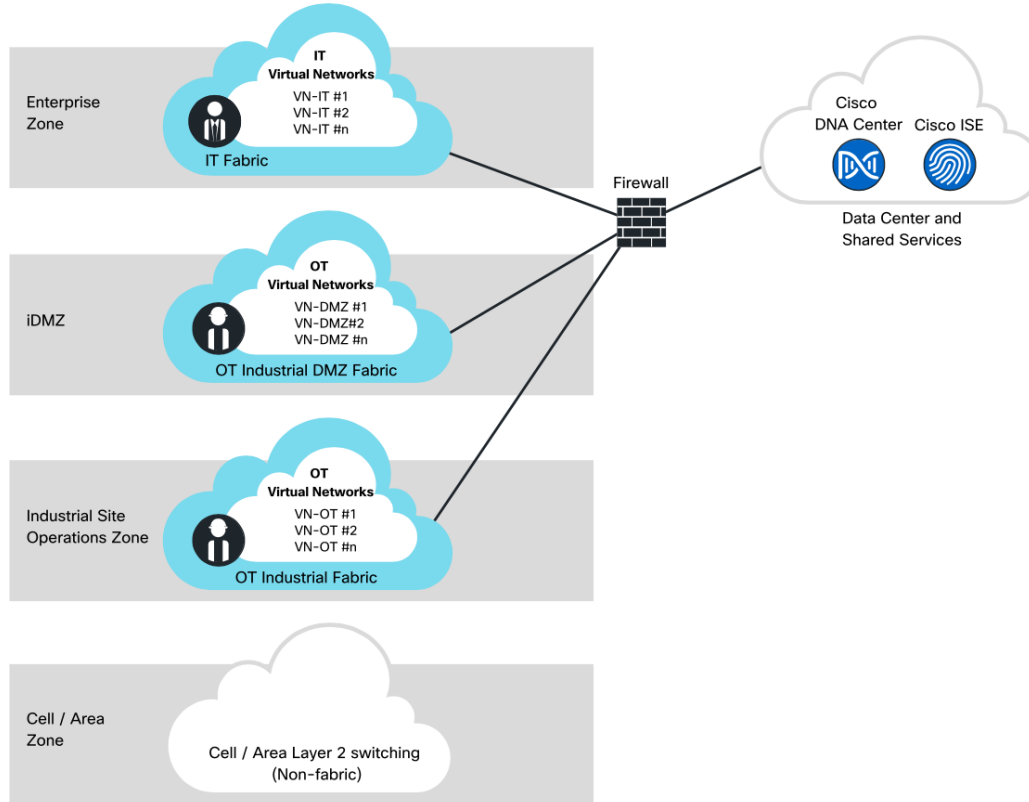
- Each site hands off VNs to the firewall
- Firewall provides shared services access to data center and other services – DHCP, DNS etc.

Dedicated OT Site Physical Topology



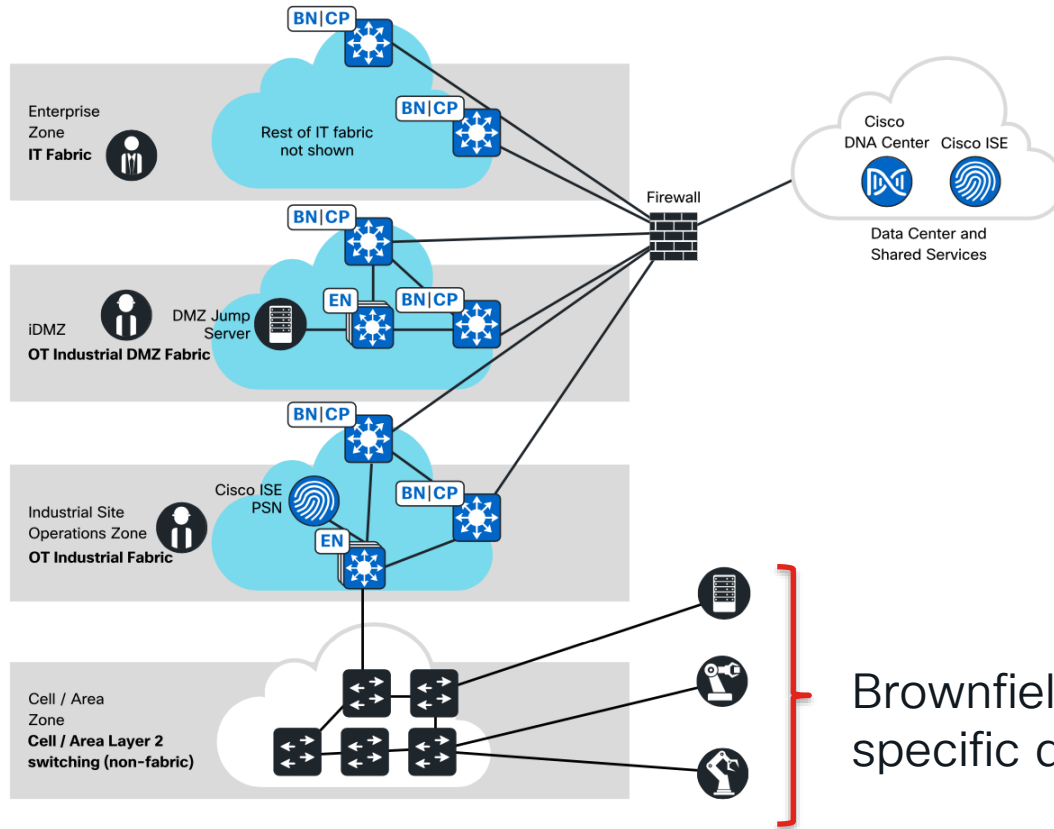
- Full Physical Segmentation between IT and OT Parts.
- Common Segmentation constructs of VN and SGT

Purdue Model Mapped Design



- Separate OT fabrics for Industrial DMZ and OT security
- Common multi-zone firewall between layers of Purdue

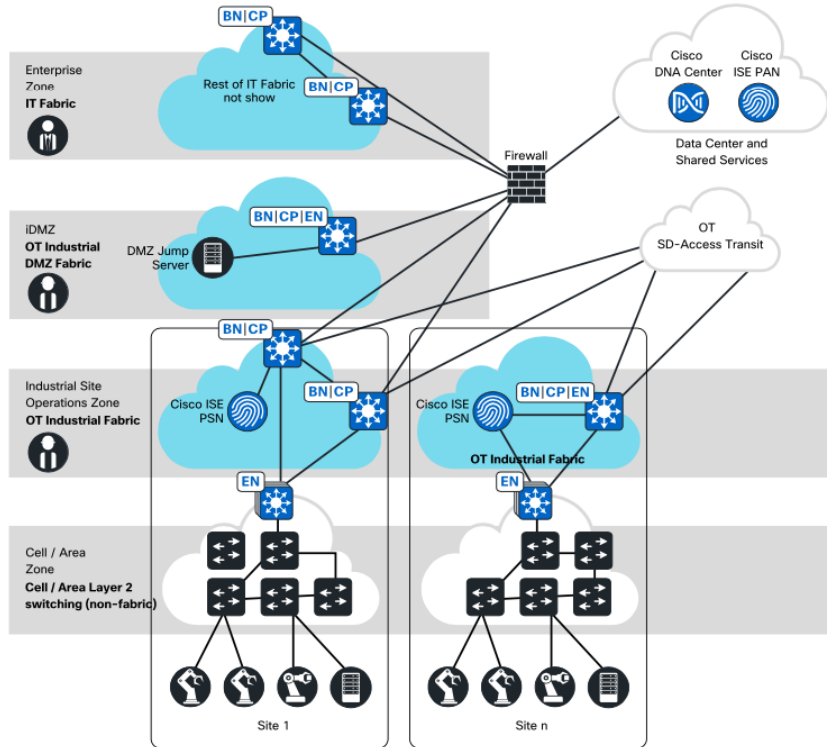
Mapping Cisco SD-Access with Purdue Model



- Dedicated ISE PSN for OT security.
- Control Loops – This can be an SDA Ex network or a separate L2 Network

Brownfield Scenario or Vendor specific design , Direct attach

SD-Access Multi Plant architect

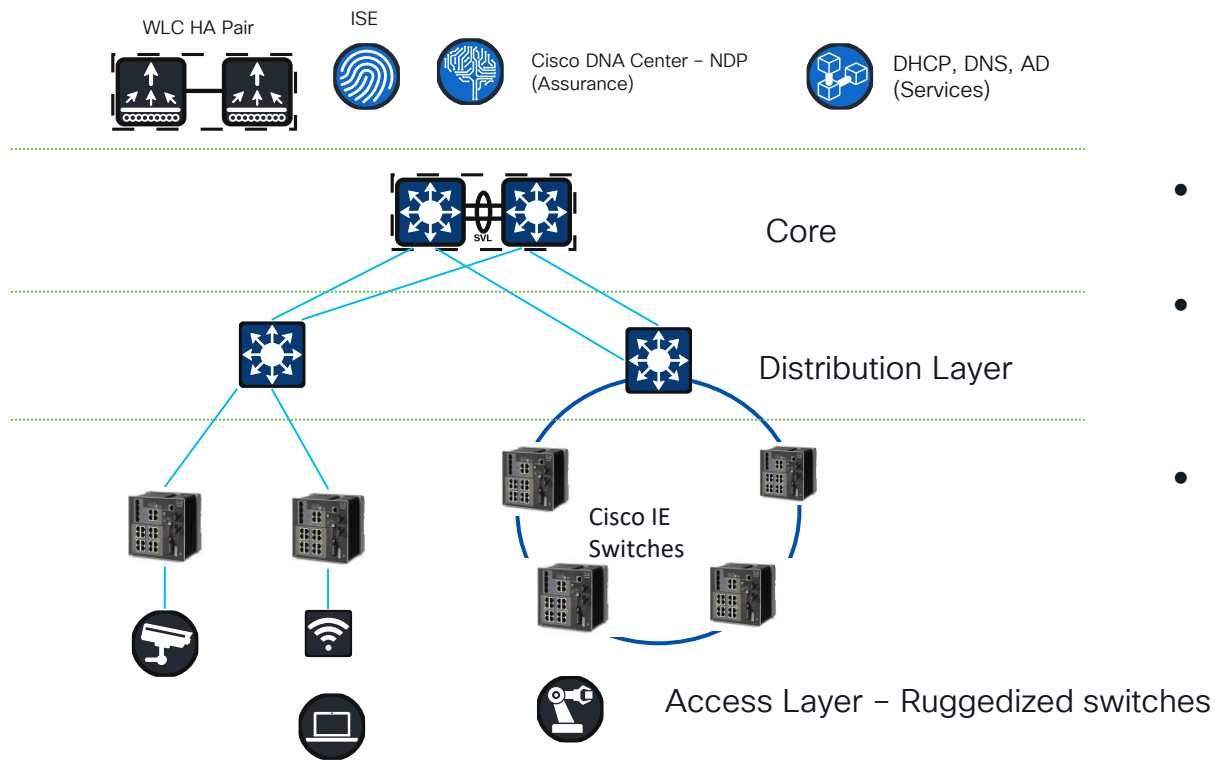


- Multi-plant interconnect via SD-Access Transit

*Assuming Plants with Campus Fibre Connectivity

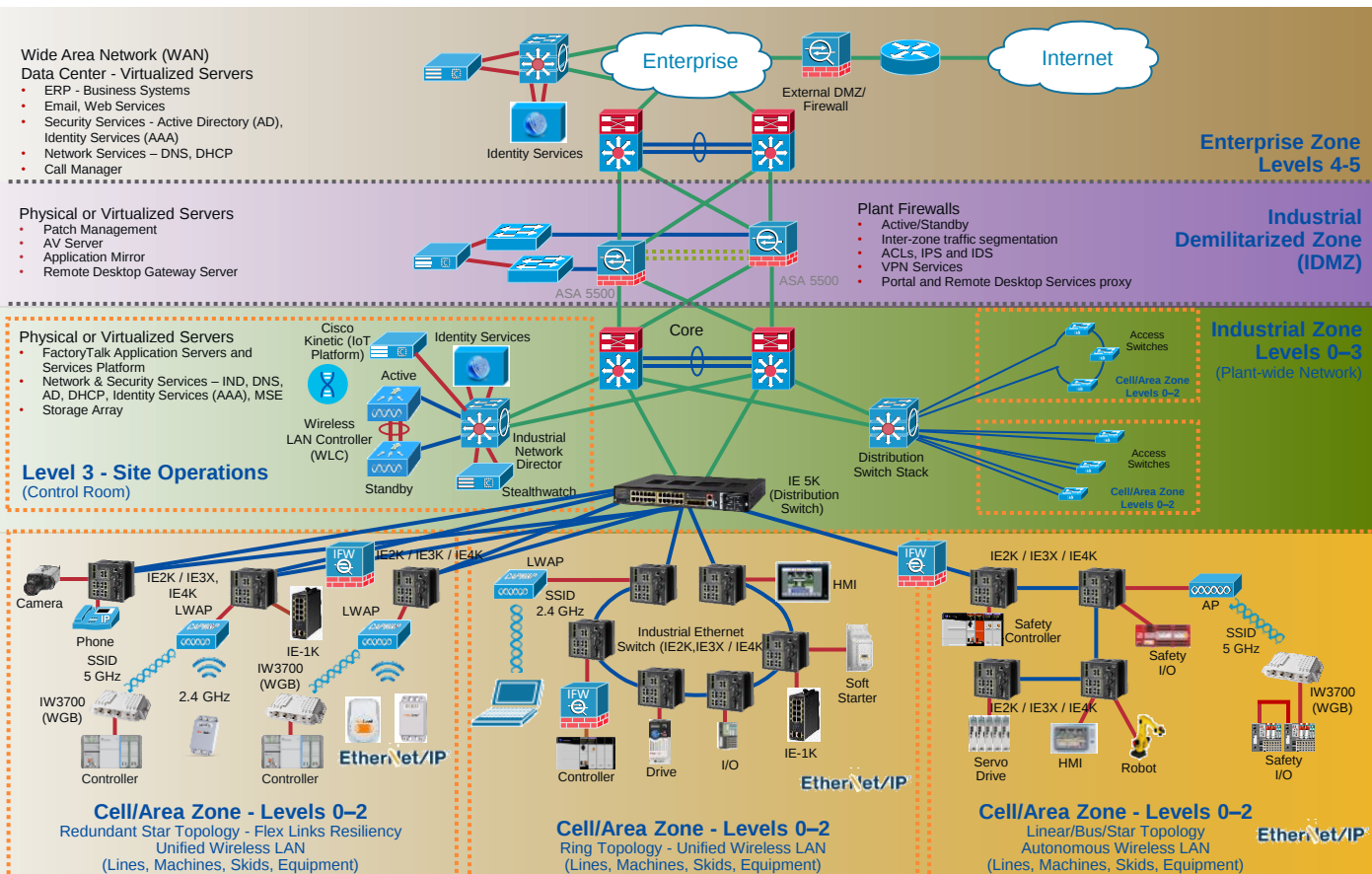
Network Extension: Non-SDA or Mixed environment

Non-SDA Network Extension



- DNAC for assurance
- Distribution/Access layer using IoT switches
- Access Layer using IoT protocols like REP

Converged Plantwide Ethernet (CPwE)

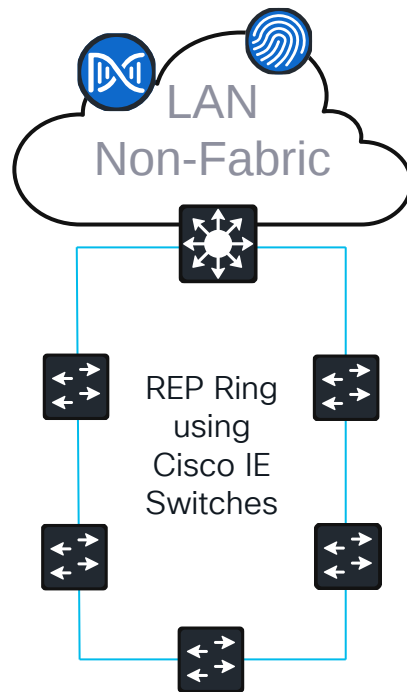


Non-SDA REP Ring Configuration

Step – 1 : STP Ring Onboarding

Step – 2 : STP Ring To REP Ring Conversion

Similar to SDA , DNAC will convert STP ring to REP



Points to be noted: DNAC REP Automation

- This is a feature list for DNAC 2.3.4.0 release.
- IOS & IOS-XE versions : (DNAC supported and long-term version)
 - IE4000, IE4010, IE5000 >= IOS 15.2(7)E3
 - IE3300, IE3400, IE3400H >= IOS-XE17.3.4
- From the Inventory > Topology tab user should select a root device and two adjacent nodes belonging to the same ring.
- REP workflow process identifies the existing STP topology and validates for closed ring using the CDP neighbor.
- If multiple links are present between two devices, then the links should be configured as port-channel before the REP ring is triggered.
- REP edge and primary/secondary are configured by the REP workflow on the selected root device
- REP segment will be autogenerated by the DNAC.
- All the interfaces part of the ring should be configured in “switchport mode trunk”.
- Supported list of devices:
 - Classic IE switches : IE3000, IE4000, IE4010, IE5000
 - Catalyst IE Switches : IE 3200, IE 3300, IE 3400, IE 3400H, ESS 3300, IE 93x0.

Non-SDA REP ring configuration

Steps to configure Non-SDA REP ring

Using Workflows : Click on Menu > Workflows > Configure REP Ring (Non-Fabric) widget

Library [Choose An Intent](#) ▾

 Setup Wireless Network <i>BETA</i> Design and provision wireless network on a non-fabric site. Wireless	 Site to Site VPN Create VPN configuration between two sites. Wired	 Umbrella Deployment Configure Cisco Umbrella on network elements, which send DNS queries for Umbrella to enforce security/content policies. Wireless Wired	 Create Layer 3 Virtual Networks. Create Layer 3 network overlays for segmenting routed traffic.	 Create Layer 2 Virtual Networks Create Layer 2 network overlays for segmenting switched traffic.
 Create Fabric Sites and Fabric Zones Scope a single SD-Access fabric which comprises at least one Border node, Control Plane node and Fabric Edge node.	 Create Anycast Gateways For each IP Pool, create an Anycast Gateway across Fabric Edge nodes.	 Create a Port Channel Create a Port Channel step by step.	 Configure Multicast Configure a Cisco SD-Access fabric site to support multicast routing in Layer 3 Virtual Networks.	 Configure REP Ring (Fabric) Configure a REP Ring to enable redundancy on the Extended Nodes.
 Configure REP Ring (Non-Fabric) Configure a REP Ring to enable redundancy on the Extended Nodes.	 Telemetry Appliance Setup Configure Switch Port Analyzer (SPAN) and Encapsulated Remote Switch Port Analyzer (ERSPAN) sessions to share IP traffic for application assurance and endpoint analytics. Wired	 Create Sensor Test Build a wireless test template for monitoring real-world client experiences. Wireless	 Replace Device Replace your device in a few quick easy steps. Wired Wireless	 Access Point Refresh Replace Your Access Points with New ones. Wireless

Adding/Deleting nodes to REP ring:

Adding a node from the existing REP ring:

Automated in Non-Fabric, No downtime

- Delete the existing REP ring.
- Then the add node physically to the topology and wait for the onboarding of the new node to be completed.
- From Provision > Inventory page, manually run the “Resync” of all the devices (including Edge) part of the ring.
- Then trigger the REP ring workflow

Deleting a node from the existing REP ring:

- Delete the existing REP ring.
- Then delete the node from the fabric site followed by DNAC inventory.
- From Provision > Inventory page, manually run the “Resync” of all the devices (including Edge) part of the ring.
- Then trigger the REP ring workflow

Advisories REP

- Scale numbers:
 - By default, a maximum of 18 devices can be onboarded in a single REP ring.
 - If there is a use case for more than 18 nodes in a single REP ring, customer needs to increase the BPDU timer using command `"spanning-tree vlan <infra VN VLAN> max-age 40"`.
 - Customers can achieve this using the DNAC custom Templates.
- If multiple links present between two devices, then the links should be configured as port-channel before the REP ring is triggered.
- Ensure all the interfaces which are part of ring should be the trunk port
- The device which is selected as a root bridge should have third link through which has reachability to DNAC (other two links are part of the ring)
- Ring of rings and multiple rings within a given REP ring is not supported.

DNA-Center: REP Troubleshooting

- REP ring workflow failures:
 - If REP ring creation/deletion fails with the error – “Discovery request failed” :
 - Using the “Command Runner” try to check the ‘CDP neighbors’ status’ for all the devices (including Edge node) part of the STP ring, which is being converted to REP ring.
 - Using the “Command Runner”, make sure there is no redundant link between devices in ring. If so, bundle them or make one interface down
 - Using the “Command Runner”, ensure all the interfaces which are part of REP ring should be in trunk mode
 - Manual Resync of devices – From Provision > Inventory page, manually run the “Resync” of all the devices (including Edge) part of the ring.
 - Once all the above steps yield a positive outcome, try to retrigger the REP ring creation workflow.
 - If REP ring creation/deletion fails halfway through :
 - The most likely reason would be the device going unreachable more than the expected wait time or unreachable for any other extraneous reasons.
 - Try to fix the device reachability issues. Once the device is reachable, try to manually run the “Resync” of all the devices from the ‘Inventory’ page and then ”reinitiate” the failed REP ring workflow.

Network: REP Troubleshooting

- Navigate to the REP rings tab and click on the REP Status button. To get the current status of the REP ring.
- Check the REP Ring status by using the command in the “command runner”
 - “show rep topology segment <REP_Segment_number>”

```
Command Runner C9300-edge@1.1.1.1
```

Welcome to **Cisco DNA Center** command runner.

You can access this window from anywhere using the key combination Q+T.
You can access recently viewed devices using the key combination Q+D.

Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

```
C9300-edge> show rep topo seg 38
REP Segment 38
BridgeName                               PortName  Edge Role
-----
C9300-edge                               Gil/0/12  Pri  Open
IE-3k-3                                  Gil/0/12  Open
IE-3k-3                                  Gil/0/1   Open
IE-3k-2                                  Gil/9     Alt
IE-3k-2                                  Gil/3     Open
IE-3k-1                                  Gil/3     Open
IE-3k-1                                  Gil/5     Open
C9300-edge                               Gil/0/14  Sec  Open

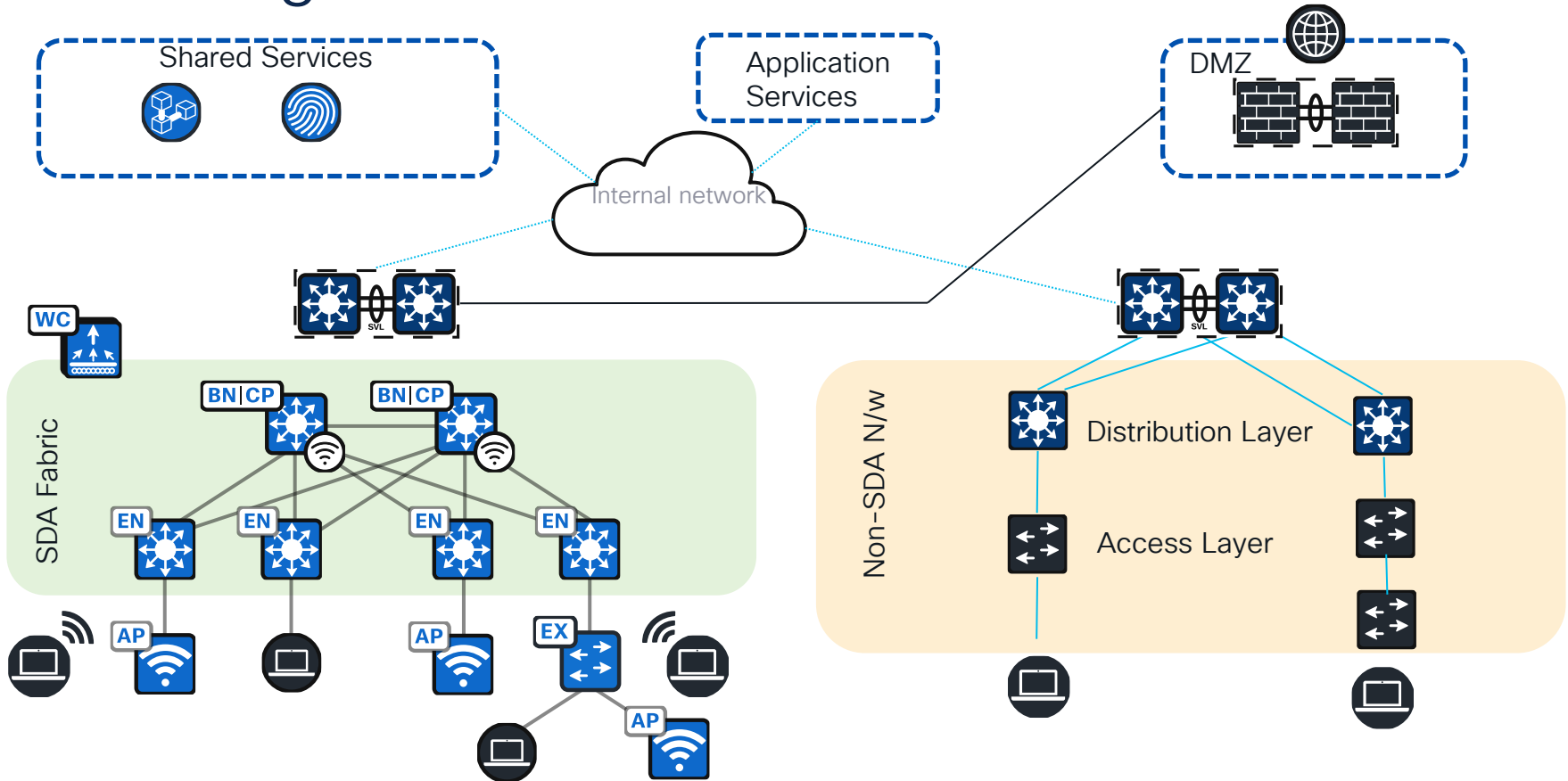
C9300-edge>
```

DNA-Center: Topology View Troubleshooting

A missing link in the topology view for an STP ring:

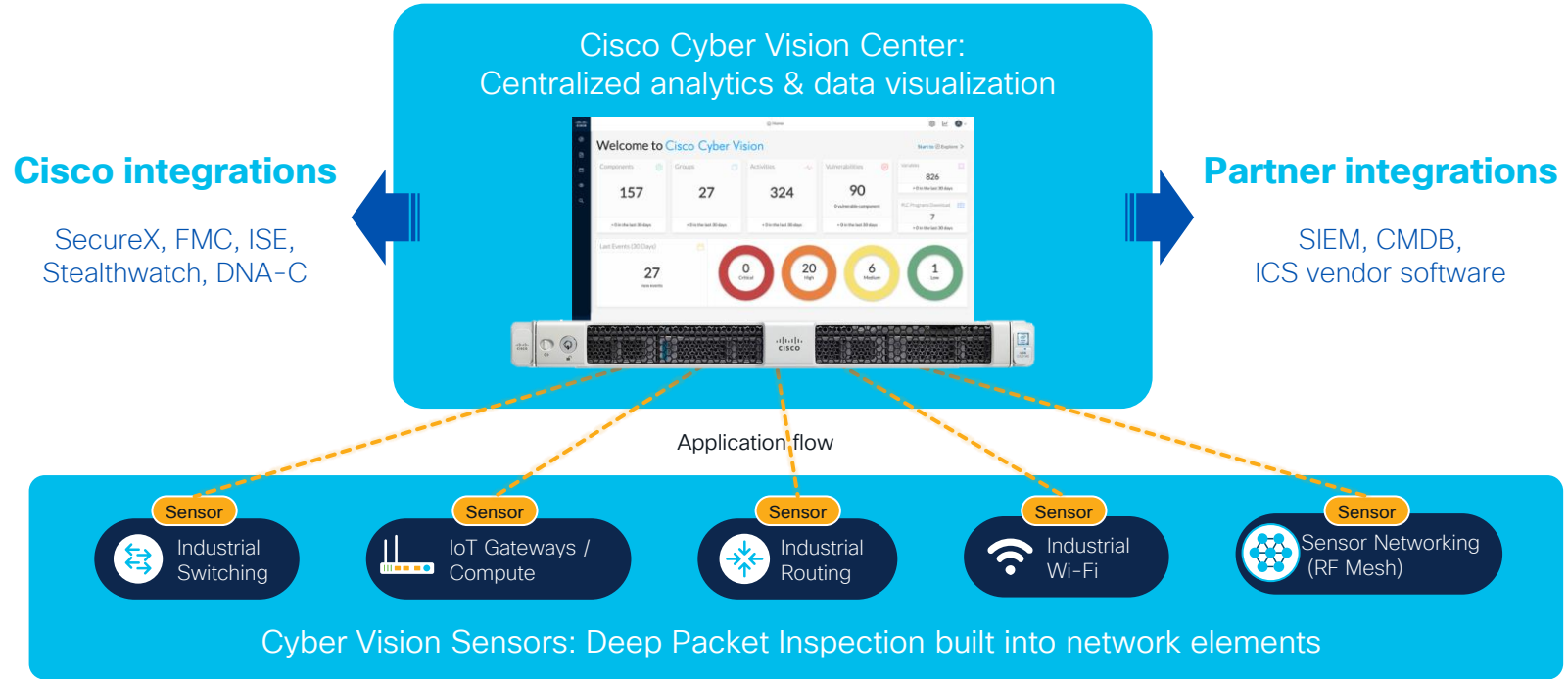
- When we onboard a STP ring, in a rare instance there might be a link missing and it would end up showing as two daisy chains instead of a STP ring in the fabric topology view.
- Workaround for this case is, manual Resync of devices - From Provision > Inventory page, manually run the “Resync” of all the devices part of the ring.

Converged Architecture



Extended Enterprise Monitoring via Cybervision

Industrial cybersecurity that can be deployed at scale



Cisco Cyber Vision **portfolio**

Cyber Vision Center

Hardware Appliance

UCS based servers with Hardware RAID



CV-CNTR-M5S5

- 16 core CPU
- 64 GB RAM
- 800GB drives

CV-CNTR-M5S3

- 10 core CPU
- 32 GB RAM
- 480GB drives

Software Appliance

Virtual Machines



VMWare ESXi OVA



HyperV VHD

Minimum requirements

Intel Xeon, 4 cores
16GB RAM and 200GB SSD
1 or 2 network interfaces



Amazon Web
Services



Microsoft Azure

Minimum requirements

Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Cyber Vision Sensors



Catalyst IE3300 10G
and IE3400
Switches



Catalyst IE3400HD
IP67 Switch



Catalyst
IR1101
LTE Gateway



Catalyst IR8300
Multiservice Router



Catalyst 9300/9400
Aggregation Switch



IC3000 Industrial Compute

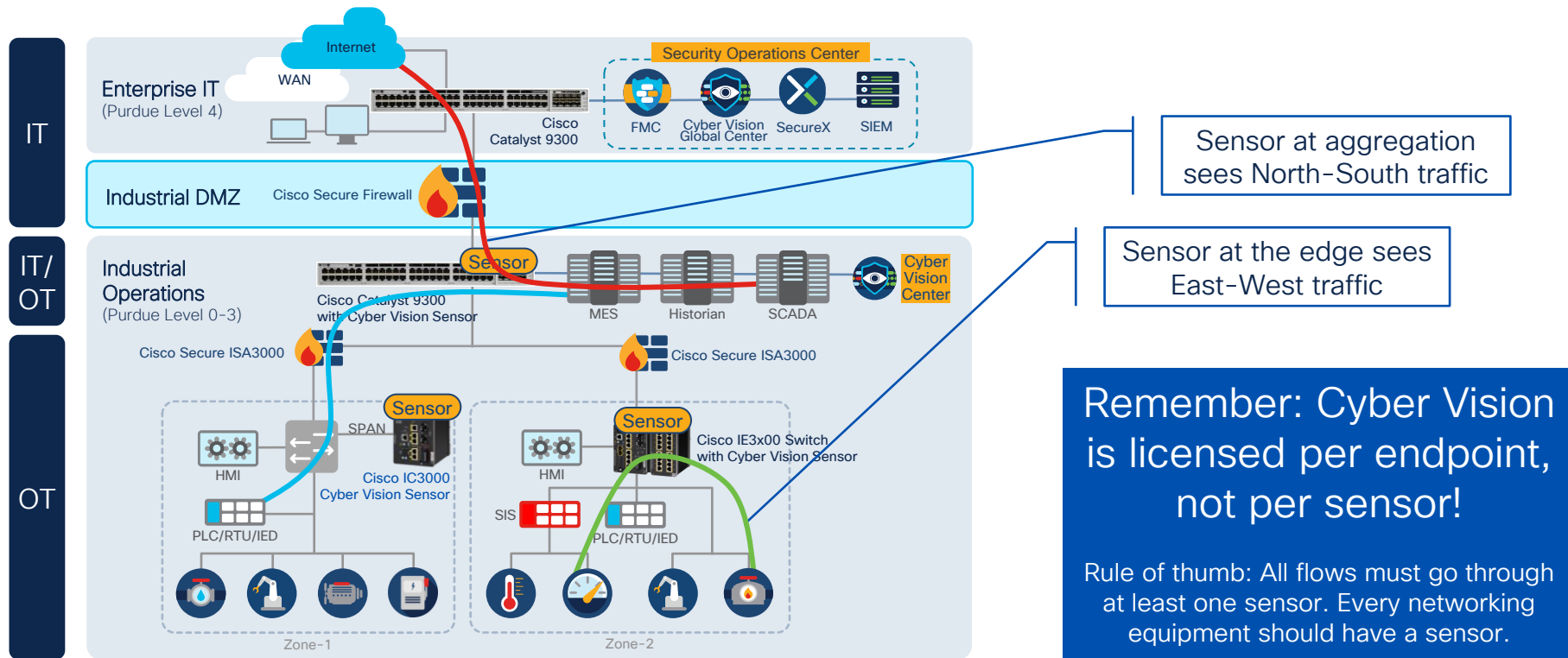
Network-Sensors

Deep Packet Inspection built into network-elements eliminating the need for SPAN

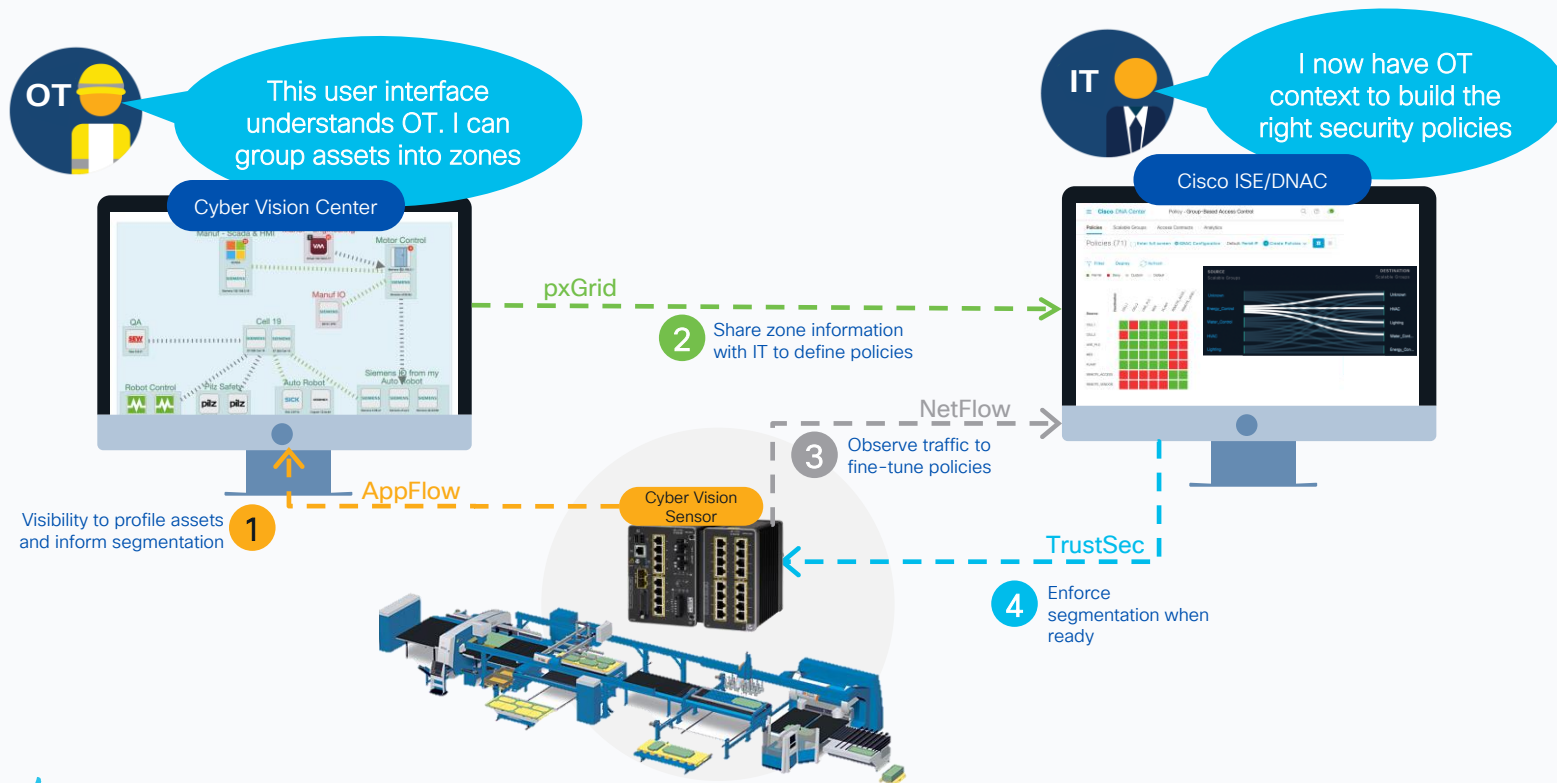
Hardware-Sensor

DPI via SPAN to support brownfield

Sensor Architecture

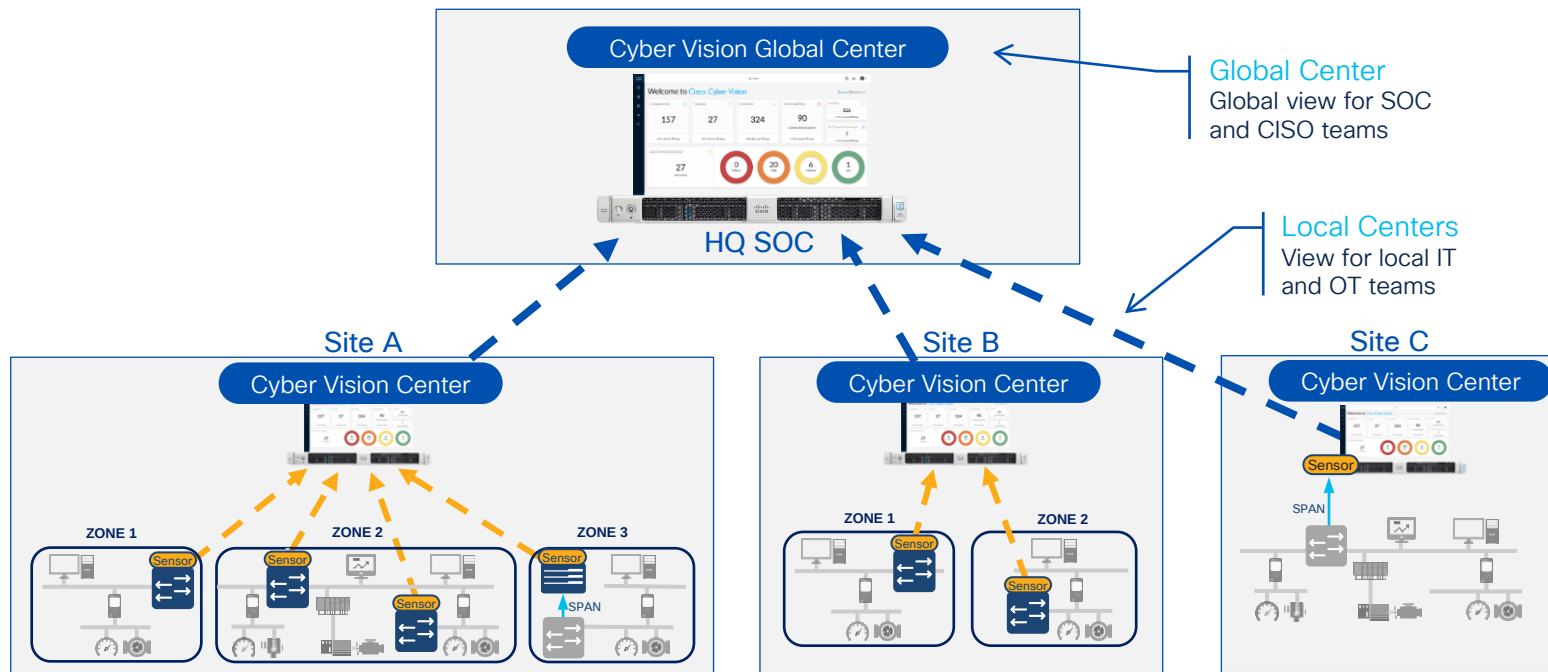


Profiling OT assets enables dynamic segmentation



Cisco Cyber Vision Global Center

Global visibility on all sites from a central console



Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

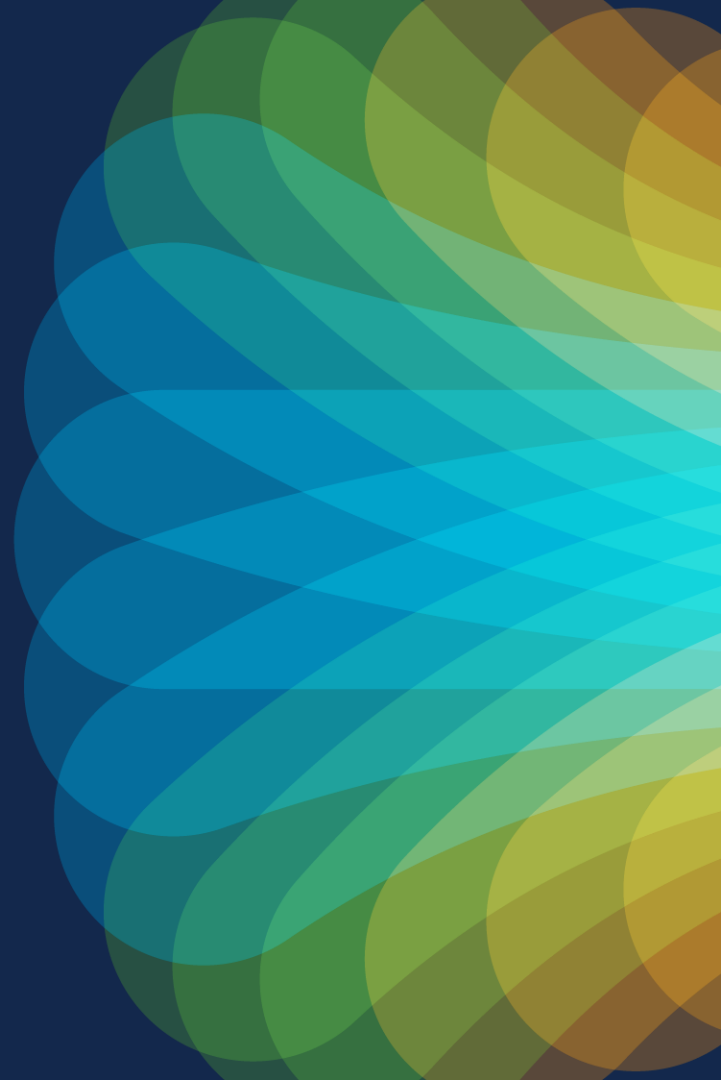


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

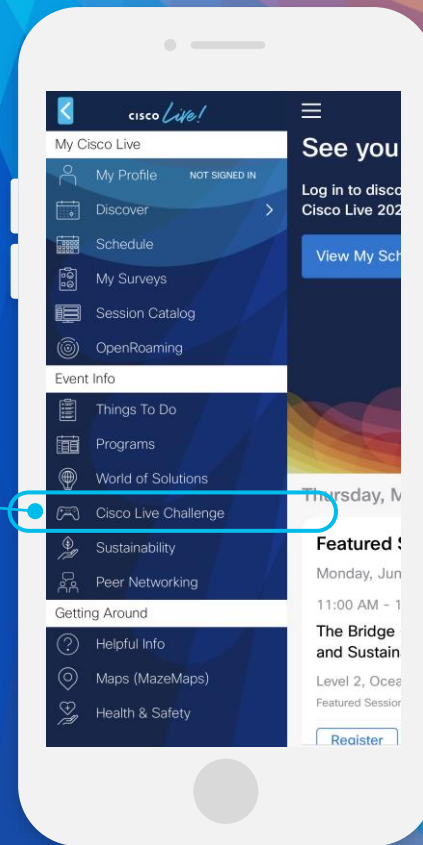
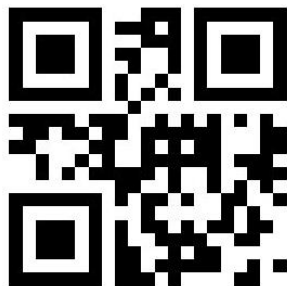


Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are large, flowing, wavy shapes in similar colors, giving the overall composition a sense of movement and energy.

cisco *Live!*

Let's go

#CiscoLive