

CISCO *Live!*



#CiscoLive



The bridge to possible

Extending Cisco SD-Access Beyond Enterprise walls

Policies, Rings, Daisy Chains

Vinay Saini , Principal Architect
BRKENS-2832



#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.



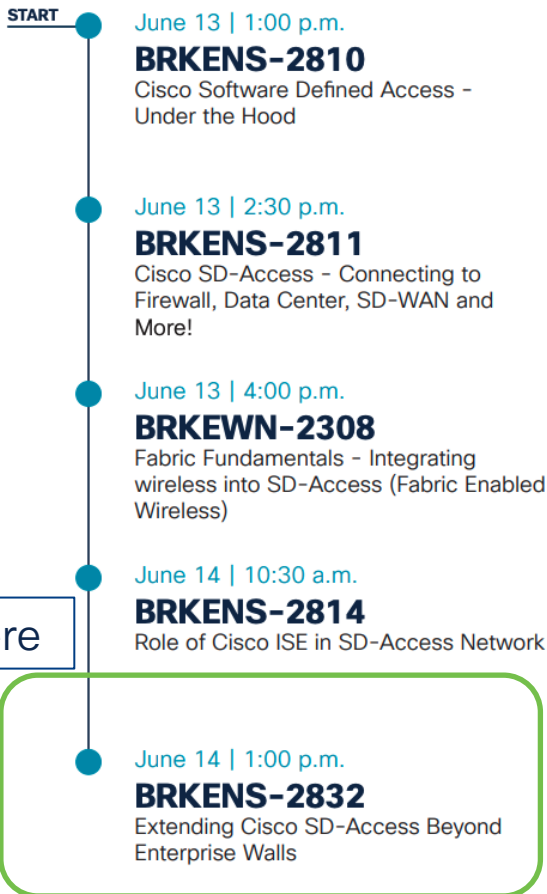
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2832>

Networking

SD-Access

Learn about Cisco's Software Defined Access (SD-Access) solution that provides a secure, dynamic, and automated solution to meet the security and operational challenges faced by an ever-changing environment. The Cisco SD-Access sessions provide a comprehensive overview regarding best practices, design, deployment, migration and monitoring of a Cisco SD-Access architecture.

You are here



If you are unable to attend a live session, you can watch it On Demand after the event.

Session Expectations

What is covered

- Cisco SD-Access Network Extensions using IE Switches
- Policy Extension using EN/PEN/SBEN
- Architecture, Use-cases & Topologies
- Daisy Chains / REP Rings With extended nodes

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
 - Ring Automation using DNA-C
 - Supported topologies
- REP rings Operations using DNA-C
 - Ring conversion STP to REP
 - Addition and deletion of node
 - Extension with Cat9k



Your Presenter Today

Vinay Saini

Principal Architect – Cisco CX (Advanced Solutions)

CCIE-38448 and CWNE#69

Active Contributor – DevNet/CCIE/CCNP Exam Tracks

Architect – Enterprise n/w, IIoT, SP WiFi



What is Extended SDA Network

Need and Use-cases



Extended Enterprise – Local Extension

Extended Enterprise

Ruggedized Industrial
Networking Products



Non-carpeted/ Outdoor Spaces



Industrial Ethernet and Wireless Devices



Roadways



Parking Lot



Distribution Center



Airport



Manufacturing

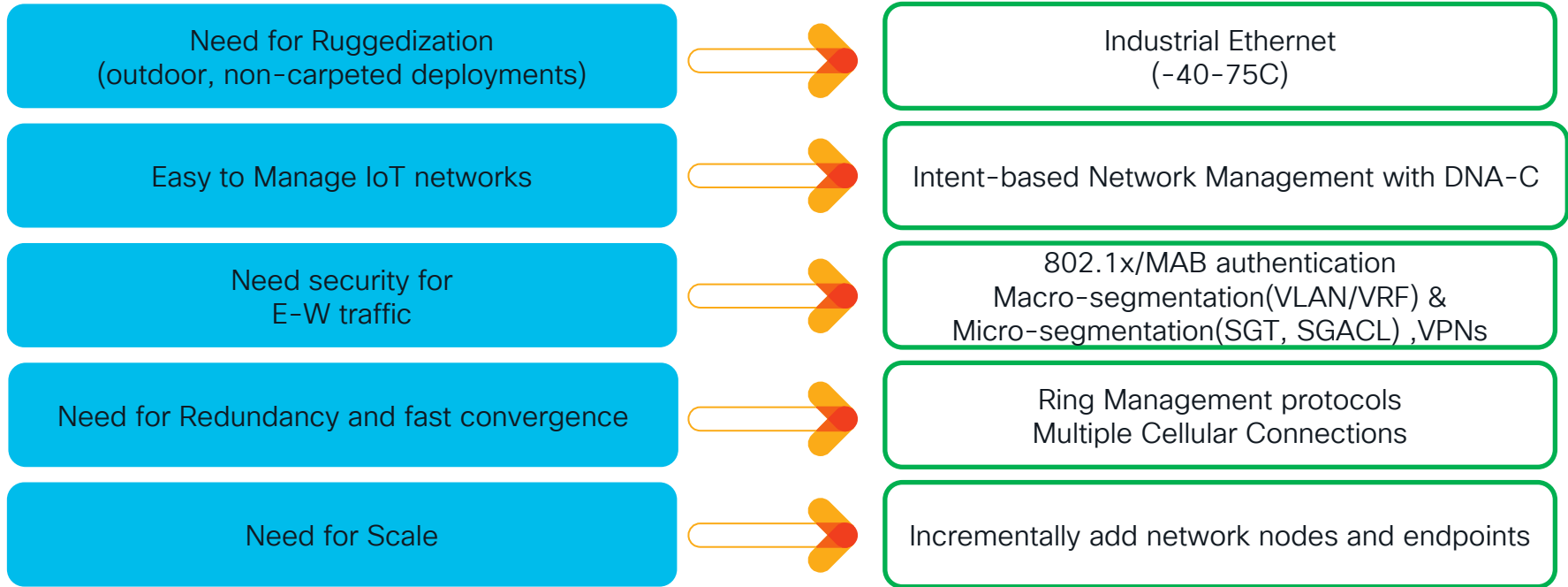


Port/Terminal



Warehouse

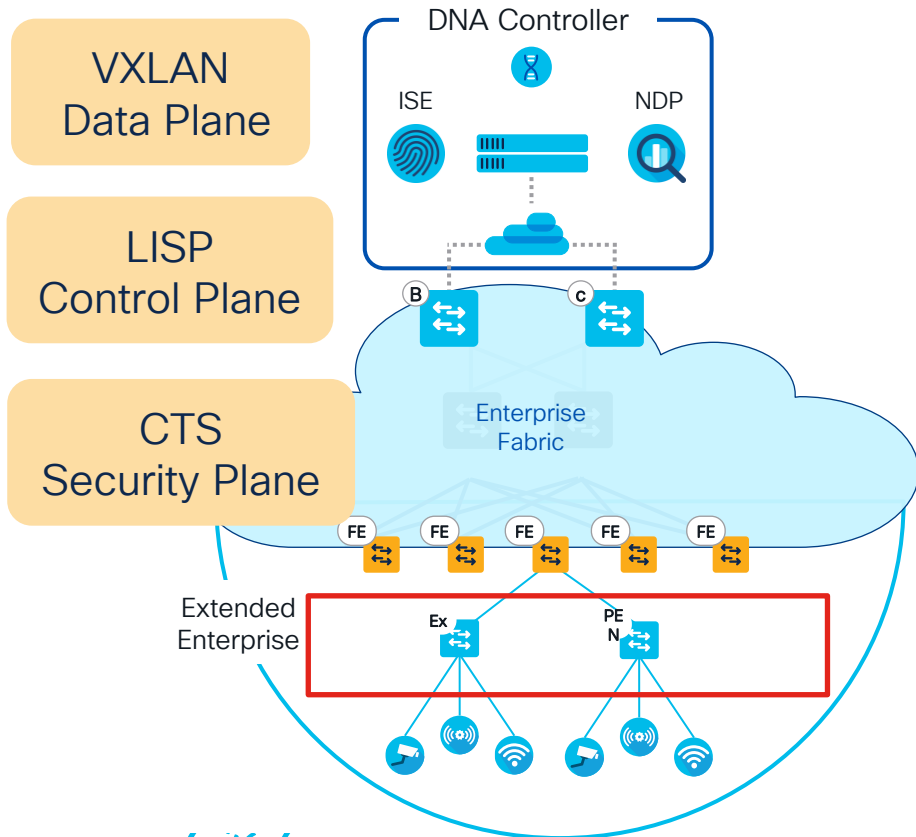
Expectations from this extended network?



Local Extension With Cisco SD-Access



SD – Access Architecture for Extended Networks

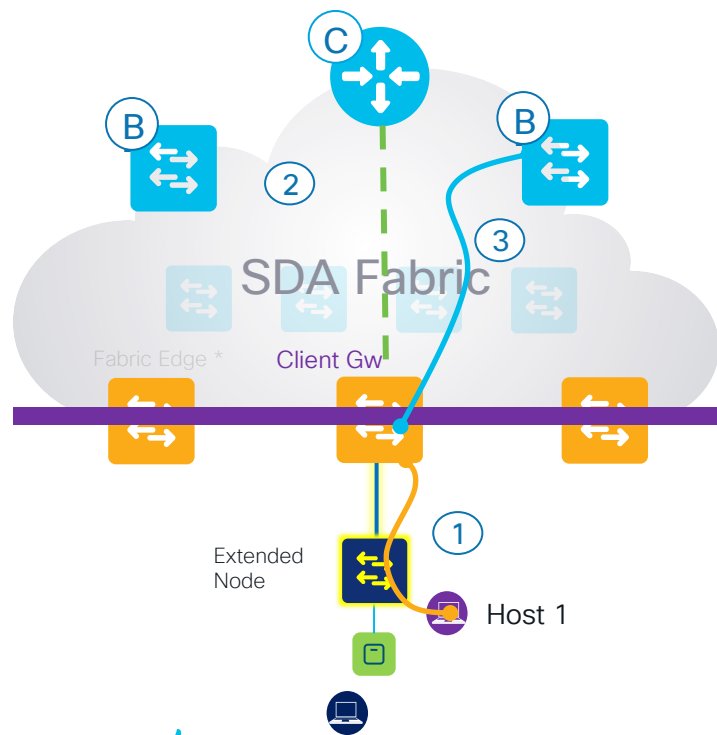


- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context.
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Control Plane Nodes** – Map 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
- **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

[illegible]

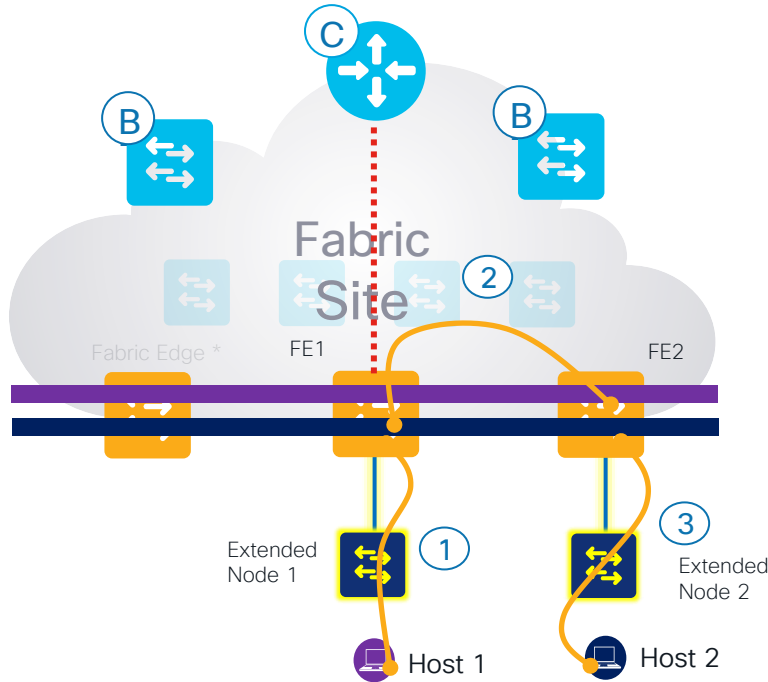
- The port channel can be over single or multiple links between Extended node and single Edge node.

Client External Communication



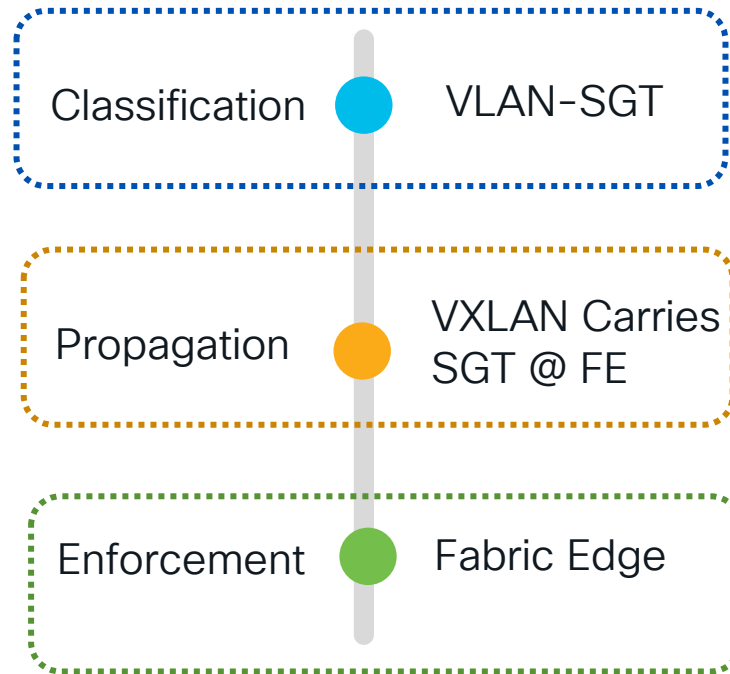
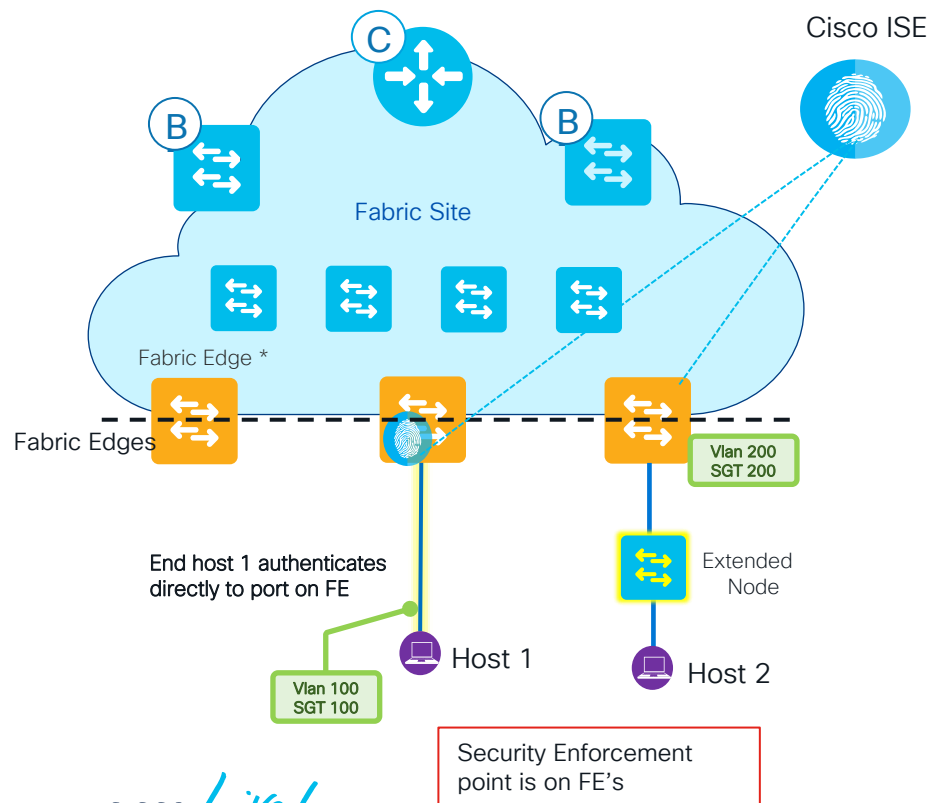
- ① The host connecting to the extended node sends traffic to fabric edge node as the default gateway exists on the fabric edge node.
- ② The fabric edge node will consult the control plane on where to send traffic.
- ③ Control Plane node tells clients to go via Border node.

Extended Nodes- Host To Host communication

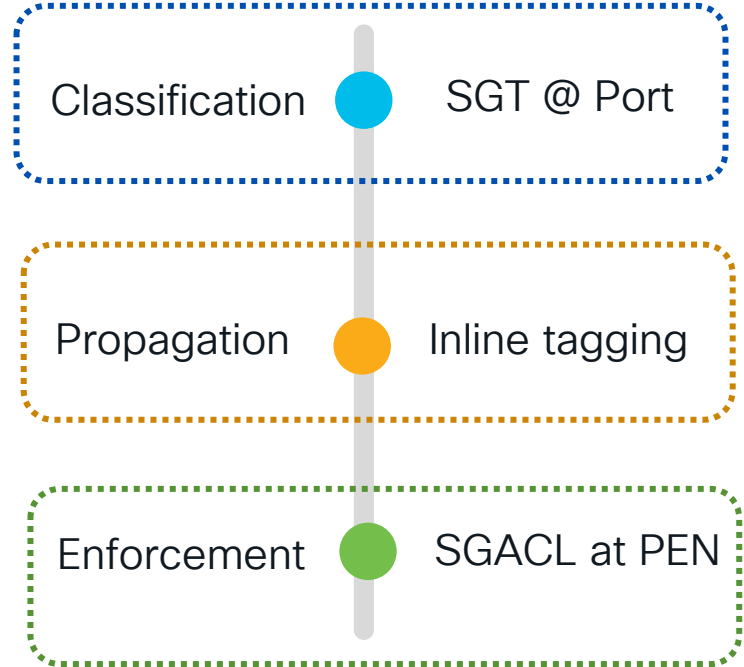
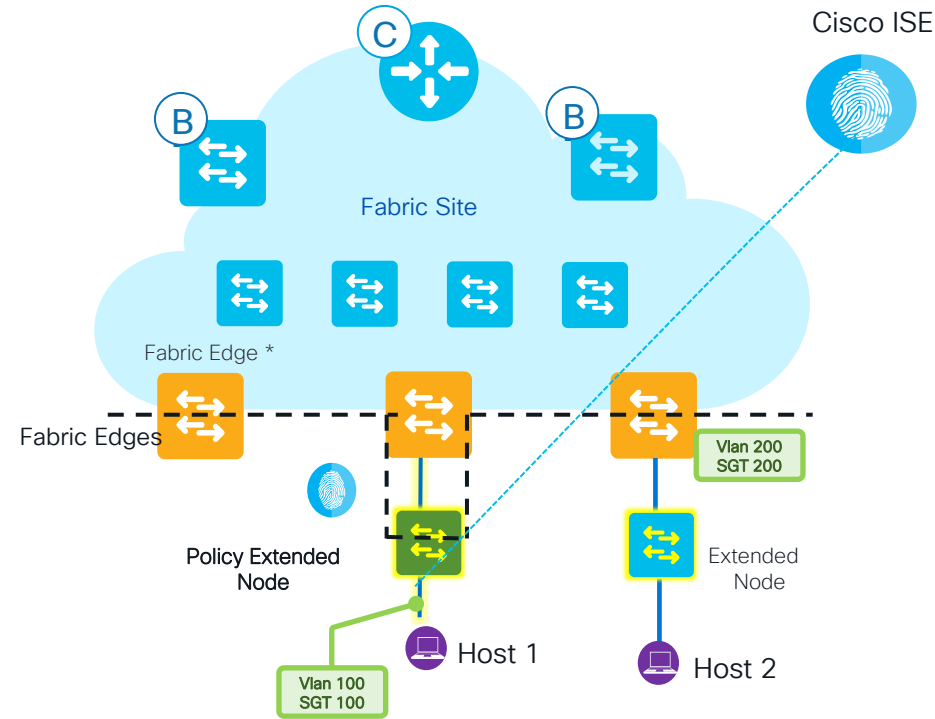


- 1 The host connecting to the extended node sends traffic to fabric edge node as the default gateway exists on the fabric edge node.
- 2 The fabric edge node will consult the control plane on where to send traffic and ensures the traffic reaches to the destination (VXLAN encap). In this case it is sent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

Extended Node - Policy Application



Policy Extended Node (PEN)



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 Intfcae  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: 000200B8000300010004001009A36B6CC5A29B316392861C48BB83350006009C0003010099C6F4B234D1E5786564661DB99FCCB9
5B7BA68D1E077DF92008C6DD757EAF5FB821D4CE73FA9031AC67537E741D29081E23E6BC0566C8DB64C2B307B780B553CB0063A3DAEFC9C4EF72
73BF7A389F1F46000FC6582D4A95B30FBE44CB236827A9A058E57B7B1D688B8689FA964A6F636DD58EECD97EDBBE0E
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 Intfcae  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...

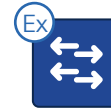
Current configuration : 122 bytes
!
interface GigabitEthernet1/12
 description PNP STARTUP VLAN
 switchport mode trunk
 channel-group 1 mode desirable
end
```

Show CTS PAC
Show CTS Env

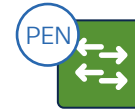
Use-cases



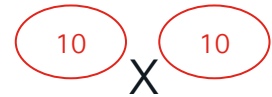
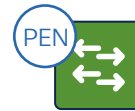
Controlled Inter VLAN access



Controlled Intra-VLAN Access



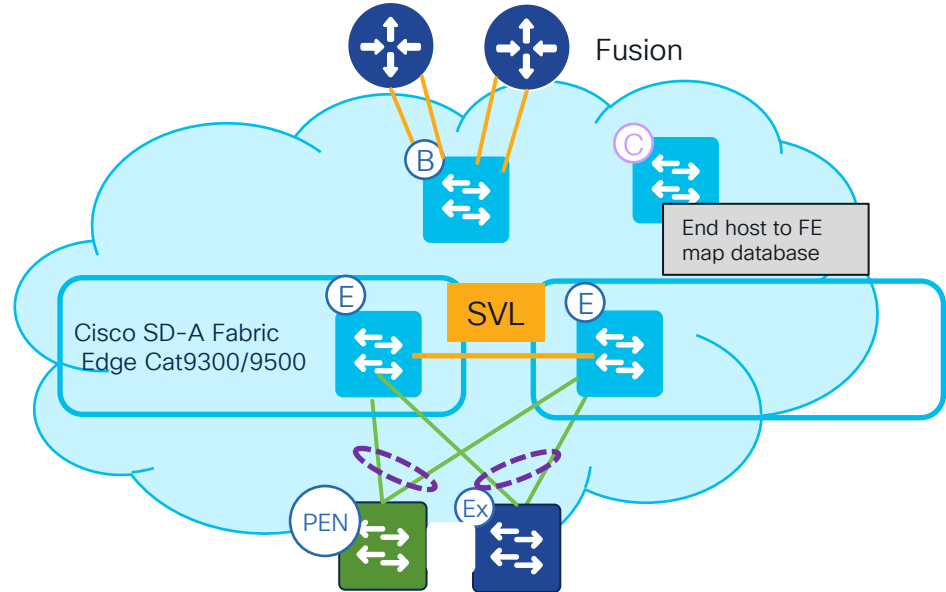
Peer to Peer Blocking within VLAN



Same SGT deny Policy

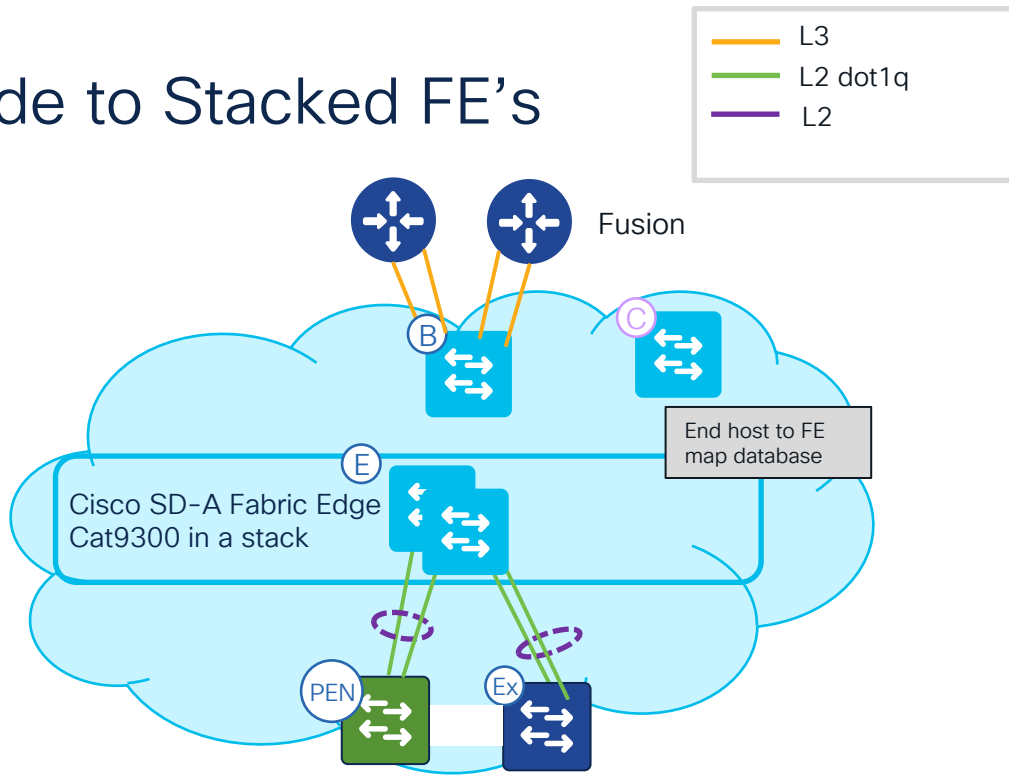
Supported Topology – FE with SVL Links

EN/PEN uses Port-channel to connect with FE with SVL Link



Supported: Extended node to Stacked FE's

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



IE Extended Node, Policy extended node platforms

Extended Node

Industrial Ethernet
IE5000



Industrial Ethernet
IE4010



Industrial Ethernet
IE4000



Catalyst IE3300
Rugged Series



Catalyst IE3400 (H)
Rugged Series



Cisco 3560-CX



Policy Extended Node

Catalyst IE3400
Rugged Series



Catalyst IE3400H
Heavy Duty Series



CA/IE 9300



Upcoming release
EN/PEN
IE 9300 REP
CA9300-
PEN/EN/Daisy
Chain

Migrating EN to Policy Extended Node

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

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



Poll Question

Are you using REP Rings with or without SDA?



REP Rings and Extended Nodes

Network Resiliency Protocols

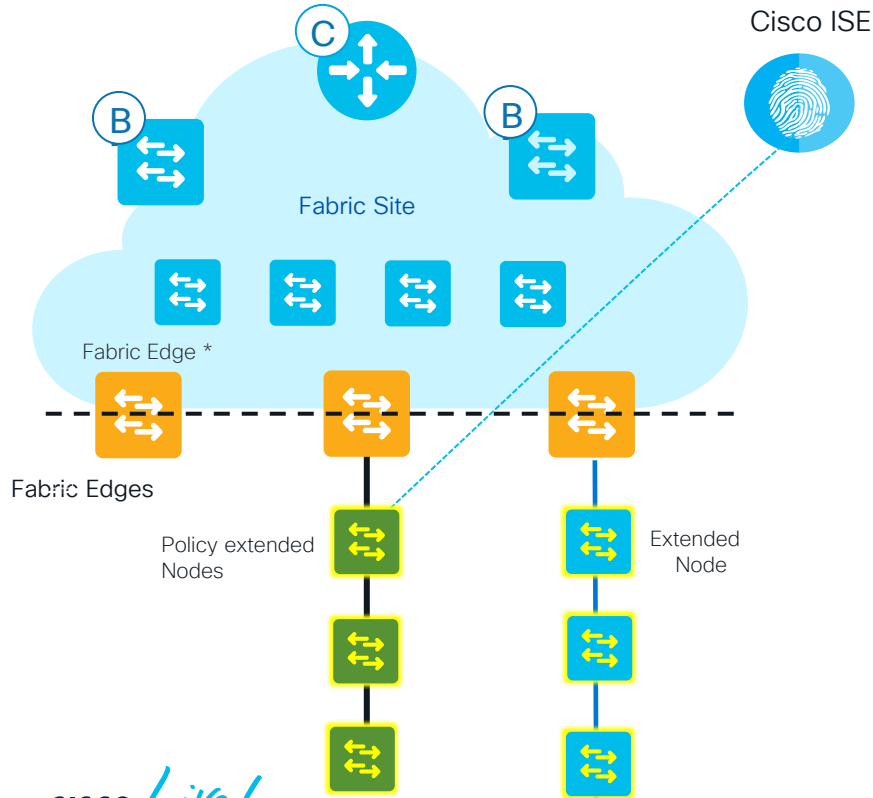
Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Net Conv >250 ms	Net Conv 50-100 ms	Net Conv < 0~10 ms	Layer 3	Layer 2
STP (802.1D)	●	●	●					●
RSTP (802.1w)	●	●	●	●				●
MSTP (802.1s)	●	●	●	●				●
PVST+		●	●	●				●
REP		●			●			●
EtherChannel (LACP 802.3ad)	●		●		●			●
MRP (IEC 62439-2)*	●	●		●	●			●
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

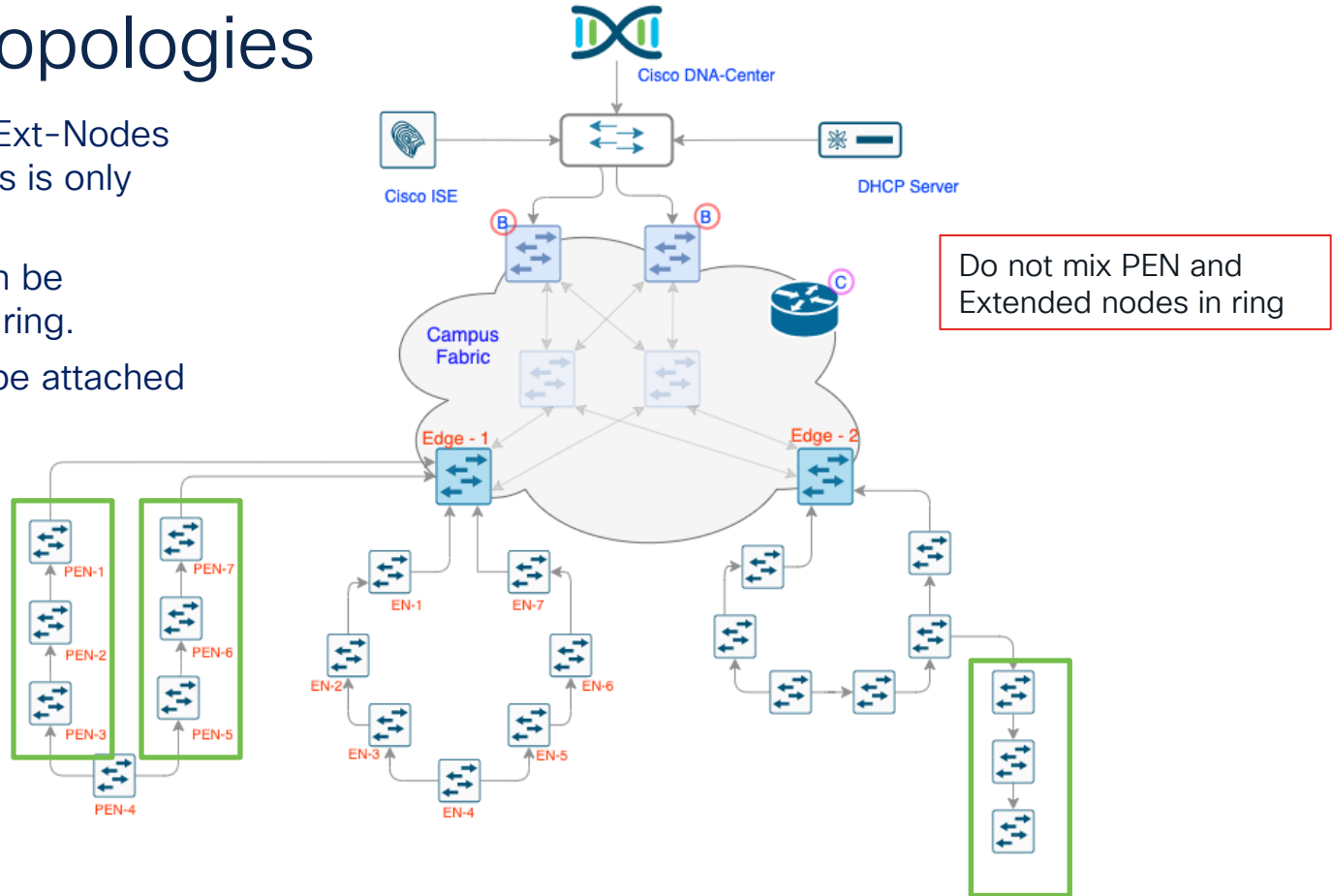


- Linear Daisy Chain topology of either EN/PEN
- FE + 18 nodes

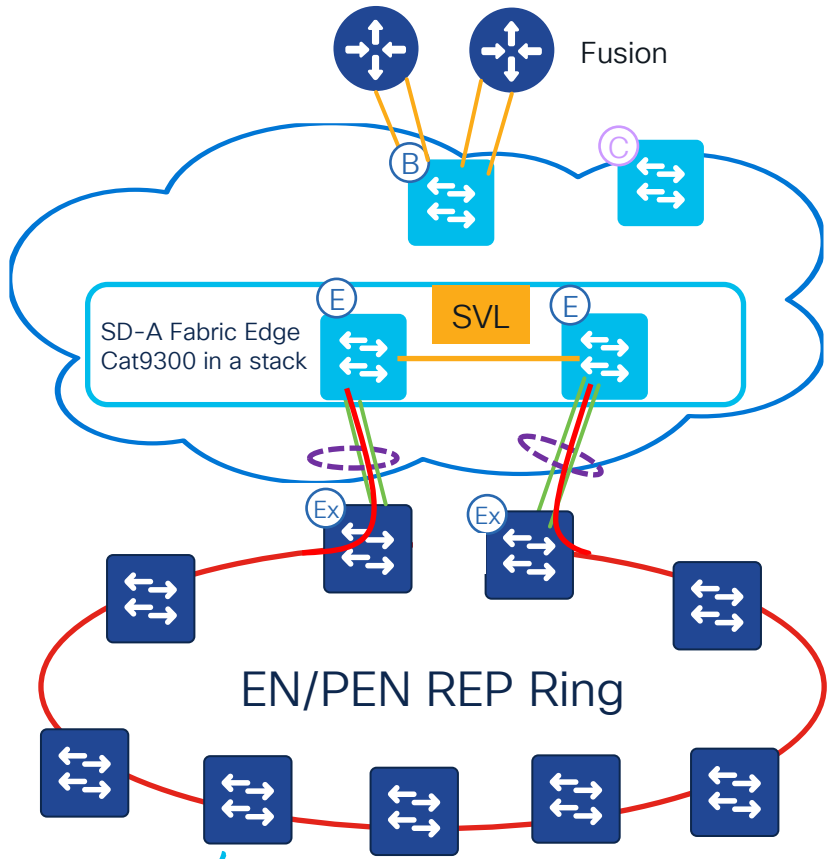
Available from DNA-C Release : 2.2.x (GA)

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.

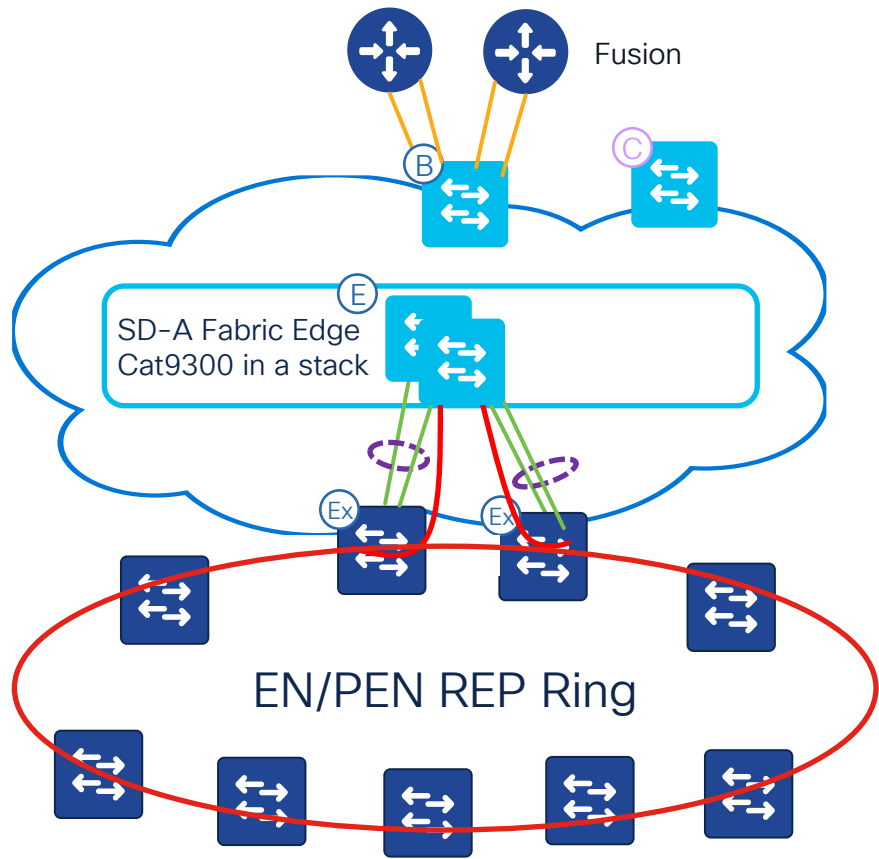


Supported Topologies

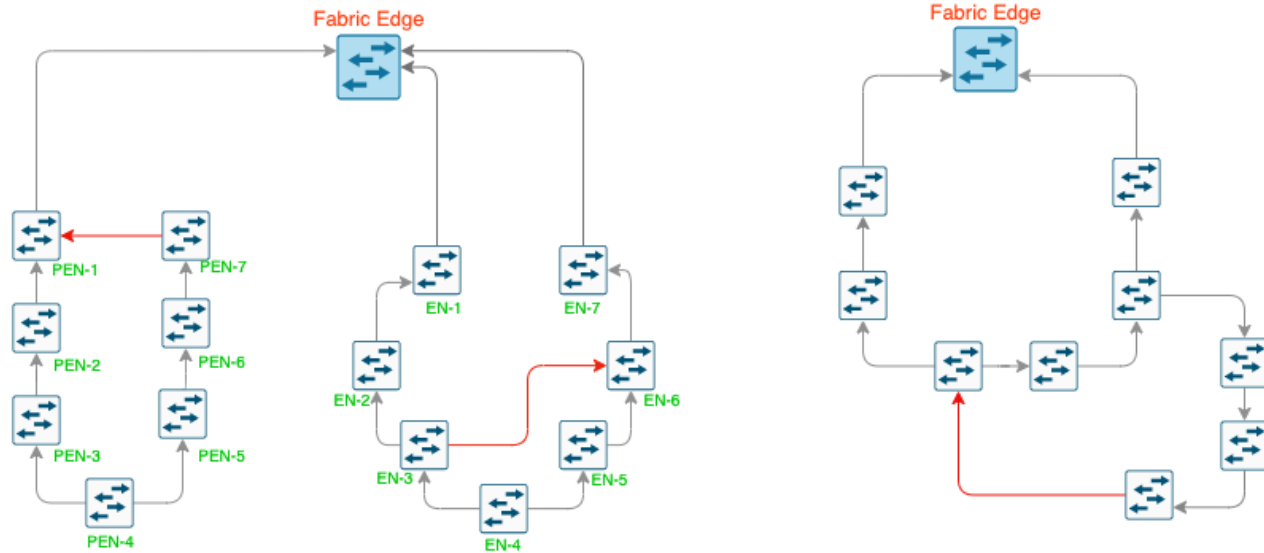


CISCO *Live!*

Available from DNA-C Release TBD: 2.2.3 (EFT)

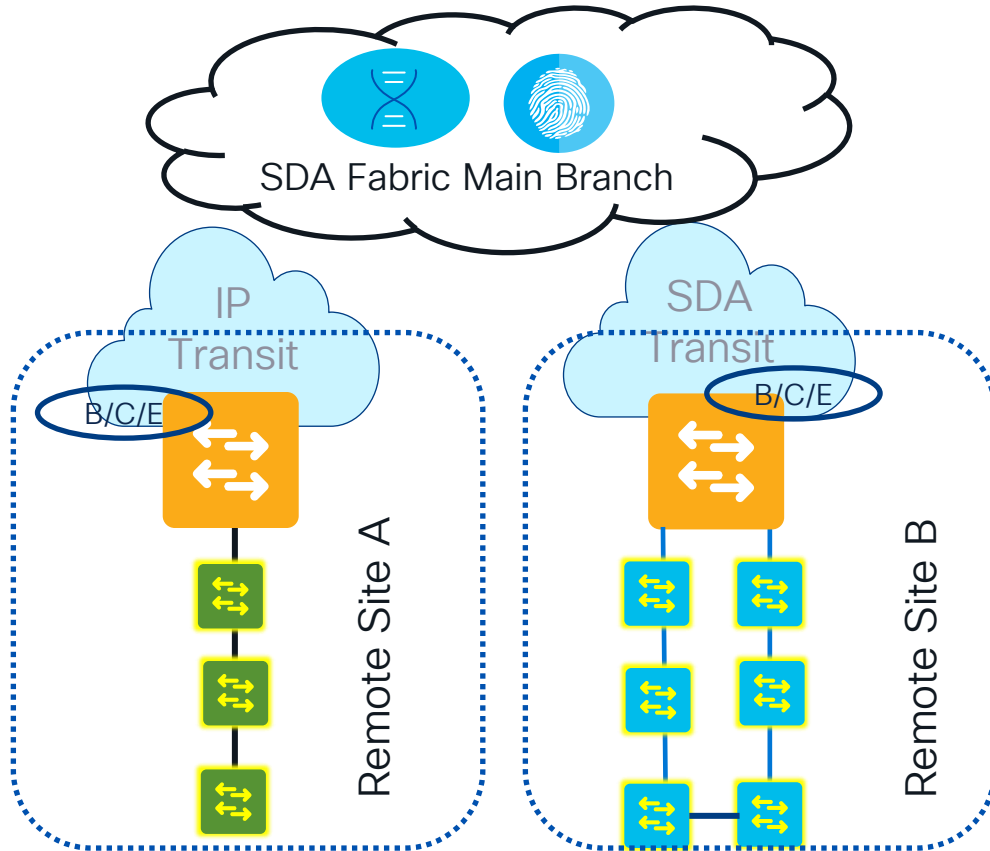


Un-Supported Topologies



- 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



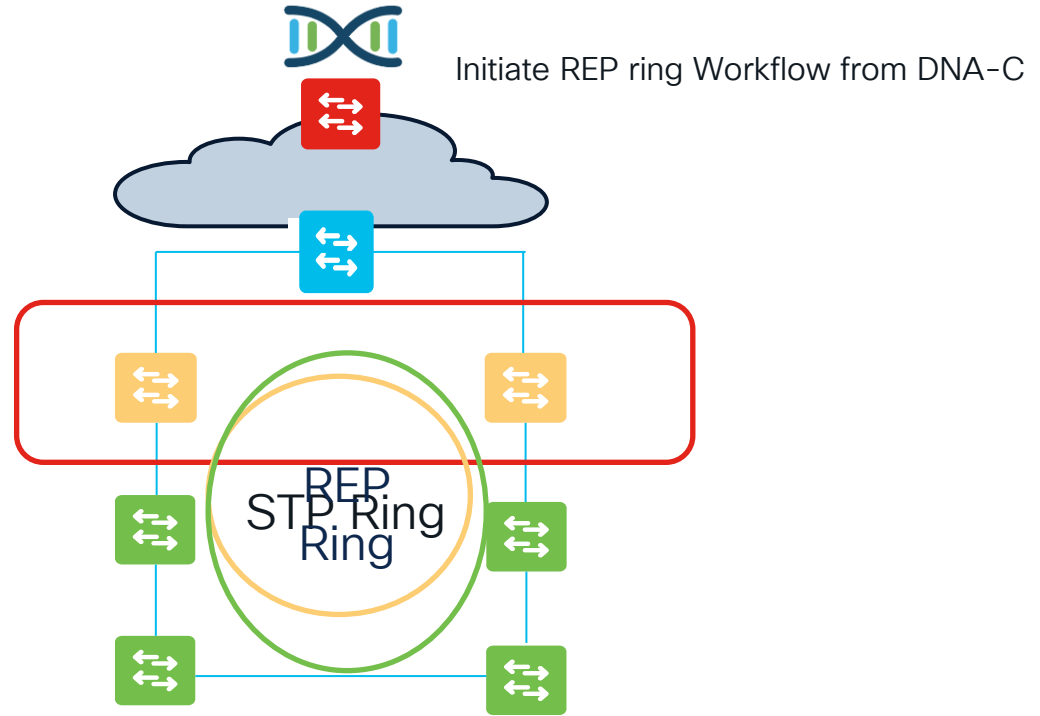
- Border , Control and Edge all in one device
Supports EN/PEN topologies
- Ring and Daisy Chain support
- Allows remote Extension

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 (EFT) + GA

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

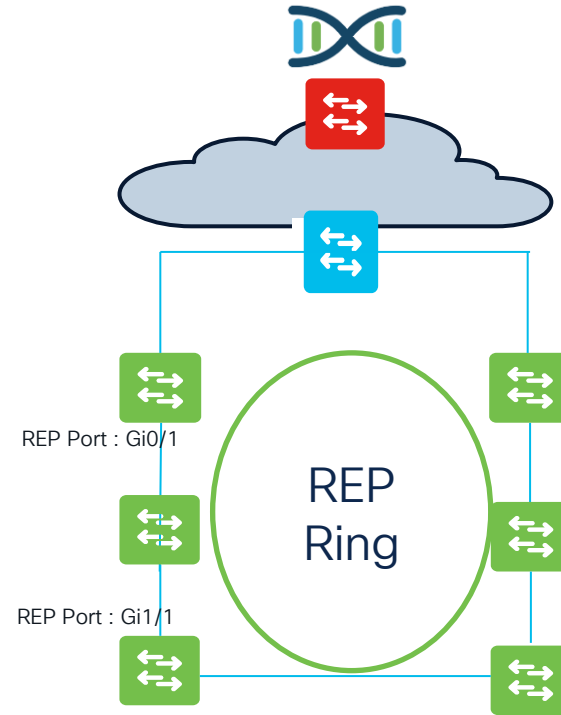
REP Topology Status:

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

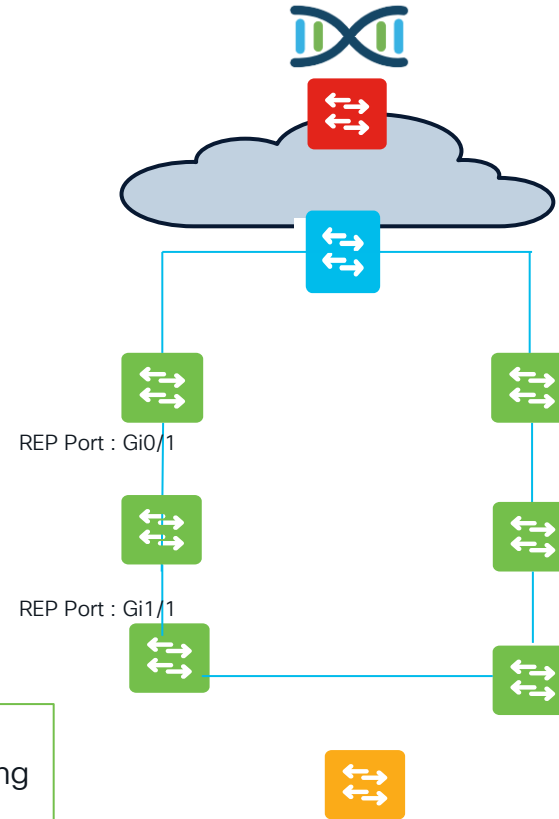
- Remove faulty EN/PEN Node
- Connect REP ports back
- Node part of REP ring

Available from 2.3.2.x [CA]



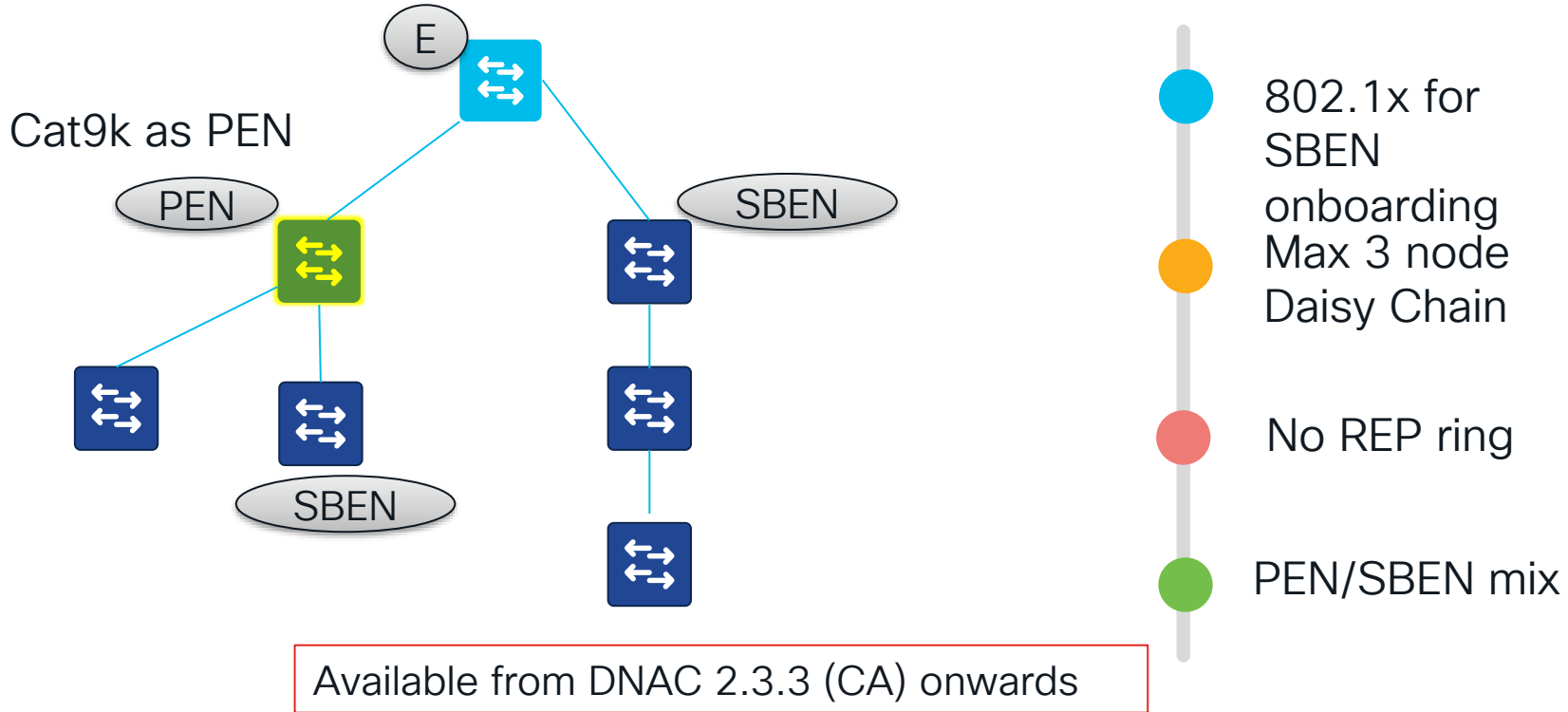
Ring Operations : Adding a node

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



Advanced feature to Dynamically Discover and On-board new node in existing REP ring is coming soon in next release.

Supplicant Based EN – CAT9k only



Conclusion

- Choose the Extended node types (EN/PEN/SBEN) based on current and future needs.
- Choose the Topology and Policy enforcement points based on use-case. (Hub-Spoke, Daisy Chain, Ring)
- Consider FIAB for remote extension use-cases

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

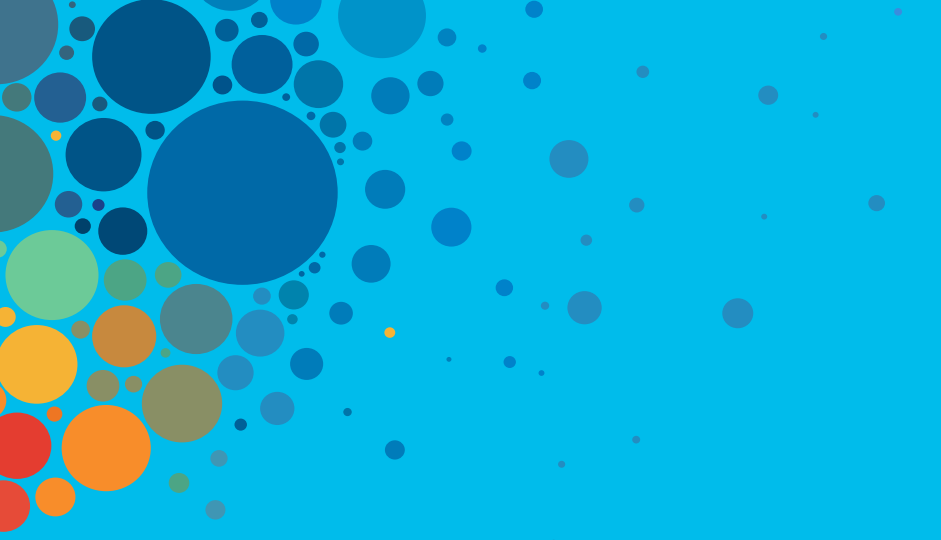
Cisco Guided Study Groups

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

Q & A



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive

DNA Licensing – Extended Node

2 DNA license (Advantage, Essentials)

- Essentials is for pure networking buyers
- Advantage required for SDA Extended Node
- DNA license purchased for 3,5 year terms

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