cisco

You make **possible**

Extending Cisco SD-Access

Beyond Enterprise Walls

Vinay Saini, Solutions Architect   @vinsaini

BRKCRS 2832

Barcelona | January 27-31, 2020

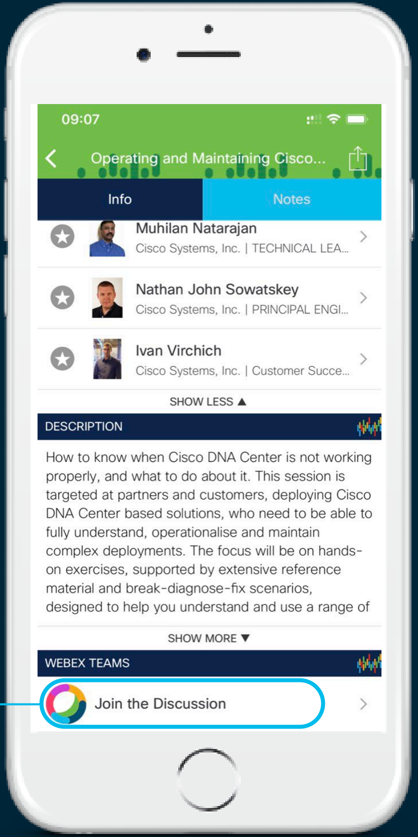
Cisco Webex Teams

Questions?

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

How

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



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

What’s the Extended Enterprise?

Extended Enterprise

Ruggedized Industrial Networking Products

+

Non-carpeted/ Outdoor Spaces

Roadways

Parking Lot

Distribution Center

Airport

Manufacturing

Port/Terminal

Warehouse

CISCO
IE 4000
CONSOLE

Expectations from this extended network?

Need for Ruggedization (outdoor, non-carpeted deployments)	Industrial Ethernet (-40-75C)
Easy to Manage IoT networks	Intent-based Network Management with DNA-C
Need security for E-W traffic	802.1x/MAB authentication Macro-segmentation(VLAN/VRF) & Micro-segmentation(SGT, SGACL)
Need for Redundancy and fast convergence	Ring Management protocols
Need for Scale	Incrementally add network nodes and endpoints

Your Presenter Today

Vinay Saini

Solutions Architect – Cisco CX

- 15+ years in Enterprise & IIoT Industry
- CCIE Wireless#38448, CWNE#69
- Active Contributor to Cisco Certification programs.
- Tsdsi (3gpp) member.

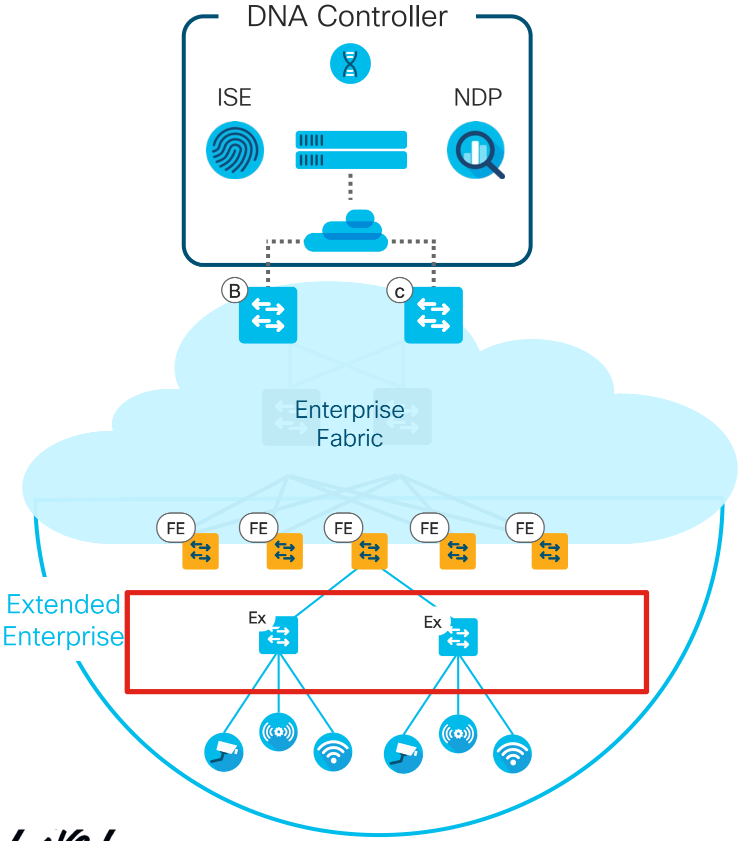
Agenda

- Introduction.
  - Need and use-cases for extended networks
- Cisco SD-Access Basics
  - Quick look into Fabric constructs
- Methods to Extend Network
  - Networks without Fabric
  - Networks with existing Fabric
- Deep Dive
  - Fabric design with Extended Nodes
  - Fabric design with policy extended nodes
  - Packet walks
  - Supported topologies

Cisco SD-Access for Extended Network

SD – Access Architecture for IoT

Component Roles & Terminology



- 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 – A Edge access device that connects Wired IoT Endpoints to the SDA Fabric via a Fabric Edge Node

Why Cisco SDA for Extended Nodes?

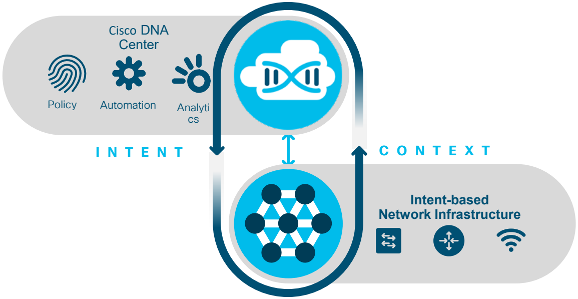
Common workflow, enabling more use cases

Centralized Management
Automated configuration and
IBN management

Security enforcement at network Edge

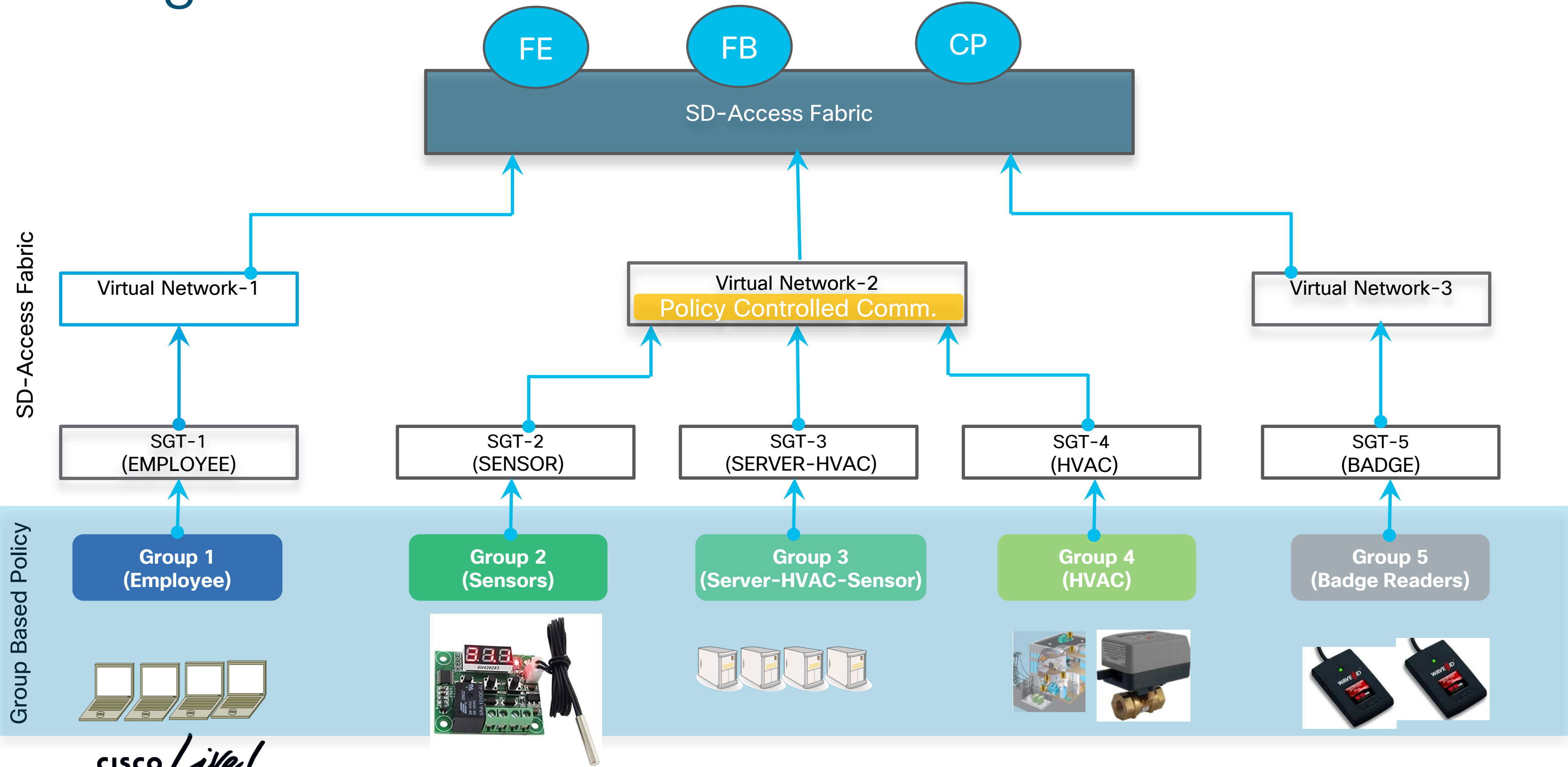
Consistent Policy
Macro & Micro segmentation

Network Admin focus on ‘Intent’,
and how to build Policies.



Operational Simplicity

Segmentation constructs in Fabric



FE

FB

CP

SD-Access Fabric

SD-Access Fabric

Virtual Network-1

Virtual Network-2

Policy Controlled Comm.

Virtual Network-3

SGT-1
(EMPLOYEE)

SGT-2
(SENSOR)

SGT-3
(SERVER-HVAC)

SGT-4
(HVAC)

SGT-5
(BADGE)

Group Based Policy

**Group 1
(Employee)**

**Group 2
(Sensors)**

**Group 3
(Server-HVAC-Sensor)**

**Group 4
(HVAC)**

**Group 5
(Badge Readers)**

Extended Enterprise - Deployment Scenario's

Non-Fabric with Cisco DNA-C

- Traditional Network – Collapsed core or Three layer
  - DNA Centre Appliance and license

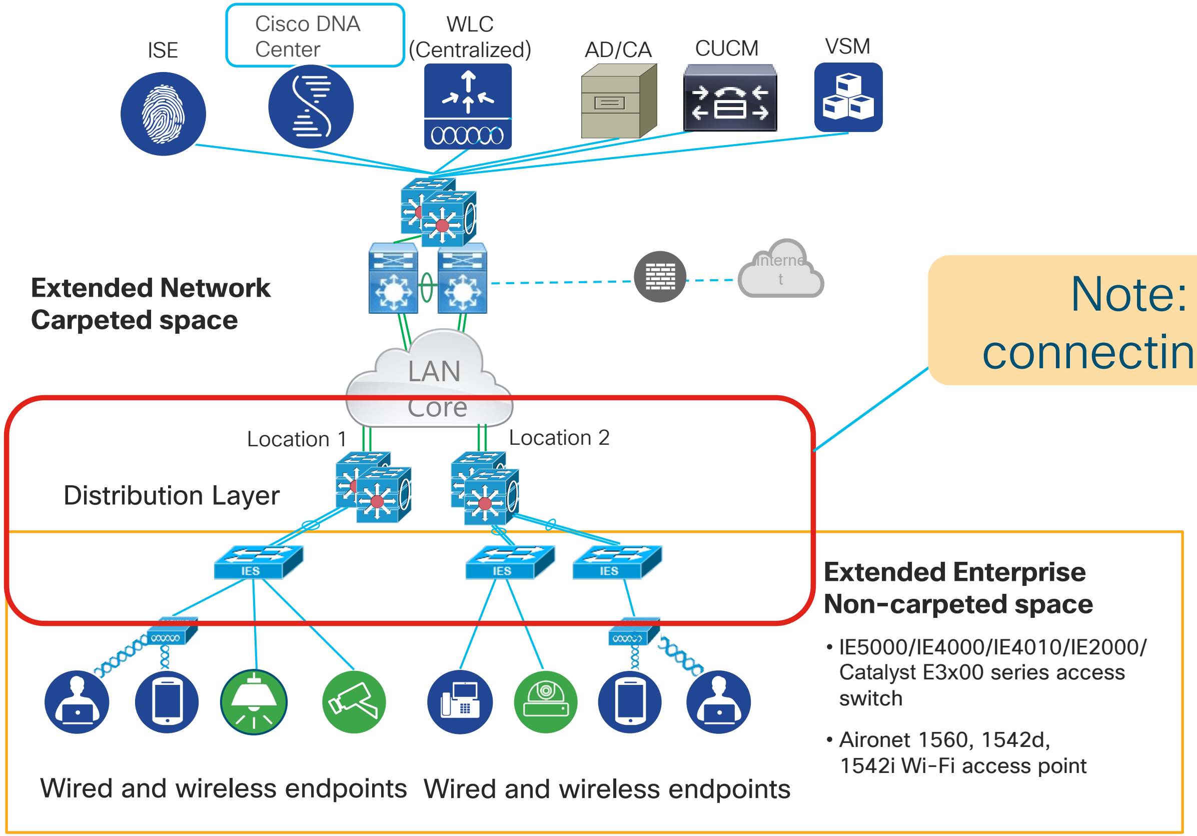
Cisco SD-Access Fabric with Cisco DNA-C

- Cisco SD-Access Fabric with Control, Border and edge nodes
  - DNA Centre Appliance and license

Extending Non-Fabric Network

Seems like Fabric is missing

Non-Fabric Extended Enterprise Deployment



Extended Network Carpeted space

Note: IE switches connecting to distribution

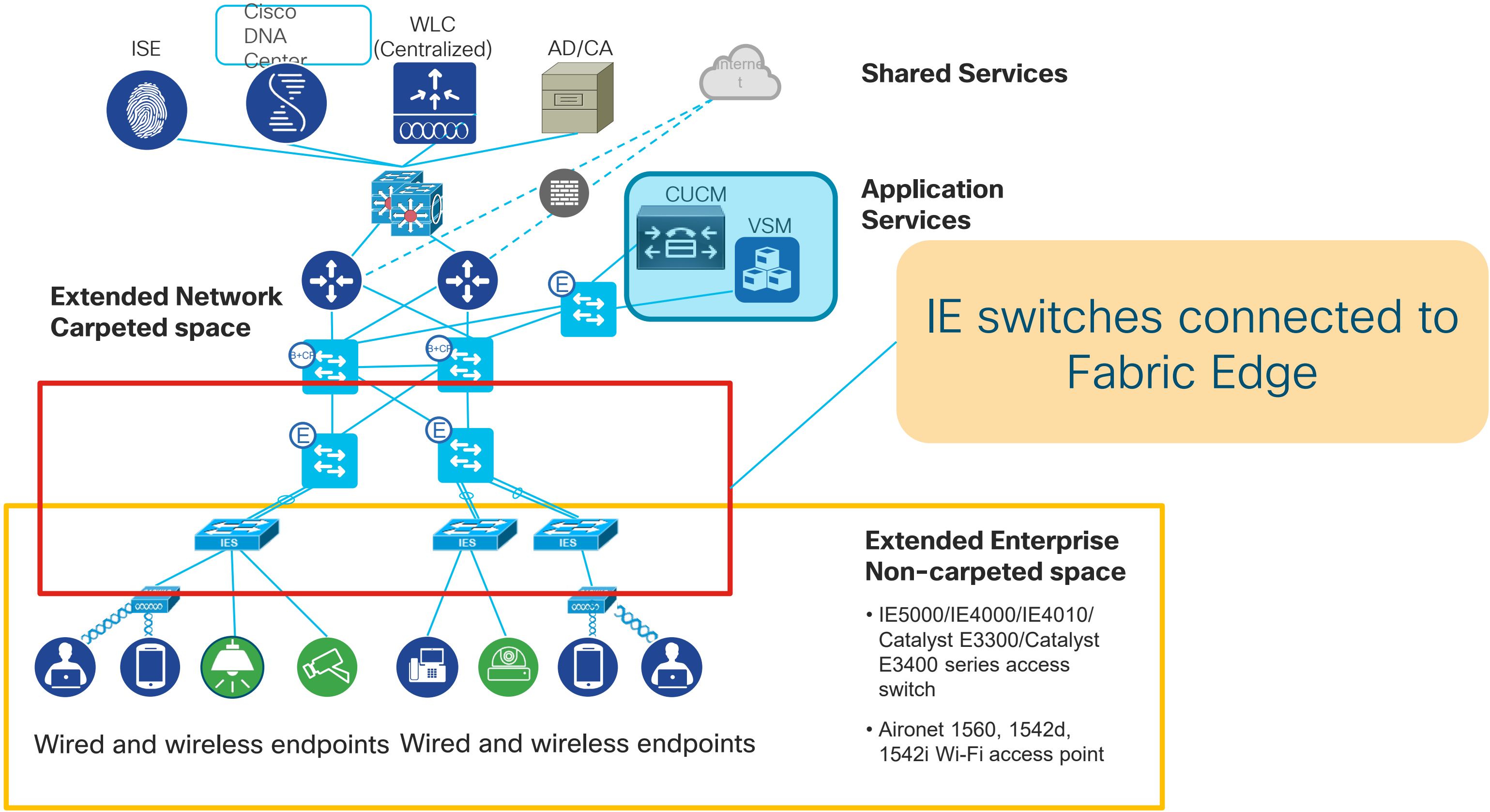
Extended Enterprise Non-carpeted space

- IE5000/IE4000/IE4010/IE2000/ Catalyst E3x00 series access switch
- Aironet 1560, 1542d, 1542i Wi-Fi access point

Extending Cisco SDA Fabric Network

Fabric – lot of options

Extended Enterprise SD-Access Deployment



Shared Services

Application Services

Extended Network Carpeted space

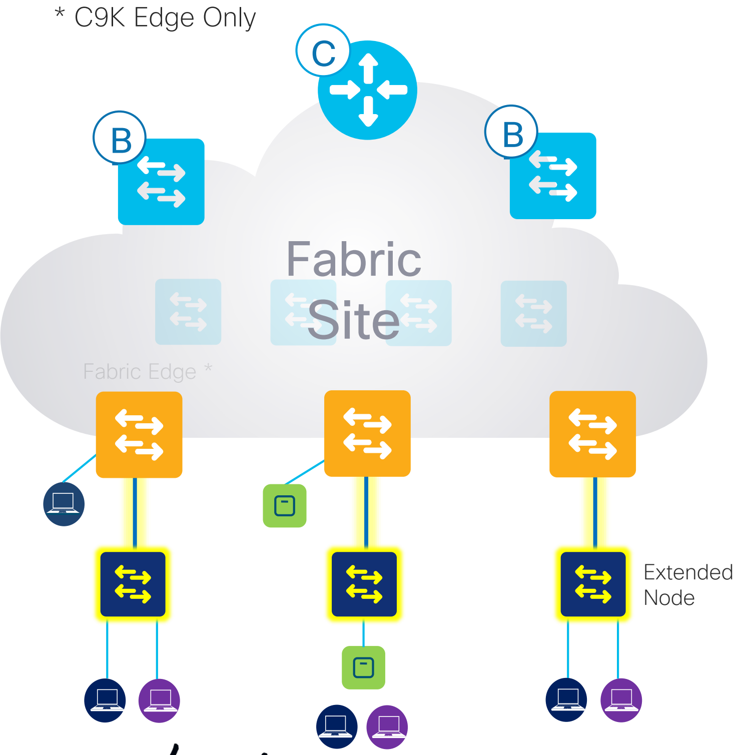
IE switches connected to Fabric Edge

Extended Enterprise Non-carpeted space

- IE5000/IE4000/IE4010/ Catalyst E3300/Catalyst E3400 series access switch
- Aironet 1560, 1542d, 1542i Wi-Fi access point

Wired and wireless endpoints Wired and wireless endpoints

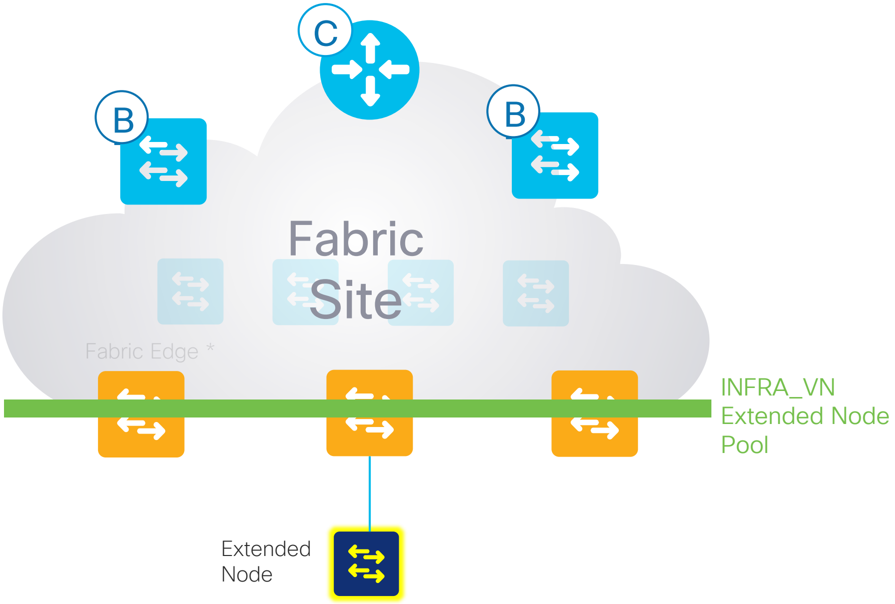
SD-Access Extended Node



- Extended node connects to a fabric Edge node using an 802.1Q Trunk port .
- Extended node initial bring up using plug & play (PNP).
- Switch ports on the Extended node can then be statically assigned to an appropriate IP Pool or dynamically assigned using authentication via DNA Center.
- Policy tagging is done on the fabric edge nodes.
- Group based policy enforcement performed at the Fabric Edge node.

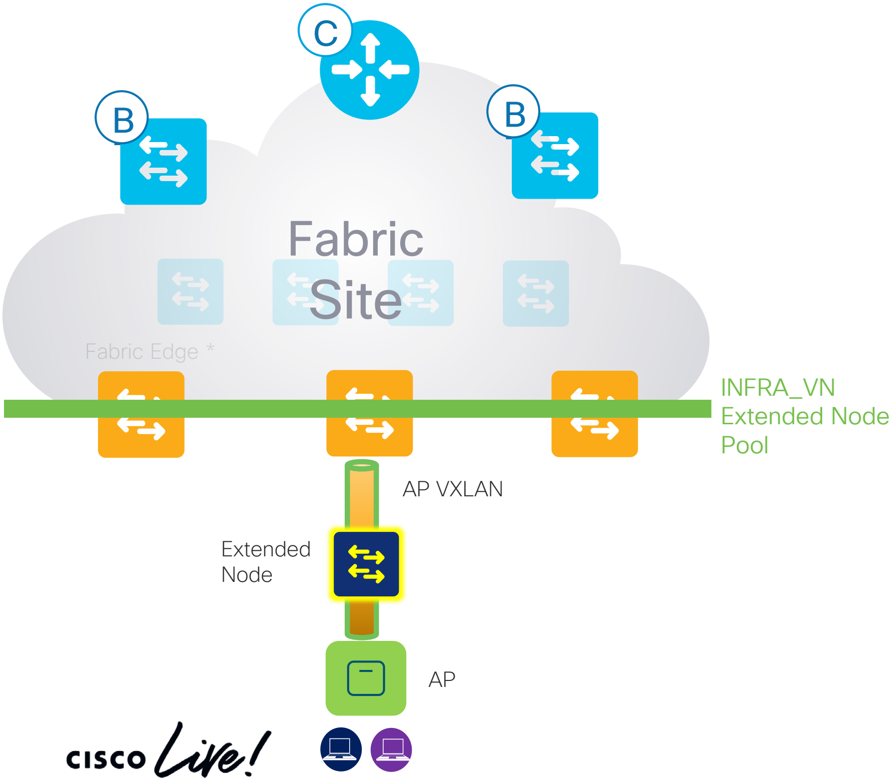
Let’s see some Packet Flows

Extended node Deployment Details



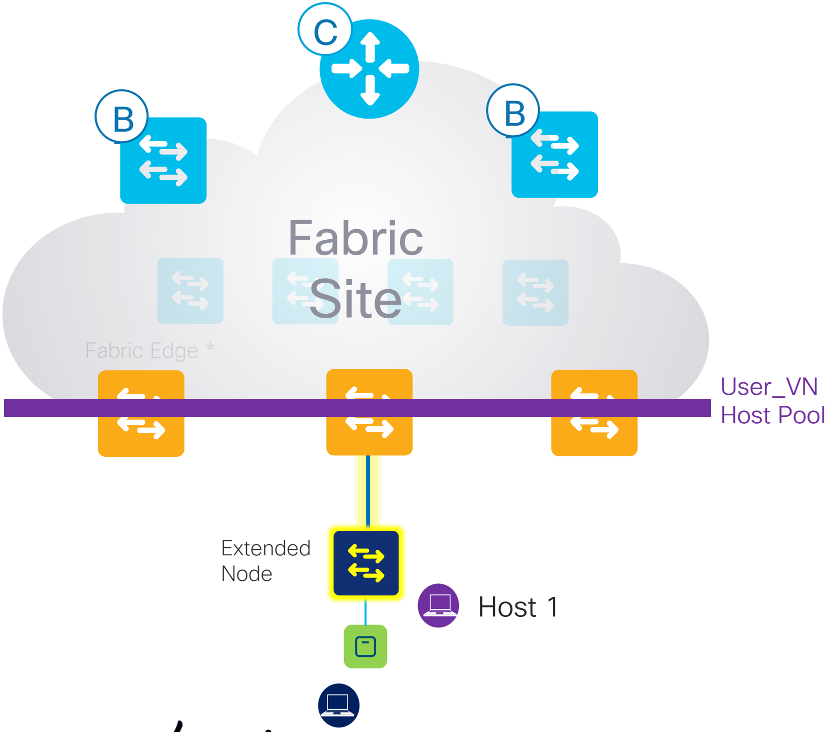
- User and Management IP Subnets range is picked from the Fabric IP Pools.
- Every Extended node will have one Management IP Pool, in the INFRA_VN and registered with the Control Plane.
- MACRO running on the edge nodes automatically detects the Extended Nodes.
- The Border advertises Extended nodes IP Pool to the external world as with other IP Pools.

Extended node: Access Point Connectivity

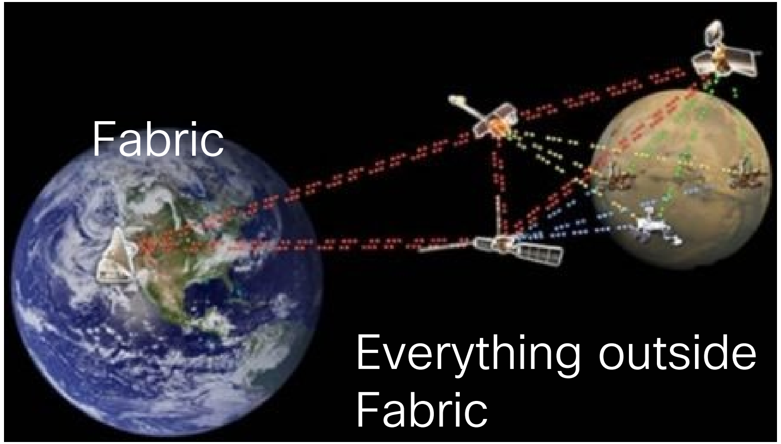


- AP Management IP Subnets range is picked from the AP IP Pools
- MACRO running on the Extended nodes automatically detects the AP and places them in the right subnet
- AP creates a VXLAN overlay tunnel to the fabric edge node
- User traffic from Wireless Client to Fabric follows the AP VXLAN tunnel

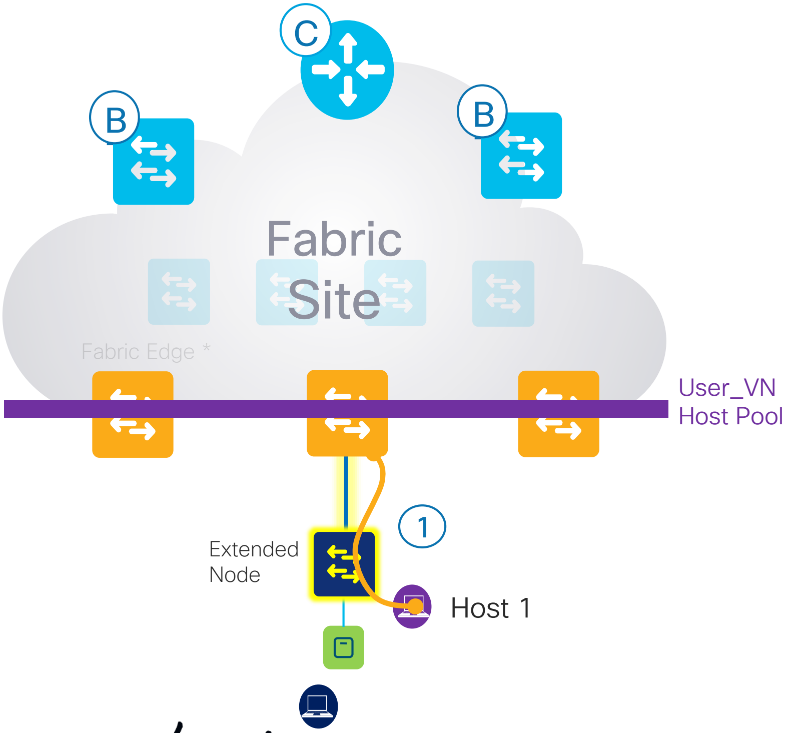
Packet Flow- Extended Nodes



0 Host 1 wants to talk to the external world

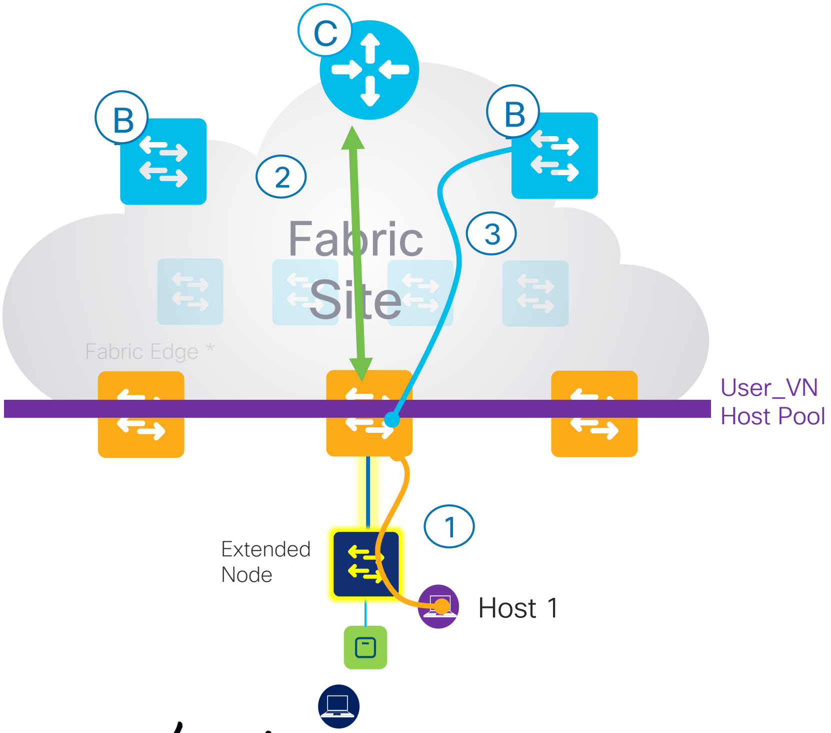


Packet Flow- Extended Nodes



1 The host connecting to the extended node sends traffic to fabric edge node as the default gateway exists on the fabric edge node.

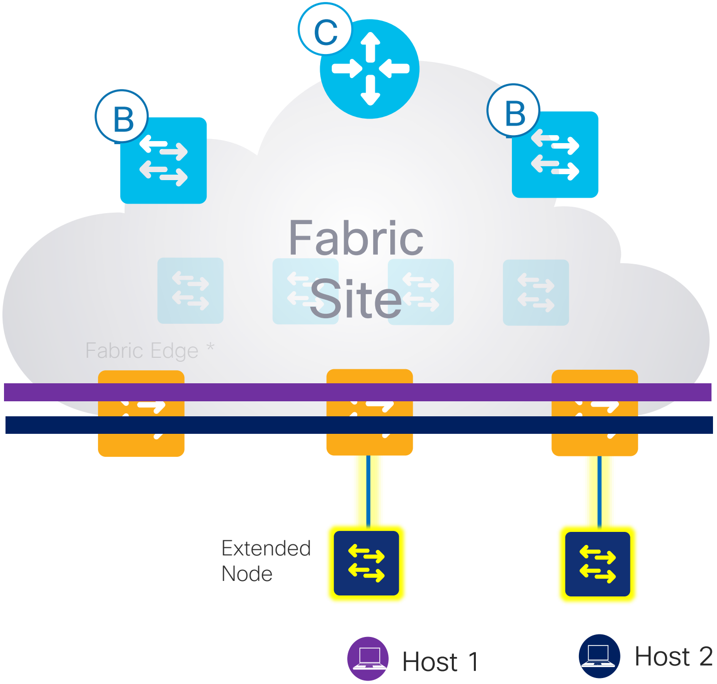
Packet Flow- Extended Nodes



2 The fabric edge node will consult the control plane on where to send traffic.

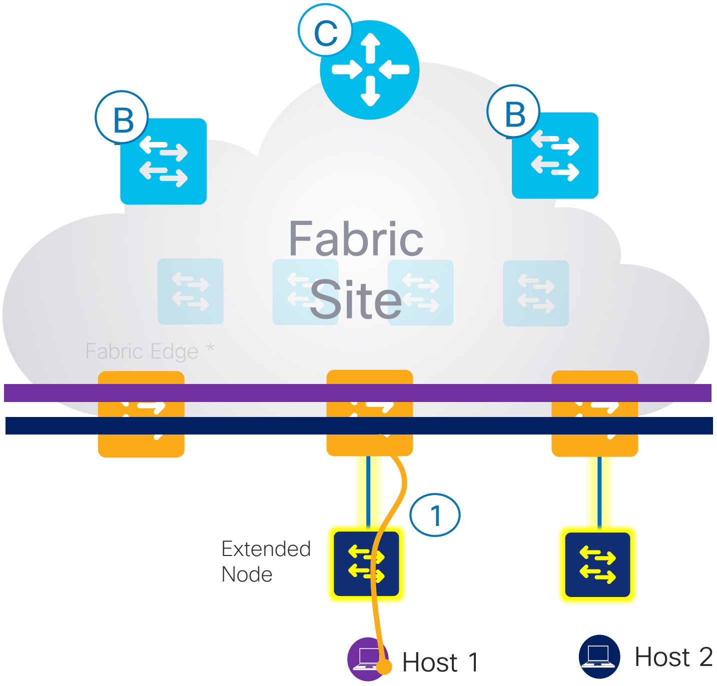
3 CP node tells to go via Border node.

Packet Flow- Extended Nodes



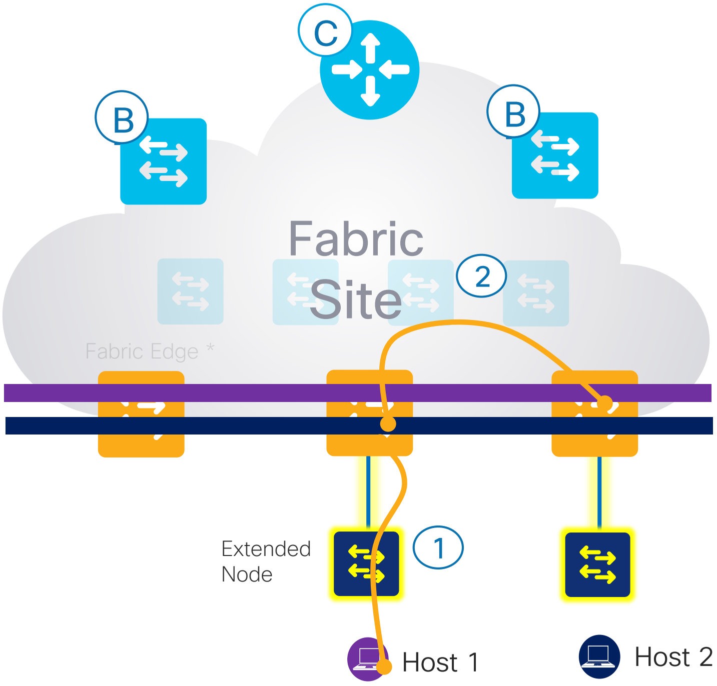
0 Host 1 wants to talk to Host 2

Packet Flow- Extended Nodes



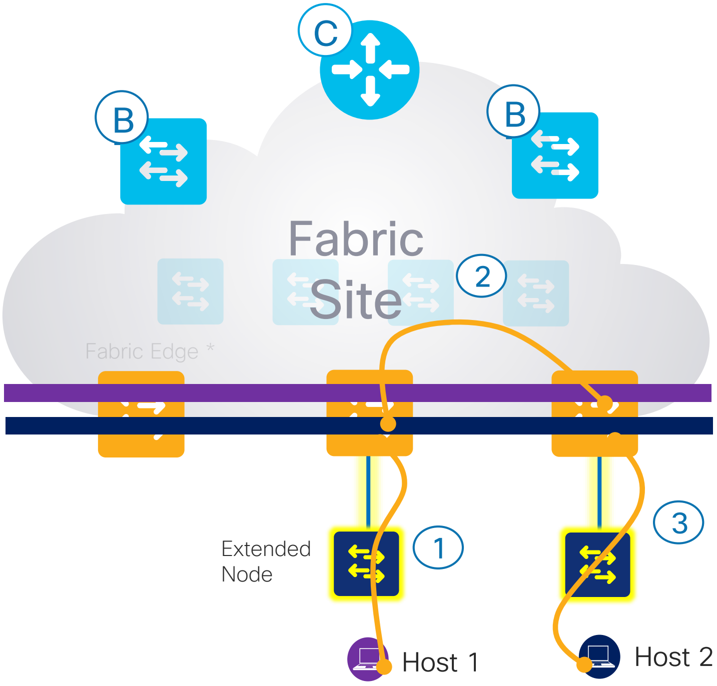
1 The host connecting to the extended node sends traffic to fabric edge node as the default gateway exists on the fabric edge node.

Packet Flow- Extended Nodes



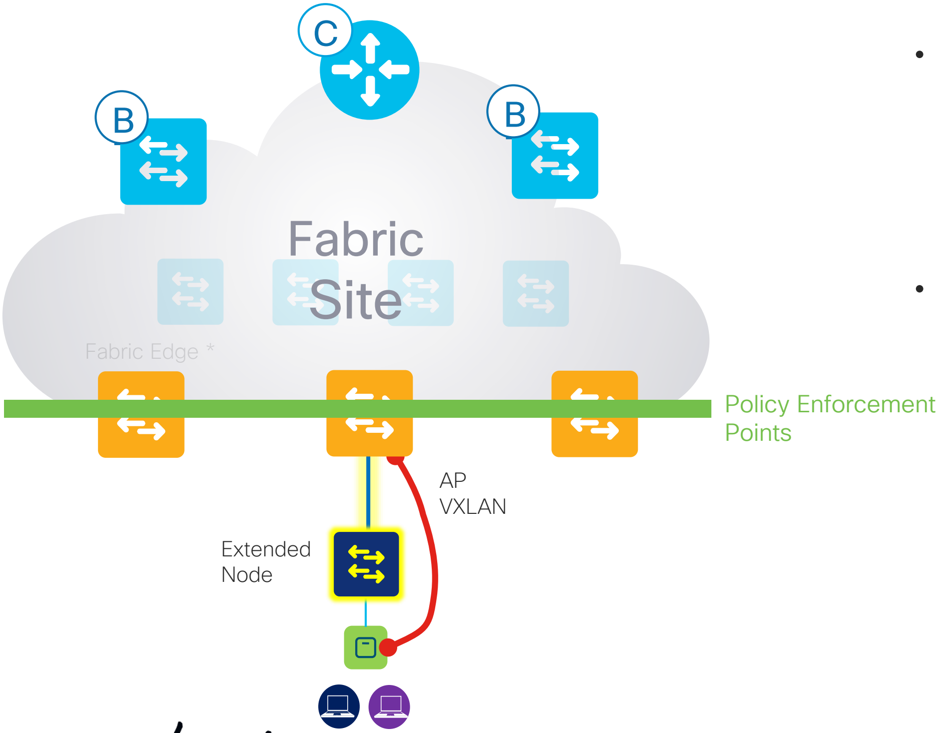
2 The fabric edge node will consult the control plane on where to send traffic and ensures the traffic reaches to the destination (VXLAN encap). In this case it is sent to the other edge node.

Packet Flow- Extended Nodes



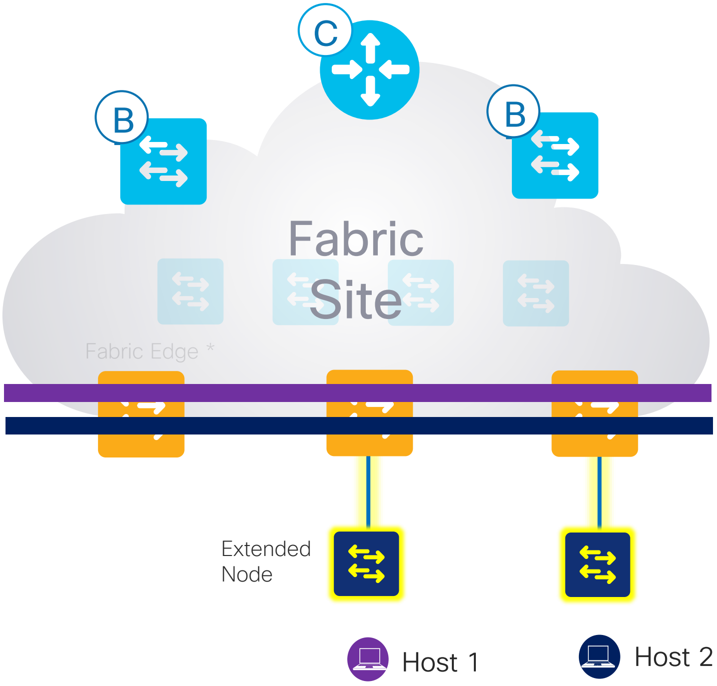
3 The destination fabric edge sends traffic to the destination host.

Policy Enforcement - Extended Nodes



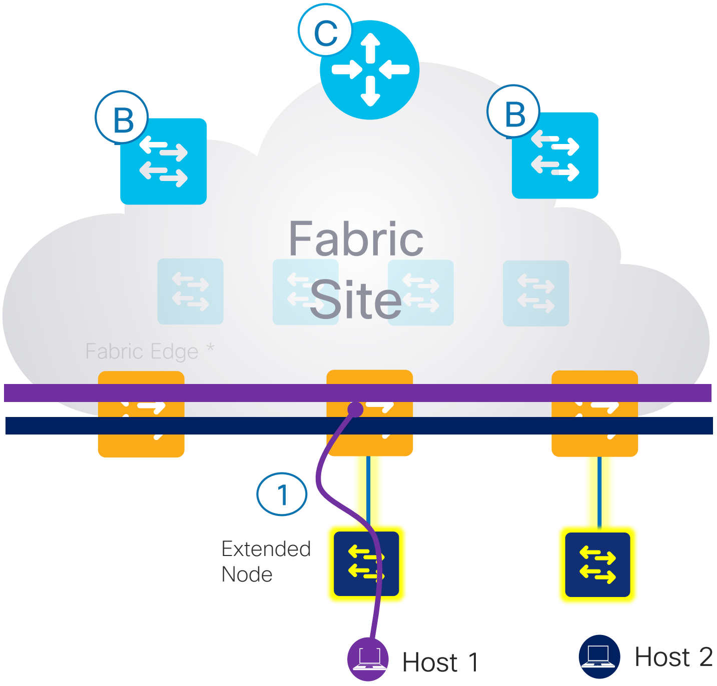
- SGT tagging/mapping for policy is done as below
  - ➢ Subnet to SGT mapping via DNAC on the fabric edge node
- Traffic policy enforcement based on SGT’s/SGACL’s is done at the fabric edge node.

Policy Enforcement - Extended Nodes



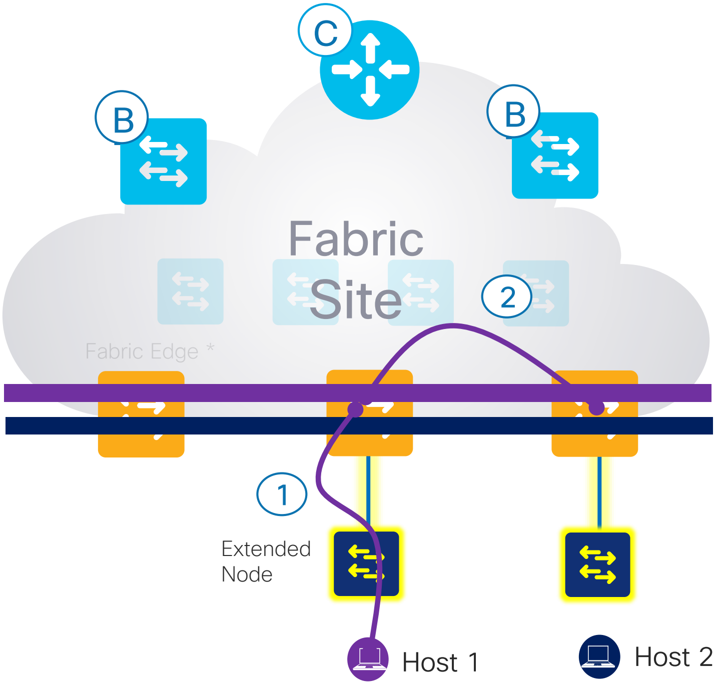
0 Based on policy Host 1 cannot talk to Host 2

Policy Enforcement - Extended Nodes



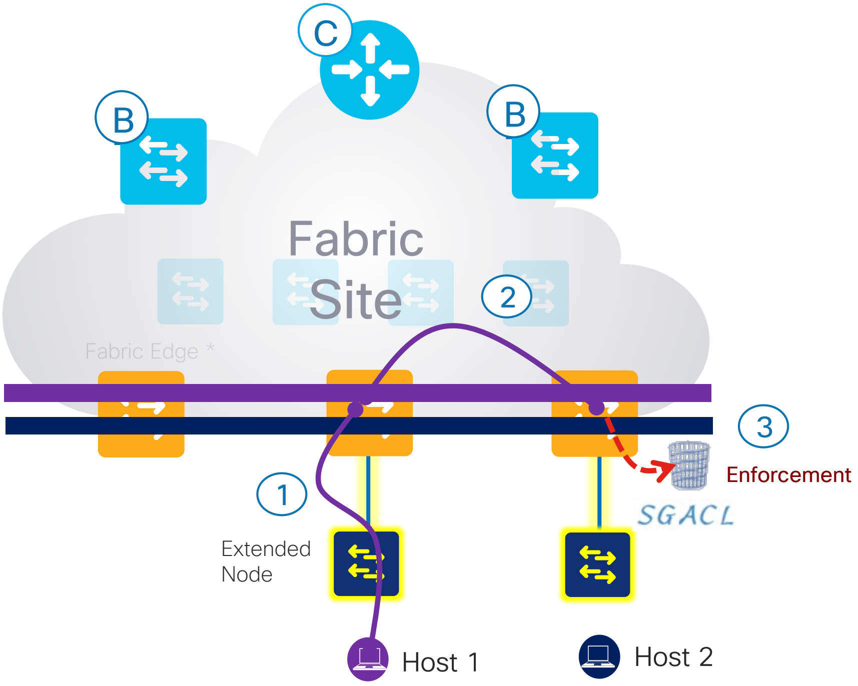
1 When traffic from Host 1 comes to the fabric edge node its tagged with the SGT value for the IP Subnet of Host 1.

Policy Enforcement - Extended Nodes



2 The SGT tagged Traffic gets to the destination edge node where policy is enforced.

Enforcement - Extended Nodes



3 The traffic is dropped as the policy does not allow it.

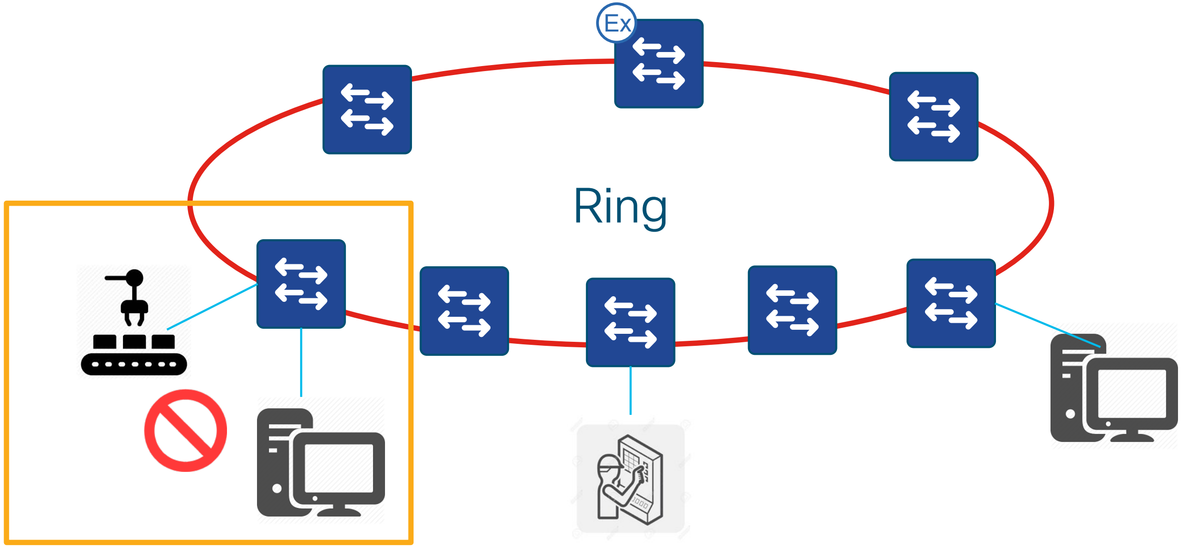
Policy Says:

Host 1 IP subnet cannot talk to Host 2 IP subnet.

Anything Missing ???

Real world IoT Networks

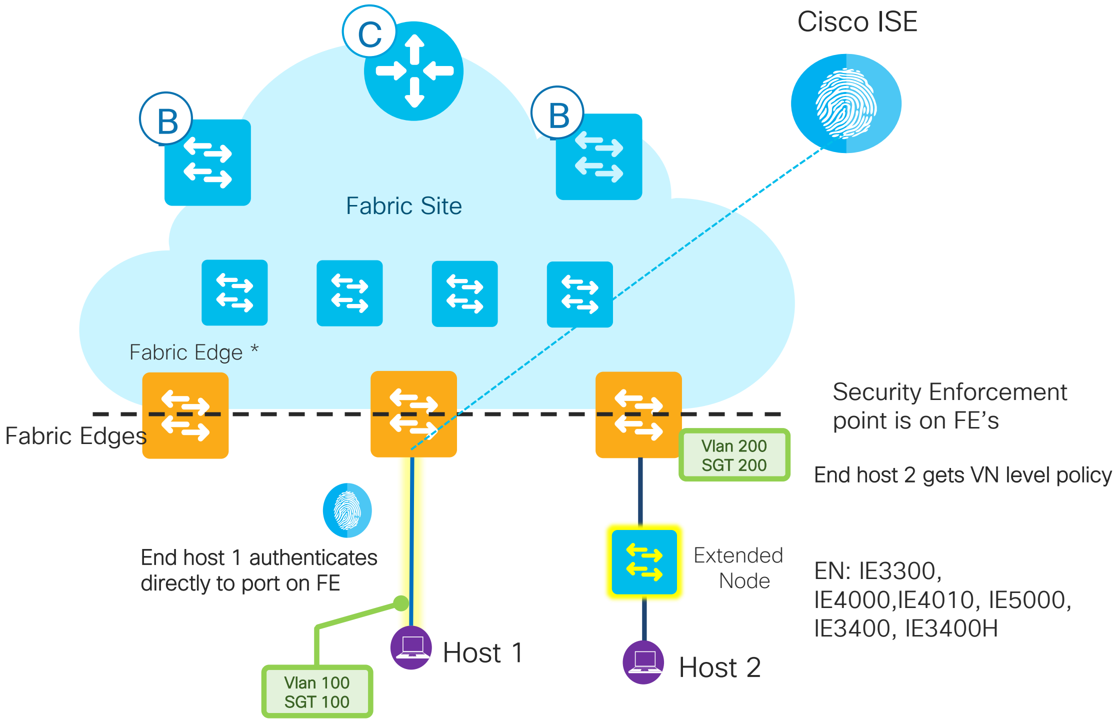
Security Required on East-West Traffic and at access level



Policy Extended Nodes (SEN)

Security to next level

SDA Security Before Policy Extended Node

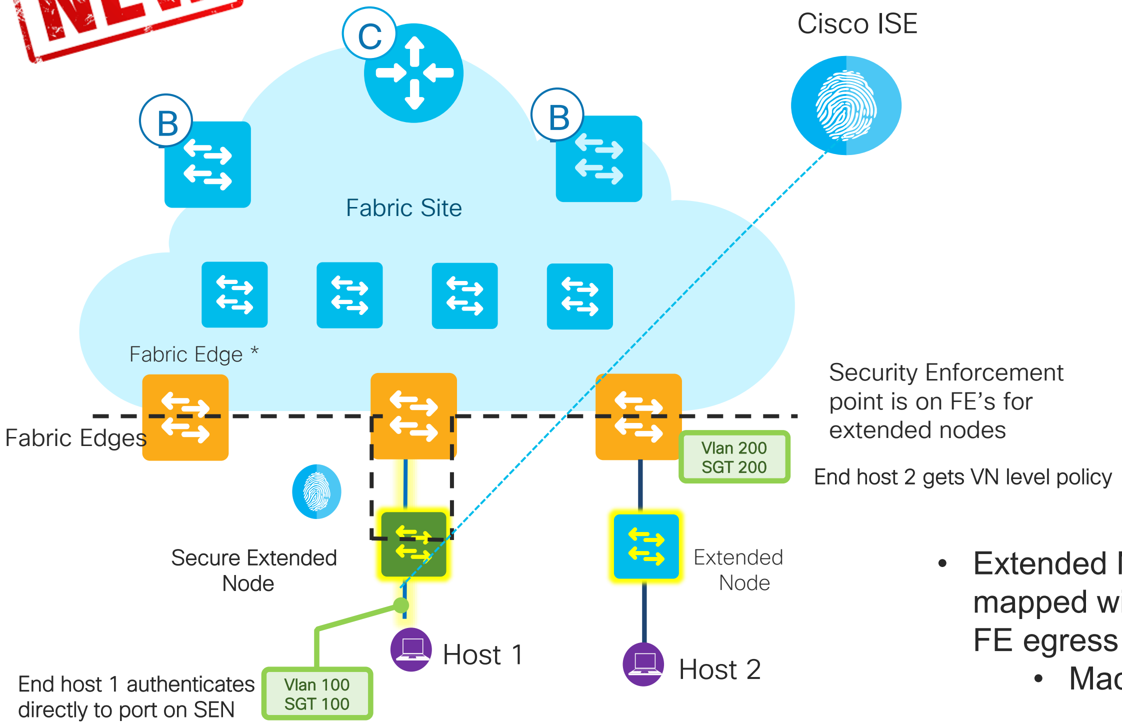

Cisco ISE
C
B
B
Fabric Site
Fabric Edge *
Fabric Edges
Security Enforcement point is on FE's
Vlan 200
SGT 200
End host 2 gets VN level policy
End host 1 authenticates directly to port on FE
Extended Node
EN: IE3300, IE4000,IE4010, IE5000, IE3400, IE3400H
Host 1
Host 2
Vlan 100
SGT 100

- The ***Fabric Edge*** will have 802.1x/MAB Authentication enabled to talk to ISE and to download the right vlan and **Secure Group Tag** attributes to the end points
- Fabric Edge is LISP and ISIS with VXLAN
  - Not in Extended Node
  - Extended Node is Layer 2 only
- Fabric Edge performs security (SGACL) enforcement on egress interface
- End devices connected to Extended Node are put in default SGT / SGACL group for the Virtual Network/VLAN

SDA Security with Policy Extended Node

NEW

with Cisco DNA-C 1.3.3

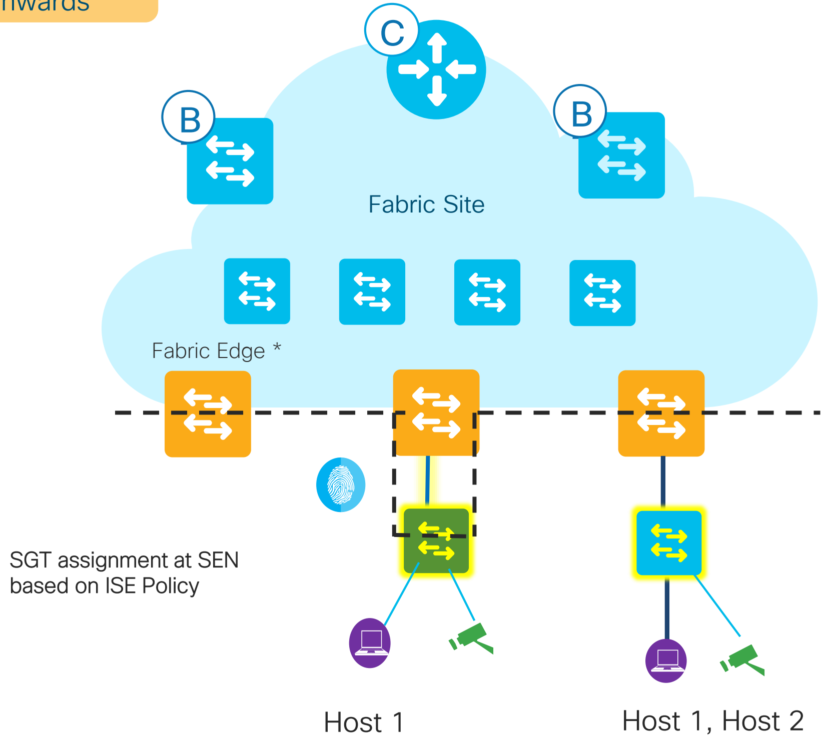


Cisco ISE
C
B
B
Fabric Site
Fabric Edge *
Fabric Edges
Security Enforcement point is on FE's for extended nodes
Vlan 200 SGT 200
End host 2 gets VN level policy
Secure Extended Node
Extended Node
Host 1
Host 2
End host 1 authenticates directly to port on SEN
Vlan 100 SGT 100

- The ***Policy Extended Node*** will have 802.1x/MAB Authentication enabled to talk to ISE and to download the right vlan and **Secure Group Tag** attributes to the end points
- Policy Extended node performs security (SGACL) enforcement on egress interface.
  - Micro Segmentation
- Extended Node puts end devices in default SGT group mapped with VLAN at the FE port. Enforcement for Host 2 on FE egress port.
  - Macro Segmentation

SDA Security with Policy Extended Node

Available in DNAC 1.3.3 onwards



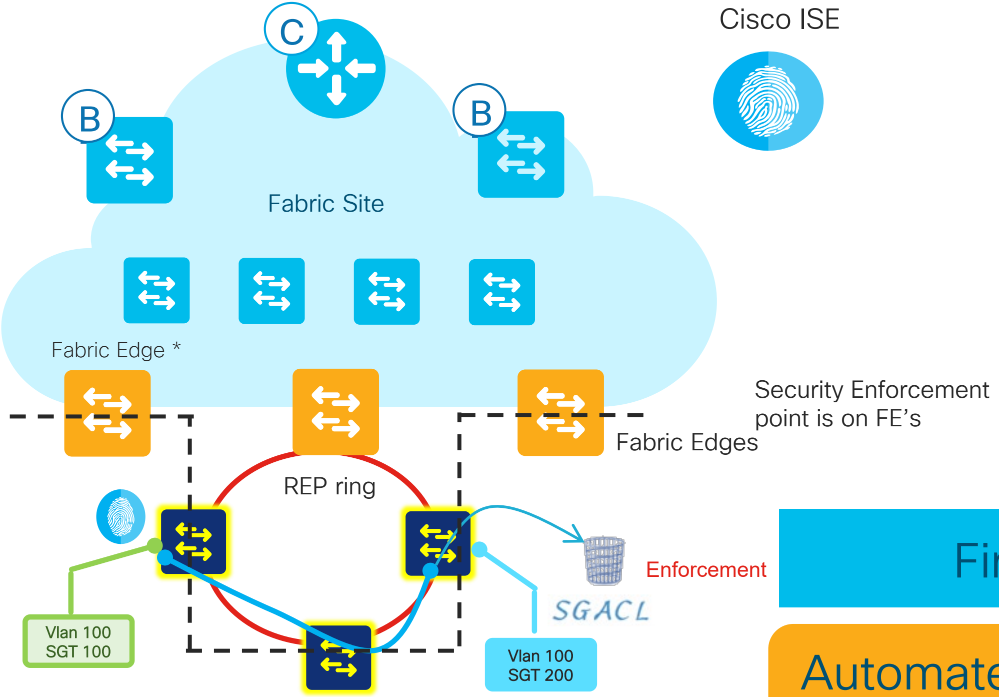
Simplify configuration with policy extended node

- No Individual VLAN for Hosts requiring segregation
- SEN will interact with ISE and provide port level SGT mapping.

Extended Nodes

Number of VLANS = Segregation groups

Policy Extended Node - SGACLs policy enforcement



- Rings have **East – West** traffic, not North – South. All traffic in same Vlan
- In a ring, Ethernet frames may not reach Fabric Edge ports.
- For Rings, there is no security without policy extended node
- **SGACL enforcement** is always done at the destination **policy extended node** egress port

First Step towards REP Rings

Automated Ring support not available today not with latest1.3.3 DNA-C release

IE Extended Node, Policy extended node platforms

Extended Node

Industrial Ethernet
IE5000

Catalyst IE3300
Rugged Series

Industrial Ethernet
IE4010

Catalyst IE3400
Rugged Series

Industrial Ethernet
IE4000

Catalyst IE3400H
Heavy Duty Series

Policy Extended Node

Catalyst IE3400
Rugged Series

Catalyst IE3400H
Heavy Duty Series

Extended Node, Policy Extended Node & Fabric Edge

	Extended Node	Policy Extended Node	Fabric Edge
Layer	Layer 2 node	Layer 2 node	Layer 3 node
Macro-segmentation	VLAN to VRF mapping	VLAN to VRF mapping	Direct to VRF
Micro-segmentation		Secure Group Tag (Inline Tagging)	Secure Group Tag (Inline Tagging)
Security Enforcement		SGACL At IoT Edge	SGACL at Fabric Edge

DNA Licensing – Extended Node

05059
050590
Nur gültig mit Kontrollabriss
Eintrittskarte
Aufbewahren und auf Verlangen vorzeigen
050590
050

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/IE3400H	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

Supported Topologies

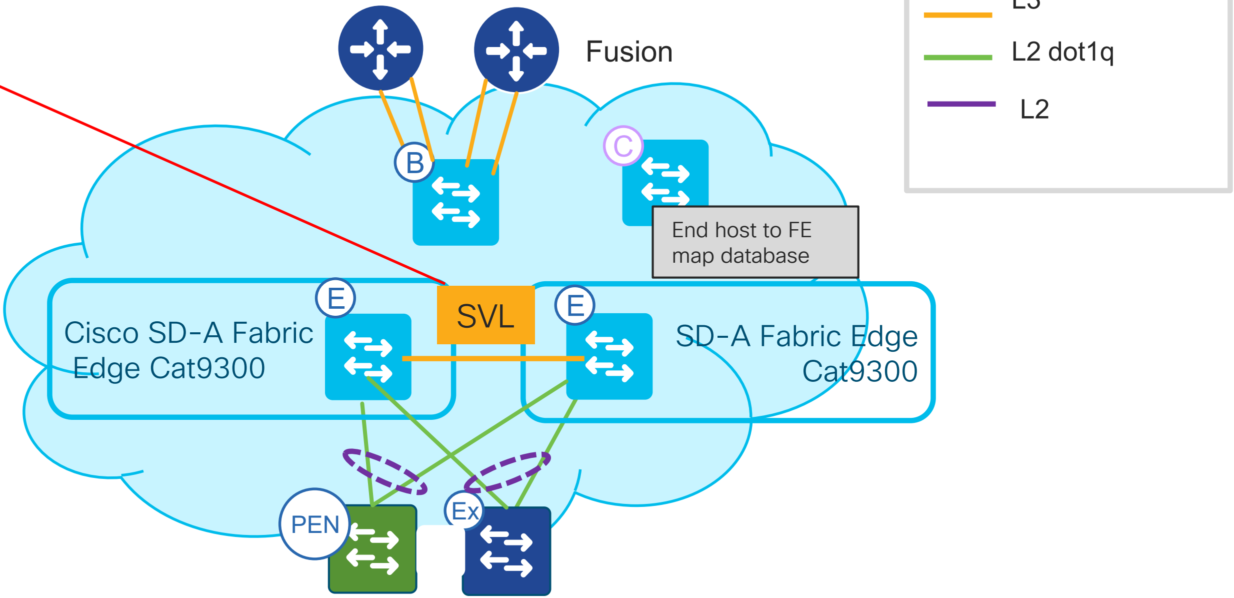
Checking all options

Supported: Extended Node with SVL on FE's

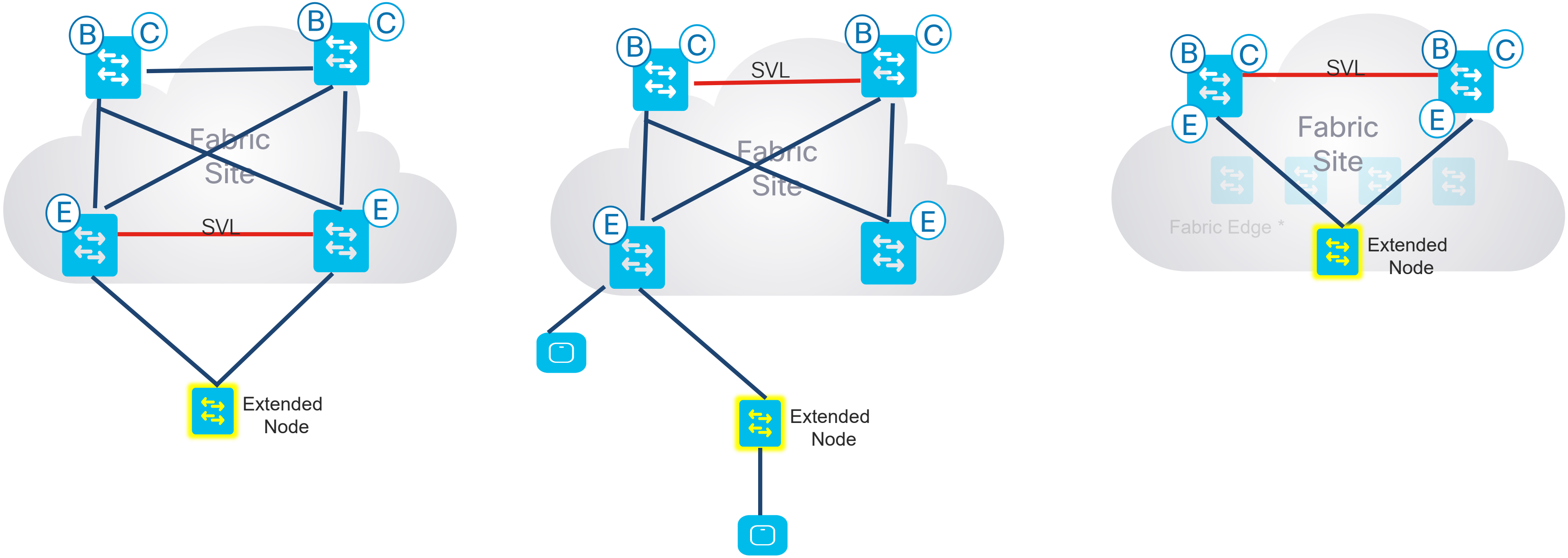
NEW

SVL on Edge supported from DNA-C 1.3.3

Better redundancy with multi chassis connection with SVL between Fabric edges



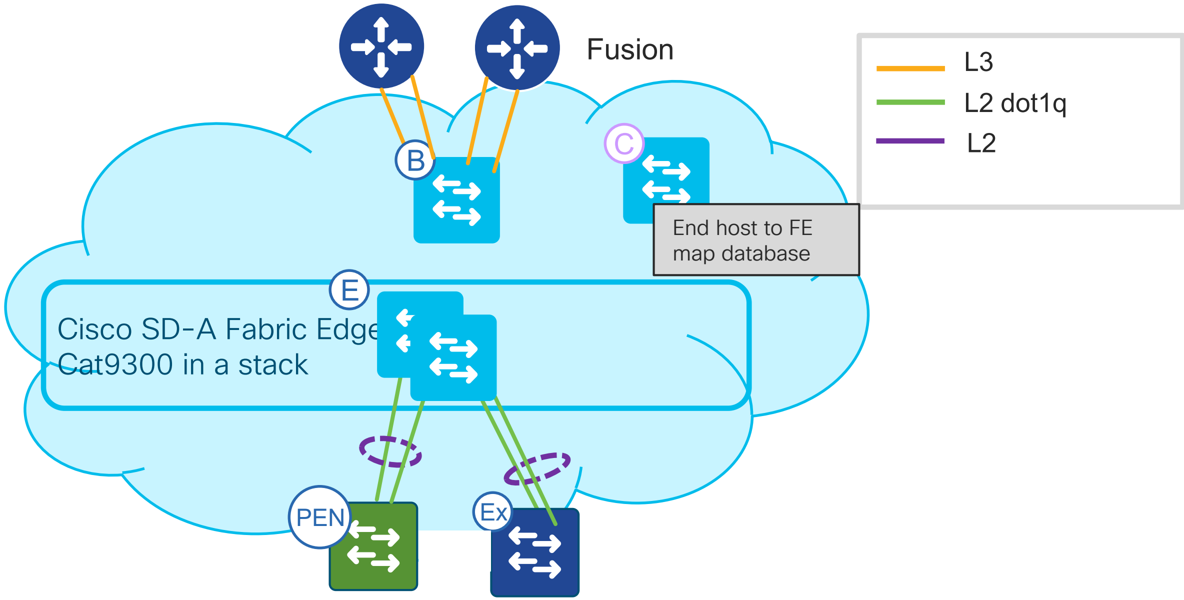
Extended Nodes with SVL



Wireless AP cannot connect directly with nodes connected via SVL : DNA-C 1.3.3

Supported: Extended node to Stacked FE’s

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



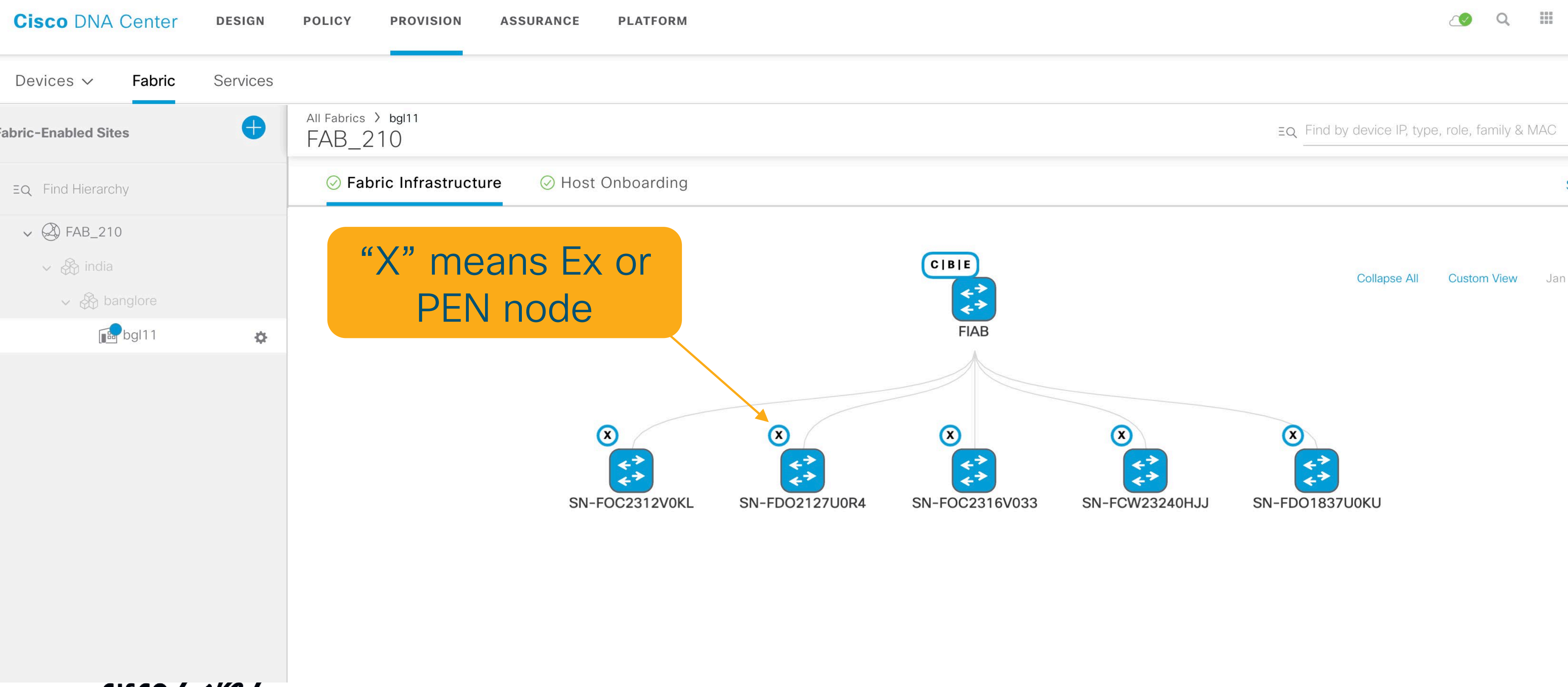
End host to FE map database

Cisco SD-A Fabric Edge Cat9300 in a stack

Extended and policy extended nodes work with Fabric in a Box as well

5113
5115

FIAB with Extended and PEN nodes



"X" means Ex or PEN node

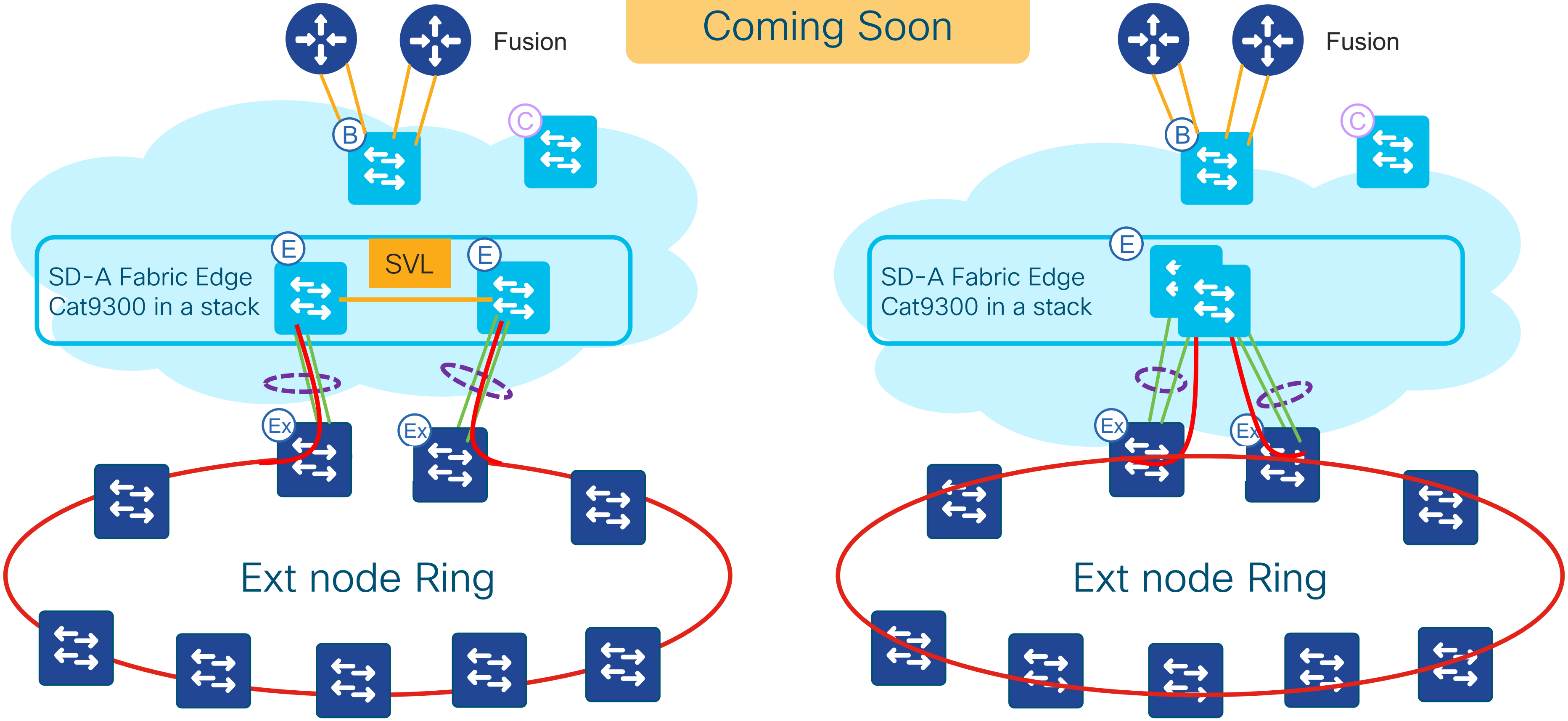
Let’s see what’s coming soon …..

Much desired Six pack features
for
Extended network

Planned for Future releases

🟧	L3
🟩	L2 dot1q
🟥	L2 dot1q + REP
🟪	L2

Coming Soon



Deployment & Provisioning

Simple like a magic

cisco Live!

Ex/PEN Zero Touch Provisioning

Plan

Provision

Design

3 Step Process

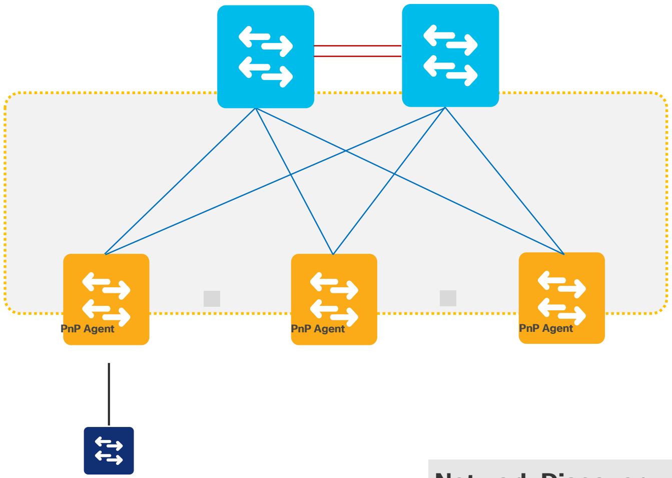
IoT Ready Network

cisco Live!

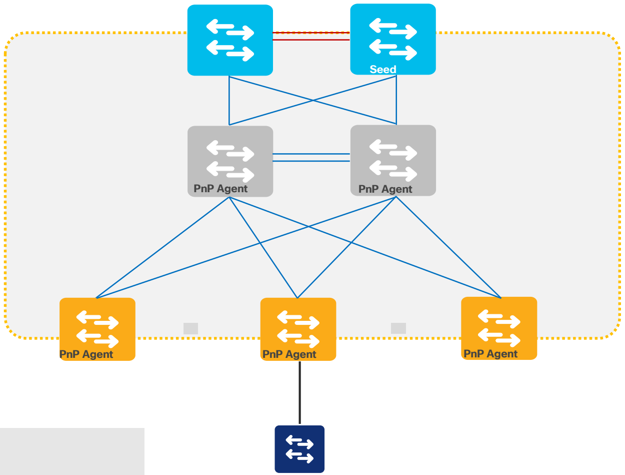
Plan –Step1: Network Design

Cisco DNA Center

2 Tier – Collapsed Core Design



3 Tier – Campus Design



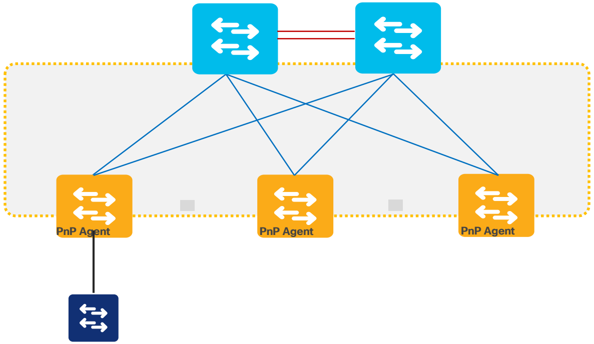
Network Discovery

- Dynamic and on-demand network discovery process
- Fabric edge node programmed to on-board new Extended node switches with zero configurations

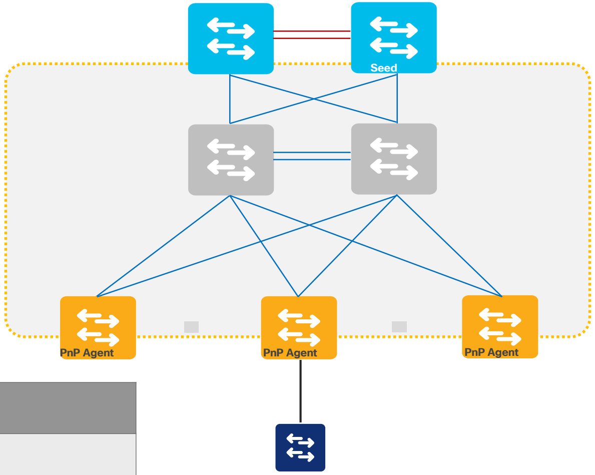
Plan – Step2: Catalyst Switch Role support

Cisco DNA Center

2 Tier – Collapsed Core Design

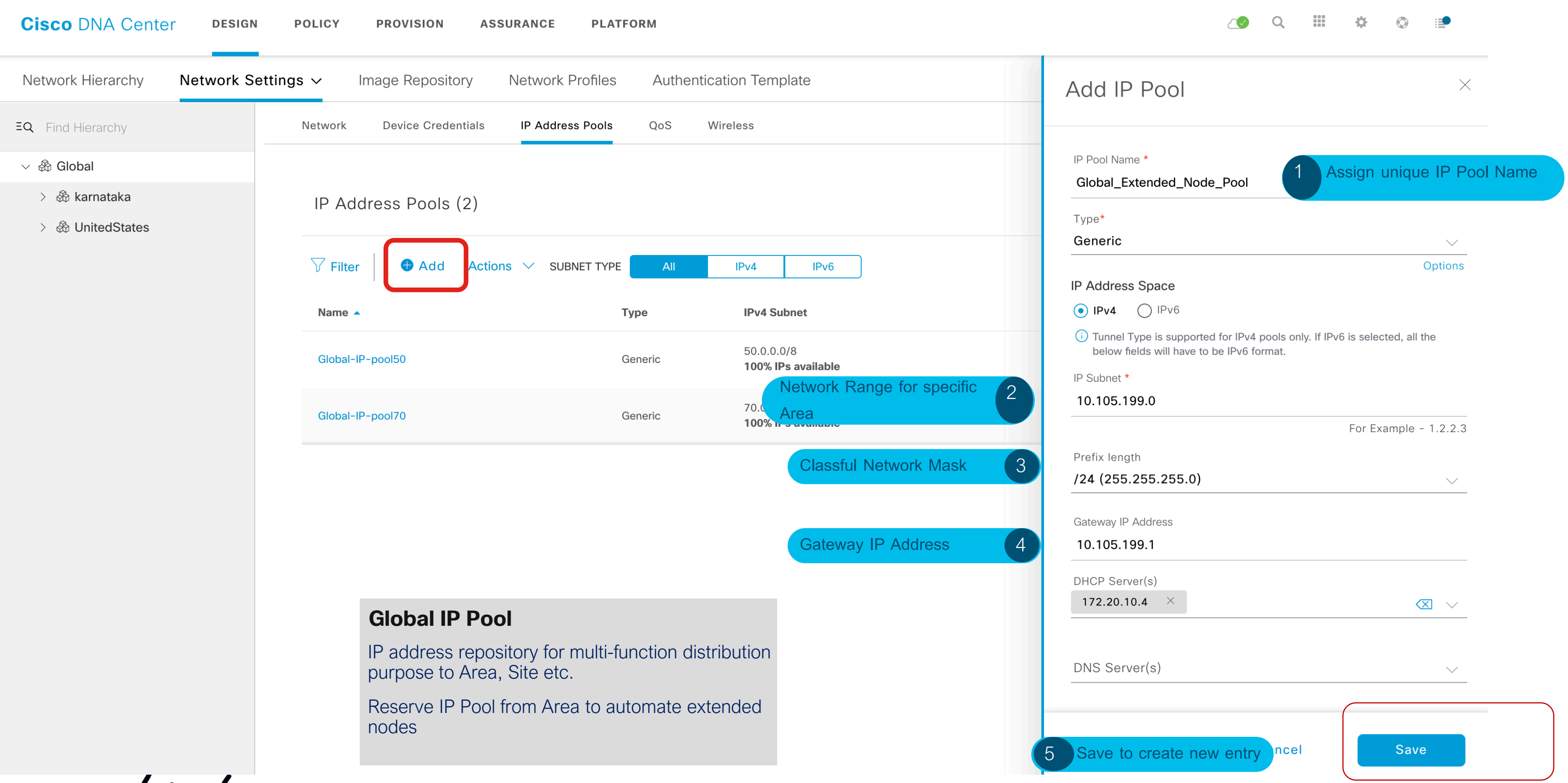


3 Tier – Campus Design



Layer	Role	Supported Switch
Fabric Edge	PnP Agent	Catalyst 9K
Extended Nodes Nodes		3560CX, CDB,IE4K/5K
policy extended nodes nodes		IE3400/IE3400H

Design –Step1: Configure Global IP Range



IP Address Pools (2)

Name	Type	IPv4 Subnet
Global-IP-pool50	Generic	50.0.0.0/8 **100% IPs available**
Global-IP-pool70	Generic	70.0 100%

Add IP Pool

IP Pool Name *: Global_Extended_Node_Pool

Type*: Generic

Options

IP Address Space: ● IPv4 ○ IPv6

Tunnel Type is supported for IPv4 pools only. If IPv6 is selected, all the below fields will have to be IPv6 format.

IP Subnet *: 10.105.199.0

For Example - 1.2.2.3

Prefix length: /24 (255.255.255.0)

Gateway IP Address: 10.105.199.1

DHCP Server(s): 172.20.10.4

DNS Server(s)

ncel

Save

1 Assign unique IP Pool Name

2 Network Range for specific Area

3 Classful Network Mask

4 Gateway IP Address

5 Save to create new entry

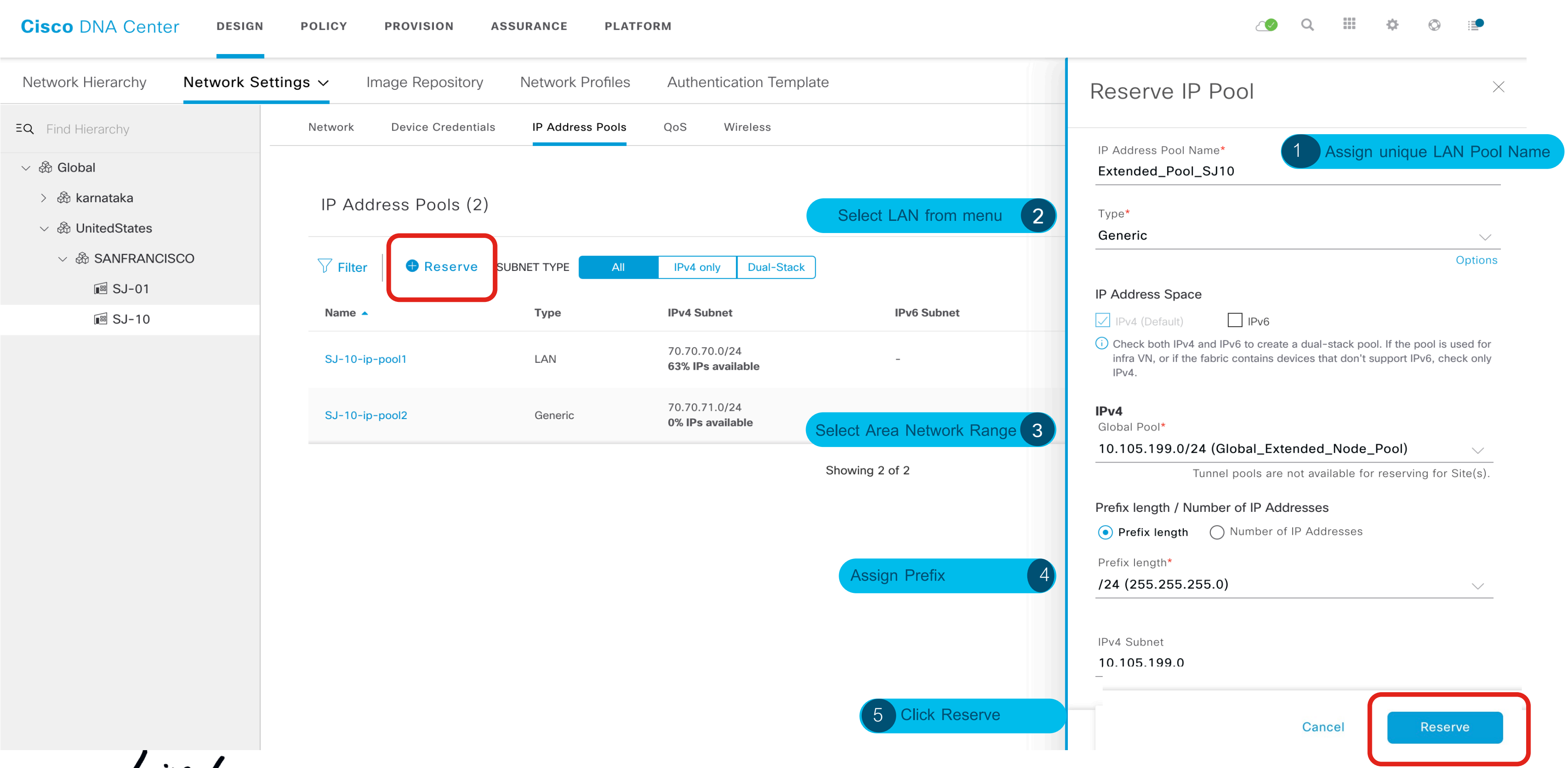
Global IP Pool

IP address repository for multi-function distribution purpose to Area, Site etc.

Reserve IP Pool from Area to automate extended nodes

cisco Live!

Design –Step2: Configure LAN Pool for Site



Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

Network Hierarchy | Network Settings | Image Repository | Network Profiles | Authentication Template

Network | Device Credentials | IP Address Pools | QoS | Wireless

Find Hierarchy

- Global
  - karnataka
  - UnitedStates
    - SANFRANCISCO
      - SJ-01
      - SJ-10

IP Address Pools (2)

Filter | Reserve | SUBNET TYPE: All | IPv4 only | Dual-Stack

Name	Type	IPv4 Subnet	IPv6 Subnet
SJ-10-ip-pool1	LAN	70.70.70.0/24 63% IPs available	-
SJ-10-ip-pool2	Generic	70.70.71.0/24 0% IPs available	

Showing 2 of 2

Reserve IP Pool

IP Address Pool Name*: Extended_Pool_SJ10

Type*: Generic

Options

IP Address Space

☑ IPv4 (Default) ☐ IPv6

Check both IPv4 and IPv6 to create a dual-stack pool. If the pool is used for infra VN, or if the fabric contains devices that don't support IPv6, check only IPv4.

IPv4

Global Pool*: 10.105.199.0/24 (Global_Extended_Node_Pool)

Tunnel pools are not available for reserving for Site(s).

Prefix length / Number of IP Addresses

● Prefix length ○ Number of IP Addresses

Prefix length*: /24 (255.255.255.0)

IPv4 Subnet: 10.105.199.0

Cancel | Reserve

1 Assign unique LAN Pool Name

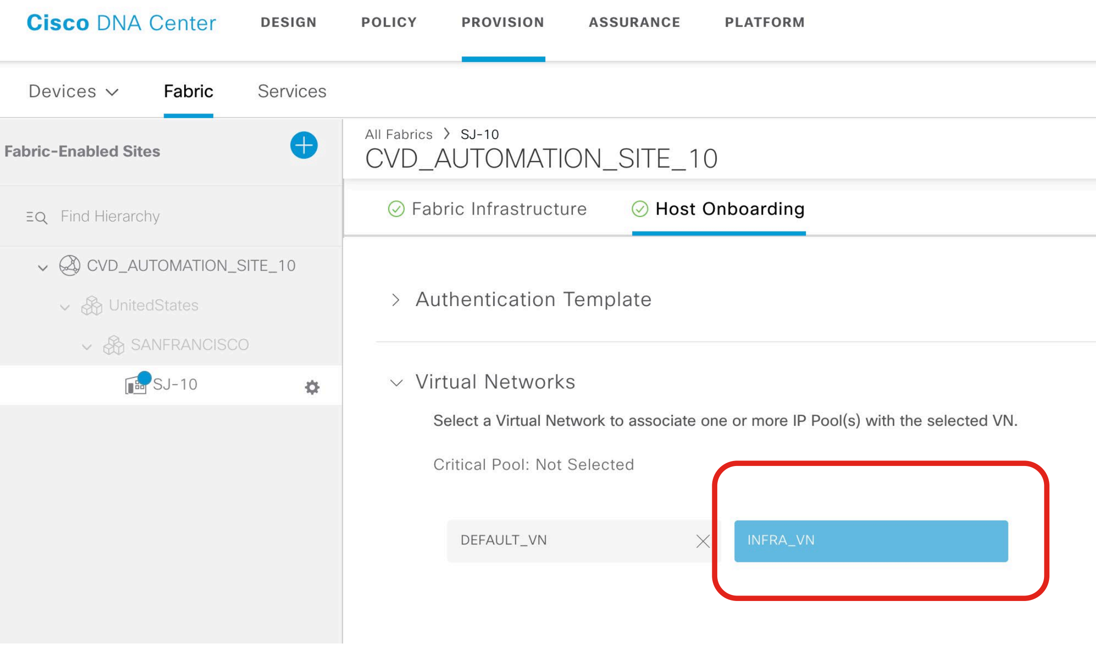
2 Select LAN from menu

3 Select Area Network Range

4 Assign Prefix

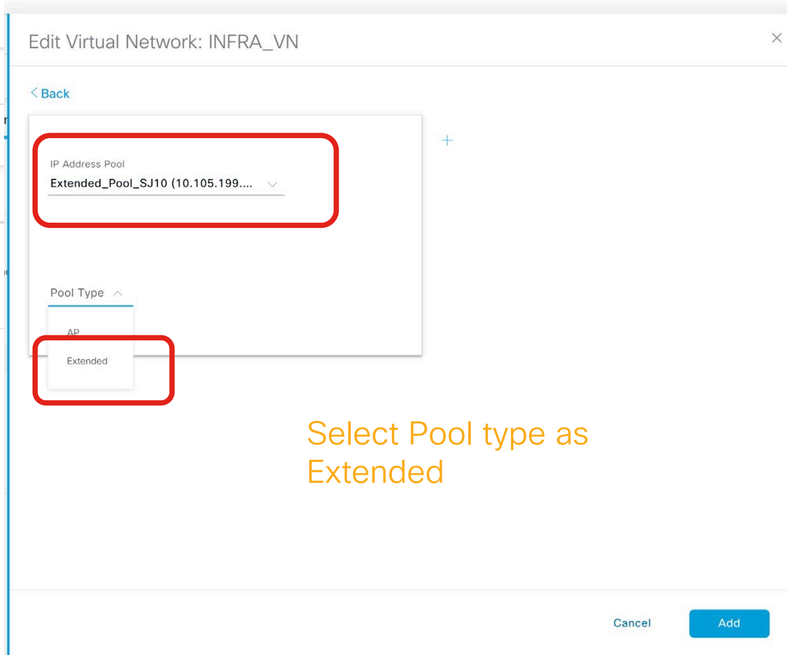
5 Click Reserve

Provision- Step1:Enabling Fabric Extension



Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Critical Pool: Not Selected



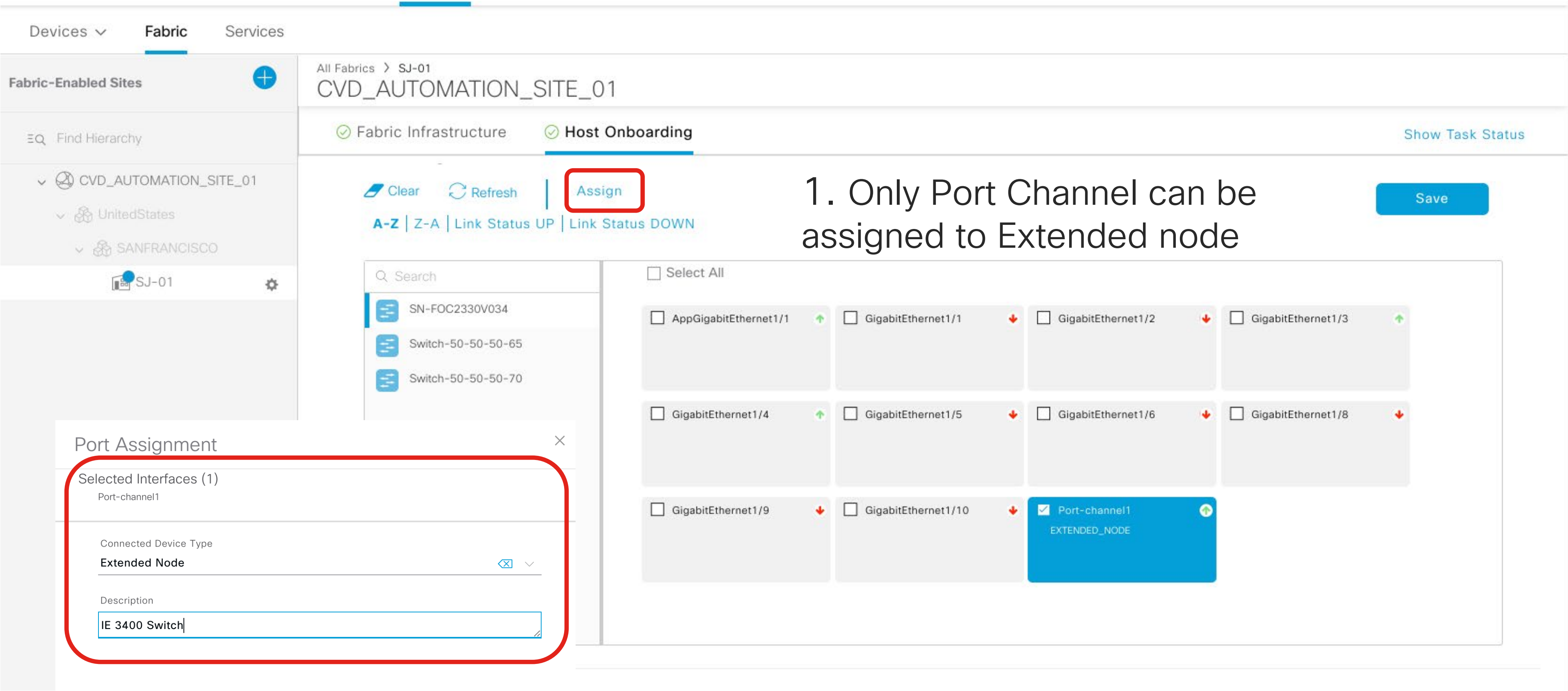
IP Address Pool: Extended_Pool_SJ10 (10.105.199....

Pool Type: AP / Extended

Select Pool type as Extended

Select an IP Pool for the INFRA_VN and enable it for Extended Nodes.

Provision- Step2: Enable FE for on-boarding



1. Only Port Channel can be assigned to Extended node

Port Assignment

Selected Interfaces (1)

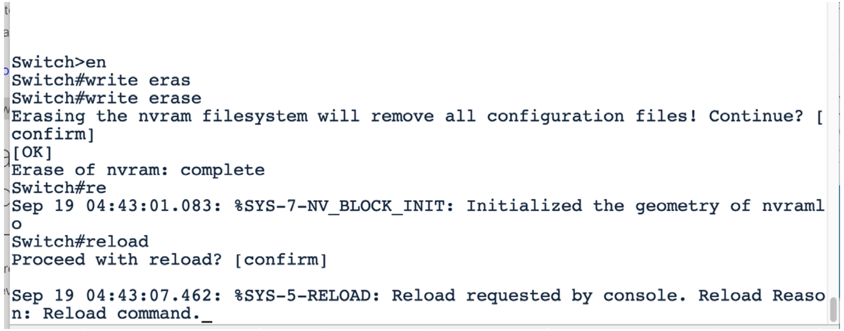
Port-channel1

Connected Device Type: Extended Node

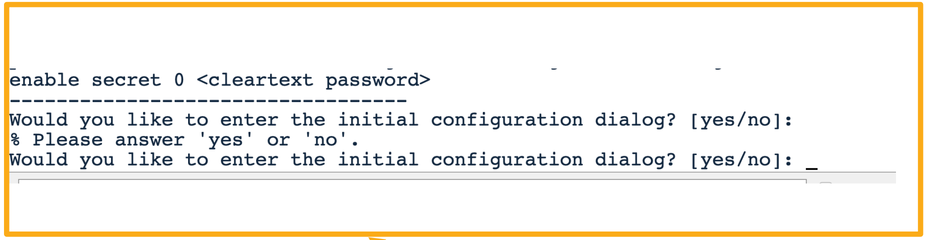
Description: IE 3400 Switch

Quick Tips for adding devices as Ex/PEN to Fabric

- Extended/policy extended node switches must not have any configuration.
- Write erase and reload, if any existing configuration is there.
- Fabric Edge switches should be running supported code for Extended/PEN.
- Configured Pool in DHCP (extended node) should be configured for PnP pointing to DNA-C provisioning IP



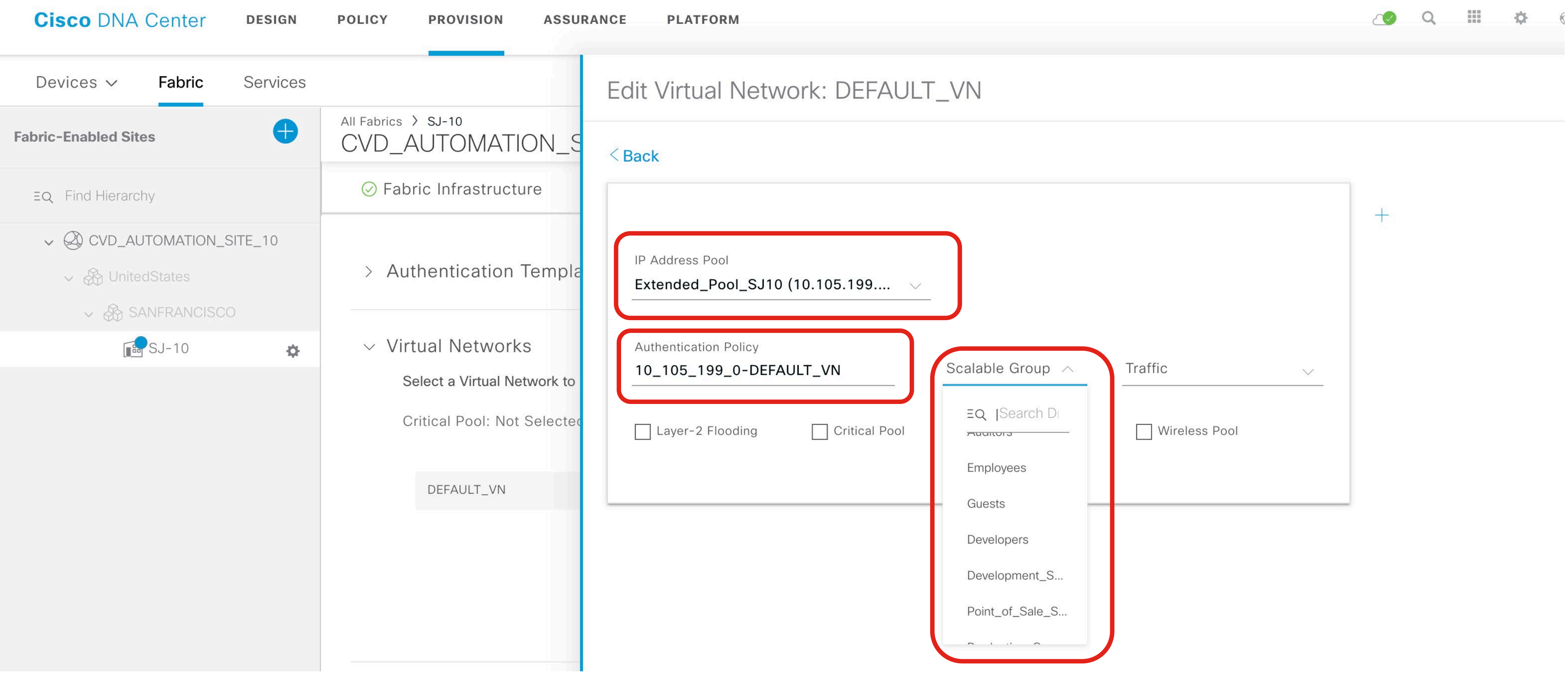
```
Switch>en
Switch#write eras
Switch#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [
confirm]
[OK]
Erase of nvram: complete
Switch#re
Sep 19 04:43:01.083: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvraml
o
Switch#reload
Proceed with reload? [confirm]

Sep 19 04:43:07.462: %SYS-5-RELOAD: Reload requested by console. Reload Reaso
n: Reload command._
```



```
enable secret 0 <cleartext password>
------------------------------------
Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: _
```

Switch should be at this prompt

Policy Mapping - SGT



Edit Virtual Network: DEFAULT_VN

IP Address Pool: Extended_Pool_SJ10 (10.105.199....

Authentication Policy: 10_105_199_0-DEFAULT_VN

Scalable Group

Traffic

□ Layer-2 Flooding □ Critical Pool □ Wireless Pool

ISE must be configured for adding SGT mapping

We have extended intent based networking to Non-Carpeted areas.

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**