The bridge to possible

A Tale of Two Ships

SD-Access and BGP EVPN Designs and Deployments on Cruise Ships

Cheeho Yan, Sr. Technical Leader
Yianni Thallas, Product Management Architect

BRKENS-2822

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2822

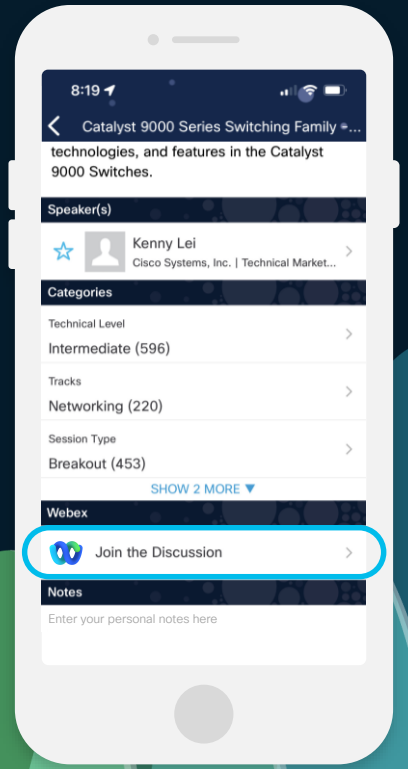
Questions?

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 7, 2024.



How Did the Tale of Two Ships Start?

- Network implementation started from around 2022-23
- SD-Access LISP (SDA) & BGP EVPN deployed on two ships from two different cruise lines
- Several additional ships might implement the same solutions across both fleets
- We will get to how the tale ended

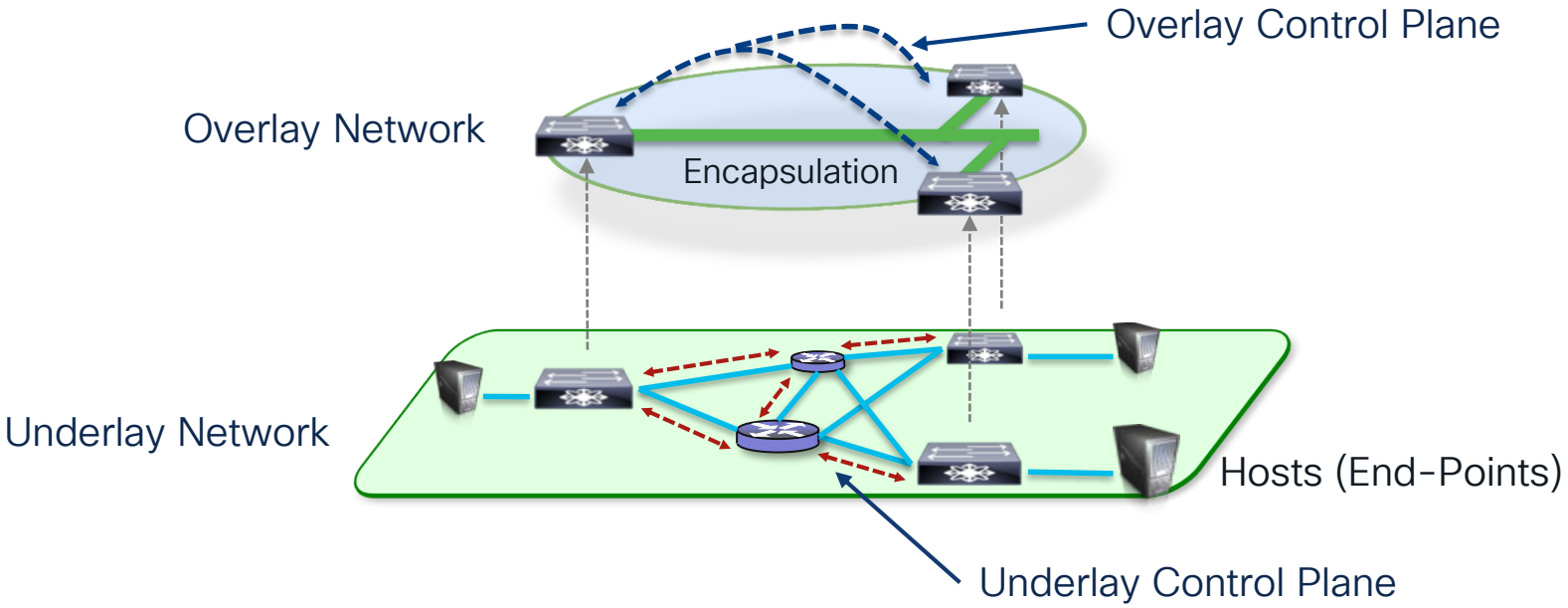
Agenda

- Fabric Choices: SD-Access vs. BGP EVPN
- Business Requirement
- Ship #1: SD-Access Solution
- Ship #2: BGP EVPN Solution
- Plan, Design, Implementation, and Support Best Practices
- Sneak Preview: Catalyst Center Orchestrated BGP EVPN

Fabric Choices: SD-Access vs. BGP EVPN

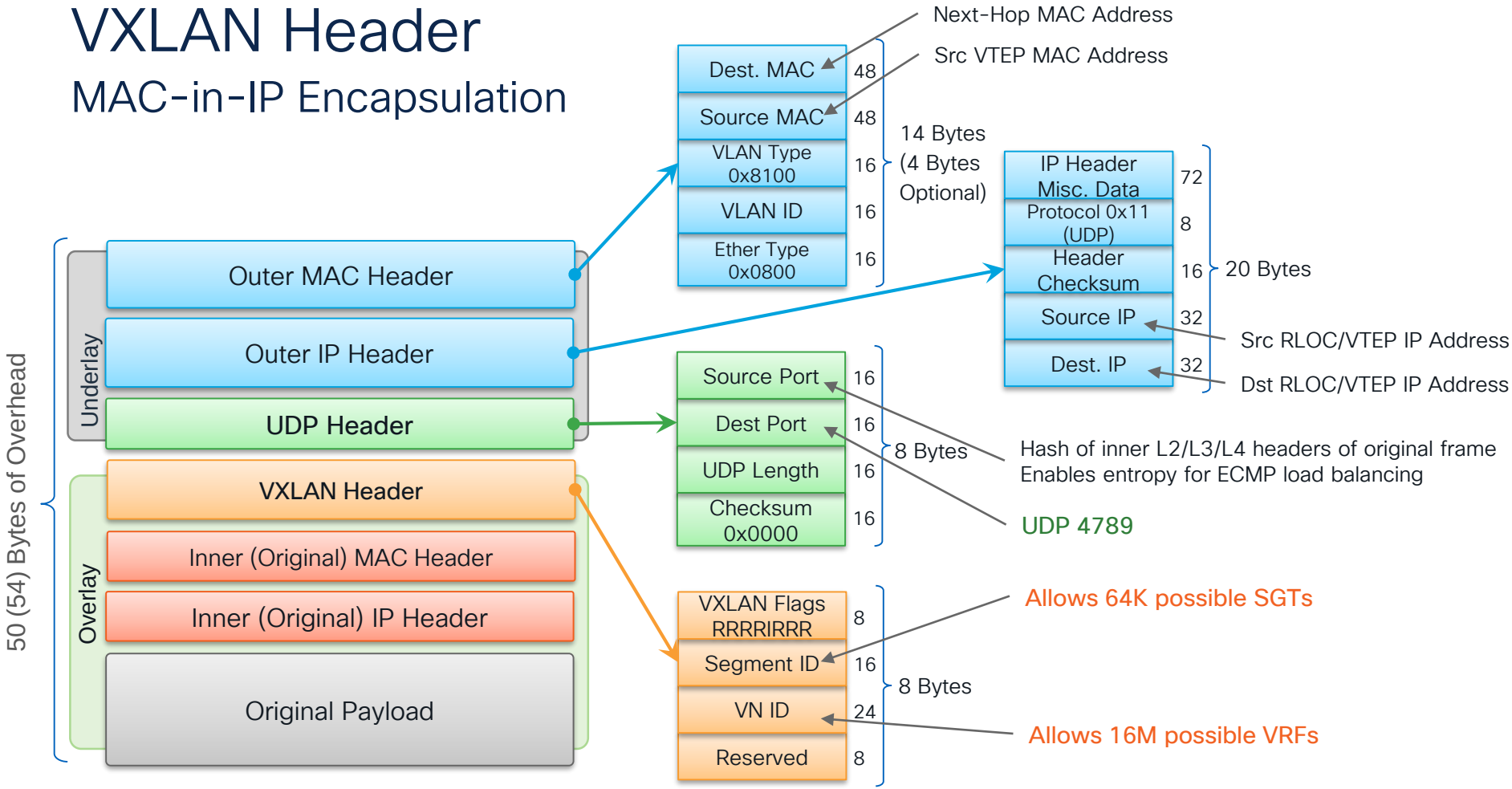
A Fabric is an Overlay

- A logical topology used to virtually connect devices, built on top of physical underlay topology
- Provides additional services not provided by the underlay



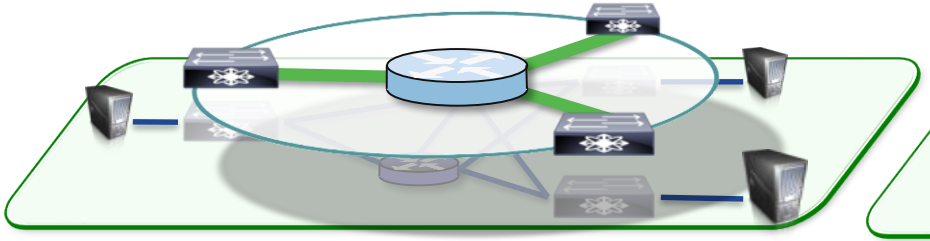
VXLAN Header

MAC-in-IP Encapsulation



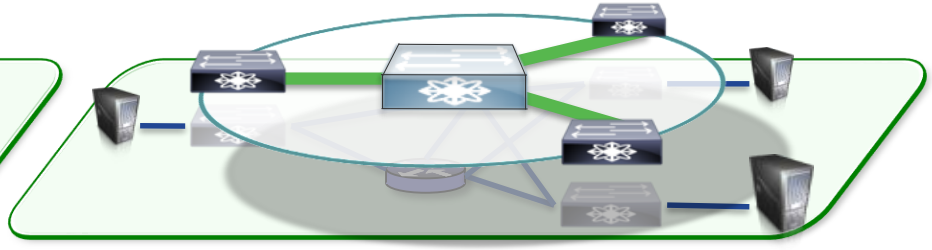
Fabrics with VXLAN Encapsulation

VXLAN Provides a Network with Segmentation & Scale



SDA LISP

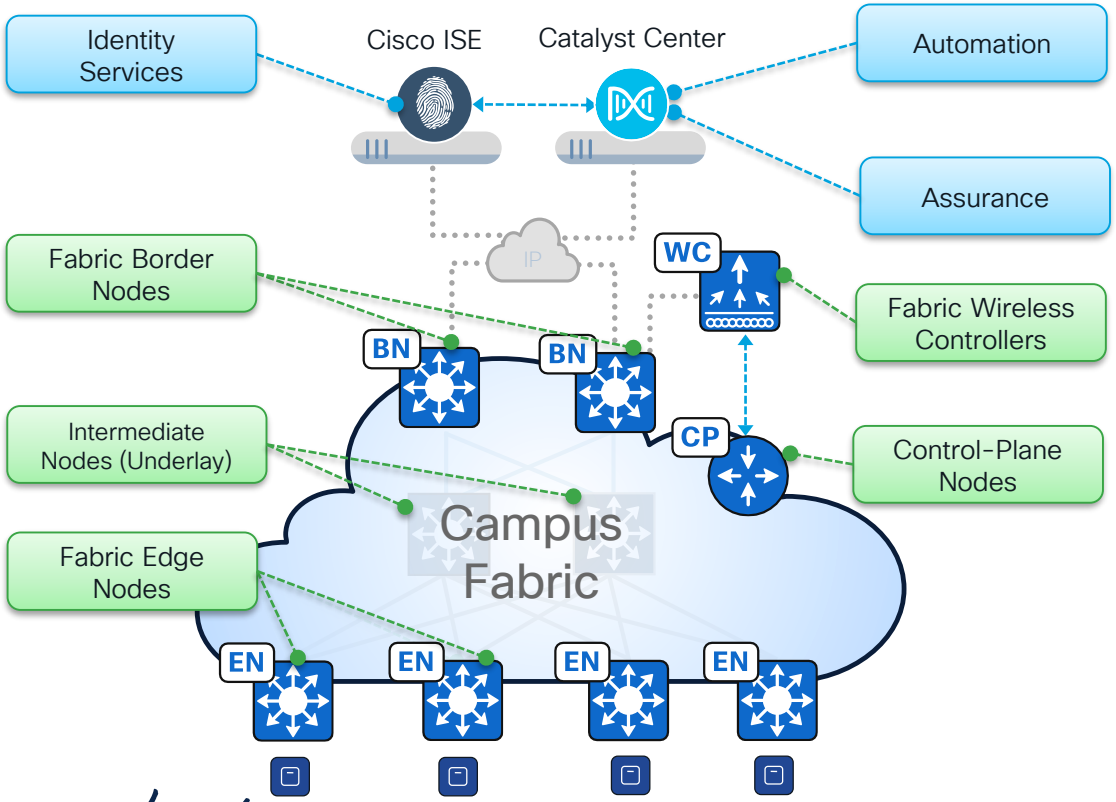
- Network Simplification Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired/wireless
- Mobility First Requirement Fabric Integrated Wireless, L2 mobility, enhanced wireless performance
- Segmentation Zero-Trust Architecture with Micro and Macro Segmentation. Unified Wired + Wireless policy



BGP EVPN

- One Fabric Architecture (Campus & DC) Operational ease with a single familiar protocol
- Multi-vendor interoperability Vendor-agnostic solution
- Flexibility Customizable overlay network types and topologies

SD-Access Fabric Roles



- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric network status
- **Identity Services** – NAC & ID Services (e.g. ISE) 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 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Enterprise Campus BGP EVPN Drivers

Industry Standard	✓ Multi-vendor IT strategy
One Fabric Architecture	✓ Unified operation across network infrastructure
Proven and Scalable	✓ BGP protocol history. Minimum new learning curve
Hierarchical Fabric Domain	✓ Multi-tier overlay network architecture
Flexible Overlay	✓ Use-case driven. Customized overlay networks types & topologies

BGP EVPN System Roles

BORDER-GATEWAY:
A gateway point of between two or more BGP EVPN administrative domain boundary

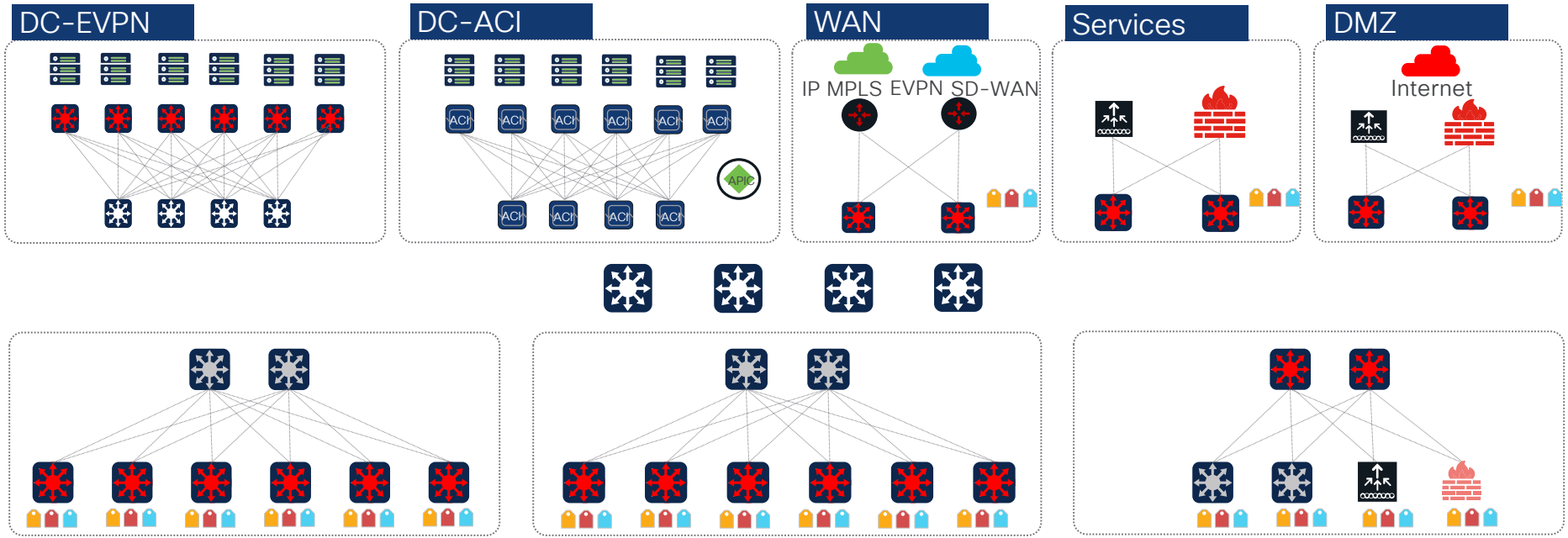
BORDER :
A gateway point of between EVPN fabric and external network domain

INTERMEDIATE :
A Layer 2 or Layer 3 (IP/MPLS) underlay network system providing basic transport and forwarding plane

SPINE :
A BGP EVPN role that reflects the L2/L3 VPN prefixes providing hierarchical neighbor peering, learning and distribution point

VTEP (LEAF) :
An origination and termination point of VXLAN enabled overlay network

Enterprise BGP EVPN Reference Architecture



Industry Standard | Unified Fabric | Proven | Hierarchical | Flexible

SDA-LISP: Recommended by Cisco for Campus

3,600+ Campus Deployments
30% Year to Year Growth

Simple

- Industry standard-based and optimized for enterprise campus
- Configurations automated based on business intent

Efficient

- Scales to a large number of endpoints
- Rapid converge

Extensible

- Simple directory structure to map endpoints to locations
- Highly extensible to address new use cases

Wired + Wireless

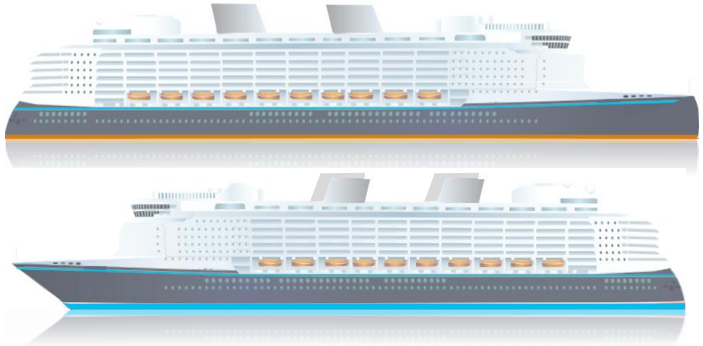
- Centralized control plane with distributed data plane
- Seamless campus wide mobility

Business Requirement

Responses to Meet Business Needs

Requirement
Business Continuity
Services to End Users
Ease of Network Deployment , Operation & Support

SD-Access



BGP EVPN

Business Continuity

- Network Downtime impacts revenue
- Network redundancy is required
- Limited network change windows
- Ships are offshore most of the time

Note: Specific to cruise line industry

Services to End Users

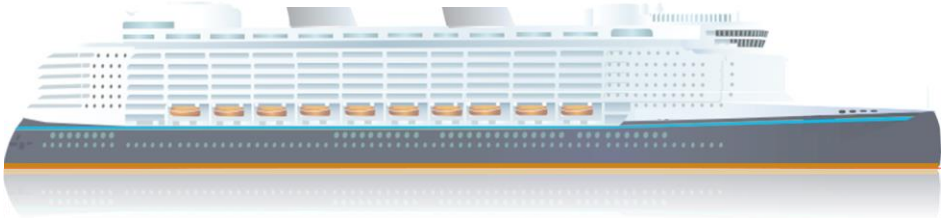
- Most endpoints are connected using wireless
- Extensive use of IP based IOT devices
- Seamless endpoint onboarding
- Ease of problem identification/troubleshooting/resolution
- Large number of APs and cabin switches

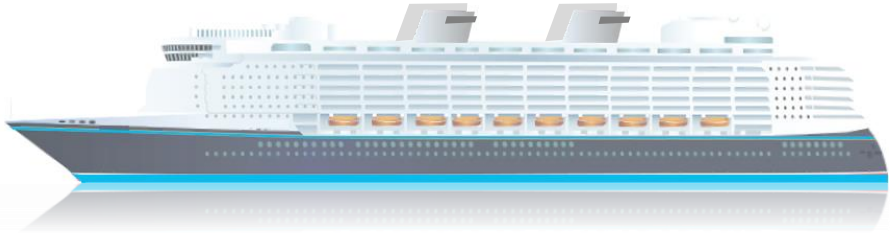
Ease of Network Deployment / Operation / Support

- Standard based network architecture
- Tight timeline for network implementation
- Secured endpoint admission control
- Security segmentation
- Onboard + Onshore IT support model

Two Cruise Ships: Similar Physical Configuration

- Passengers & Crews: 3,000 – 4,500
- Wired & Wireless Endpoints: up to 10,000
- Network Domains: Data Centers (servers) + Campus (passengers, crews)
- Network Infrastructure: Green field implementation



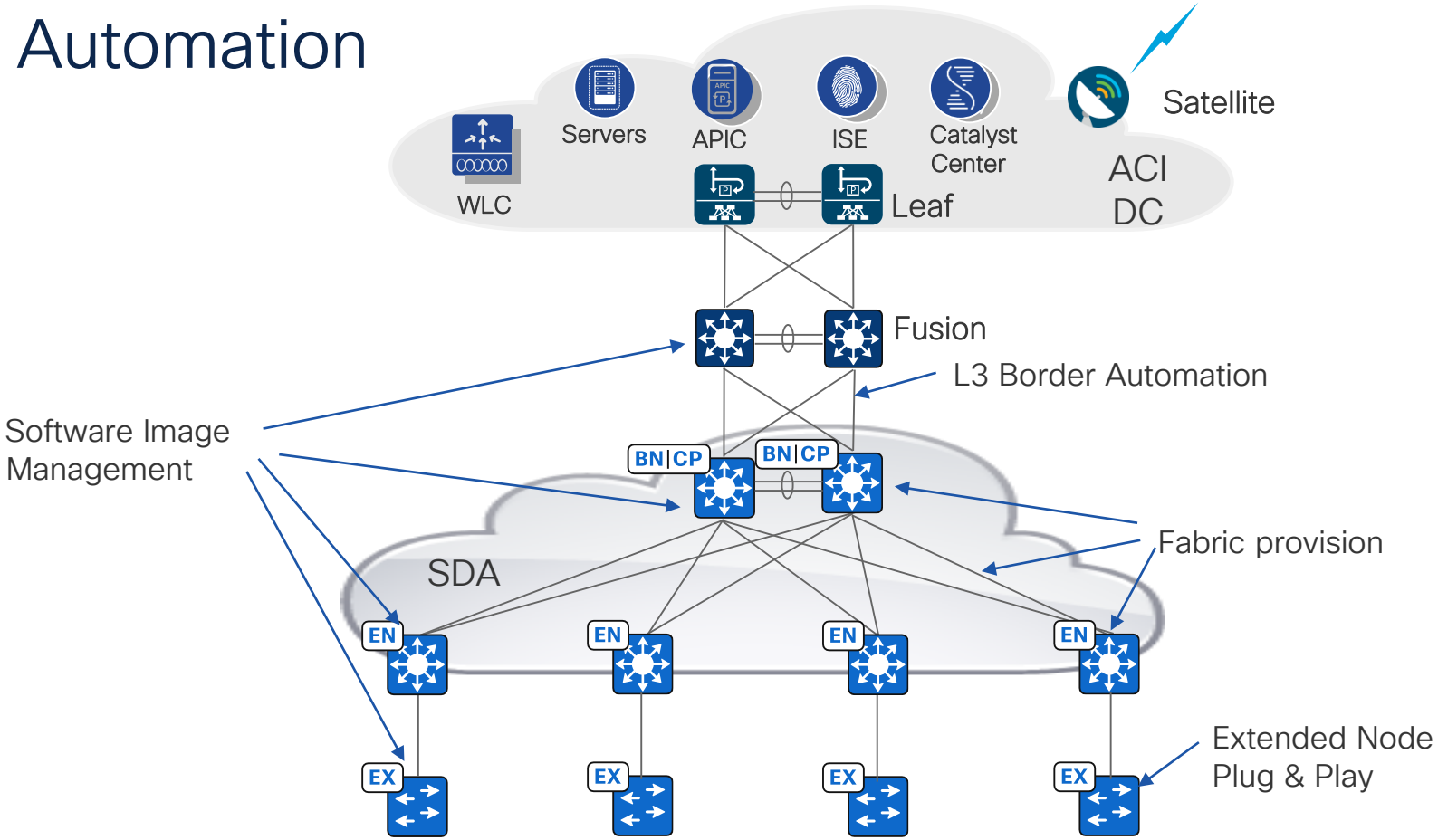


Ship #1: SD-Access Solution

Challenges & Solutions

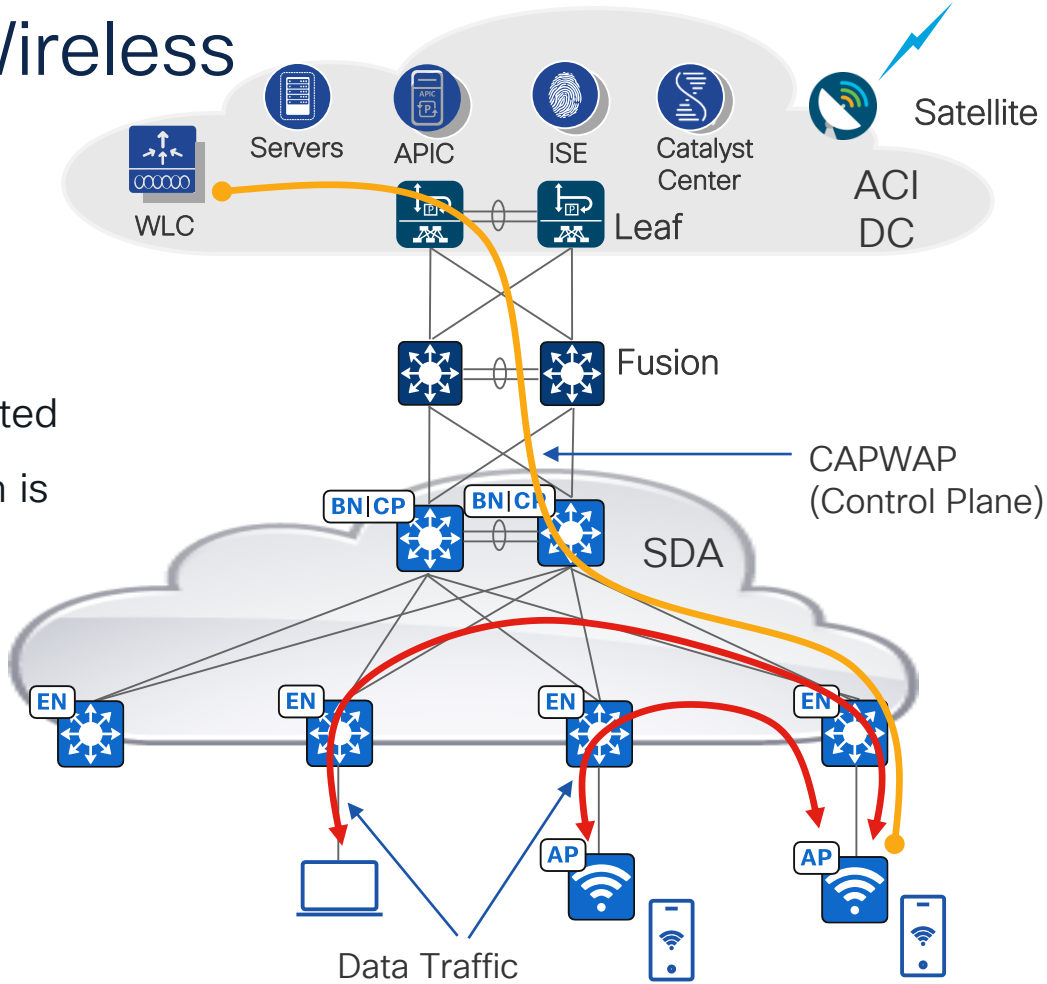
Automation, Assurance, TrustSec, Wire/Wireless integrated in Fabric	Catalyst Center / SDA
Limited Satellite Bandwidth	Catalyst Center Air-Gap
Extended Nodes Exceeding Limit	Fabric Zone
Need L2 Connectivity to Servers	Layer 2 Virtual Network
Survivability for Critical Services	Spread Network Devices Across Fire Zones

Fabric Automation



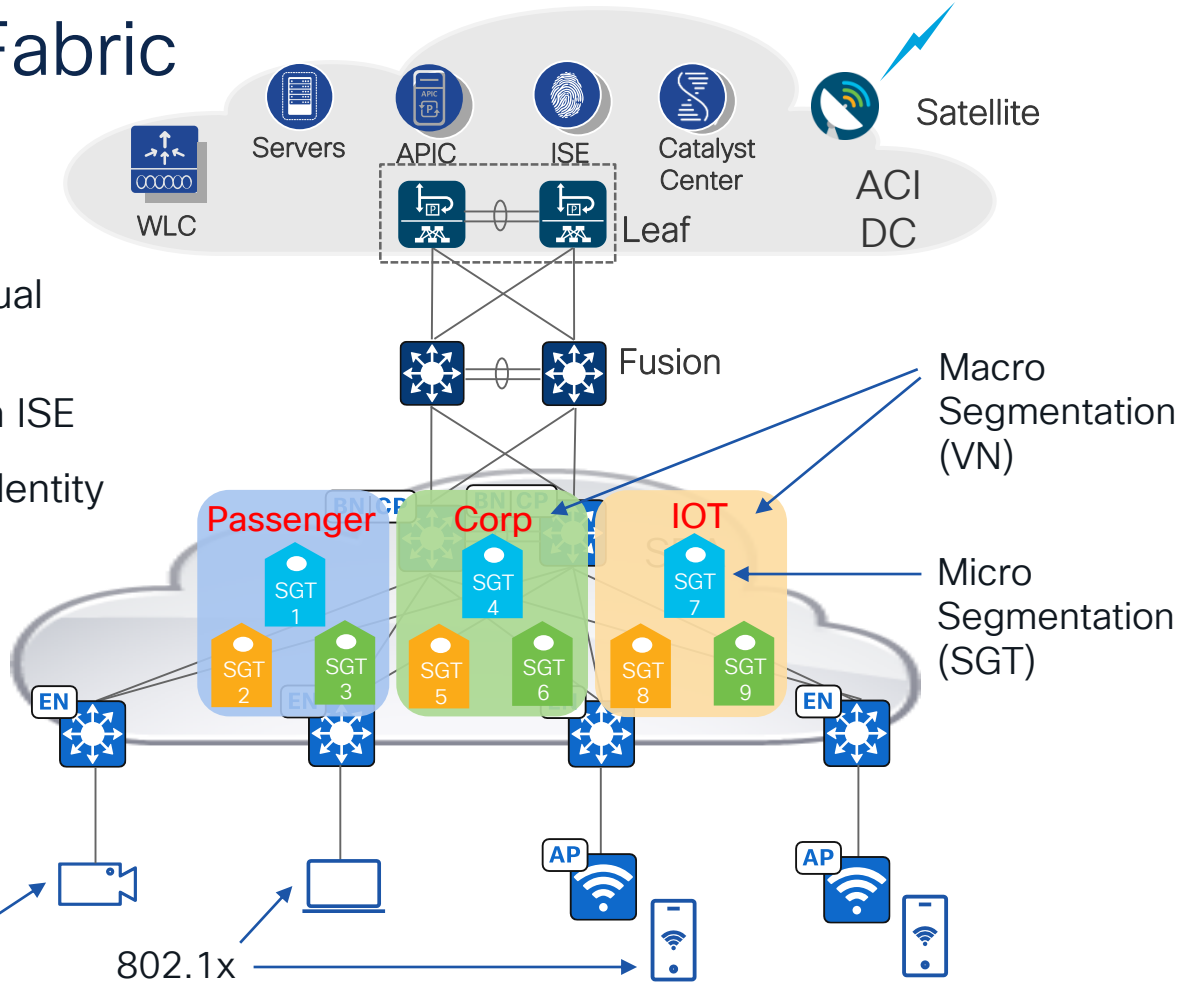
Fabric Enabled Wireless

- No air-pinning to centralized controller
- Wireless client traffic is distributed
- Wired-Wireless communication is directly through Fabric



TrustSec inside Fabric

- Macro segmentation using Virtual Networks (VN)
- Centralized policy authorized in ISE
- Endpoints grouped based on identity
- Micro Segmentation using Security Group Tag (SGT)



Fabric Assurance

Assurance Dashboard

- Health & critical issues summary
- Fabric, device & client health scores
- Wireless trends

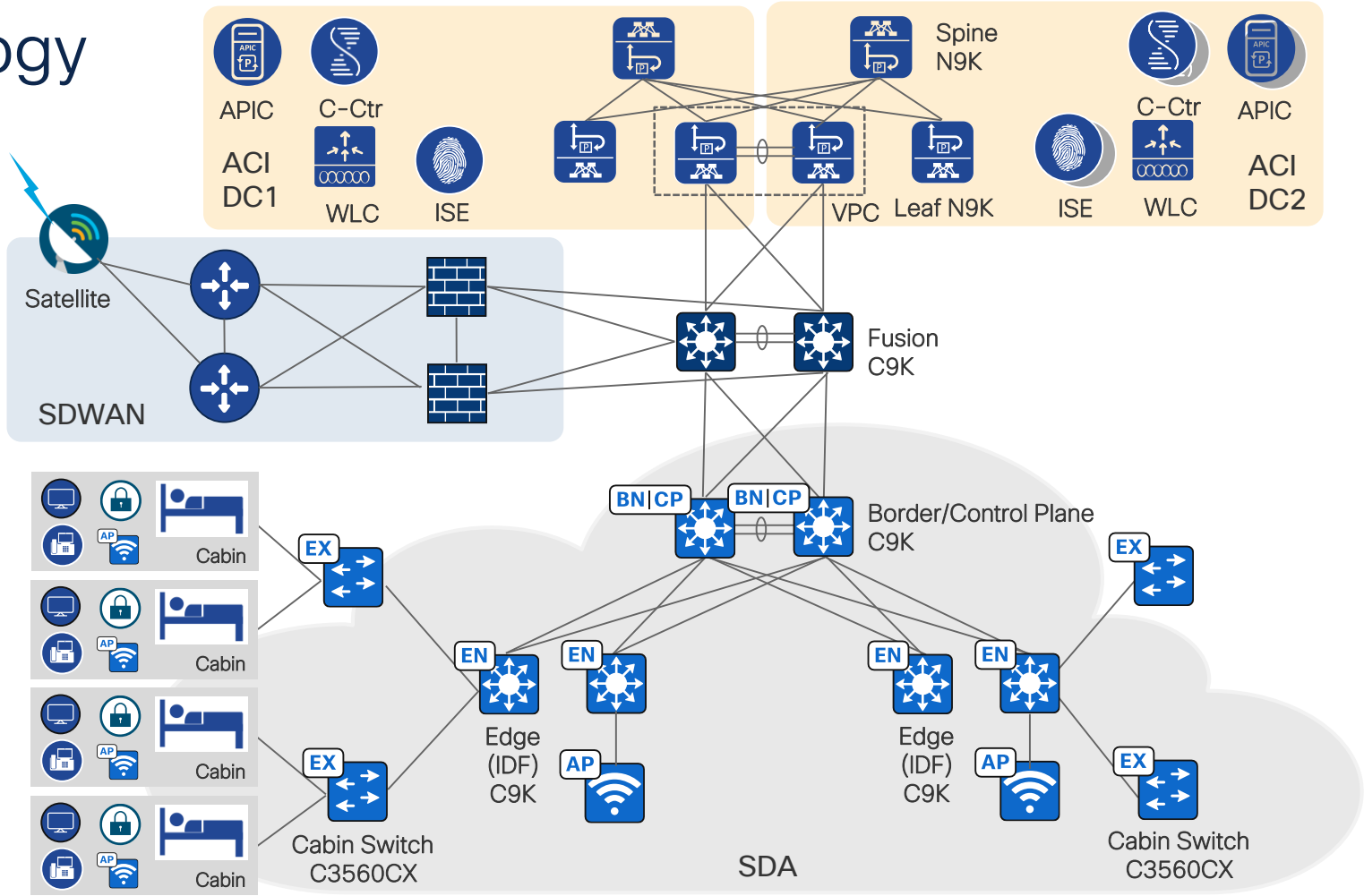
Device & Client 360 Views

- Time travel view
- View connected neighbors & clients
- Universal search for elements in the network

Troubleshooting

- Issues with explanations
- Suggested actions

Topology



Satellite Bandwidth

Challenge:

- Limited Internet bandwidth through Satellite
- Bandwidth priority is given to the paid passengers

Solution: Catalyst Center in Air-Gap Mode

Typical Use Cases

- Department of Defence
- Government

Airgap Implementation Considerations

Supported	Not Supported
Catalyst Center Software Offline Updates	Geo Maps Update
Assurance (Except AI Network Analytics)	License Manager (Devices that do not support SLR/PLR)
Application Policy, Topology, Third Party SDK, Audit Log, Global Search, Home Page, Bonjour, Plug and Play, PSIRTs	AI Network Analytics
SWIM: Manual Image Import, Manual KGV Import, Addons (Manual import required) – SMU, Sub package, APSP, APDP	SWIM Addons – ROMMON; Automated Image Download from cisco.com
SDA (with DHCP server in Airgap)	Integrations outside Airgap
License Manager (SLR/PLR Supported)	Make a Wish

Ensure Catalyst Center does not have backdoors to Internet to download online packages automatically, otherwise it would cause upgrade issues

Scale

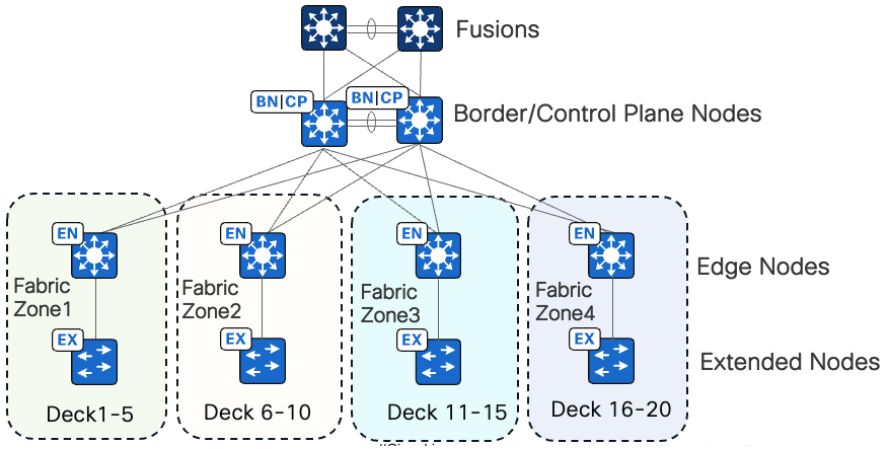
Challenge:

- Supported fabric devices per SDA Fabric site is 1,200 for DN2-HW-APL-XL
- Cruise line required 2000+ Extended Nodes to service all the cabins
- Same IP pools stretching multi-Fabric site was not an option

Solution: Fabric Zone

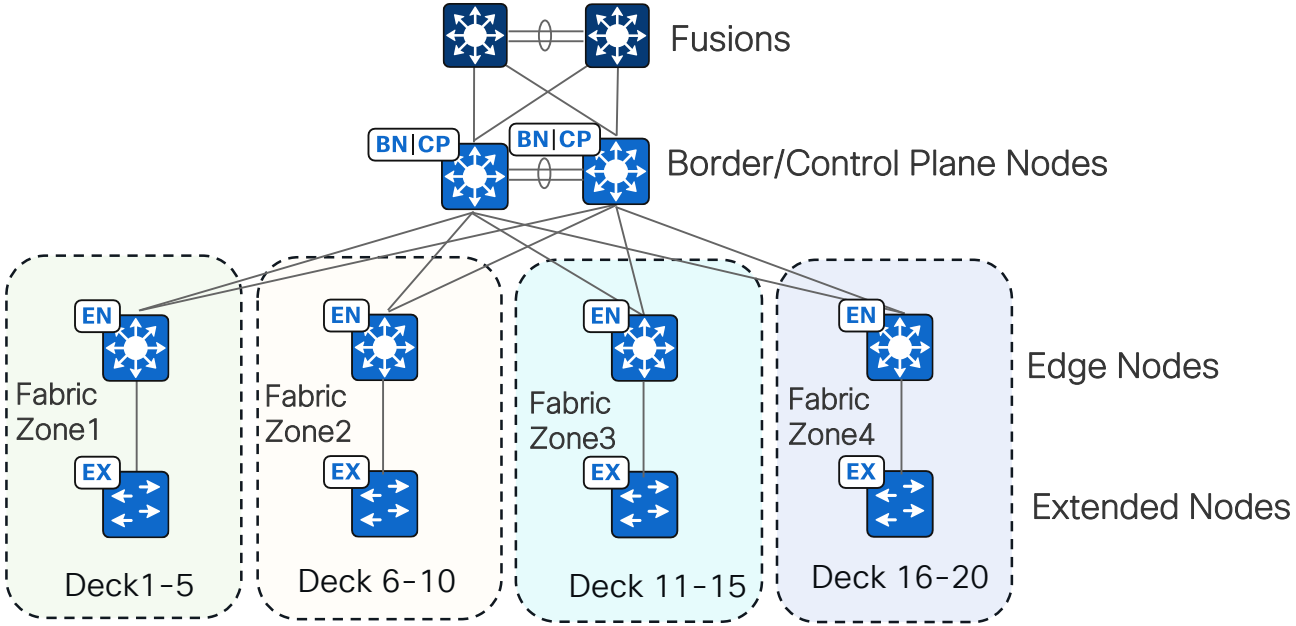
Typical Use Cases

- Manufacturing



Fabric Zones on the Ship

- 4 Zones with 500 Extended Nodes each
- No common changes to all Fabric Zones at the same time
- Onboard 50 Extended Nodes at a time



Review design with Cisco first. Multiple Fabric Site is the preferred choice in other use cases

L2 Connectivity to DC

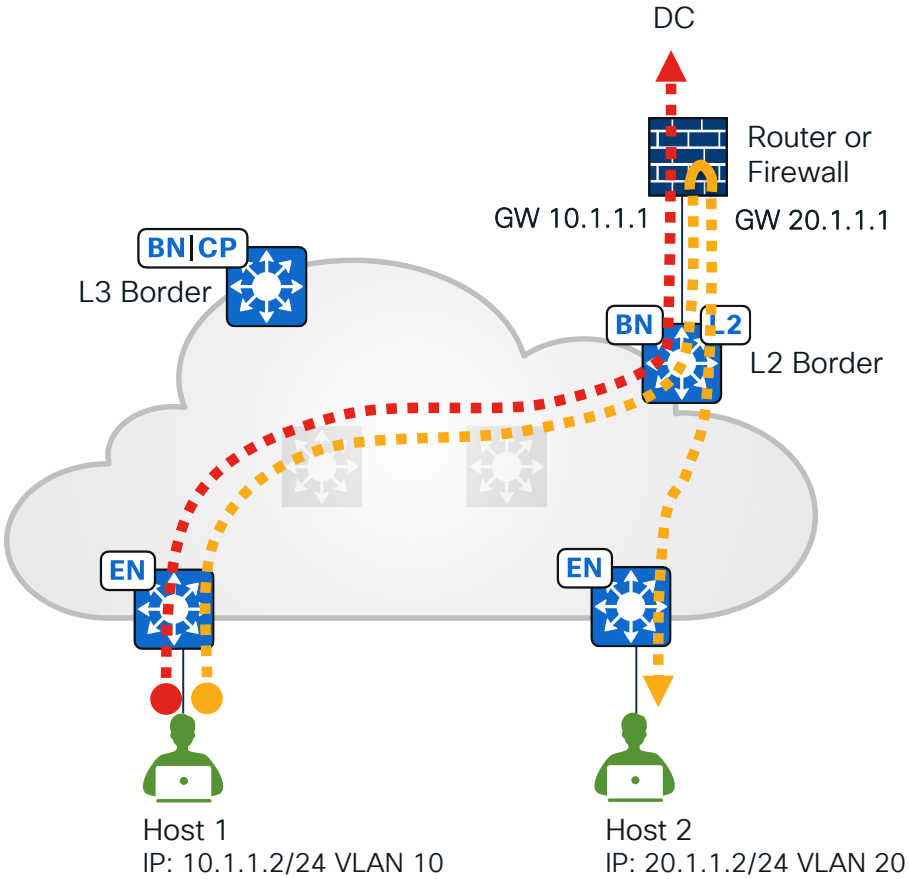
Challenge:

- Certain legacy applications require servers at DC to be on the same L2 segment as the endpoints at the Fabric
- Security requirement for Gateway of a subnet to be outside the Fabric

Solution: Layer 2 Virtual Network

Typical Use Cases

- Manufacturing
- IoT segments
- BMS



Location Redundancy

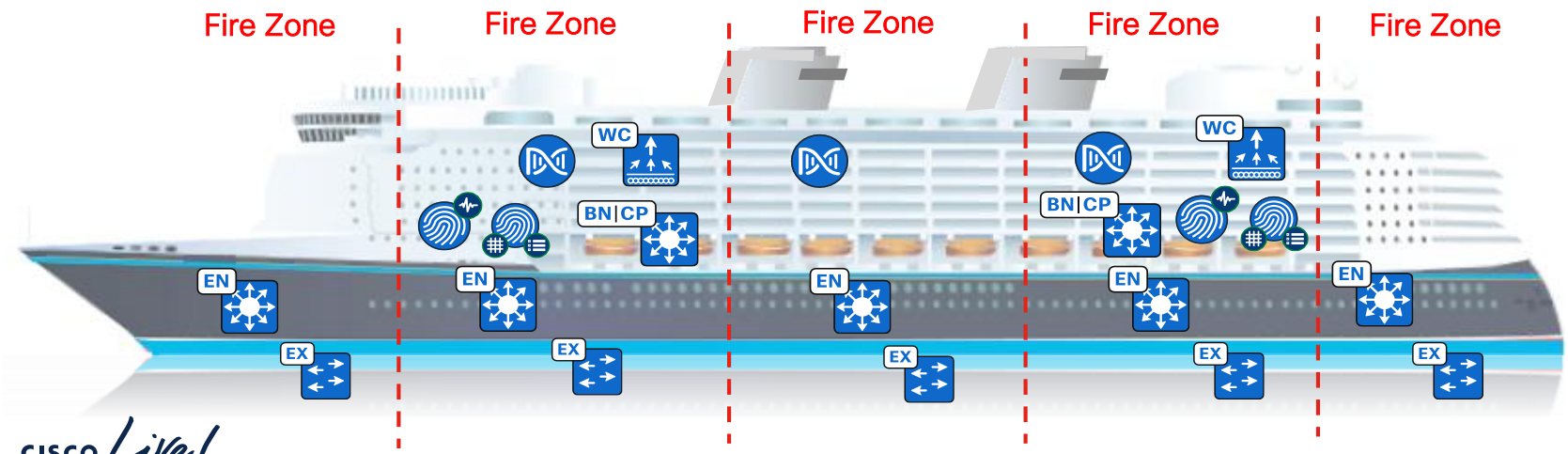
Challenge:

- DCs and critical network devices need to have location redundancy

Solution: Spread them across Fire Zones and locations

Typical Use Cases

- Transportation
- Financial



Ship #2: BGP EVPN Solution

Challenges & Solutions

Automate Fabric Overlay from DC to Campus	Use Nexus Dashboard Fabric Controller (NDFC)
Reduce Fabric Fault Domain	Multisite VXLAN BGP EVPN
L2 Connectivity to Servers	Layer 2 overlay tunnels
Survivability for Critical Services	Spread network devices across fire zones

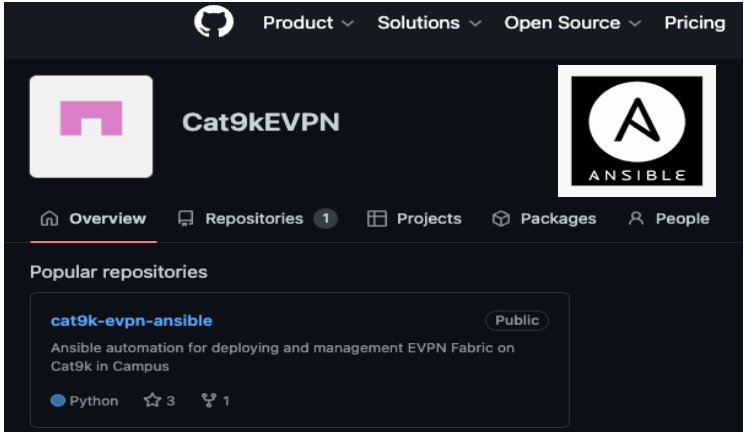
Fabric Automation

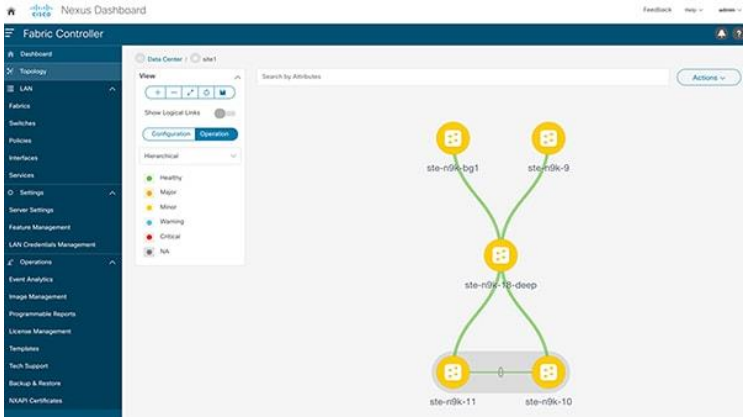
Challenge:

- Need automation for Nexus and Catalyst switches with BGP EVPN deployment with a single pane of glass

Solution:

- NDFC with built in python & CLI policies for configuration generation
- Cat 9000 programmability





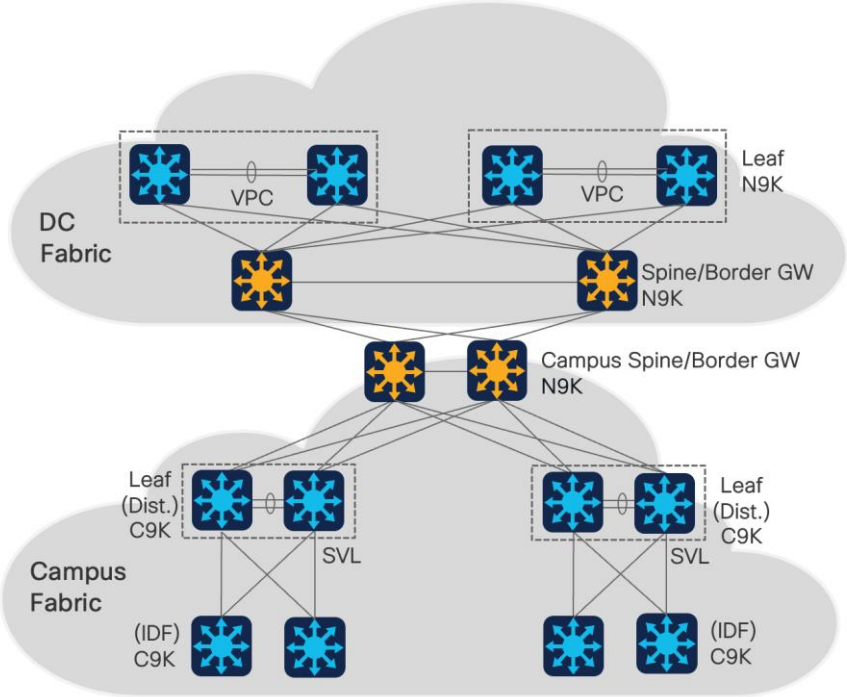
Multisite

Challenge:

- Single fabric fault domain from DC to campus is not scalable

Solution:

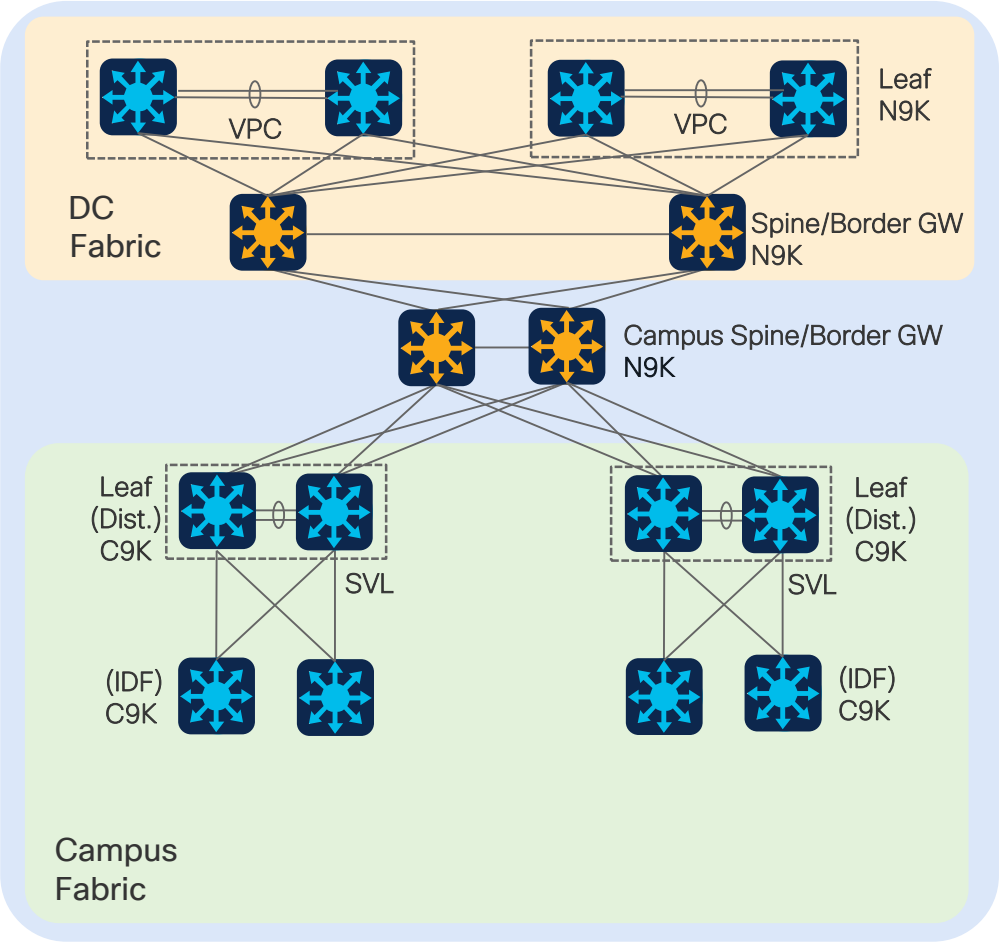
- Implement DC site and Campus site
- Back-to-back multi-site anycast BGW



Multisite

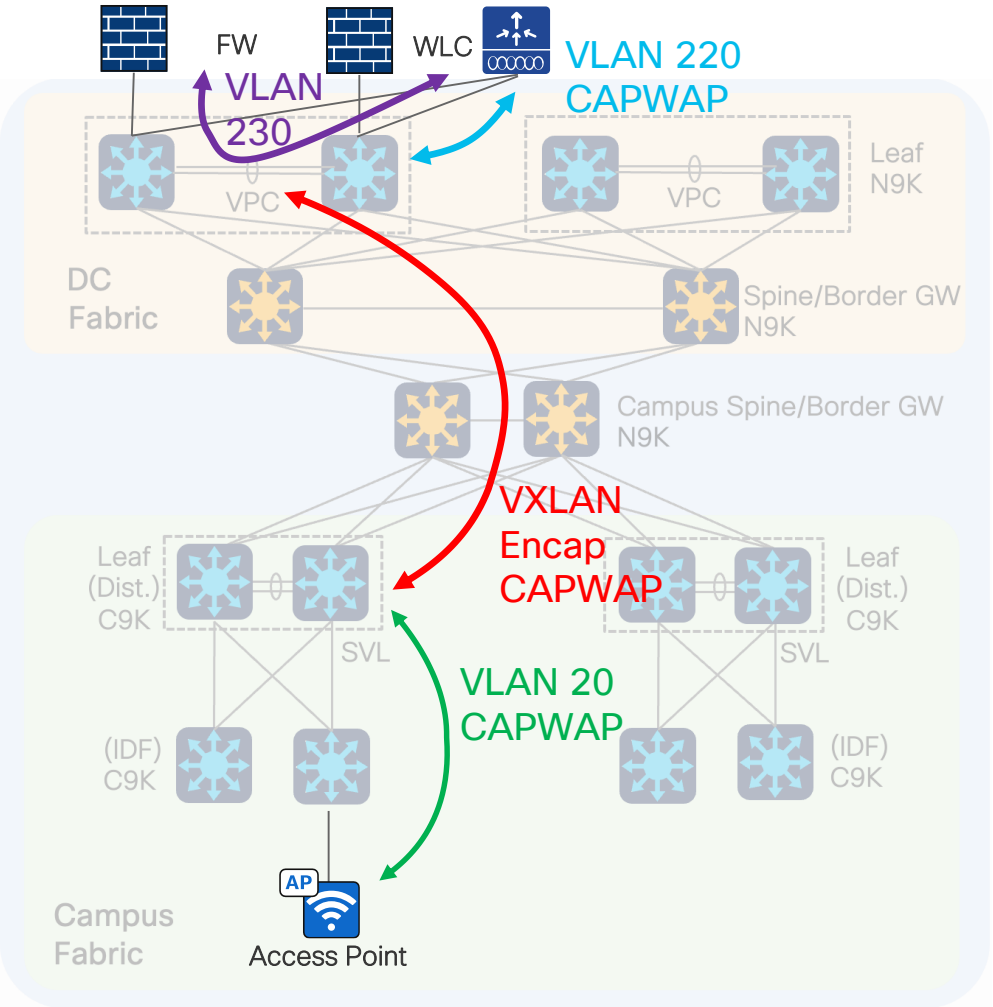
- Separate replication domains for BUM (Broadcast, Unknown Unicast, and Multicast) traffic
- Granular control on cross-site L2 and L3 communication
- Better overall scalability
- Smaller fault domain

	Micro segmentation across campus and DC is not supported



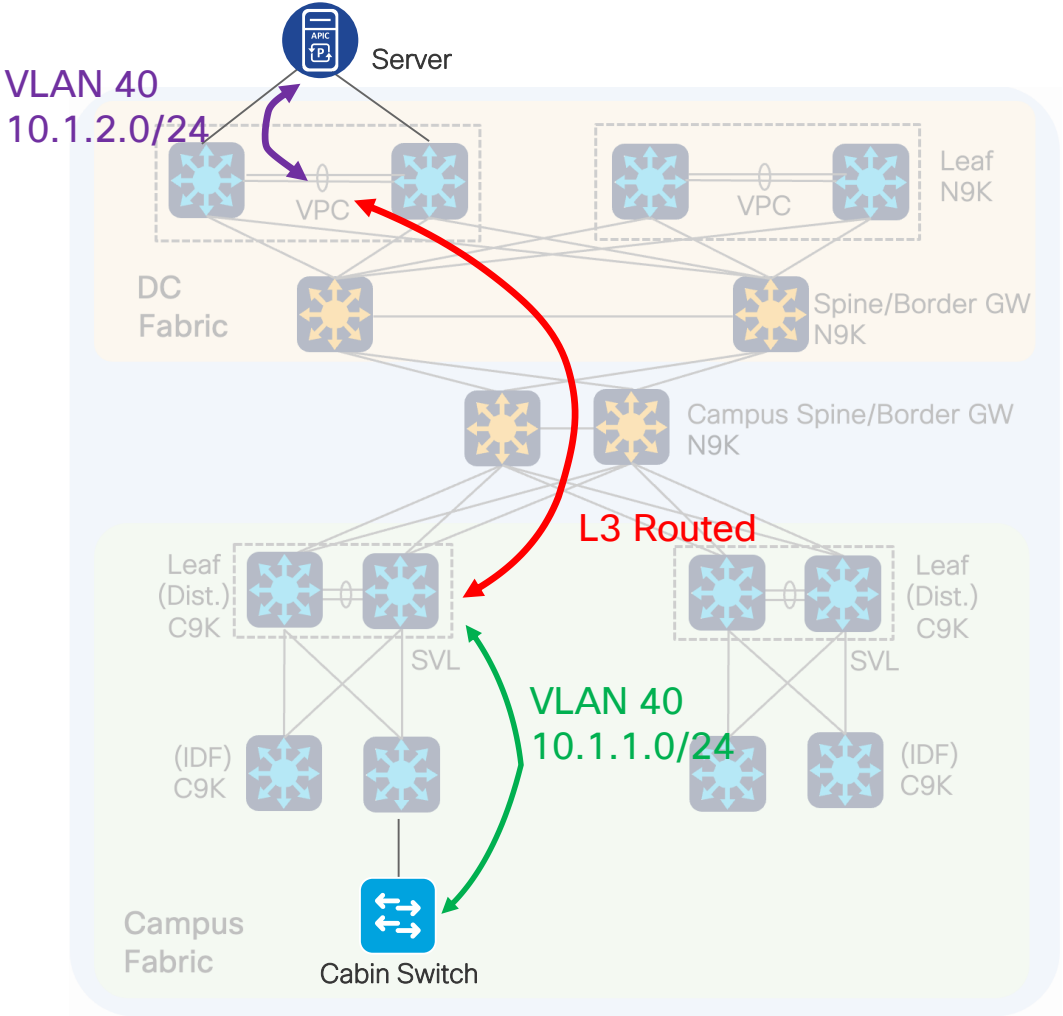
Wireless Inter-Site Traffic

- CAPWAP from Access Point reaches Leaf over VLAN 20
- CAPWAP encapsulated in VXLAN reaches DC Leaf
- CAPWAP traffic from service Leaf sent to WLC over VLAN 220 as CAPWAP
- Traffic sent as Ethernet from WLC to FW over VLAN 230

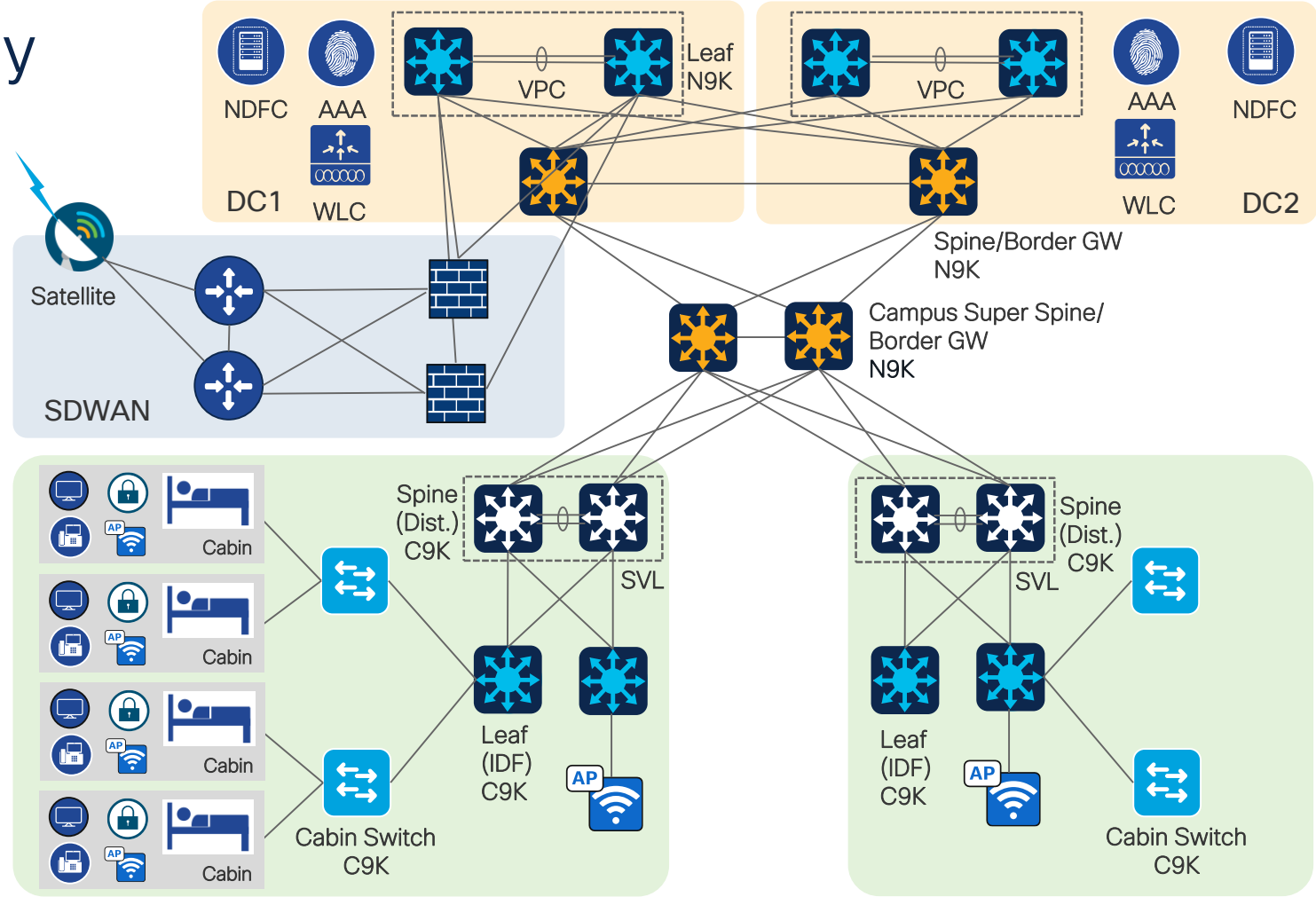


L3 Inter-Site Traffic

- Anycast Gateway required for each subnet
- Anycast Gateway for server resides in DC
- Anycast Gateway for IDF resides in Campus
- Traffic routed between different VLANs/subnets with the same L3 VNI



Topology


NDFC
AAA
WLC
DC1
VPC
Leaf
N9K
VPC
AAA
NDFC
WLC
DC2
Spine/Border GW
N9K
Satellite
SDWAN
Campus Super Spine/
Border GW
N9K
Cabin
Cabin
Cabin
Cabin
Spine
(Dist.)
C9K
SVL
Leaf
(IDF)
C9K
AP
Cabin Switch
C9K
Spine
(Dist.)
C9K
SVL
Leaf
(IDF)
C9K
AP
Cabin Switch
C9K

L2 Connectivity to DC

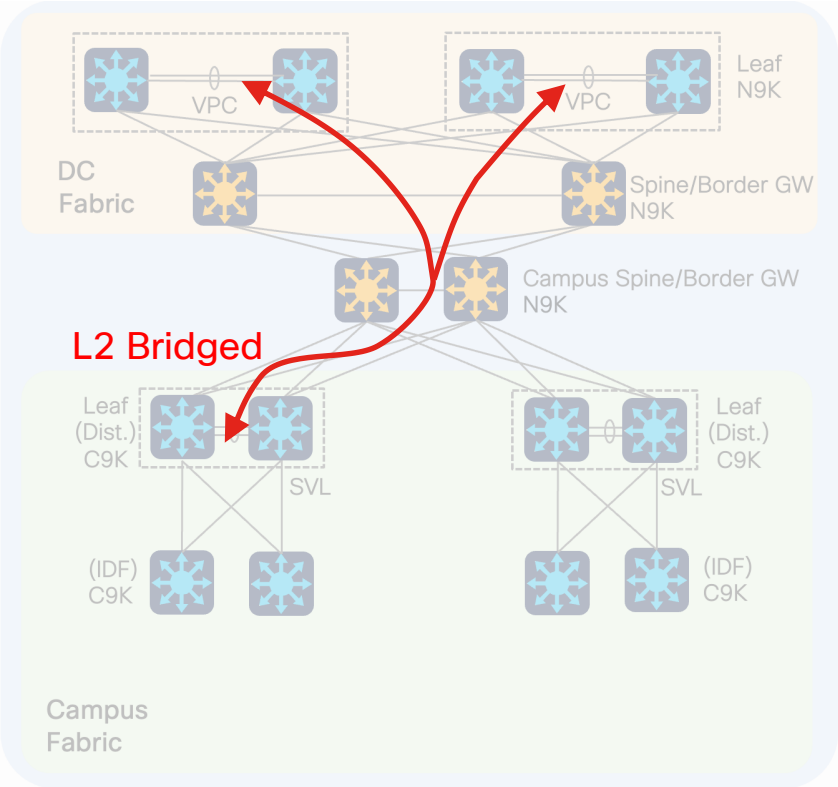
Challenge:

- Certain legacy applications require endpoints at the Campus to be on the same L2 segment as servers at DC

Solution: Layer 2 Overlay Tunnels

Typical Use Cases

- Manufacturing
- IoT



Location Redundancy

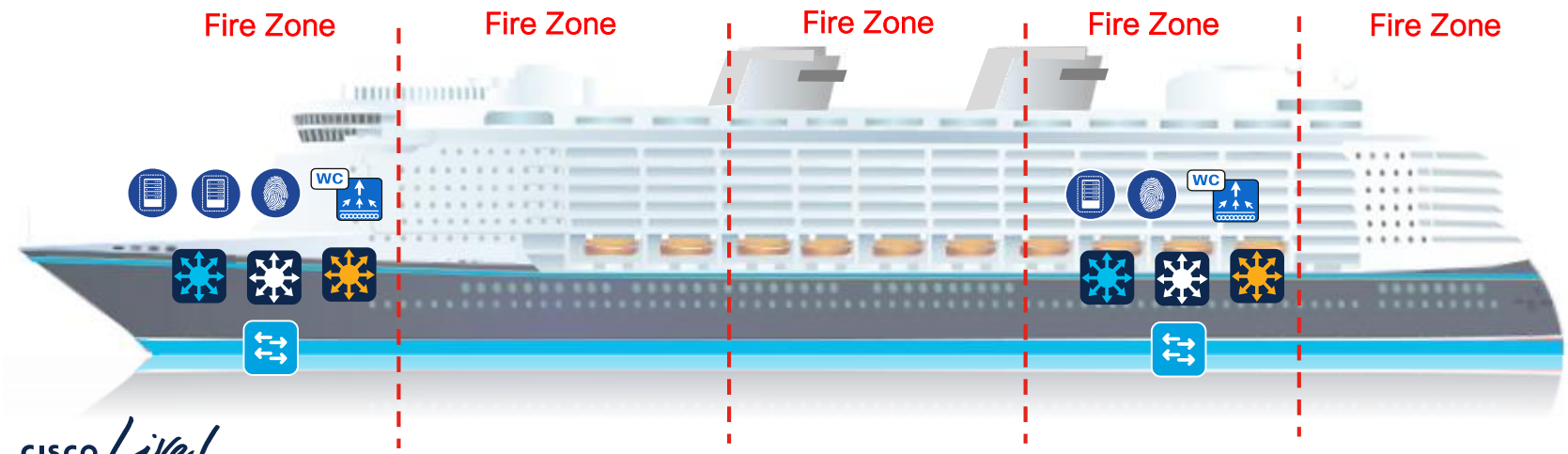
Challenge:

- DCs and critical network devices need to have location redundancy

Solution: Spread them across Fire Zones and locations

Typical Use Cases

- Transportation
- Financial

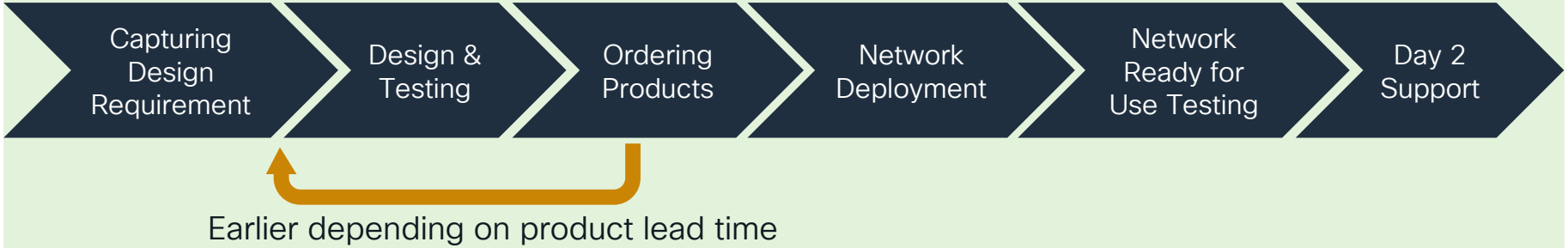


Plan, Design, Implementation, and Support Best Practices

Plan

Project Planning

- Plan according to contractually binding ship sail date
- Set major milestones



- Engage all involved parties relevant to deployment phases
- Track progress and take actions as needed

Plan

Capture Design Requirement

- Current operation model
- Priorities and approaches to meet them
- Traffic Flow: Campus – DC - Internet
- Application requirement

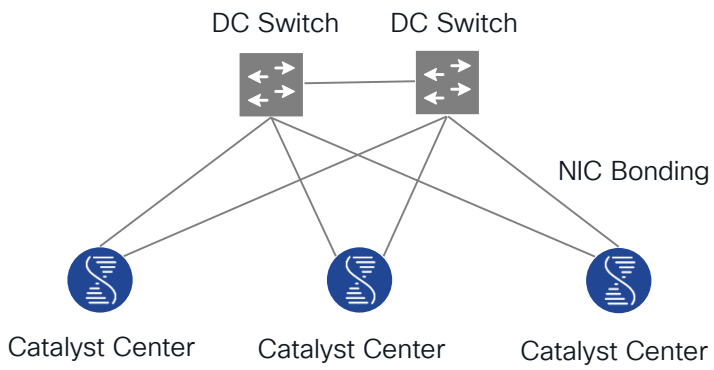
Security Policies

- Define security policies based on business requirement
- Macro and micro segmentation
- Group Based Policies
- Endpoint authentication and authorization
- Further developed in Design and fine-tuned in lab and onsite

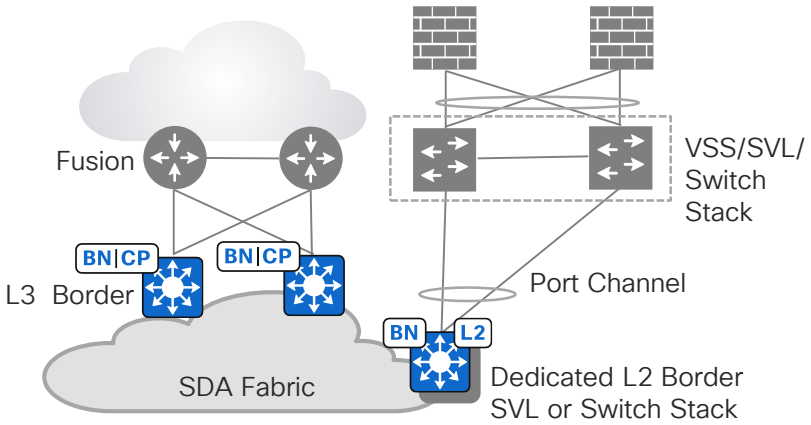
Design

Redundancy

- Link, controller and hardware redundancy
- Put critical roles on dedicated devices
- Routing if possible, bridging only if you have to



Catalyst Center 3-Node Cluster HA

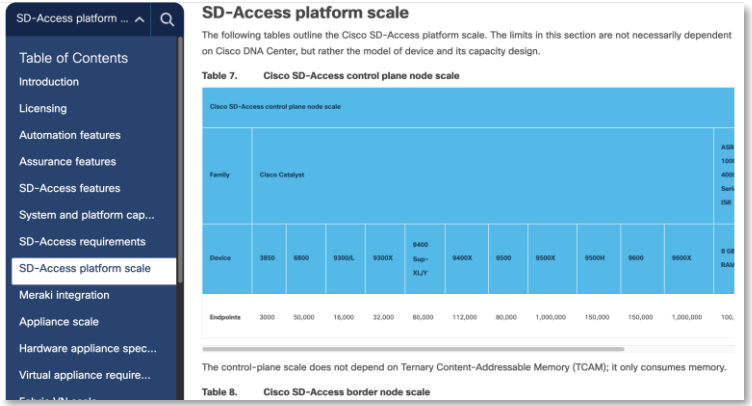


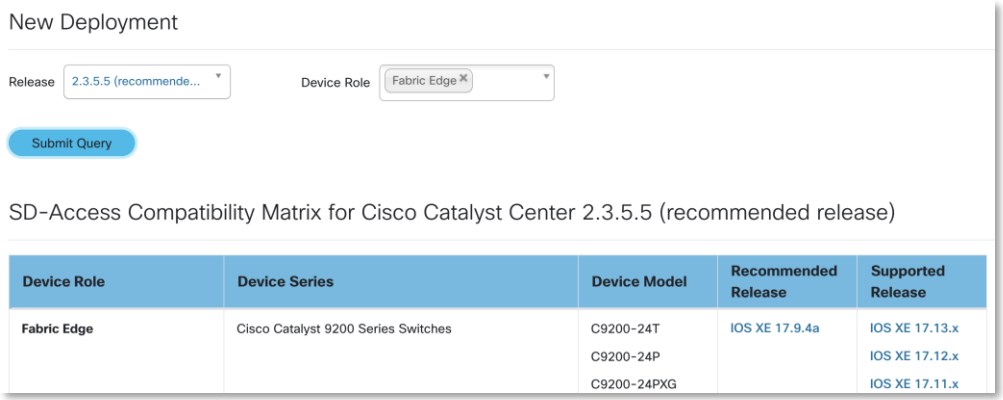
SDA L2 Border

Design

Sale & Feature Support

- Consider platform & controller scales
- Older hardware affects Fabric wide feature support
- Use recommended controller & device software versions
- Standardize network site hierarchy, scalable IP address schemes & device naming

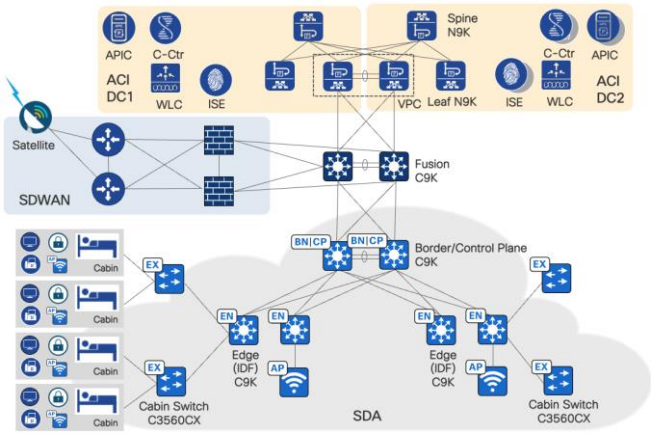


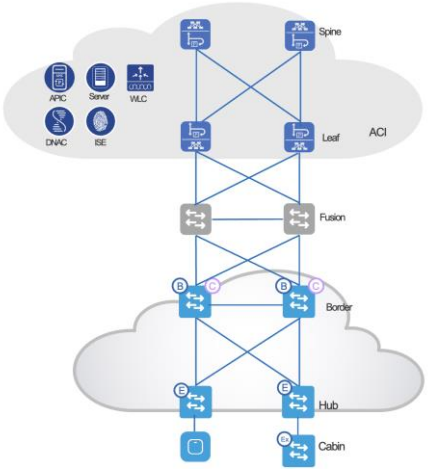


Design

Lab Environment

- Set up a scaled down proof of concept (POC) lab if feasible
- The lab assists in developing implementation procedures
- Software version and hardware certification
- Ongoing lab testing prior to implementing new features to production network



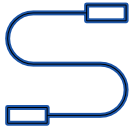


Deployment

Coordination

- Consider international shipyard construction constrains
- Address issues with shipyard construction timely:
  - Cabling
  - Unaccountable APs and Cabin switches
- Conduct post implementation WiFi RF survey before ships are in service

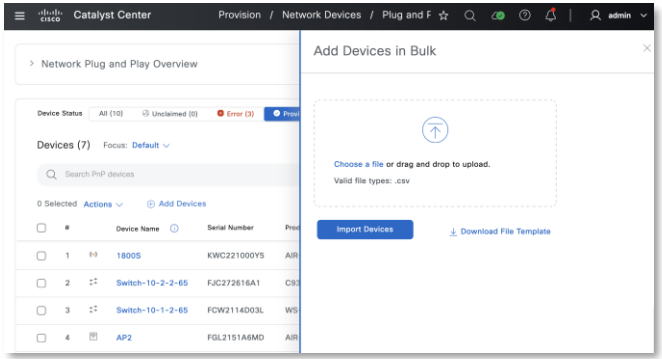





Deployment

SDA Automation

- 100s of APs and cabin switches can be connected by shipyard construction at different times
- Automate AP onboarding using a CSV template
- Large numbers of Extended Node onboarding can be automated using templates



Serial Number	Model	AP Name	Site	RF Profile
FJC253786GH	C9115AXE-B	AP-9-2-9016	Global/ADVENTURE/FABRIC_ZONE_03/DECK_09	PASSENGER
FJC253716MV	C9115AXE-B	AP-9-2-9018	Global/ADVENTURE/FABRIC_ZONE_03/DECK_09	CREW

Extended Node Onboarding

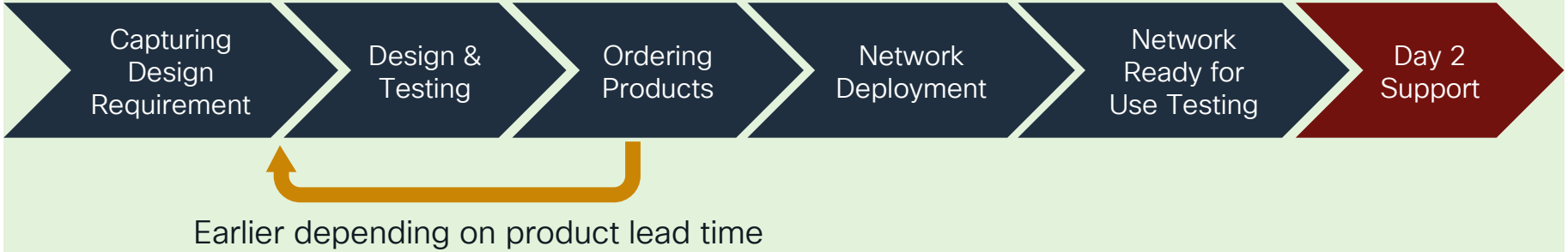
- Configure an EEM script in a template
- Push the template into upstream Edge switches by provisioning
- The Edge creates a port-channel and trunk when it sees a C3560CX as its CDP neighbor
- The C3560CX is onboarded as an Extended Node automatically
- Once all the C3560CX are onboarded, remove the EEM script from the Edge

```
event manager applet detect-3560CX authorization bypass
 event neighbor-discovery interface regexp Ethernet.* cdp add
 action 1.0 regexp "(C3560CX)" "$_nd_cdp_platform"
 action 2.0 if $_regexp_result eq "1"
 action 2.1 cli command "enable"
 action 3.0 cli command "show running-config interface $_nd_local_intf_name"
 action 4.0 regexp "(channel-group)" "$_cli_result"
 action 5.0 if $_regexp_result eq "0"
 action 6.0 cli command "enable"
 action 7.0 cli command "config t"
 action 8.0 cli command "default interface $_nd_local_intf_name"
 action 8.1 cli command "int $_nd_local_intf_name"
 action 8.3 cli command "switchport mode trunk"
 action 8.4 syslog msg "3560CX detected, no port-channel present"
 action 8.5 break
 action 8.6 else
 action 8.7 syslog msg "3560CX detected, port-channel present"
 action 9.1 end
 action 9.2 end
```

Post Implementation Support

Day 2 Support

- Design/Implementation team provides support immediately after ship launch
- Transfer network As-Built documents to Day-2 support
- Train Day-2 support team on features and technology
- Changes made to production should be reviewed, approved and implemented during change windows



Sneak Preview: Catalyst Center Orchestrated BGP EVPN

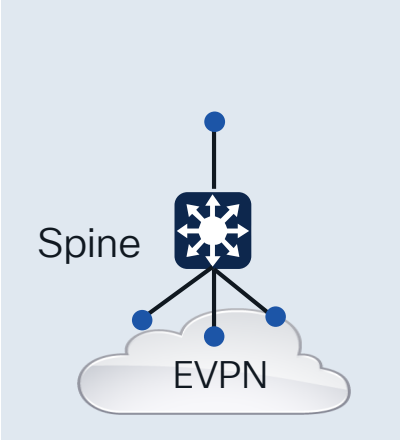
SDA-EVPN Supported Hardware

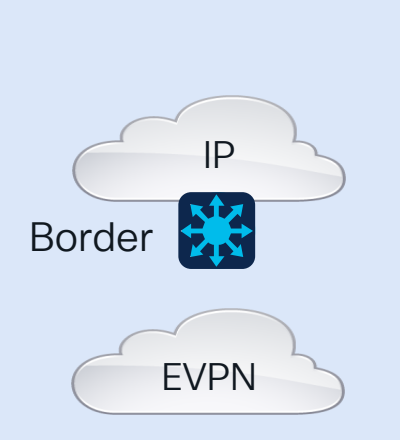
Catalyst Center		
Physical Appliance	Virtual Appliance	Cloud
DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	DN2-SW-APL	Amazon Web Services

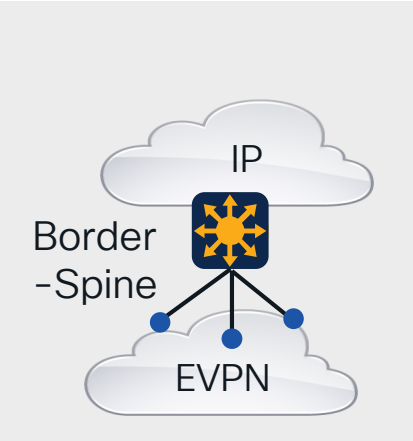
Catalyst Center can support either SDA-LISP or SDA-EVPN. Co-existence of both control-planes on single Catalyst Center is not supported

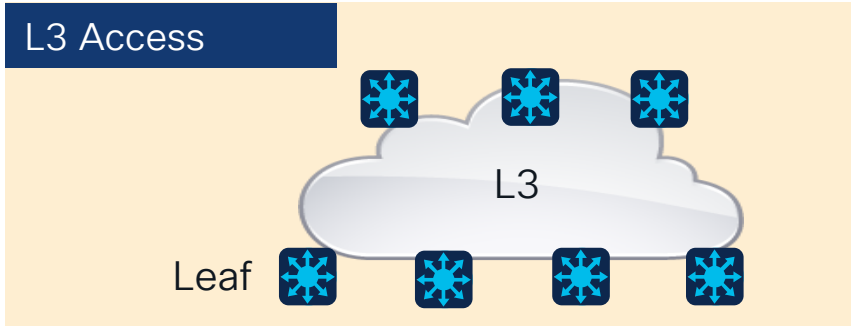
Catalyst Switches (IOS-XE 17.12.x and above)	
Core	Access
Catalyst 9500 Non-High-Performance Catalyst 9500 High-Performance Catalyst 9600 Sup-1	Catalyst 9300L/LM Catalyst 9300/9300B Catalyst 9300-X Catalyst 9400 Sup-1 Catalyst 9400-X Sup-2

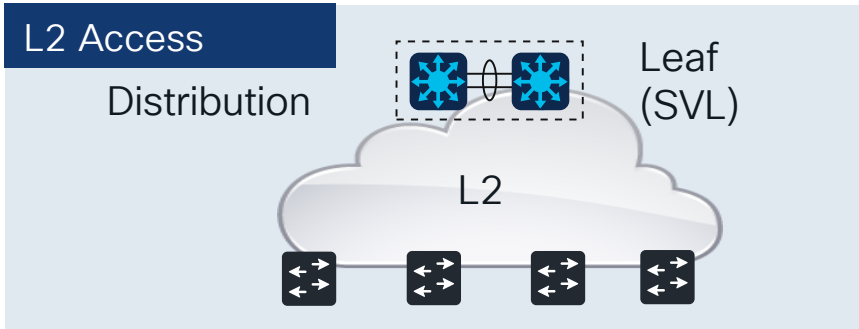
Fabric Roles and Access Modes





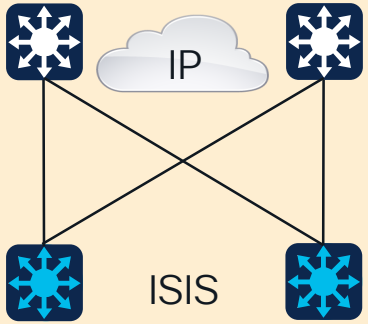




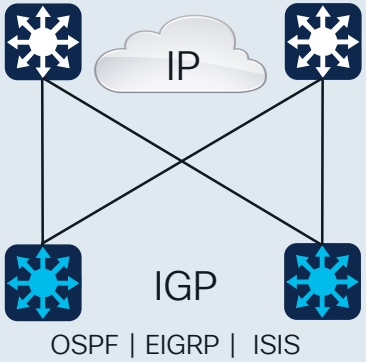


Flexible Underlay Options

LAN Automation



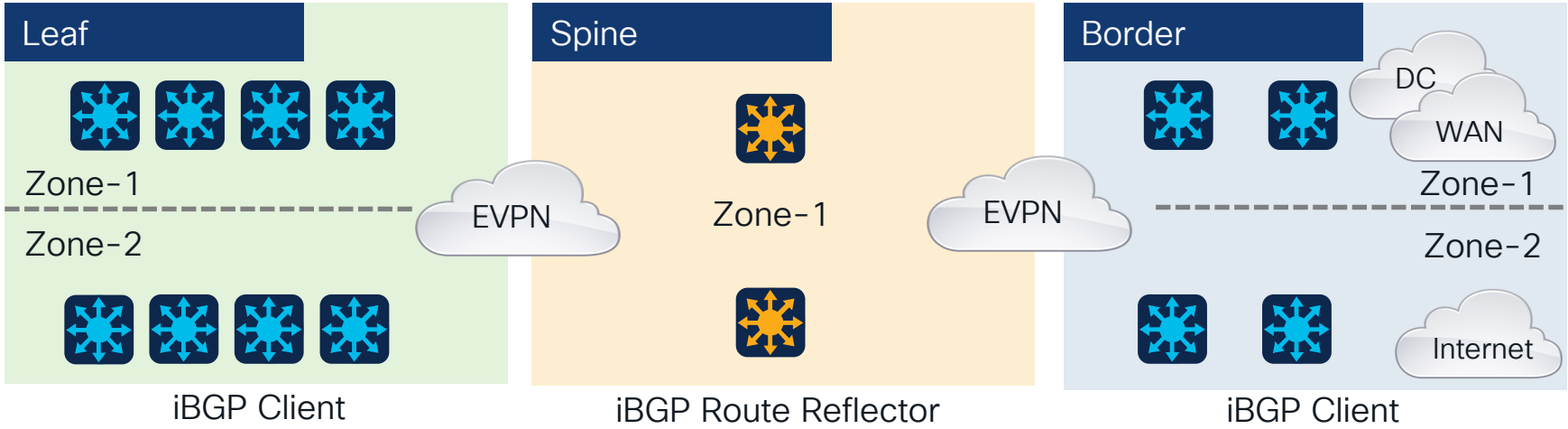
Brownfield



- Network virtualization does not mandate change to existing network
- Customers can build SDA-EVPN Fabric while managing brownfield underlay independently

SDA-EVPN does not support fabric automation on network switches with pre-configured BGP

Control Plane & Fabric Zone



Control Plane

- Underlay IGPs can be used to build iBGP sessions over loopbacks

Fabric Zone

- A device can only be associated to single Fabric Zone
- A Fabric site can have multiple Leaf and Border zones but one Spine zone only

Simplified Addressing

L3VN Address Pool

- Route-Distinguisher
- L3VNI ID
- Core VLAN
- NVE
- Default MDT Group
- Route-Target
- Data MDT Group Range

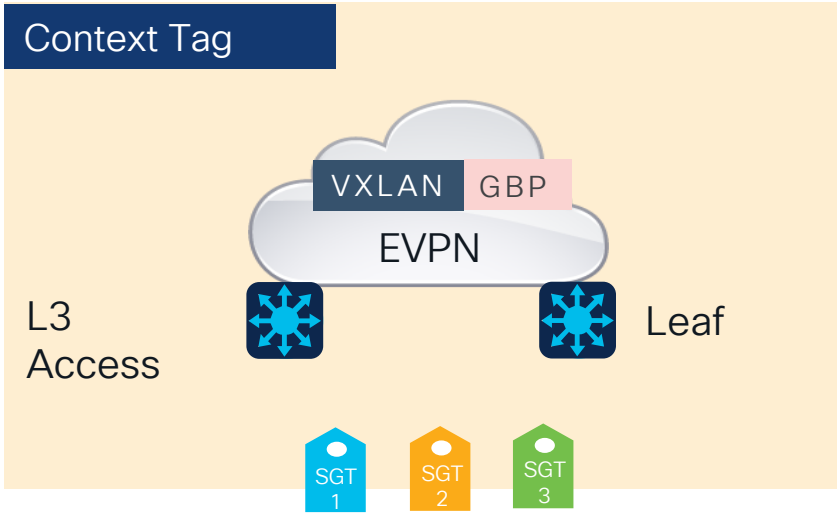
L2VN Address Pool

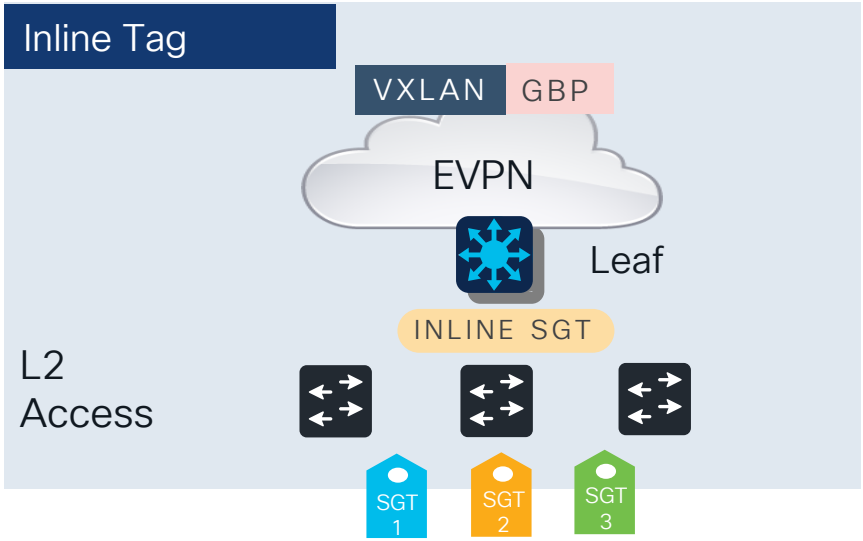
- Route-Target
- EVI Instance ID
- Multicast Replication
- L2VNI ID
- NVE
- Route-Distinguisher

- Fabric Resource Pools auto-generated
- Automation workflows dynamically reserve & release addresses to pools
- Reduces operational complexity

Fabric Resource Pool is a one-time initial fabric site configuration step. It cannot be expanded or modified once fabric site automation is completed

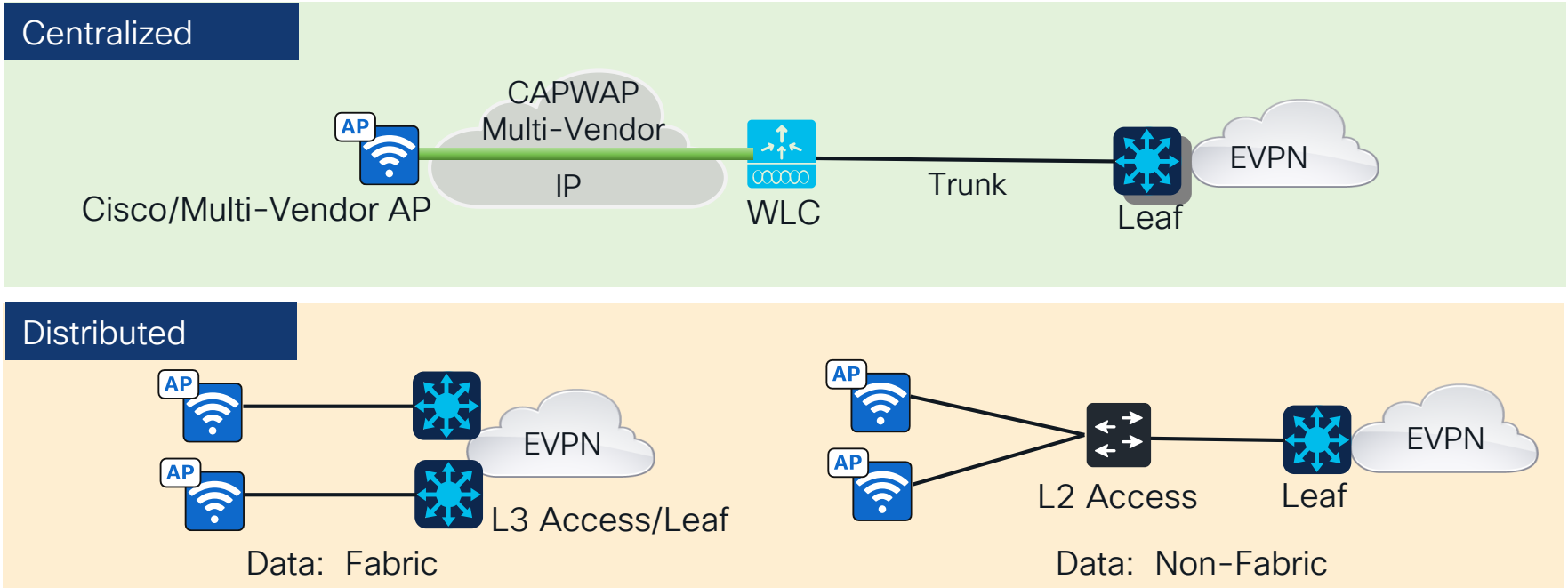
Context Aware Fabric – Micro Segmentation





- VXLAN with Group Based Policy (GBP) extension uses SGT for endpoint contexts
- VXLAN data-plane with GBP extents policy-plane across fabric

Wireless Integration



- Centralized/Distributed wireless integrated with SDA-EVPN overlay
- AP to WLC Control-plane preserved in underlay

SDA-EVPN does not automate wireless network and switch ports connected to WLC & APs

Cisco Campus BGP EVPN Solution Evolution

	Do It Yourself CLI	Programmable Ansible, Terraform	NDFC	SDA-EVPN Catalyst Center
Fabric Configuration	✓ CLI templates	✓ Automated	✓ Automated	✓ Intent-Based
Software Life Cycle Management		✓	✓	✓
Config Compliance			✓	✓
Assurance & Analytics (Endpoint, Policy & Trust)				✓
Zero-Trust Architecture				✓

Enterprise Ready Catalyst 9000 Foundation

How Did the Tale of Two Ships End?

- Network implementation started from around 2022-23
- SD-Access LISP (SDA) & BGP EVPN deployed on two ships from two different cruise lines
- Around ten vessels have been deployed using these two solutions, with more to come
- Both solutions have been very stable

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

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

Contact me at: chyan@cisco.com, ythallas@cisco.com@cisco.com

Thank you