

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

Cisco SD-Access Design and Deployment Best Practices

BRKENS-2502a

Prashanth Kumar- Technical Marketing Engineer
Enterprise Network Business Group

CISCO *Live!*

#CiscoLive

Cisco Webex App

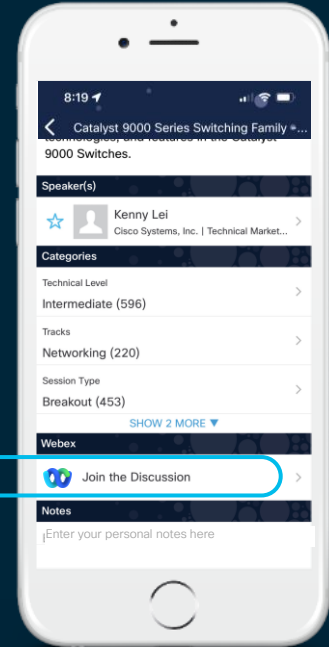
Questions?

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 17, 2022.



<https://cicolive.ciscoevents.com/cicolivebot/#BRKENS-2502a>

This Session **doesn't** cover

- ✘ Introduction to SD-Access and its components
- ✘ Feature Deep-Dive
- ✘ Packet walks.

This Session does cover

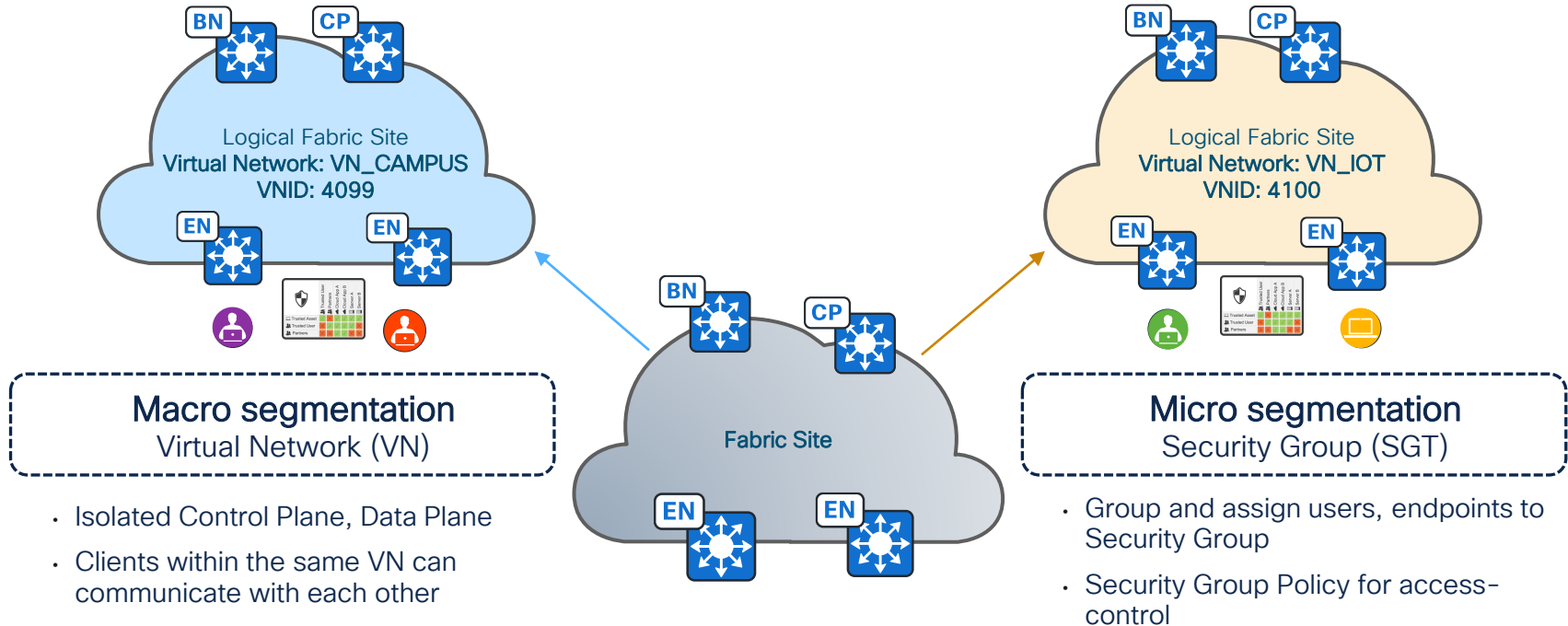
- ✓ Design options, considerations and Best practices

Agenda

- Segmentation overview
- Design
 - Considerations
 - Design
 - Scale
 - Fabric Deployment
 - Underlay Infrastructure
 - Fabric Infrastructure
 - Wireless Infrastructure
- Summary

Cisco SD-Access

Multilevel Segmentation – VN, SGT



Cisco SD-Access

Segmentation Strategy

Macro segmentation

Virtual Network (VRF)

- Each VN is a dedicated instance for control plane and data plane.
- Leverage Virtual Networks if there is a need for **complete isolation** of business function.
- Default Policy: Endpoint **cannot** communicate with other devices in different Virtual Network.
- Endpoints can communicate within their own Virtual Networks

Micro segmentation

Security-Group (SGT)

- Default Policy: Endpoints **can** communicate with other Security Groups.
- Security Group Policies can be simple permit/deny or contracts containing Layer 4 access-control entries (Application, TCP//UDP ports).
- Leverage SGT with policies to control communication between Security Groups.
- Provides location independent policy

Cisco SD-Access Security Group Policies

Policies (12096) [Enter full screen](#)

Filter Deploy Refresh

Permit
 Deny
 Custom
 Default

Source	Destination	Auditors	BYOD	Contractors	Corporate_Visi...	Developers	Development_L...	Doctors	Employees	Guests	IP_Phones	Network_Servi...	Nurses	PCI_Servers	Point_of_Sale...	Production_Se...	Prodi...	Public	Quarant...
Corporate_Visitor																			
Developers																			
Development_S...																			
Doctors																			
Employees																			
Guests																			
IP_Phones																			
NetSvcs																			
Nurses																			
PCI_Servers																			
Production_Serv...																			
Production_Users																			

Click to edit contract

Employees > Anti_Malware > Employees
 Employees > Anti_Malware > Employees

Edit Access Contract

Name* **Anti_Malware** Description **Block ports commonly exploited by**

CONTRACT CONTENT (62)

#	Action *	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Deny	Advanced	TCP	Destination Source	138 ANY	<input type="checkbox"/>	+ X
2	Deny	Advanced	TCP	Destination Source	138 ANY	<input type="checkbox"/>	+ X
3	Deny	Advanced	UDP	Destination Source	138 ANY	<input type="checkbox"/>	+ X
4	Deny	Advanced	UDP	Destination Source	138 ANY	<input type="checkbox"/>	+ X
5	Deny	Advanced	TCP	Destination Source	139 ANY	<input type="checkbox"/>	+ X
6	Deny	Advanced	TCP	Destination Source	139 ANY	<input type="checkbox"/>	+ X
7	Deny	Advanced	UDP	Destination Source	139 ANY	<input type="checkbox"/>	+ X
8	Deny	Advanced	UDP	Destination Source	139 ANY	<input type="checkbox"/>	+ X

Default Action **Permit** Logging

Cisco SD-Access

Segmentation example- Virtual Network, Security Group, IP Pools

Endpoints	Authentication	Traffic Attributes	Security Groups	Virtual Networks	Policies	Host Pools
Vending Machines	MAB	GW at Firewall*	Vending_Machine	VN_IOT	No Group-to-Group or within Group communication	VLAN 500
Badge Readers	MAB	Silent Hosts*	BDG_Readers			10.4.1.0/24
Cameras	MAB	Multicast	Cameras			10.4.2.0/24
Printers	MAB	Wake On LAN*	Printers	VN_CAMPUS	No Printer-to-Printer No Printer-to-IP Phone Restricted access to Printers	Data 10.4.16.0/20 Voice 10.4.33.0/24
IP Phones	Dot1x, MAB		IP_Phones			
Workstations	Dot1x, MAB		Employees Contractors			
Phones, Tablets	Web-Auth		Guest	VN_GUEST	No Group communication	10.4.35.0/24

*Endpoints requiring Broadcast, dedicate smaller subnet and enable Layer-2 flooding

SD-Access Platform Support

Digital Platforms for your Cisco Digital Network Architecture



For more details: cs.co/sda-compatibility-matrix

Cisco Software-Defined Access Compatibility Matrix

Select Deployment

New Deployment Upgrade

New Deployment

Release:

Device Role:

ISE
Fabric Edge
Fabric Border and Control Plane
Wireless
Extended Node or IOT Extension for SD-Access
SD-WAN Integrated Domain Solution
Collocated SD-Access Border, Control Plane and SD-WAN WAN Edge
SD-WAN Controller

[Site Map](#) [Terms & Conditions](#)

Platform support based on the Fabric Role

Cisco Software-Defined Access Compatibility Matrix

Select Deployment

New Deployment Upgrade

New Deployment

Release:

Device Role:

SD-Access Compatibility Matrix for Cisco DNA Center 2.2.3.5 (recommended release)

Device Role	Device Series	Device Model	Recommended Release	Supported Release
Fabric Border and Control Plane	Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X ASR 1006-X (RP2) More ...	IOS XE 17.6.2	IOS XE 17.6.x IOS XE 17.5.x IOS XE 17.3.x IOS XE 16.9.1s IOS XE 16.9.2 More ...

Supported Hardware and Software Version for all Cisco SD-Access components

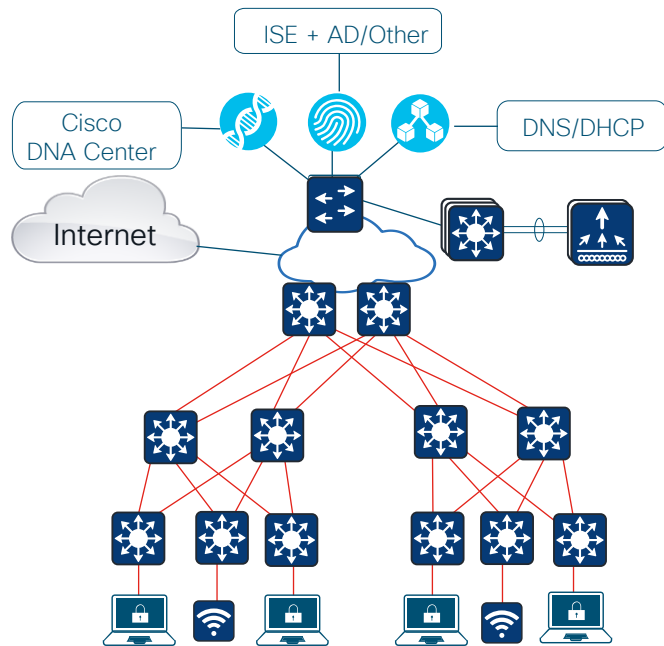


Cisco SD-Access Design Considerations

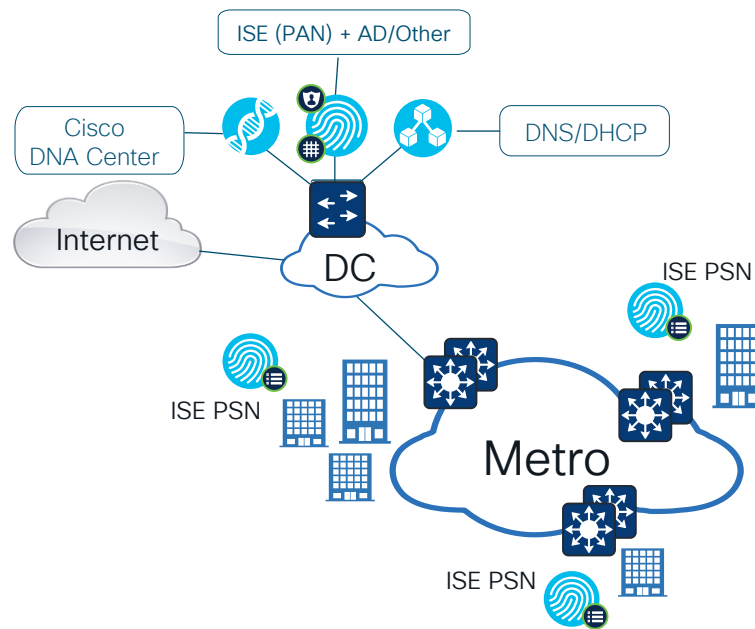
Connectivity Services

Where do I place Critical Services?

Local DC or Services Block



Remote DC



Cisco DNA Center requires access to Internet.

Cisco SD-Access Scale

For your reference

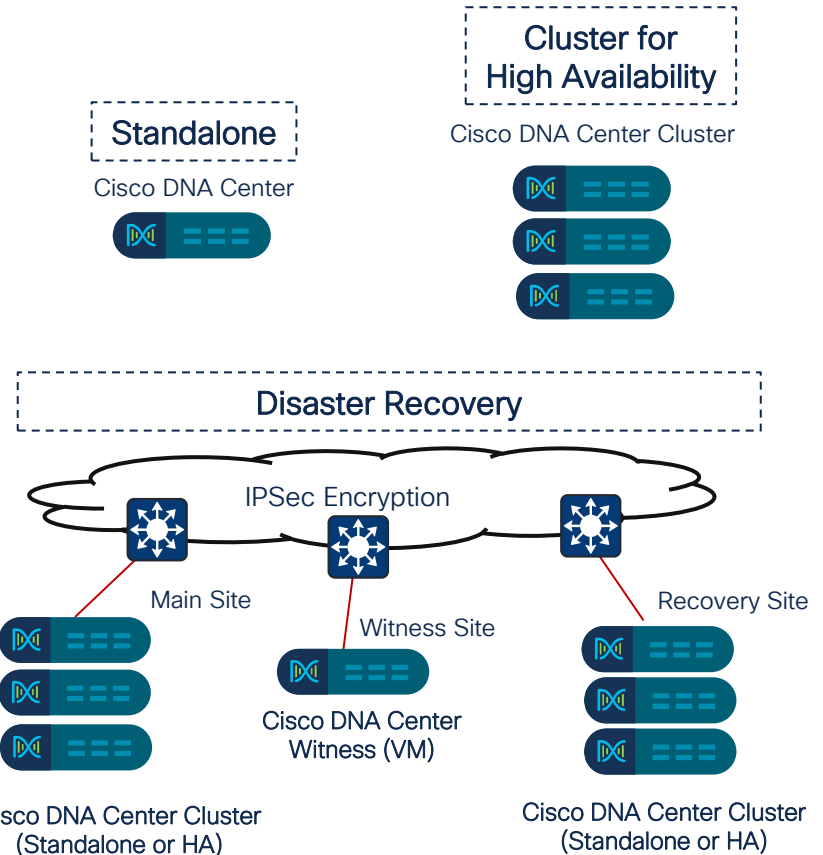
Cisco DNA Center Deployment

- Deployment Types

- Standalone
- Cluster for High Availability (HA)
 - Cluster interconnected with 10Gbps interface with <10msec latency
- Disaster Recovery (DR) for network downtime
 - Cluster connected with 1Gbps interface between main site and recovery site with <350 msec latency

- Failure detection and recovery

	High Availability	Disaster Recovery
Failure Detection time	5 minutes	3 minutes
Time taken to failover on failure detection	7-13 minutes	15-30 minutes
Failover time behavior	Service down upto 7 minutes	Service down upto 30 minutes
Failback	Automatic	Manual



Cisco Identity Services Engine

For your reference

Standalone or Distributed Deployment

- Applies to both Physical and Virtual deployment
- Compatible with load balancer



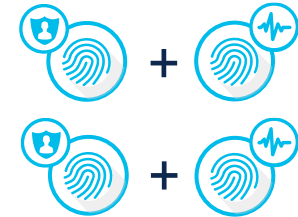
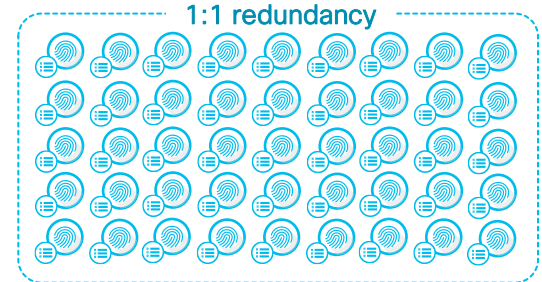
Standalone Deployment
1 x (PAN+MNT+PSN)



Small HA Deployment
2 x (PAN+MNT+PSN)



Medium Multi-node Deployment
2 x (PAN+MNT), <= 5 PSN



Large Deployment
2 PAN, 2 MNT, <=50 PSN

100 Endpoints	Up to 20,000 Endpoints	Up to 500,000 Endpoints	3500
100 Endpoints	Up to 50,000 Endpoints	Up to 2,000,000 Endpoints	3600

Cisco SD-Access

Latency Requirements

Cisco DNA Center nodes in a cluster

ISE personas in distributed deployment

Edge node

Border node

Control plane node

Wireless LAN controller

Access point



10 msec
RTT



300 msec
RTT



300 msec (RTT)*

* Longer execution time could be experienced for certain events with latency higher than 200 msec; latency beyond 300 msec is not supported.

200 msec (RTT)**

** Longer execution time could be experienced for certain events with latency higher than 100 msec; latency beyond 200 msec is not supported.

200 msec (RTT)**

** Longer execution time could be experienced for certain events with latency higher than 100 msec; latency beyond 200 msec is not supported.

100 msec RTT ***

100 msec RTT ***

100 msec RTT ***

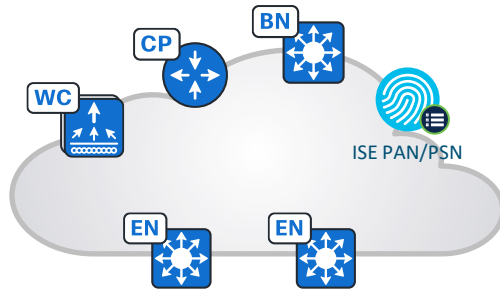
*** ISE to NAD (Network Access Device) communication, including TrustSec, uses RADIUS; RTT is therefore based on RADIUS requirements.

100 msec RTT

20 msec RTT

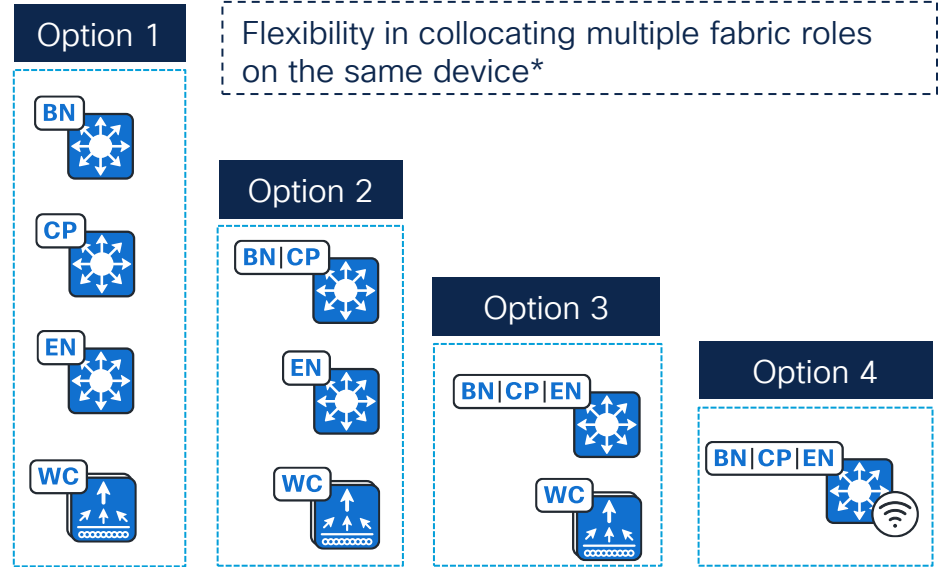
Cisco SD-Access Design Options

Fabric Site Design Options



Fabric Site

- Logical construct that contains:
 - Fabric Edge, Border, Control Plane
 - ISE PAN/PSN Node
 - (optional) Wireless LAN Controller, Access Points
 - (optional) Extended Nodes



Flexibility in collocating multiple fabric roles on the same device*

* Refer to Cisco SD-Access compatibility matrix for latest information

Cisco SD-Access

Distributed Fabric Site Design Options

Managed by single Cisco DNA Center and ISE Deployment

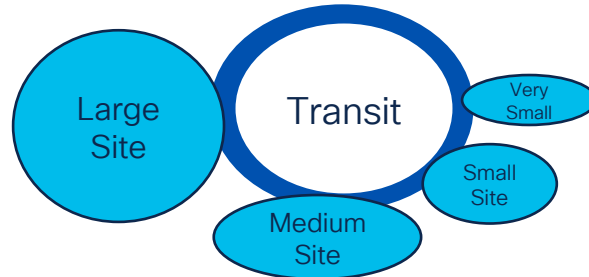


Fabric Site Design

High Availability & Scale defines Platform and Fabric Roles

Distributed Site Design

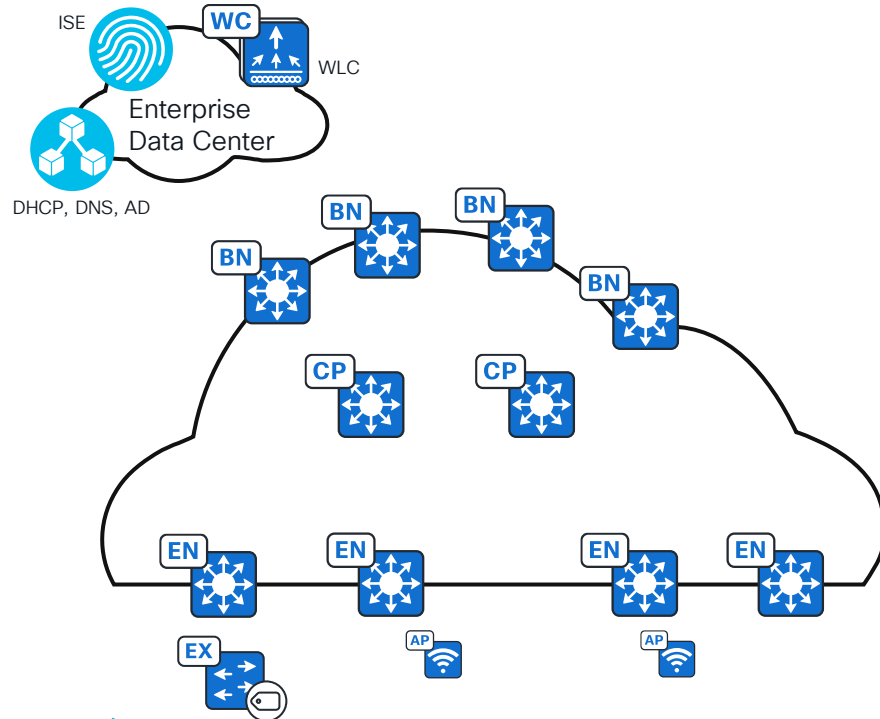
Transport connection defines Transit : IP-Based | SD-Access | SD-WAN



- Administrative domain
- Site Survivability and Scale
- End-to-End Segmentation
- Unified and Consistent Policy

Cisco SD-Access Deployment Options

Fabric Site – Large Site Design (Reference)

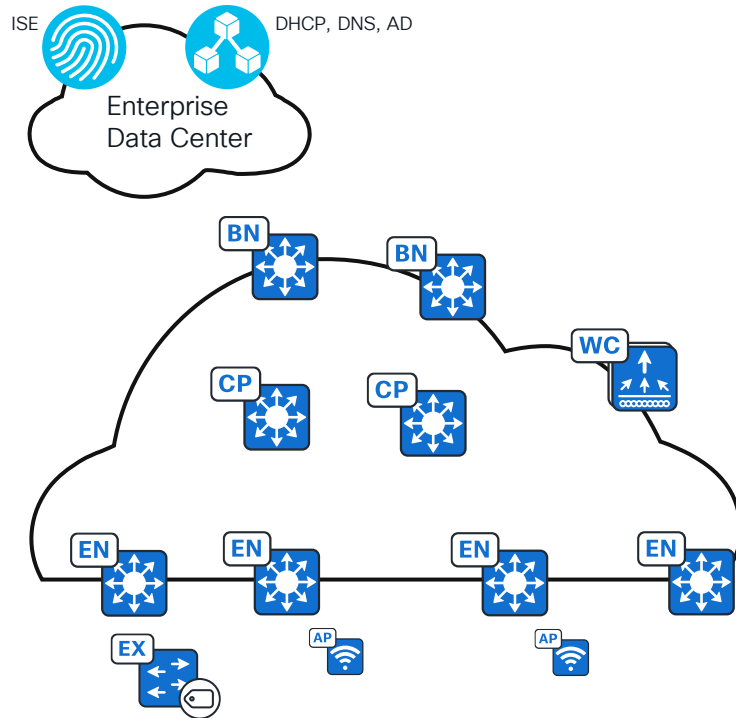


Description	Quantity
Endpoints	< 50,000
Fabric Border	2-4
Fabric Control-Plane	4 (wired infrastructure) 2* (with wireless deployment)
Fabric Edge	750
Virtual Network	< 64
IP Address Pools	< 450
Access Points	< 2,000

*WLCs can support maximum 2 Control Plane node pairs – 1 pair for guest and 1 pair for non-guest (enterprise) traffic.

Cisco SD-Access Deployment Options

Fabric Site – Medium Site Design (Reference)



Description	Quantity
Endpoints	< 25,000
Fabric Border	2
Fabric Control Plane	4 (wired infrastructure) 2* (with wireless deployment)
Fabric Edge	450
Virtual Network	< 50
IP Address Pools	< 200
Access Points	< 1,000

*AireOS WLCs can support maximum 2 Control Plane node pairs. 2 Control Plane nodes for guest and 2 for non-guest (enterprise) traffic.

Cisco SD-Access Deployment Options

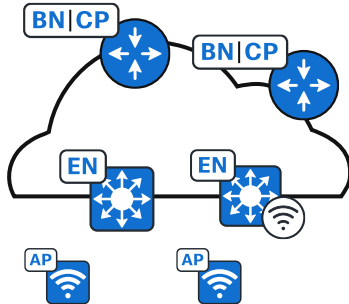
Fabric Site – Small Site Design (Reference)



Design	Option 3	Option 2	Option 1
Endpoints	< 10,000	< 2000	< 200
Fabric Border/Control-Plane co-located	2 + 2	2 (collocated)	1 (collocated)
Fabric Edge	< 75	< 50	-
Virtual Network	< 32	< 8	< 5
IP Address Pools	<100	< 20	< 8
Access Points	< 200	< 100	< 40

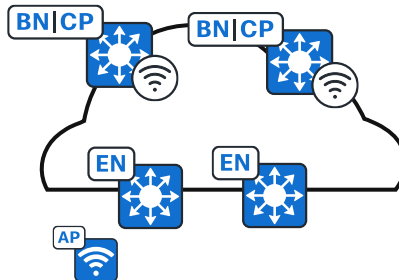
Option 3

Border Node | Control Plane Node



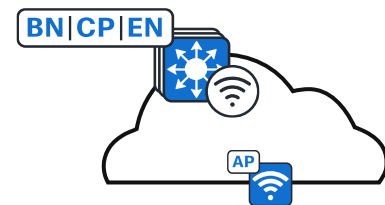
Option 2

Border Node | Control Plane Node
– with Embedded Wireless



Option 1

Fabric in a Box
– with Embedded Wireless

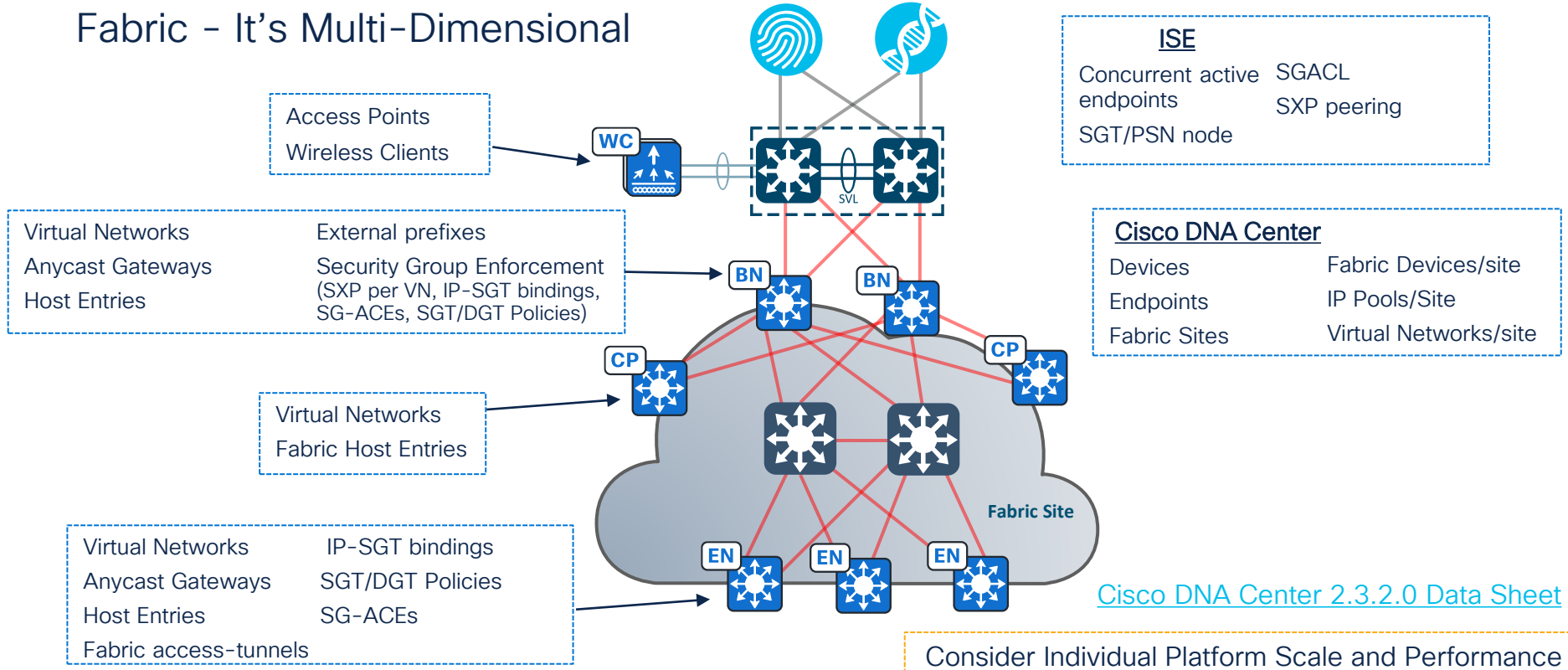




Cisco SD-Access Scale Considerations

Cisco SD-Access Scale

Fabric - It's Multi-Dimensional



Least Common Denominator (LCD) across the solution elements

Cisco SD-Access Scale

Fabric - It's Multi-Dimensional

Platform Scale

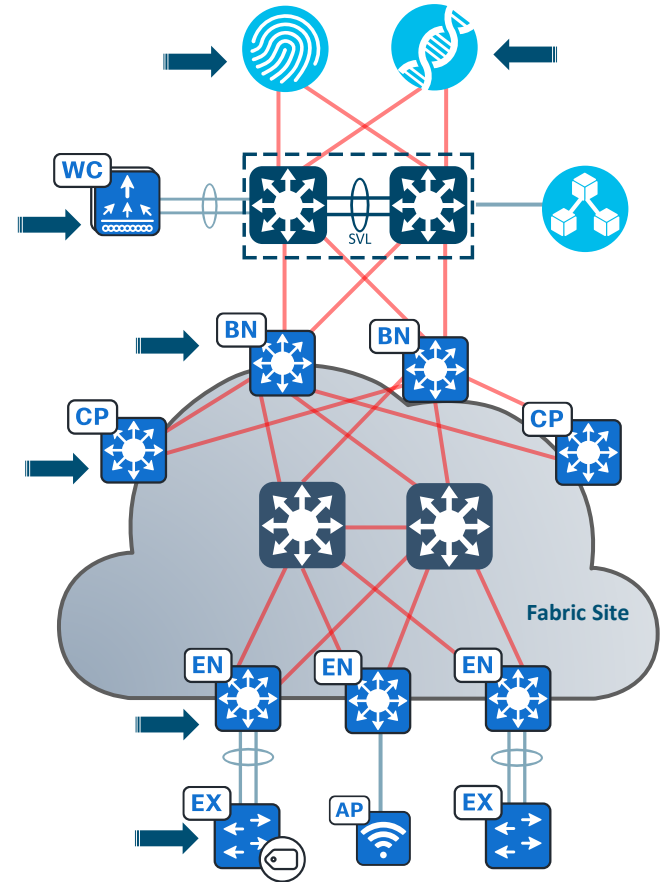
- Cisco DNA Center
- Fabric Nodes
 - Edge, Extended Node
 - Border
 - Control Plane
 - Wireless LAN Controllers
- Identity Service Engine

Features

- Endpoints count
 - Wired, Wireless
 - Fabric node
- Segmentation
 - Macro (VN), Micro (SGT)
- Network devices count/site
- IP Address Pool count/site
- Security Group and Enforcement
 - IP-SGT bindings, SG-ACEs, Policies
 - SXP

Consider Individual Platform Scale and Performance

Least Common Denominator (LCD) across the solution elements



Cisco SD-Access Scale

Cisco DNA Center Appliance Scale

For your
reference

[Cisco DNA Center 2.3.2.0 Data Sheet](#)

Description	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL	DN2-HW-APL-XL (3-node cluster)
Number of devices (switch, router, WLC)	1000	2000	5000	8000
Number of Concurrent endpoints	25,000	40,000	100,000	300,000
Number of hierarchy elements	500	1000	4000	4000
Number of Fabric sites	500	1000	2000	2000
Number of Virtual Network/site	64/site	64/site	256/site	256/site
Number of Fabric Devices/site	500/site	600/site	1200/site	1200/site
Number of IP Pools/site	100/site	300/site	1000/site	1000/site

Cisco SD-Access Scale

Cisco Identity Service Engine Scale

For your
reference

[ISE Performance and Scale](#)

Description	Limit
Max pxGrid nodes in Large or Dedicated deployment	4
Dedicated PSN nodes with SXP service enabled	4
Maximum ISE SXP peers per PSN node with SXP service enabled	200
TrustSec Security Group Tags (SGTs)	10,000
TrustSec Security Group ACLs (SGACLs)	1000
TrustSec IP-SGT Static Bindings (over SSH)	10,000

Maximum Concurrent Active Endpoints based on PSN type

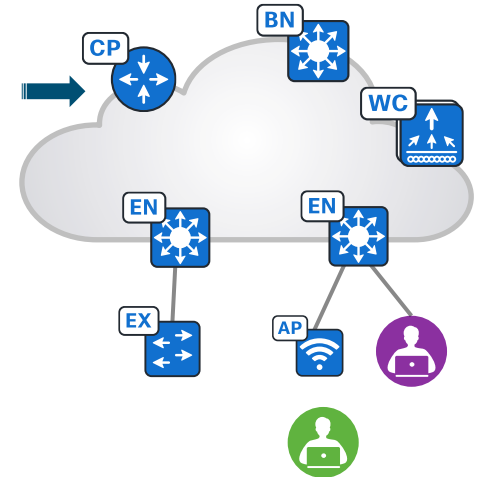
PSN Type	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
Dedicated PSN	10,000	50,000	100,000
Shared PSN	10,000	25,000	50,000

Cisco SD-Access

For your
reference

Fabric Control Plane Node Deployment

- Control Plane nodes maintains Host Tracking Database of all endpoints at a fabric site.
 - MAP-SERVER (MS) learns the EID-to-RLOC mapping from the Edge, WLC and Border nodes
 - MAP-RESOLVER (MR) resolves the EID-to-RLOC and shares the information to Edge, Border Nodes or send Negative Map Reply (NMR).
- Redundant Control Plane nodes are independent and always in active/active.
- Max Control Plane nodes
 - Wired environment: 4
 - Wired + Wireless: 2 pairs
 - 2 pair (a pair for Guest and 1 pair for non-Guest)
 - 8 pair with IOS-XE Catalyst 9800 controllers (MSRB deployment)

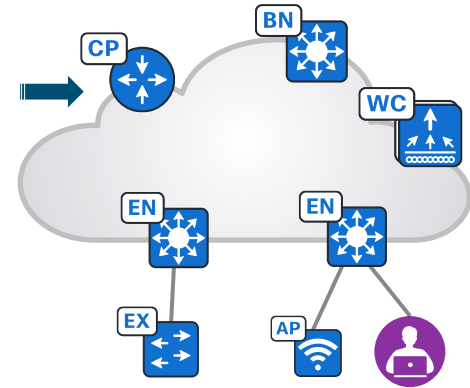


Cisco SD-Access

For your reference

Fabric Control Plane Scale consideration

- Entries refer to LISP database entry
- Each endpoint is one entry, irrespective of IPv4 or IPv6
- Endpoints includes AP, EN/PEN, wired and wireless clients



[Cisco DNA Center 2.3.2.0 Data Sheet](#)

Device	Catalyst 3850	Catalyst 9300/X/L	Catalyst 9400 Sup-XL/Y	Catalyst 9500	Catalyst 9500H	Catalyst 9600	Catalyst 6800	ASR1K, ISR4K (8 GB)	ASR1K, ISR4K (16 GB)	CSR100v
Entries	3,000	16,000	80,000	80,000	150,000	150,000	50,000	100,000	200,000	200,000

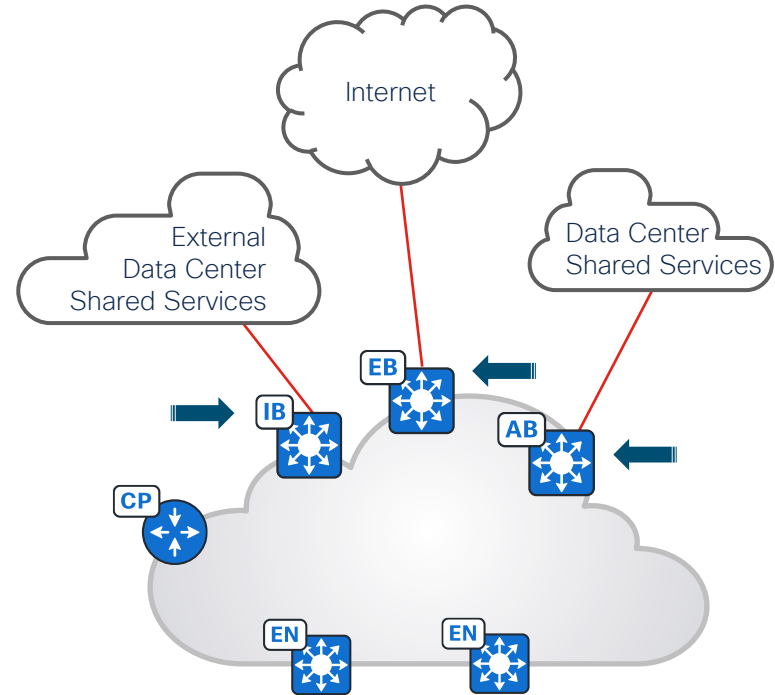
Recommendation is to maintain less than 70% of the supported scale.

Cisco SD-Access

For your
reference

Fabric Border Node Deployment

- Border nodes are the ingress and egress points for a fabric site.
- Border Node deployment options
 - **Internal** Border – **registers** external routes to LISP Control Plane
 - **External** Border – **doesn't** register any routes to LISP Control Plane, but provides **default egress point** for the fabric site
 - **Anywhere** Border – **registers** external routes to LISP Control Plane and provides **default egress point** for the fabric site.
- Advertises fabric prefixes to external domain
- Max of 4 External Border can be deployed at a site.
- Traffic to Border is always Per-Flow Load-Balanced.

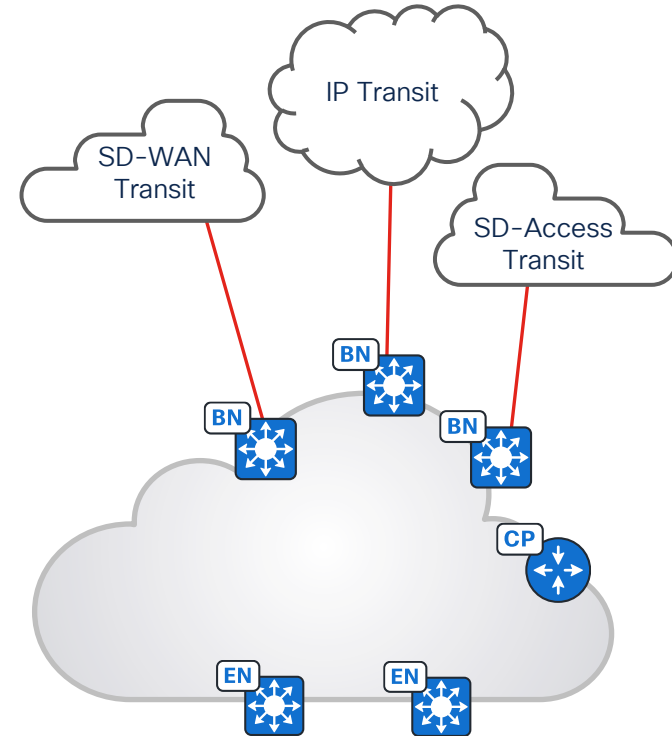


Cisco SD-Access

For your
reference

Fabric Border Node Scale consideration

- Border node with LISP **Pub-Sub** architecture caches all entries from Control Plane into its 'map-cache' table, consider host-route (HRT) entries
- Border node learns prefixes from external domain, consider IPv4/IPv6 routes.
- Enabling Security Group and policy enforcement on the Border node requires IP-SGT binding, SXP (per VN), SG-ACEs scale to be considered.



Cisco SD-Access

For your
reference

Fabric Border Scale Consideration

[Cisco DNA Center 2.3.2.0 Data Sheet](#)

Device	Catalyst 3850	Catalyst 9300/L	Catalyst 9400	Catalyst 9500	Catalyst 9500H	Catalyst 9600	Catalyst 6840 6880LE	Catalyst 6880XL	Nexus 7700	ASR1K ISR4K (8 GB)	ASR1K ISR4K (16 GB)
Virtual Networks	64	256	256	256	256	256	128	128	128	128	128
IPv4 Routes	8K	8k	64k	64k	48k	48k	60k	450k	500k	1M	4MM
Fabric Host Entries*	16K	16k	70k	70k	150k	150k	180k	450k	32k	1M	4M
IPv4:SGT binding	12K	10k	40k	40k	40k	200k	256k	256k	200k	750k	750k
SGT/DGT policies	4K	8k	8k	8k	16k	32k	30k	30k	16k	64k	64k
SG-ACEs	15K	5k	18k	18k	13k	27k	12k	30k	128k	64k	64k

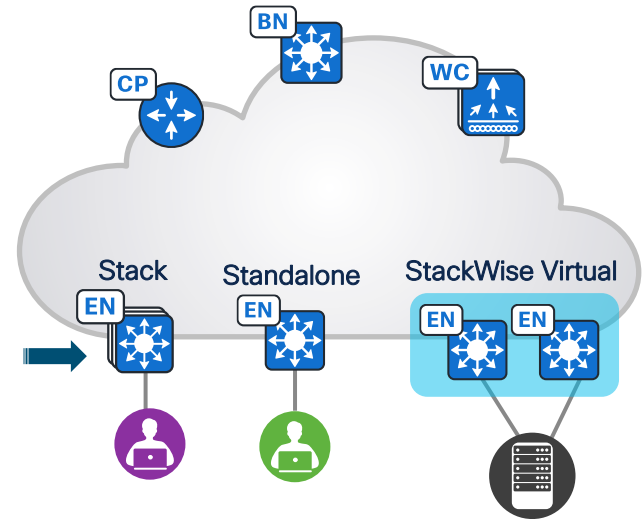
Each IPv4 host entry uses 1 TCAM entry
Each IPv6 host entry uses 2 TCAM entry except for Cat 9500H & 9600 that uses 1 TCAM entry

Cisco SD-Access

For your
reference

Fabric Edge Node Deployment

- Edge nodes are equivalent to access-layer switch (with anycast-gateway) providing connectivity to endpoints.
- Edge node can be either Standalone, Stack or StackWise Virtual switches
- Edge node within a fabric Site or fabric Zone is configured with consistent VN, VLAN and anycast-gateway.
- Access ports configured with authentication can leverage ISE to dynamic assign VLAN, Security Group or statically assign the VLAN at each port.
- Edge node will download Security Group and relevant policy from ISE to tag data-traffic and for enforcement

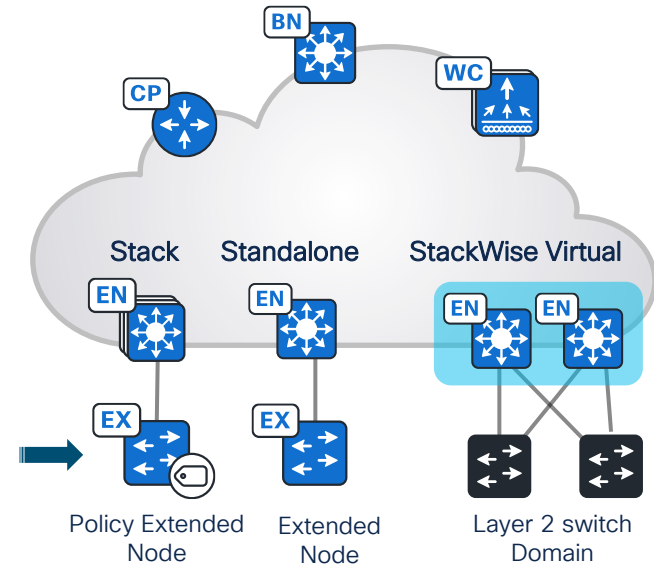


Cisco SD-Access

For your
reference

Fabric Extended Node Deployment

- Extended Node extends Layer2 enterprise network by providing connectivity to non-carpeted spaces of enterprise..
- Edge node is the anycast-gateway for Layer2 domain that includes Extended nodes, Layer 2 switch domain.
- Access ports configured with authentication can leverage ISE to dynamic VLAN or static VLAN assignment.
- Depending on the platform hardware capabilities, nodes can be Extended node, Policy Extended node.
- Policy Extended node can assign Security Group and Security Group policies for enforcement along with carrying tag to upstream Edge node.

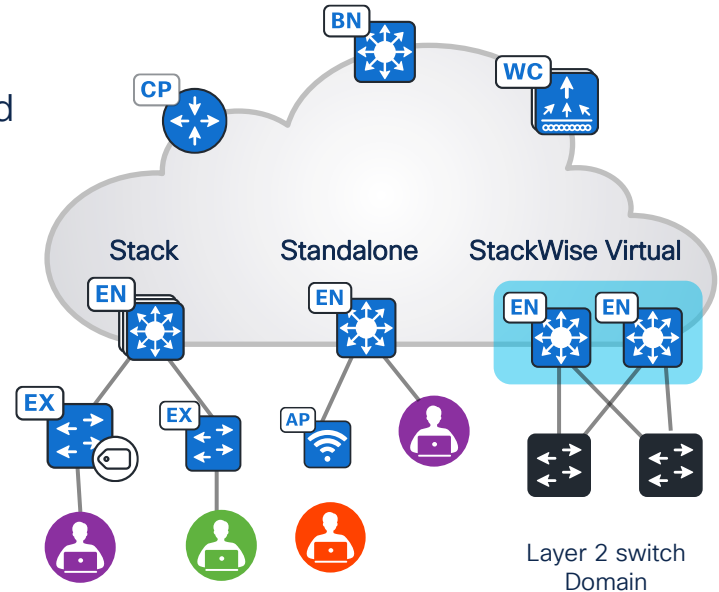


Cisco SD-Access

Fabric Edge Scale Considerations

For your
reference

- LISP database stores locally attached host (EID) entries and registers to fabric site Control Plane nodes.
- Host EIDs includes APs, Extended Nodes, wired and wireless clients
- LISP map-cache stores remote EID entries that locally connected host are interacting with.
- Security Group and Security Group Policy enforcement is enabled by default on Edge and Policy Extended node. consider IP-SGT binding, SG-ACEs, policies.



Cisco SD-Access

For your
reference

Edge Node Scale Consideration

[Cisco DNA Center 2.3.2.0 Data Sheet](#)

Device	Catalyst 3650	Catalyst 3850	Catalyst 9200-L	Catalyst 9200	Catalyst 9200 Enhanced VNs	Catalyst 9300/L	Catalyst 4500	Catalyst 9400	Catalyst 9500/H
Virtual Networks (user-defined*)	64	64	1	4	32	256	64	256	256
Endpoints	2k	4k	2k	4k	4k	6k	4k	6k	6k
IPv4:SGT binding	12k	12k	8k	10k	10k	10k	128k	40k	40k
SGT/DGT policies	4k	4k	2k	2k	2k	8k	2k	8k	8k
SG-ACEs	1350	1350	1k	1k	1k	5k	64k	18k	18k

Recommendation is to maintain less than 70% of the supported scale.

INFRA_VN is not a VRF

Each IPv4 host entry uses 1 TCAM entry
Each IPv6 host entry uses 2 TCAM entry except for Cat 9500H that uses 1 TCAM entry

For your
reference

Cisco SD-Access High Availability

Cisco SD-Access

High-Availability Considerations - Switches

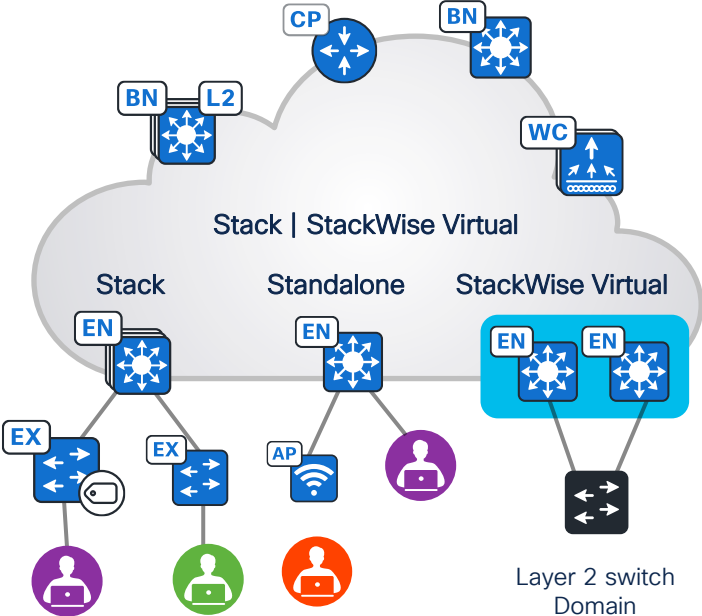
- Multiple member Switch stack acting as a single logical switch



- Two Switches acting as a single logical switch (StackWise Virtual)



Prefer Stack over StackWise Virtual



Cisco SD-Access

High-Availability Considerations – Wireless

Stateless Redundancy with N+1 HA

- WLCs remain independent of each other. Cisco DNA Center and SD-Access fabric sees them as two separate WLCs.
- For each location there is a primary and a secondary WLC.
- In a failover event, the CAPWAP tunnel is broken between AP and Primary WLC and is reinitiated with the Secondary WLC.
- APs and clients move to the Secondary WLC.



Stateful Redundancy with SSO

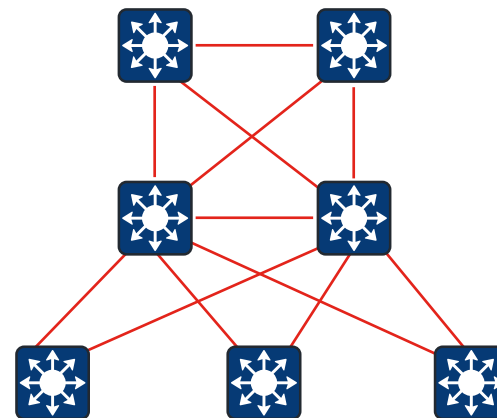
- WLC SSO is seen as a single entity.
- In a failover event, the new Active WLC will bulk update the control plane node regarding the wireless hosts.
- APs and clients stay connected during a failover event.
- For Embedded Wireless on Catalyst 9000 switches, SSO is achieved through hardware stacking on Catalyst 9300/L switches and through redundant supervisors on Catalyst 9400 switches.



Cisco SD-Access

Network Resiliency Considerations

- System-Level Resiliency
 - Nonstop Forwarding (NSF) with Stateful switchover (SSO)
- Network Level Resiliency
 - Fast Convergence (OSPF, IS-IS)
 - Bi-directional Forwarding Detection (BFD)
 - Equal Cost Multi-Path (ECMP)

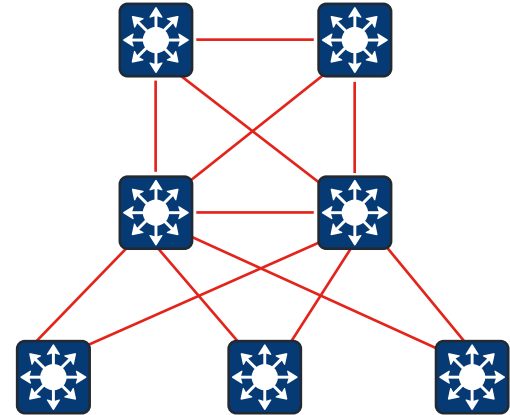


Cisco SD-Access Underlay Infrastructure

Fabric Network Infrastructure

Robust Underlay Infrastructure deployment

- Routed Access Network
- Any routing protocol
- Resilient and Redundant fast-converged connectivity with ECMP, BFD, NSF enabled.
- Loopback 0 with /32 host prefix.
- Higher MTU to accommodate VXLAN encapsulation
- Underlay multicast to optimize overlay subnet multicast/broadcast distribution



Manual | Semi-Automated Underlay

Device-by-Device onboarding and configuration either manually or through Cisco DNA Center Plug-and-Play.

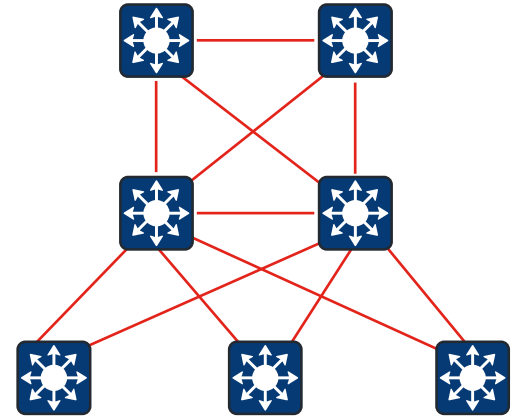
Automated Underlay

Turnkey solution to onboard multiple switches with image management and best-practices configuration.

Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation onboarding

- Automated underlay buildout with validated best practice configuration.
- L3 routed access network with IS-IS routing protocol.
- (optional) enable multicast in the underlay to build optimized Broadcast, Unknown-unicast and link-local Multicast traffic distribution.
- Zero-Touch Image Management with device onboarding.



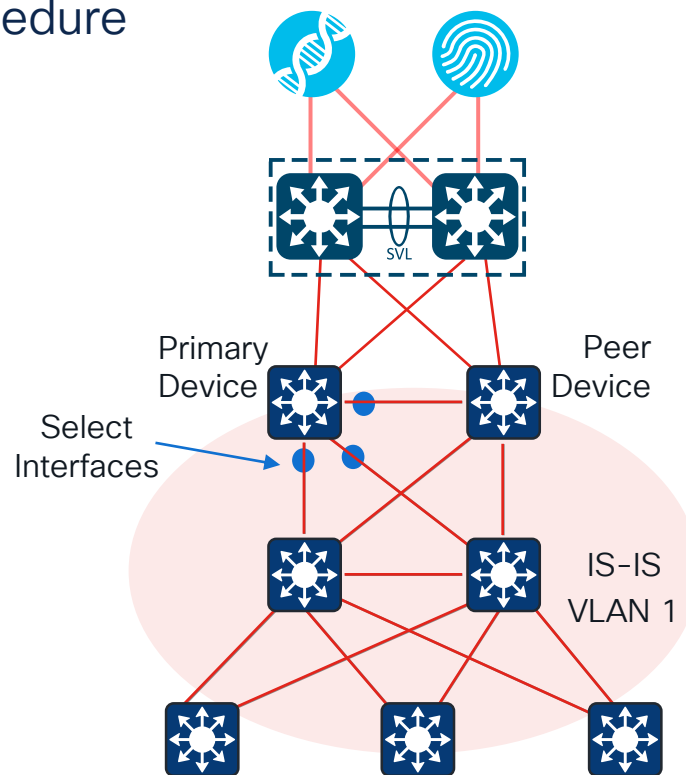
Automated underlay

Turnkey solution to dynamically discover, onboard and provision switches to simplify network operations.

Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation Procedure

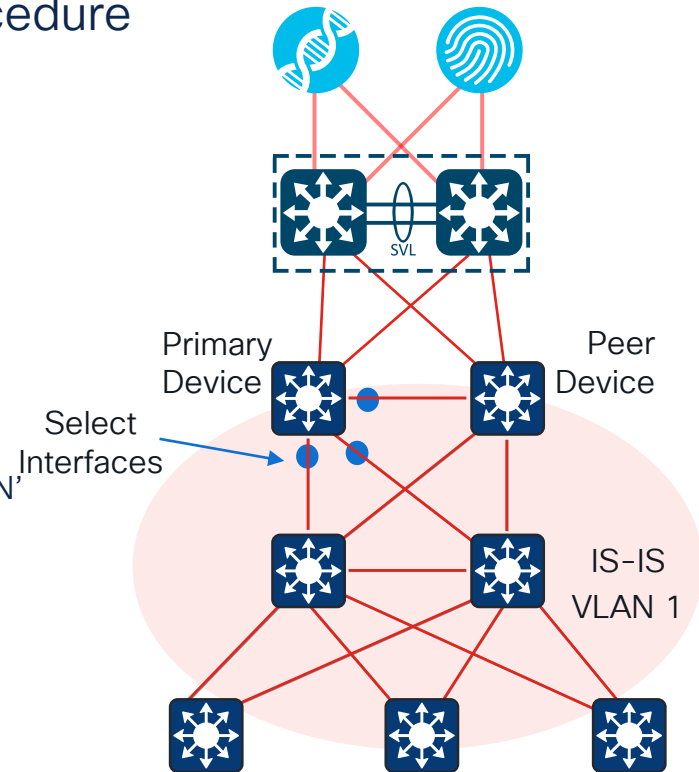
- Define Network Settings
 - Network - Network Hierarchy
 - Device Credentials - CLI, SNMP, HTTP(s) Credentials
 - IP Address Pools - IP Pool to build underlay infrastructure
- Provision network devices
 - Select Seed devices - Primary/Peer Device and Interfaces
 - Start LAN Automation - Discover network devices, image management and assigned to site.
 - Stop LAN Automation - configure routed-access



Fabric Network Infrastructure

Underlay Infrastructure: LAN Automation Procedure

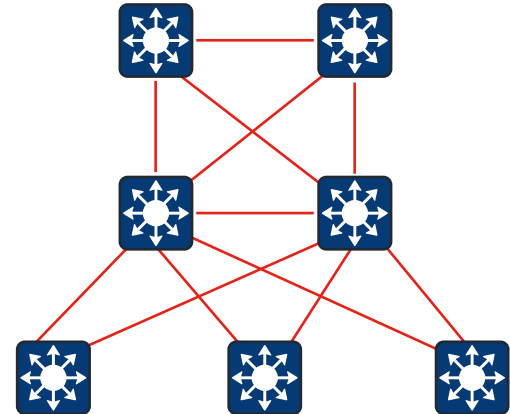
- Primary and Peer Device should be discovered and managed in Cisco DNA Center.
- Network Devices must be running Network Advantage license.
- Redistribute IS-IS routing protocol into other routing protocol, ensuring the LAN Automation ip address pool has reachability to Cisco DNA Center.
- LAN Automation IP Address Pool should be reserved as type 'LAN' with minimum supported prefix is $\leq /26$
- LAN IP Address Pool is split into 3 sub-pool to reserve:
 - Temporary DHCP Pool on the Primary Device.
 - Configure Pt-to-Pt link subnet (/31 prefix)
 - Configure Loopback 0 interface with host (/32) prefix address



Fabric Network Infrastructure

Underlay Infrastructure: Plug-and-Play onboarding

- Cisco DNA Center provides an alternative approach to discover, claim and provision the discovered device.
- Cisco Plug-and-Play is a device-by-device onboarding with flexibility to define custom template configuration.
- Image update can be performed as a part of device onboarding.
- Flexibility to onboard the device on any switch port (management port or front-facing interface port).



Semi-Automated underlay

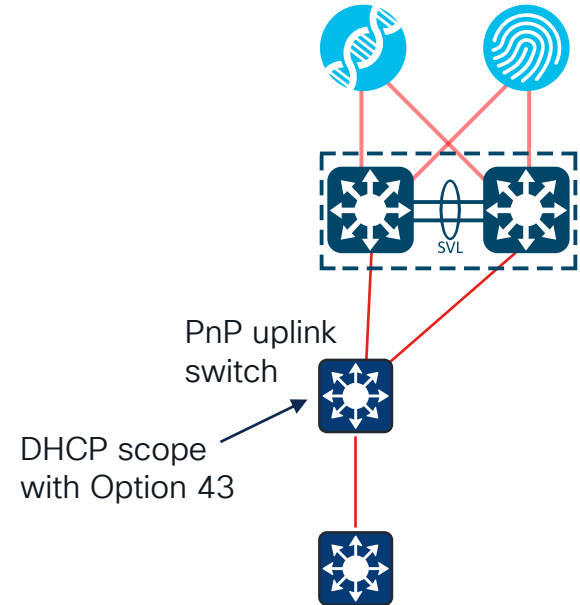
Device-by-Device onboarding and with standard template through Cisco DNA Center Plug-and-Play

Fabric Network Infrastructure

For your
reference

Underlay Infrastructure: Plug-and-Play Procedure

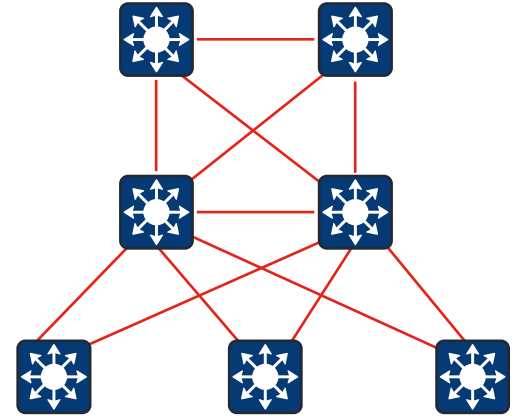
- Define Network Settings
 - Network - Network Hierarchy
 - Network - AAA, NTP, DHCP, DNS settings
 - Device Credentials - CLI, SNMP, HTTP(s) Credentials
- Define Template
 - Template Editor - Day-0 configuration
- Define Network Profiles
 - Associate Day-0 template to the site.
- Provision uplink switch with
 - DHCP Scope with option 43 (pointing to Cisco DNA Center)
 - Change the PnP startup-vlan (default is vlan 1)
- Connect the device, Claim the device in Cisco DNA Center Plug and Play
- Upgrade Image with SWIM and Provision the device to the site.



Fabric Network Infrastructure

Underlay Infrastructure: Manual onboarding

- CLI based device-by-device configuration.
- Flexibility to configure network device with configuration that fits your enterprise requirements.
- Discover and Manage the device in Cisco DNA Center.
- Software Image Management can be performed
- Provision/Assign the device to a site in Cisco DNA Center.

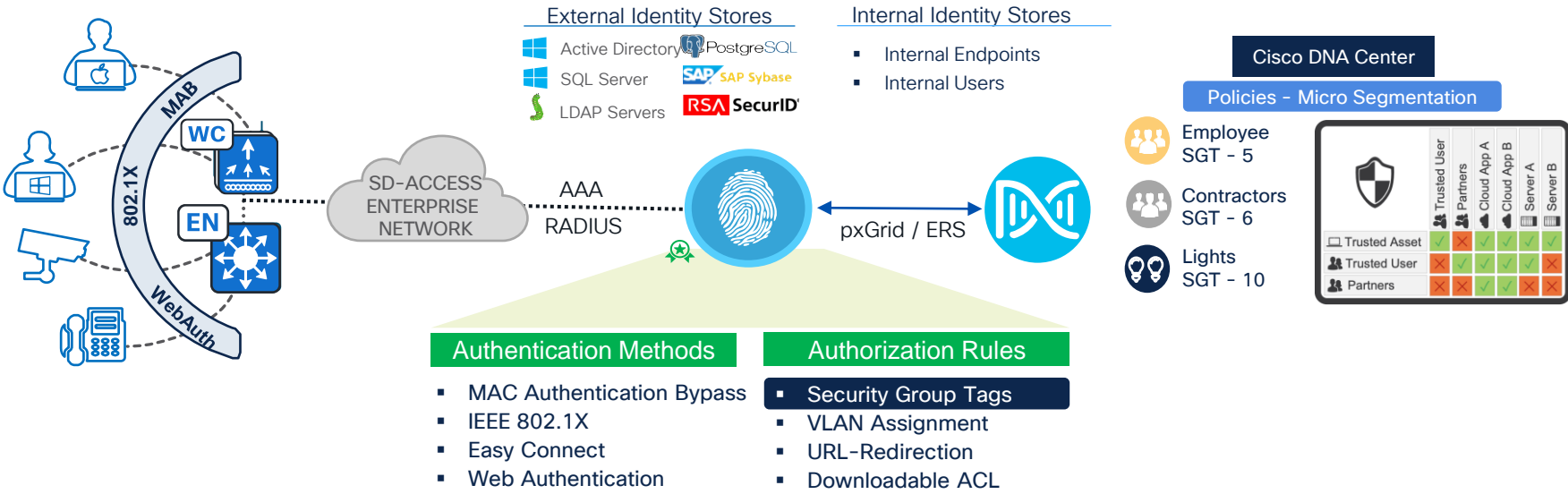


Manual underlay

CLI based manual configuration, followed by discover and manage device in Cisco DNA Center.

Cisco SD-Access

ISE – Securing Onboarding with Micro-Segmentation



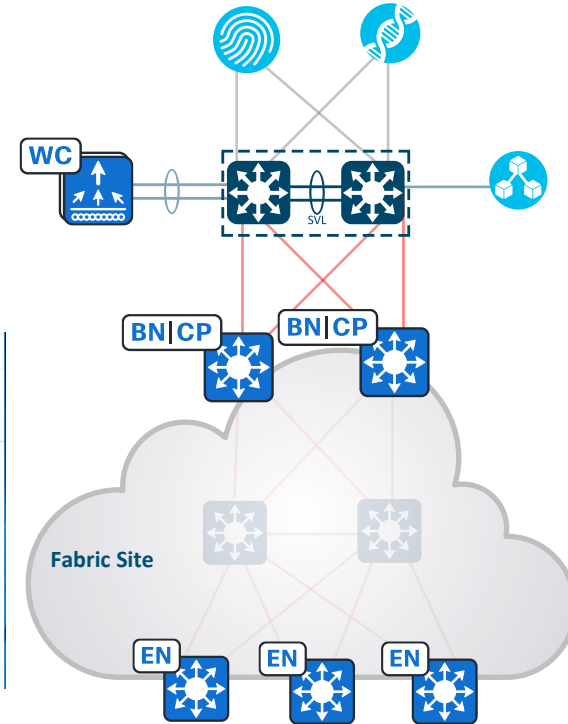
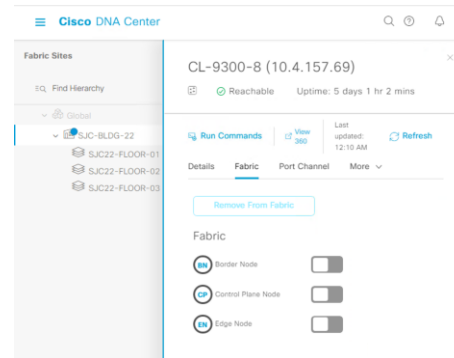
Cisco SD-Access Fabric Infrastructure

Fabric Network Infrastructure

Cisco SD-Access Overlay deployment

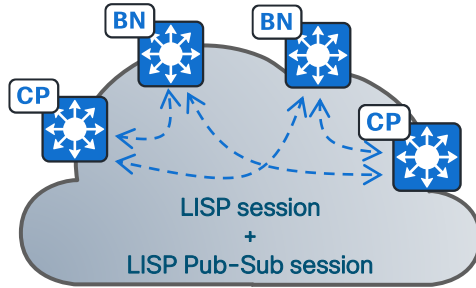
SD-Access application on Cisco DNA Center provides easy-to-deploy workflow-based network Segmentation and overlay Services.

- Provision network devices to the site.
- Create
 - Fabric Site
 - Transits or Peer Networks
- Assign
 - Fabric role to network devices
 - Associate Transit Networks(s) to Border nodes.

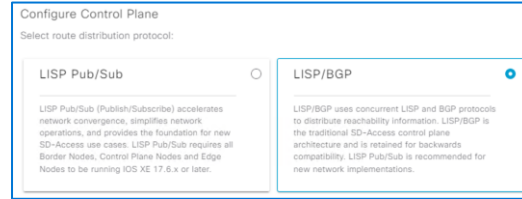


Fabric Network Infrastructure

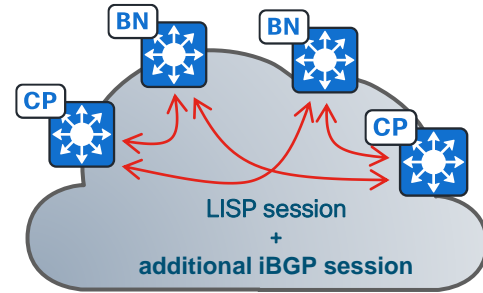
Cisco SD-Access Fabric Control Plane enhancements



LISP Pub/Sub



IOS-XE \geq 17.6.2
DNAC 2.2.3.x



LISP / BGP

- Publisher-Subscriber model provides LISP Instance-ID table subscription from CP, TCP to Border nodes.
- Faster convergence within fabric site (N-S traffic) and across SD-Access transit.
- LISP Pub/Sub provides backbone for fabric innovations such as Dynamic-Default Border, Active-Backup Internet (with SD-Transit) and more..

- Required in non-collocated Border, Control plane and SD-Access Transit deployment.
- iBGP session between B - CP and B - TCP node to share prefixes.
- Convergence overhead with additional protocol, redistribution and additional lookups

Fabric Network Infrastructure

Fabric Site Default Authentication Template

Cisco SD-Access leverage IBNS 2.0 based configuration.

Authentication Template Options:

- Closed Authentication

Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.

- Open Authentication

Network-access without having to go through 802.1X authentication

- Low Impact

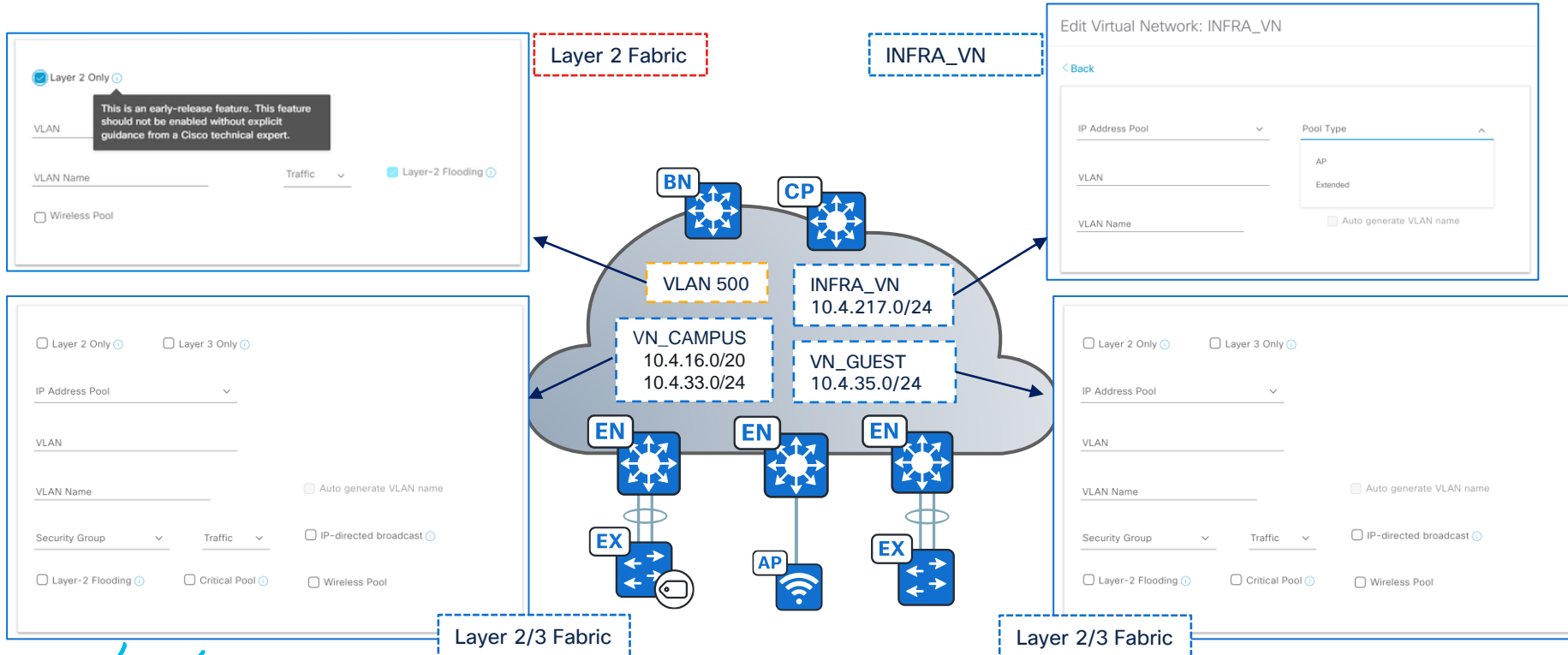
Limited network access prior to authentication with Pre-Authentication ACL. After a host has been successfully authenticated, additional network access is granted.

- None

The screenshot displays the Cisco SD-Access configuration interface for SJC-BLDG-22. The 'Host Onboarding' section is active, and the 'Authentication Template' tab is selected. The 'Closed Authentication' template is chosen, and a modal window is open, showing configuration options for the 'First Authentication Method' (802.1X), '802.1X Timeout' (21 seconds), 'Wake on LAN' (No), and 'Number of Hosts' (Unlimited).

Fabric Network Infrastructure

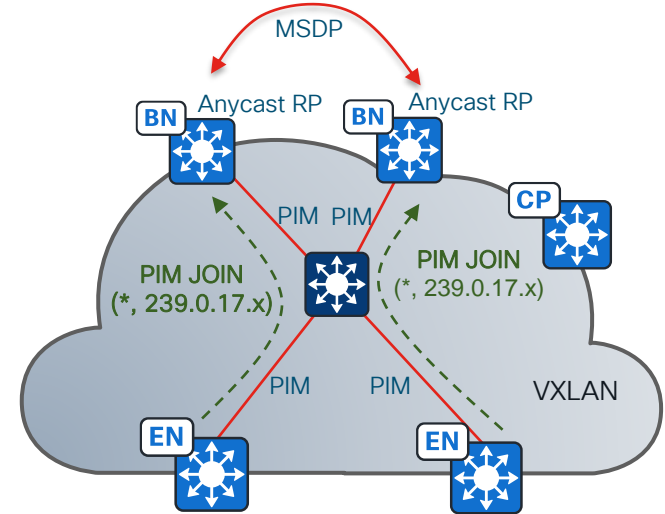
Cisco SD-Access Overlay Subnet deployment



Cisco SD-Access

Layer 2 Flooding

- Broadcast, Unknown-Unicast, link-local Multicast traffic is not forwarded by default in Fabric.
- L2 flooding feature makes this possible by encapsulating the subnet broadcast in the underlay-multicast group (239.0.17.x).
- Every Edge node with the subnet will subscribe to the underlay-multicast group.
- Underlay PIM ASM must be configured to build the underlay-multicast distribution tree.
- Usecases such as Silent Host, Layer2-Handoff, Layer2 Fabric requires the layer2 flooding to be enabled.



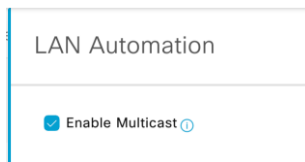
Edge nodes configured with Anycast RP rp-address

```
instance-id 8203
  remote-rloc-probe on-route-change
  service ethernet
  eid-table vlan 2223
  broadcast-underlay 239.0.17.1
  flood unknown-unicast
  database-mapping mac locator-set rloc_xxxx
  exit-service-ethernet
```

Cisco SD-Access

Underlay ASM for Layer2 Flooding

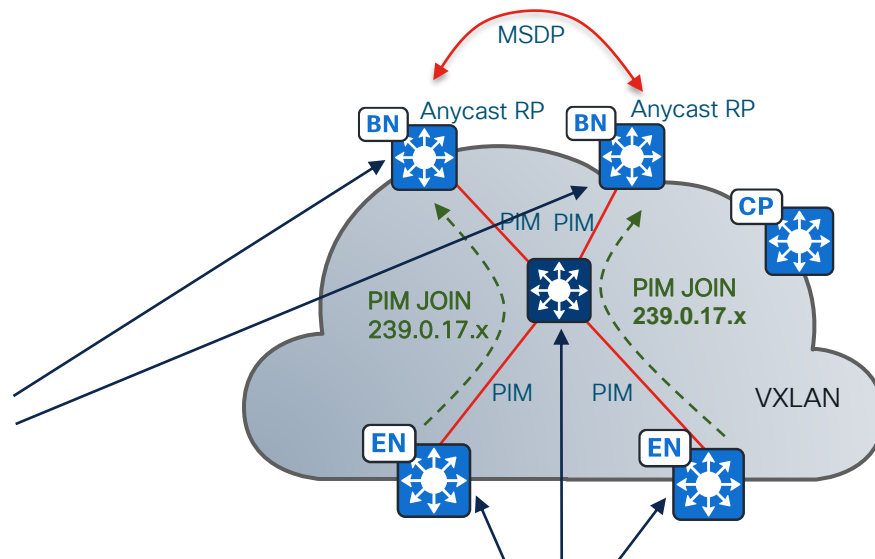
- Enable Underlay ASM with LAN Automation



- Manual ASM configuration:

```
ip multicast-routing
!
interface Loopback60000
 ip address 10.4.157.65 255.255.255.255
 ip pim sparse-mode
 ip router isis
!
interface range Loopback0, <uplink/downlink interface>
 ip pim sparse-mode
!
ip pim rp-address 10.4.157.65
!
ip msdp peer <peer_Loop0_address> connect-source Loopback0
ip msdp originator-id Loopback0
```

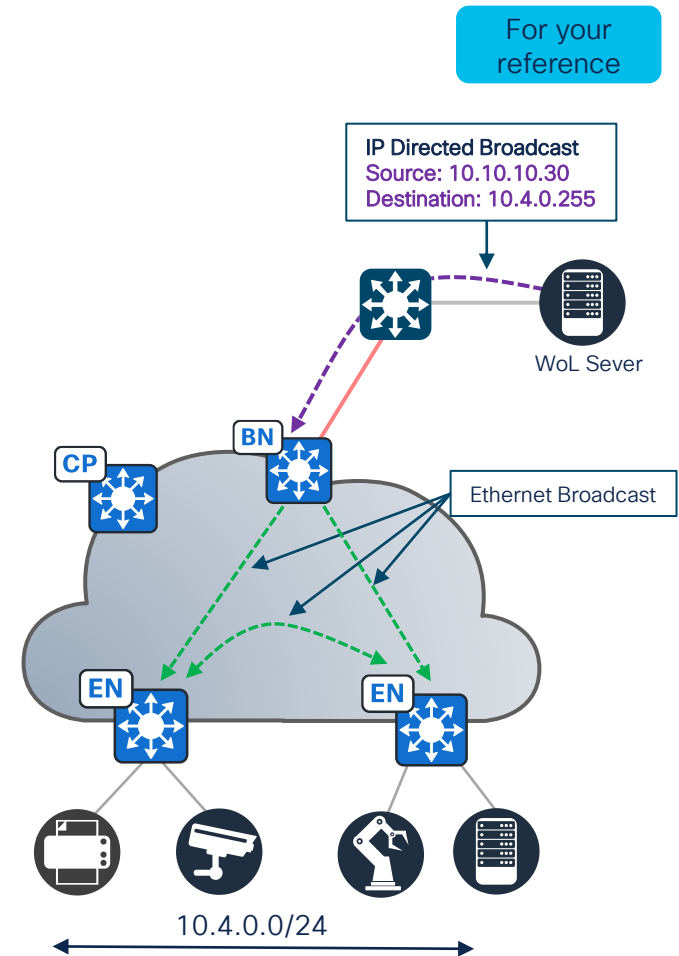
```
ip multicast-routing
!
interface range Loopback0, <uplink/downlink interface>
 ip pim sparse-mode
!
ip pim rp-address <anycast_RP_Address>
ip pim register-source Loopback0
```



Cisco SD-Access

Broadcast use-case – Silent/Sleeping Host

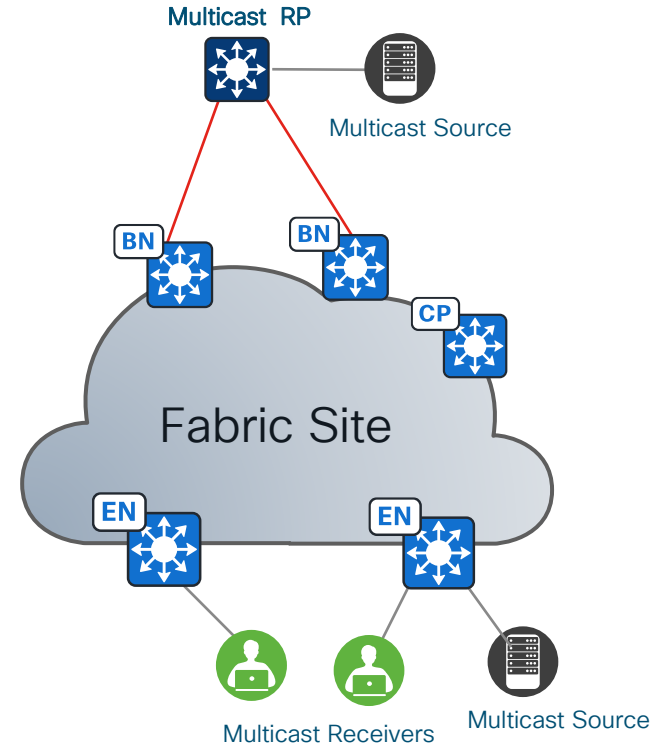
- An endpoint connected in the fabric may move into passive/power-save mode (Silent/Sleeping Host).
- An endpoint whose location in fabric is not known because it has not sent any packets or frames.
- To onboard such clients, broadcast frame must be forwarded across the subnet across the Edge nodes at a fabric site.
- In case the Wake-on-LAN server outside the fabric, Border node can convert an IP-directed broadcast into an Ethernet broadcast and flood to all endpoints in the destination VLAN.



Cisco SD-Access

Multicast in Fabric

- SD-Access supports Multicast packet delivery in VXLAN encapsulation, enabled for each Virtual Network
- Deployment Model: ASM or SSM.
- Modes of Delivery: Headend Replication or Native Multicast.
- Multicast source can be inside or outside the fabric.
- Rendezvous Points can be either:
 - Inside or Outside the fabric
 - Inside and Outside the fabric with MSDP peering
 - Note: Internal RP must be provisioned per Virtual Network.



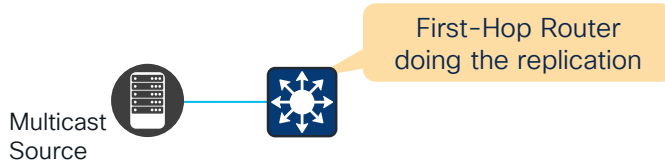
Cisco SD-Access

Multicast in Fabric

Delivery Model: Headend Replication or Native Multicast

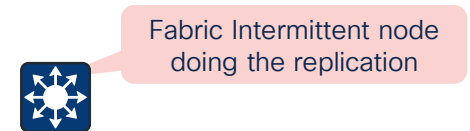
Headend Replication

- Forwarding in Overlay
- Multicast over Unicast in Fabric
- Easier to troubleshoot, replication at the first-hop router
- No network requirements



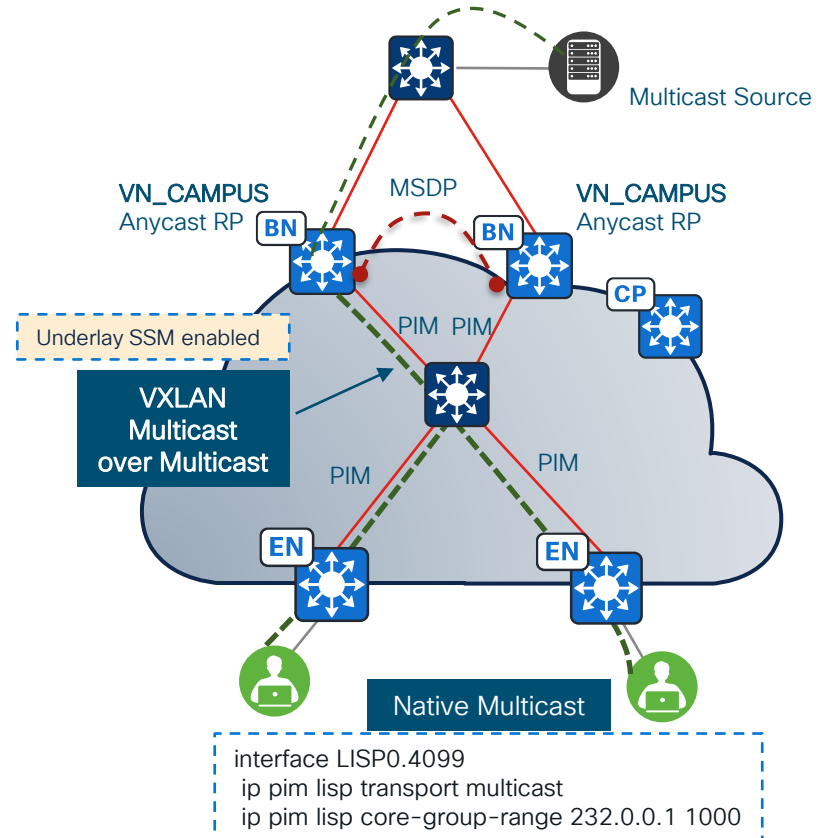
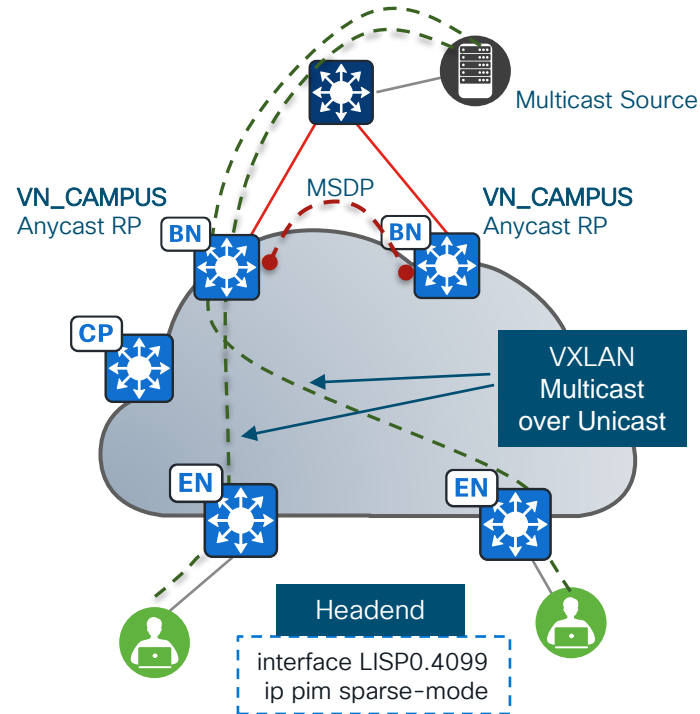
Native Multicast

- Forwarding in Underlay
- Multicast over Multicast in Fabric
- Efficient way to distribute multicast packets, replication at intermediate nodes
- Underlay network must be enabled with SSM multicast



Cisco SD-Access

Headend v/s Native Multicast



Cisco SD-Access Wireless Design

Cisco SD-Access

Fabric Wireless Integration

Centralized Wireless Control Plane

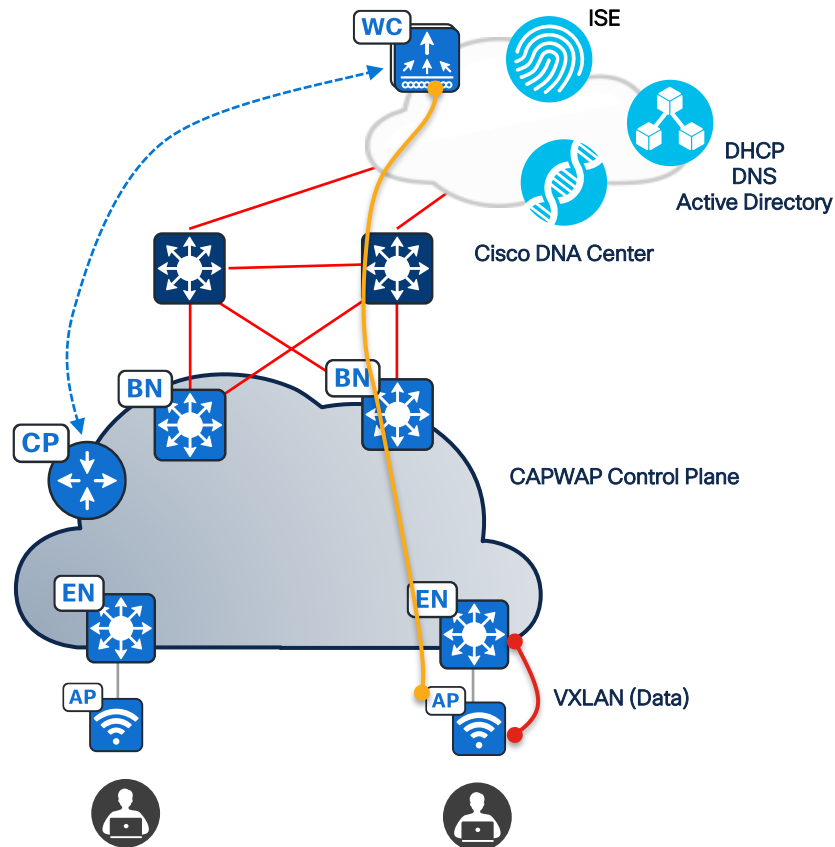
- WLC still provides client session management
- AP Management, Mobility, RRM, etc.
- Same operational advantages of CUWN

LISP control plane Management

- WLC integrates with LISP control plane
- WLC updates the CP for wireless clients
- Mobility is integrated in Fabric with LISP CP

VXLAN from the AP

- Carrying hierarchical policy segmentation starting from the edge of the network

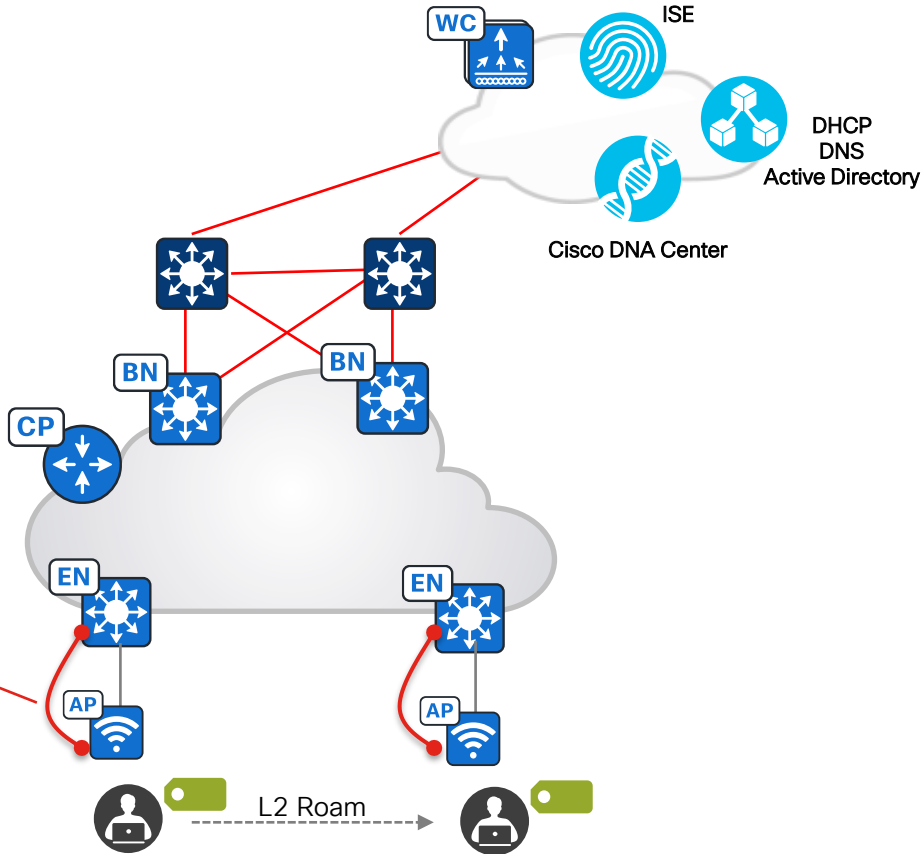
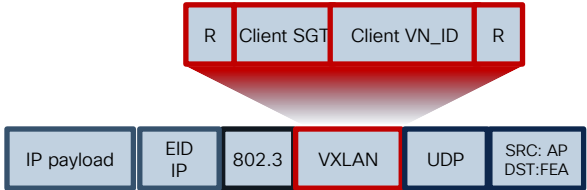


Cisco SD-Access

Fabric Wireless Data Plane

Optimized Distributed Data Plane

- Fabric overlay with Anycast GW + Stretched subnet
- VLAN extension with no complications
- All roaming is Layer 2



Cisco SD-Access Wireless

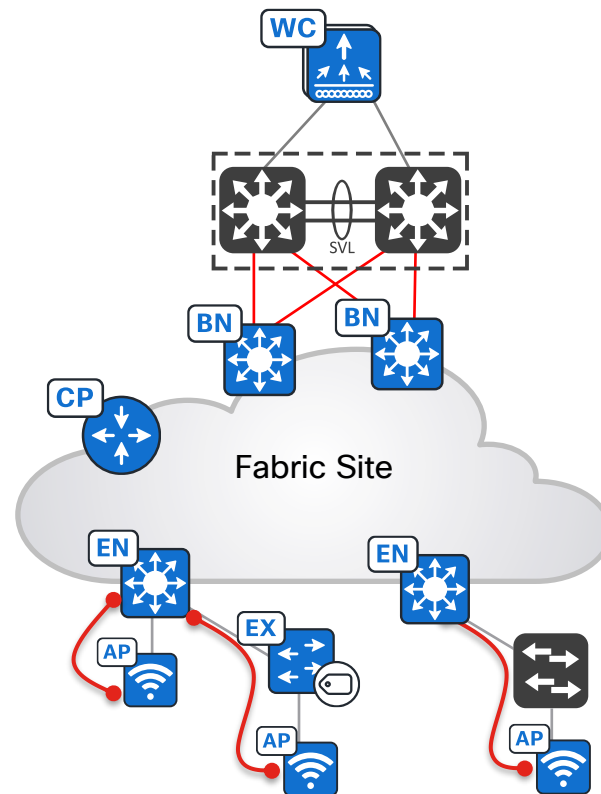
Fabric Wireless Design Considerations

Access Points

- AP can be connected directly to Edge, Extended node or third-party switch connected to Edge node.
- AP is part of fabric overlay, INFRA_VN specifically.
- AP joins the WLC in Local mode and latency must be < 20msec.
- Edge node establishes access-tunnel to Fabric AP to encapsulate data packets in VXLAN.

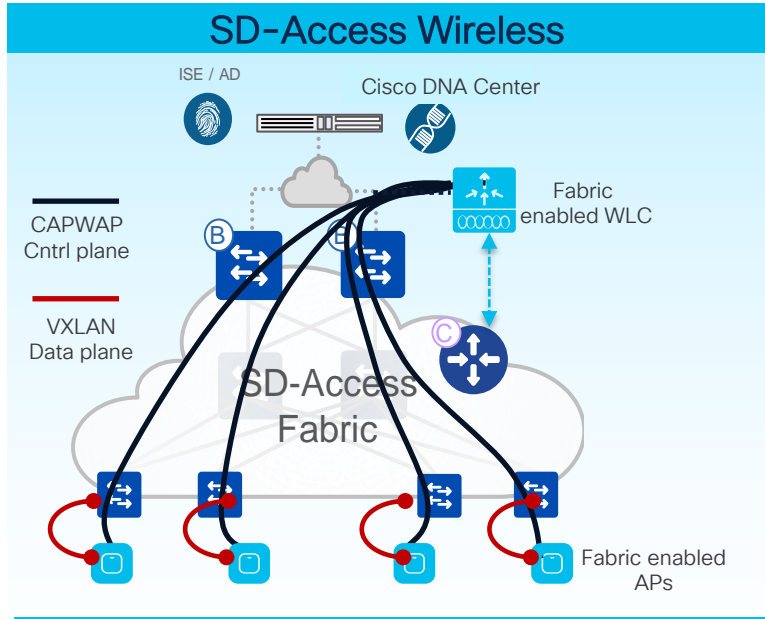
WLC

- Wireless Controller is connected outside Fabric.
- Embedded Wireless Controller can be installed on Catalyst 9000 series switches with supported fabric roles
- Wireless Controller can be part of one Fabric Site.



Cisco SD-Access Wireless

Wireless Deployment options

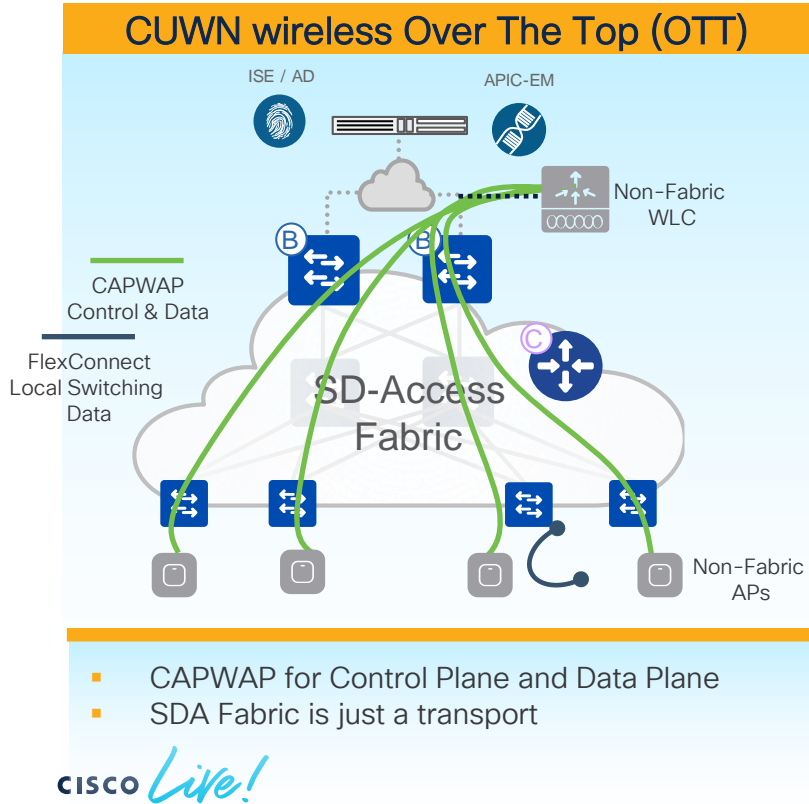


- CAPWAP Control Plane, VXLAN Data plane
- All integrated in Fabric, SD-Access advantages
- Optimized for 802.11ac Wave 2 and 11ax APs

- True wireless integration with Fabric
- Provides all the advantages of SDA for wireless clients:
 - Full automation with Cisco DNA Center
 - Hierarchical segmentation (VRF and SGT)
 - Consistent policy- wired and wireless
 - Distributed Data Plane with no drawbacks
 - Optimized traffic path for Guest
- Recommended option

Cisco SD-Access Wireless

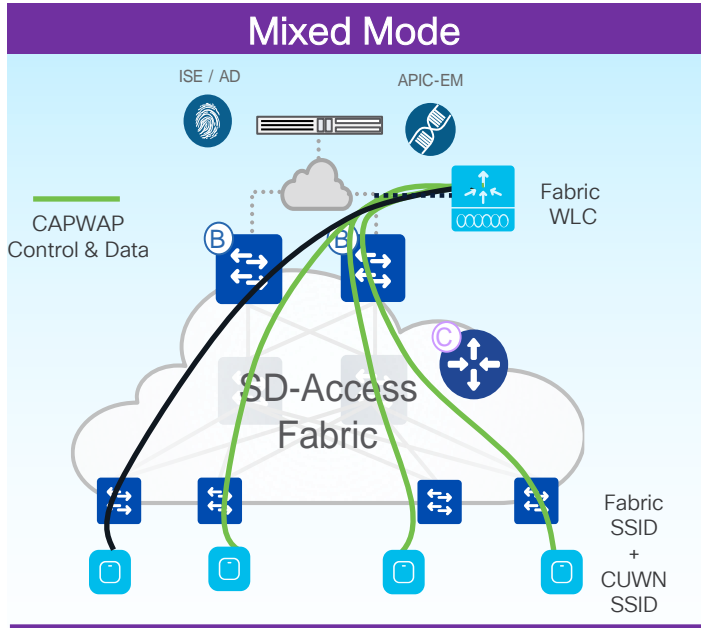
Wireless Deployment options



- No SDA advantages for wireless
- Migration step to Cisco SD-Access
- Customer cannot migrate to Fabric (older APs, need to certify the new software, etc.) or 3rd Party wireless
- Wireless Data plane can be either centralized or Flex Local-Switching.

Cisco SD-Access Wireless

Wireless Deployment options

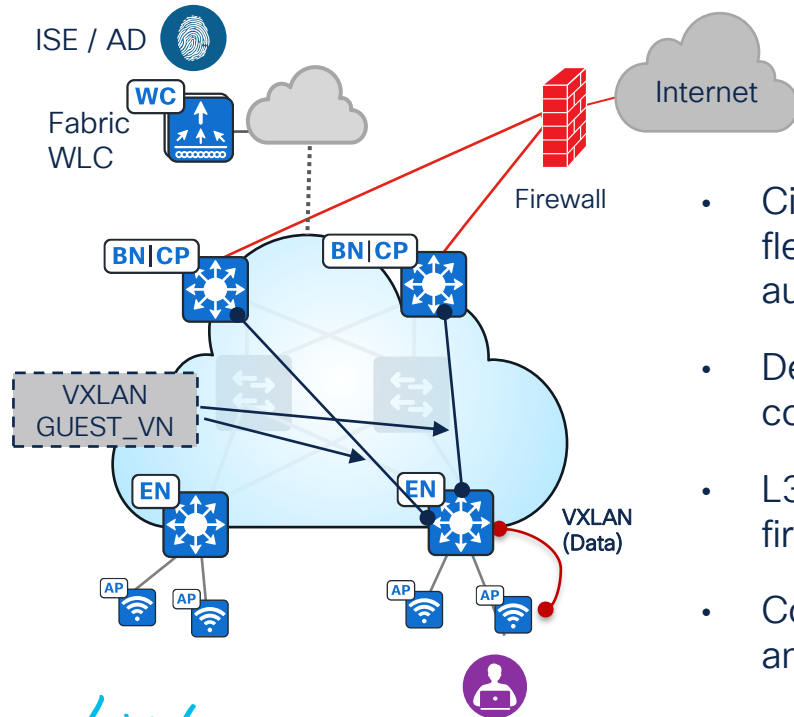


- Mixed mode: mix of Fabric and non-Fabric (centralized) SSIDs
- Mixed mode is supported both on the same AP or different APs
- Automation for Foreign-Anchor Guest SSID is supported in Cisco DNA Center

- non-Fabric SSID: client traffic is CAPWAP encapsulated to WLC
- Fabric SSID: client traffic is VXLAN encapsulated

Cisco SD-Access Wireless

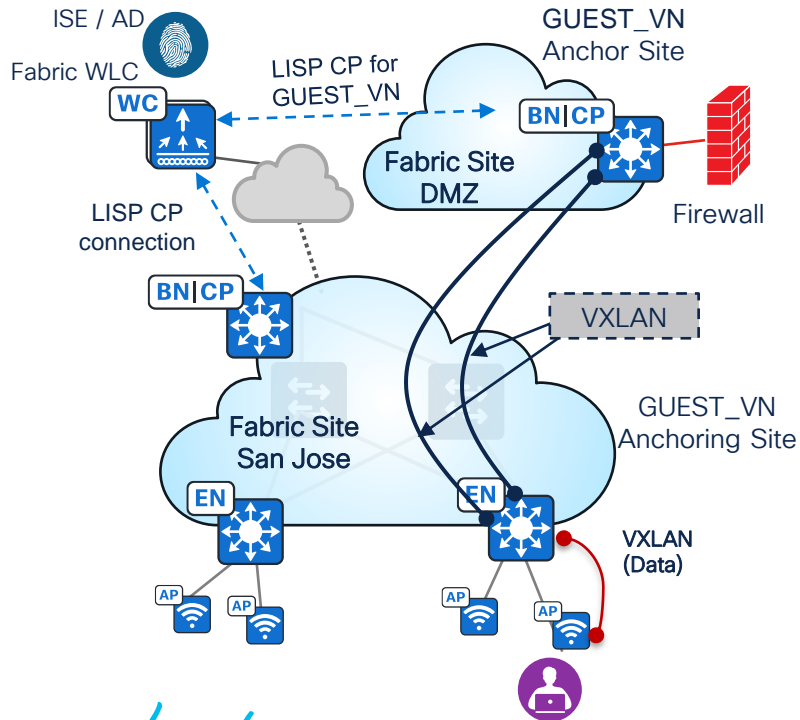
Wireless Guest Design – Dedicated Virtual Network



- Cisco DNA Center Guest-SSID workflow provides flexibility to create custom Guest portal with ISE authorization policies.
- Dedicated Virtual Networks for segmentation provides control plane and data plane isolation
- L3 Handoff with BGP peering between Border and firewall.
- Consistent network and policy deployment for wired and wireless infrastructure

Cisco SD-Access Wireless

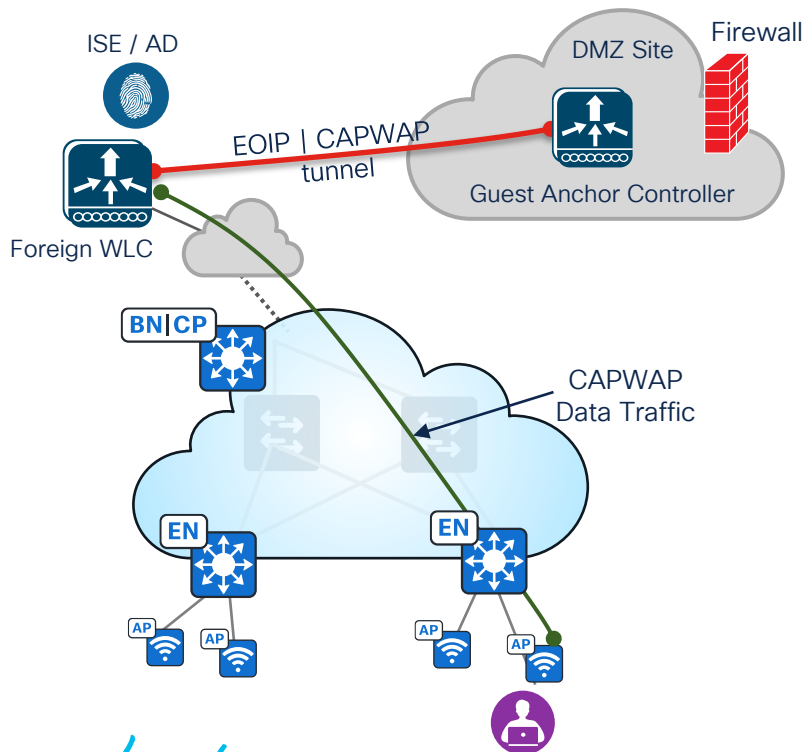
Wireless Guest Design – Dedicated Virtual Network with MSRB



- Multisite Remote Border (MSRB) allows a Virtual Network to be anchored to a different fabric site's Border, Control Plane nodes providing traffic egress point flexibility.
- Edge node (Anchoring site) encapsulates VXLAN with destination as remote-site Border (Anchor site) for the VN.
- VXLAN cannot be fragmented, higher MTU must be supported across the sites
- Catalyst 9800 can support up to 8 Control Plane node pairs.
- AireOS WLCs can support maximum 2x Control Plane node pairs

Cisco SD-Access Wireless

Wireless Guest Design – Guest Anchor Controller



- Wireless is deployed in the Over-the-Top model, where the wireless client traffic is centrally switched to WLC.
- Guest WLAN anchored at Guest Anchor in DMZ
- Well proven CUWN solution, protecting investment
- Restriction of 71 Guest Tunnels
- Separate solution for Wired Guest, Anchor WLC managed differently
- Embedded wireless LAN controller doesn't support Guest Anchor deployment model.

Cisco DNA Center System Scale

For your
reference

Parameters	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No of Devices (Switch/Route/WLC)	1000	2000	5000
No of Access Points	4000	6000	13000
No of Endpoints (Concurrent)	25,000	40,000	100,000
No of Endpoints (Unique/Transient) over 14 days	75,000	120,000	250,000
No of endpoints – wired: wireless ratio	Any	Any	Any
Number of Site Elements	500	1000	4000
No of WLC	500	1000	2000
API rate limit	50 APIs/min	50 APIs/min	50 APIs/min
Ports	48,000	192,000	480,000

SD-Access WLC Scale

For your
reference

Device	Number of access points	Number of clients
Aironet 3504	150	3000
Aironet 5520	1500	20,000
Aironet 8540	6000	40,000
Catalyst 9800-L	250	5000
Catalyst 9800-40	2000	32,000
Catalyst 9800-80	6000	64,000
Catalyst 9800-CL (4 CPU / 8 GB RAM)	1000	10,000
Catalyst 9800-CL (6 CPU / 16 GB RAM)	3000	32,000
Catalyst 9800-CL (10 CPU / 32 GB RAM)	6000	64,000

SD-Access embedded wireless controller scale

Device	9300-L	9300 standalone	9300 stack	9400	9500/H
Access points	50	100	200	200	200
Wireless endpoints	1000	2000	4000	4000	4000

- 9200 and 9200L not supported as embedded wireless controller

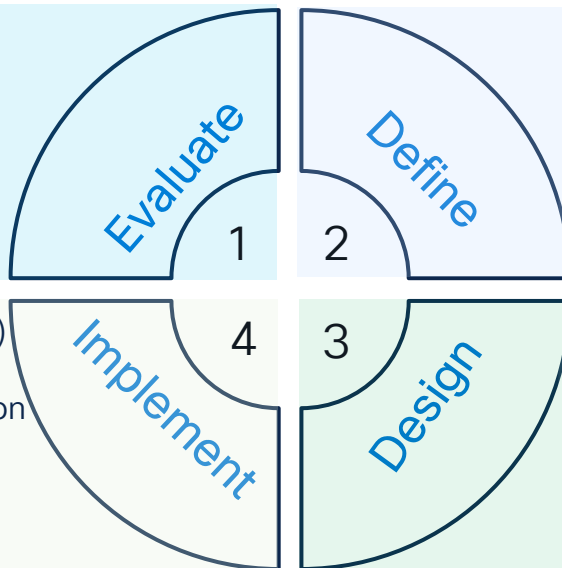
For your
reference

Summary

Cisco SD-Access

Deployment Lifecycle

- Understand current network
- (wired, wireless, IoT, WAN)
- Platform in the network
- Endpoints, traffic types
- Subnets
- Current access-policies



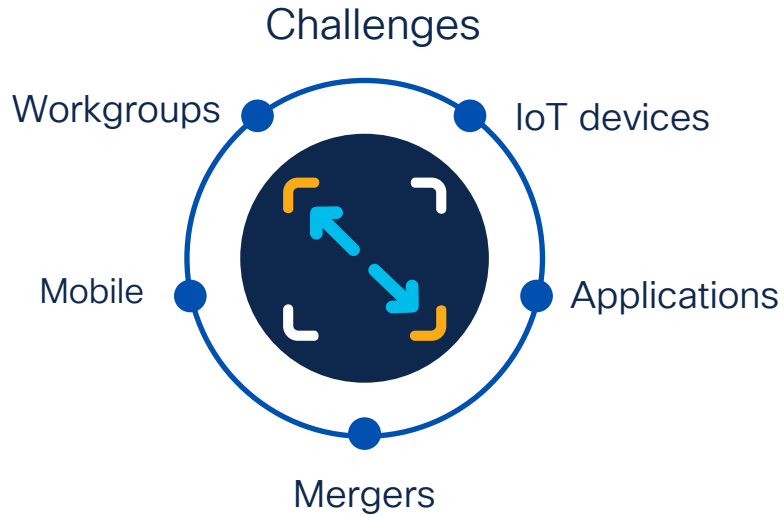
- Segmentation (macro, micro)
- Policy/access-control
- Single or Multi site
- Scale
- Integration with other domains

- Hands on - Lab it !(small-scale PoC)
- Learn the technology.
- Leverage workflow-based automation to built robust network
- Validate your network
- Continue to add usecases
- Integrate with ecosystems

- Start small and build to scale
- Research and pick right platform
- Segmentation strategy
- Strategize for robust/resilient network
- Migration strategy
- Leverage Design Tool to help here..

<https://fwm.cisco.com/>

Network Provisioning Time Savings

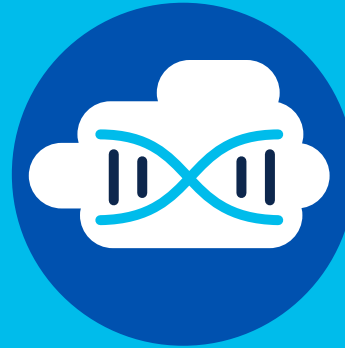


95%

network changes performed manually

Cisco SD-Access

- Deploy & secure services faster!
- Policy-based automation



Software-defined segmentation

Automated policy management

Single network fabric



Routers



Switches



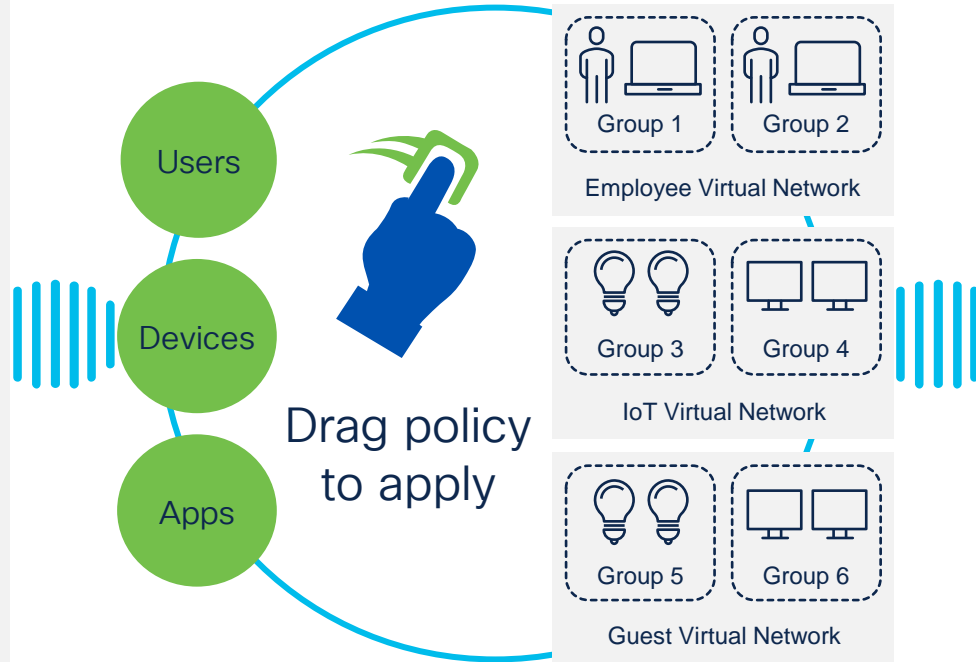
Wireless

Secure onboarding of users and devices

Segmentation and Access Control

Before SD-Access

- VLAN and IP address based
- Create IP based ACLs for access policy
- Deal with policy violations and errors manually



After SD-Access

- No VLAN or subnet dependency for segmentation and access control
- Define one consistent policy
- Policy follows Identity

Completely Automated

Group-Based Policy

Policy follows Identity

SD-Access Resources

Would you like to know more?



cisco.com/go/dna

cisco.com/go/sdaccess

- [SD-Access At-A-Glance](#)
- [SD-Access Ordering Guide](#)
- [SD-Access Solution Data Sheet](#)
- [SD-Access Solution White Paper](#)



cs.co/en-cvds

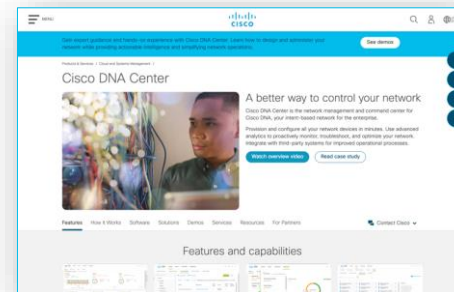
Validated Architectures, Prescriptive Guidance, Confidence to Deploy

- 6 Validated Design Guides
- 12 Prescriptive Deployment Guides



cisco.com/go/dnacenter

- [Cisco DNA Center At-A-Glance](#)
- [Cisco DNA ROI Calculator](#)
- [Cisco DNA Center Data Sheet](#)
- [Cisco DNA Center 'How To' Video Resources](#)



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

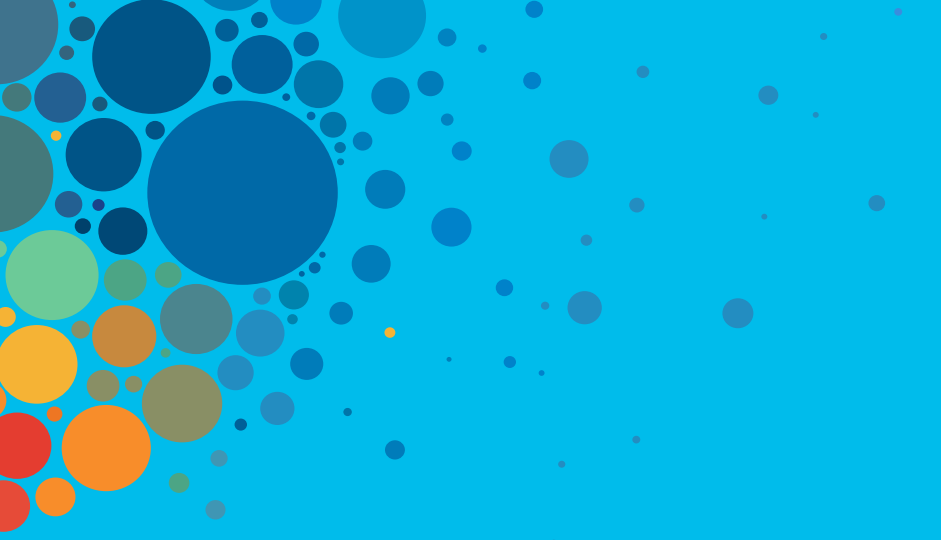
Cisco Guided Study Groups

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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

ALL IN

#CiscoLive