

Goodbye CLI, hello cloud:

The future of campus networking with IOS-XE and dashboard

Leigh Jewell
Solution Engineer
Cisco Networking

cisco Live !



Photo attribution Andrés Dallamonti <https://unsplash.com/license>

Do we trust car auto-pilots as much as planes?

Cisco Webex App

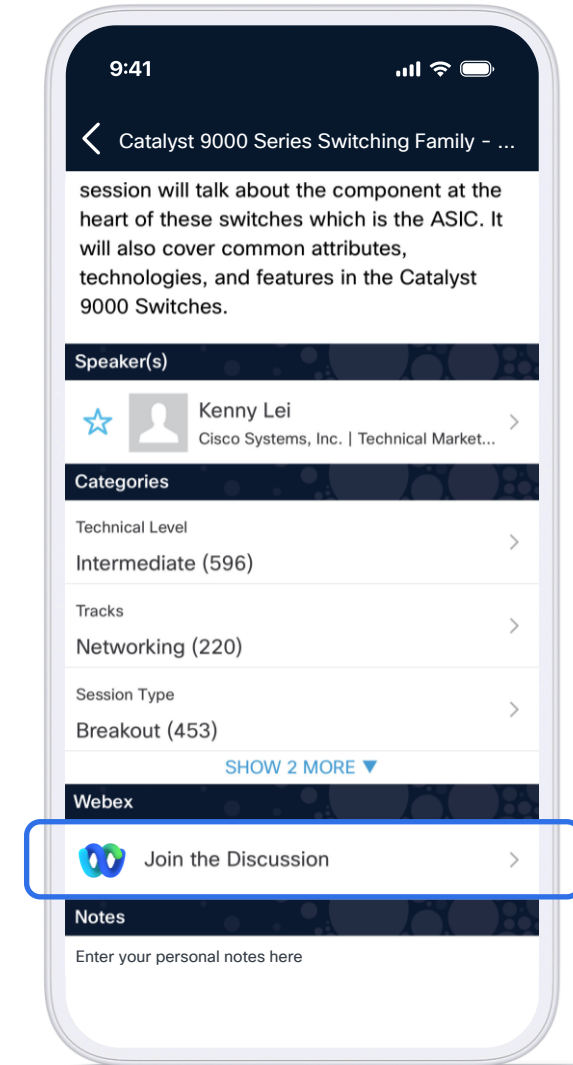
Questions?

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 14 November 2025.



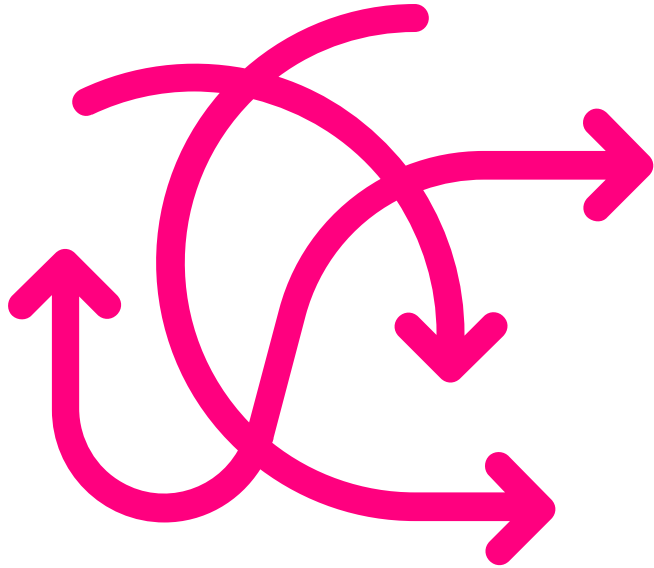
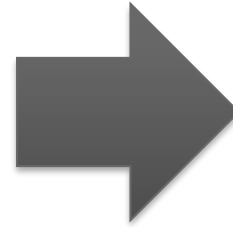
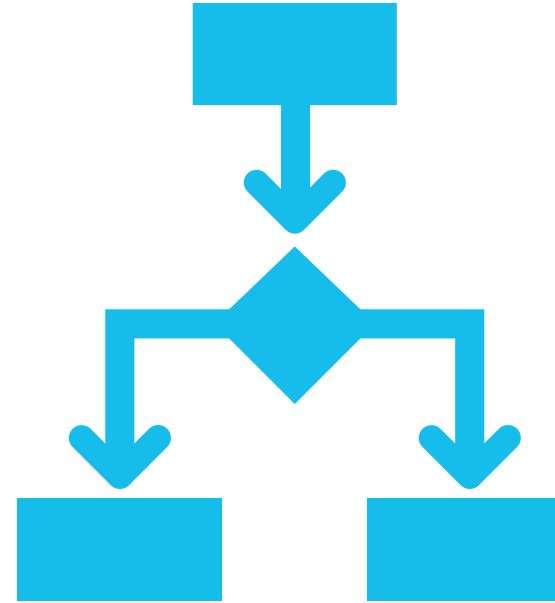
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2601>

Agenda

- 01 Why cloud?
- 02 IOS-XE in the cloud
- 03 High availability improvements
- 04 Advanced routing
- 05 Security enhancements
- 06 Cloud fabric
- 07 Campus wireless

Session outcome

“Know what is now possible with Cloud for Campus”



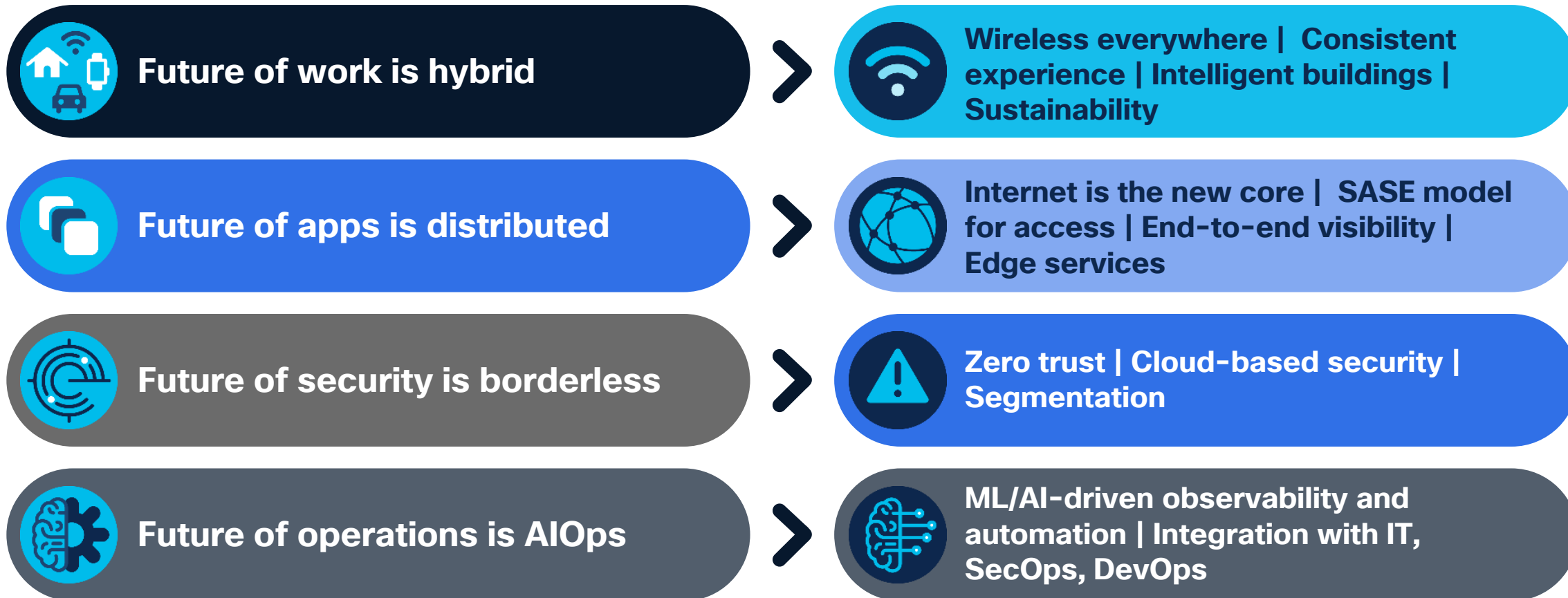
Cloud for Campus ?

Cloud for Campus !

Turn a question mark into an exclamation point.

Why a campus cloud?

Trends that have implications for your network

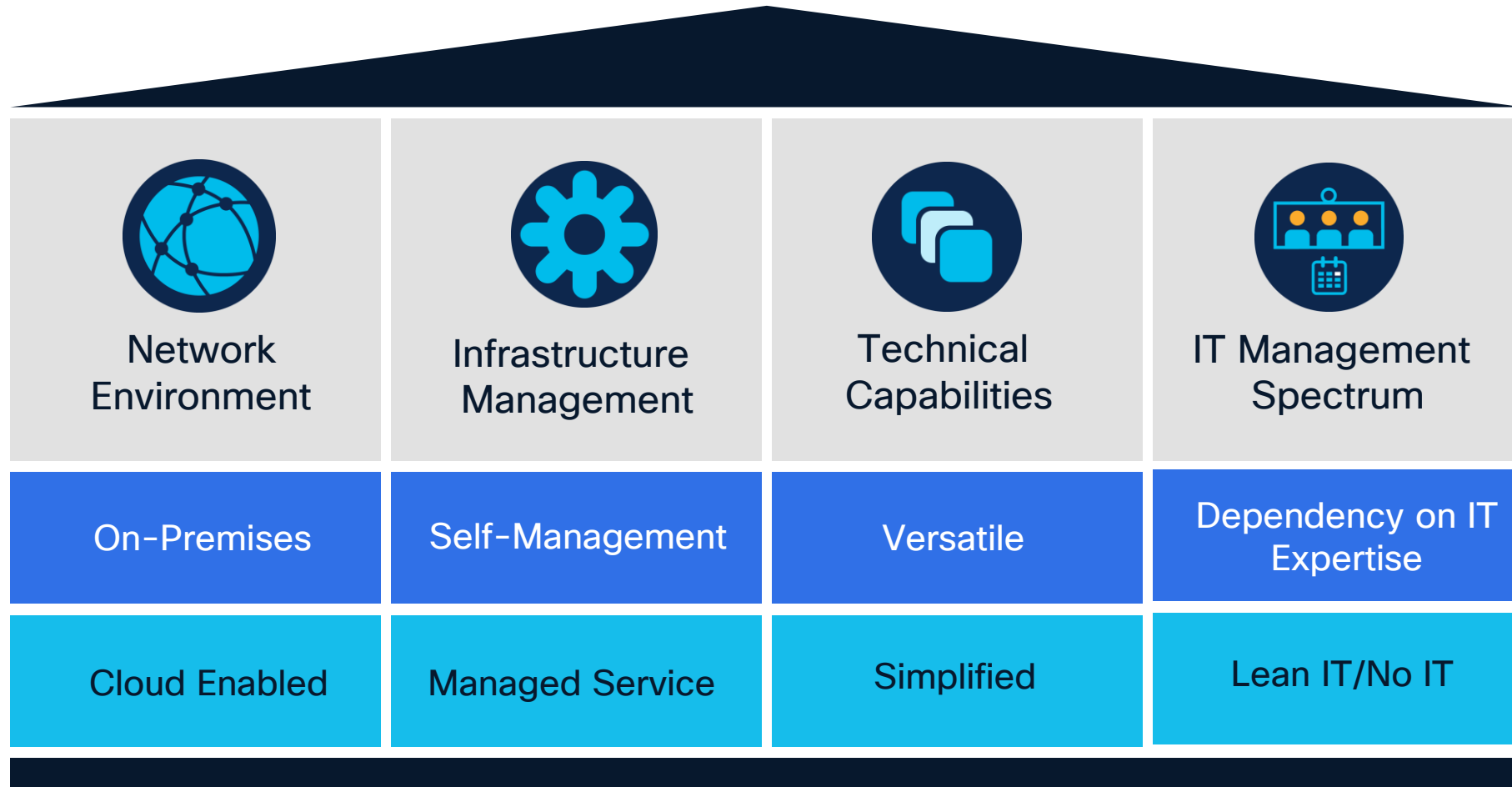


Easy to buy | Easy to deploy | Easy to use

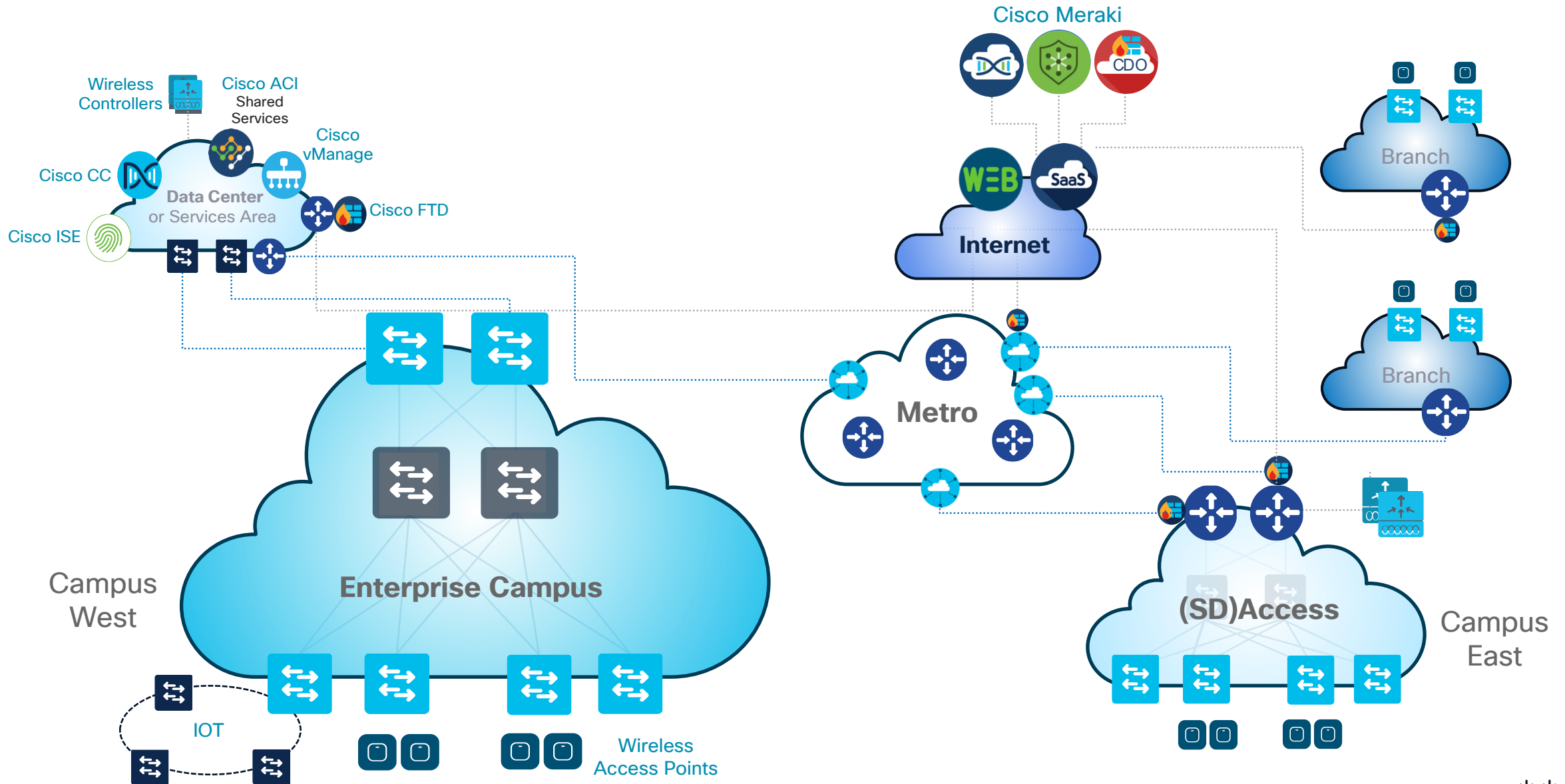


Key factors

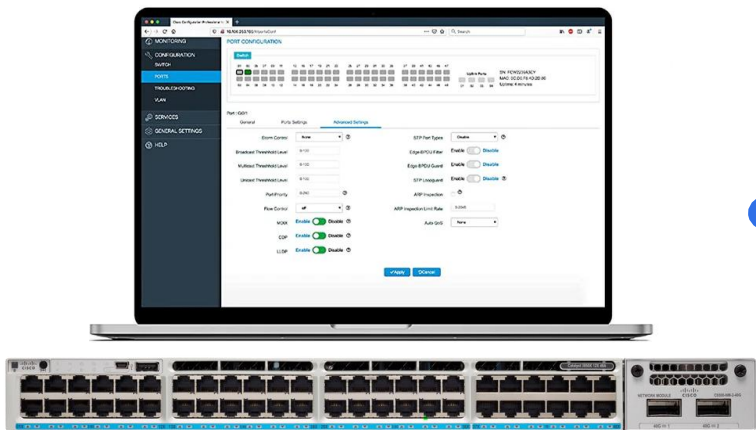
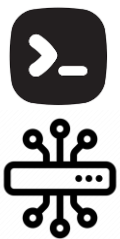
Influencing your **network management platform** selection



Evolving complexity and growth in the enterprise networks

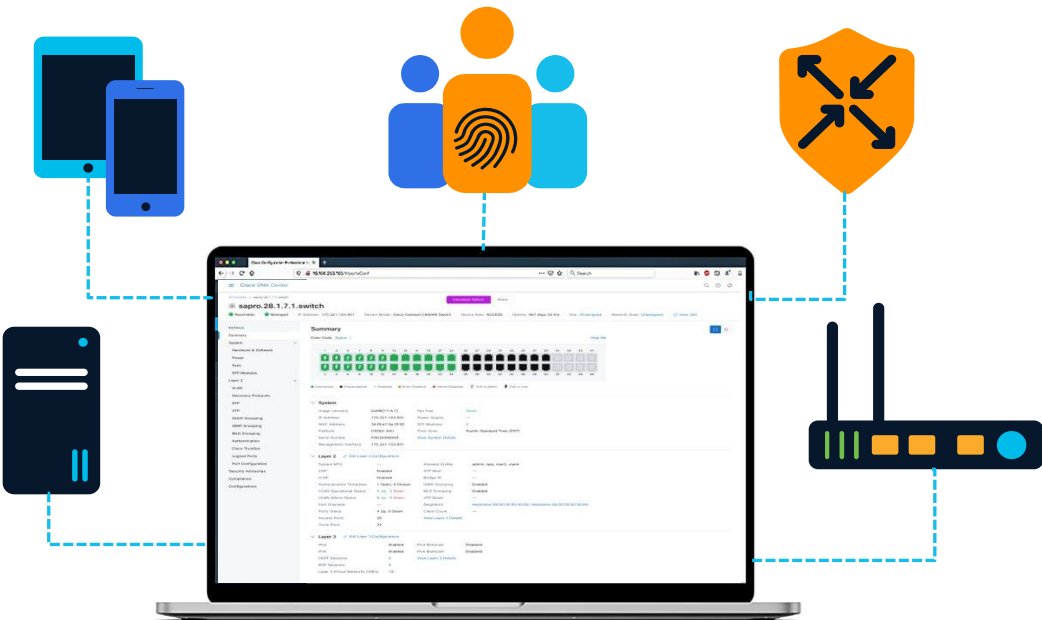


The shift to unified network management platforms



Traditional way of management

- Cisco IOS XE software Command-Line Interface
- Graphical User Interface (GUI) for Switches
- Simple Network Management Protocol (SNMP)



Network management tool

- Unified device management from a single dashboard
- Real-time performance analytics and reporting
- Automated configuration backups and firmware updates
- Advanced security features for threat detection and mitigation

Why haven't we used cloud for campus before?

Programmability mountain



***Software Defined Networking (SDN) has been around for over 15 years.
So why aren't we all doing it?***

Programmability: the path to cloud

nsd5-sw2

C9300-48U cc:5a:53:d8:e7:80

Port 1

Return to port list

Historical data

for the last day

Port traffic

1 b/s

0.75 b/s

0.5 b/s

0.25 b/s

0 b/s

18:00

Port schedule

Unscheduled

Tags

+

Type

Trunk

Access

Native VLAN

20

Allowed VLANs

1-1000

RSTP

Enabled

Disabled

STP guard

Disabled

Port isolation

Enabled

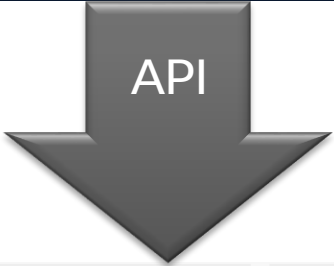
Disabled

Yang

```
# NETCONF <config> payload (XML) for VLAN 20 access mode on Gi1/0/1
VLAN_CONFIG = """
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
    <interface>
      <GigabitEthernet>
        <name>1/0/1</name>
        <switchport>
          <mode>
            <access/>
          </mode>
          <access>
            <vlan>20</vlan>
          </access>
        </switchport>
      </GigabitEthernet>
    </interface>
  </native>
</config>
"""

# Connect to the device and push the config
with manager.connect(**DEVICE) as m:
    netconf_reply = m.edit_config(target="running", config=VLAN_CONFIG)
    print("NETCONF Response:")
    print(netconf_reply)

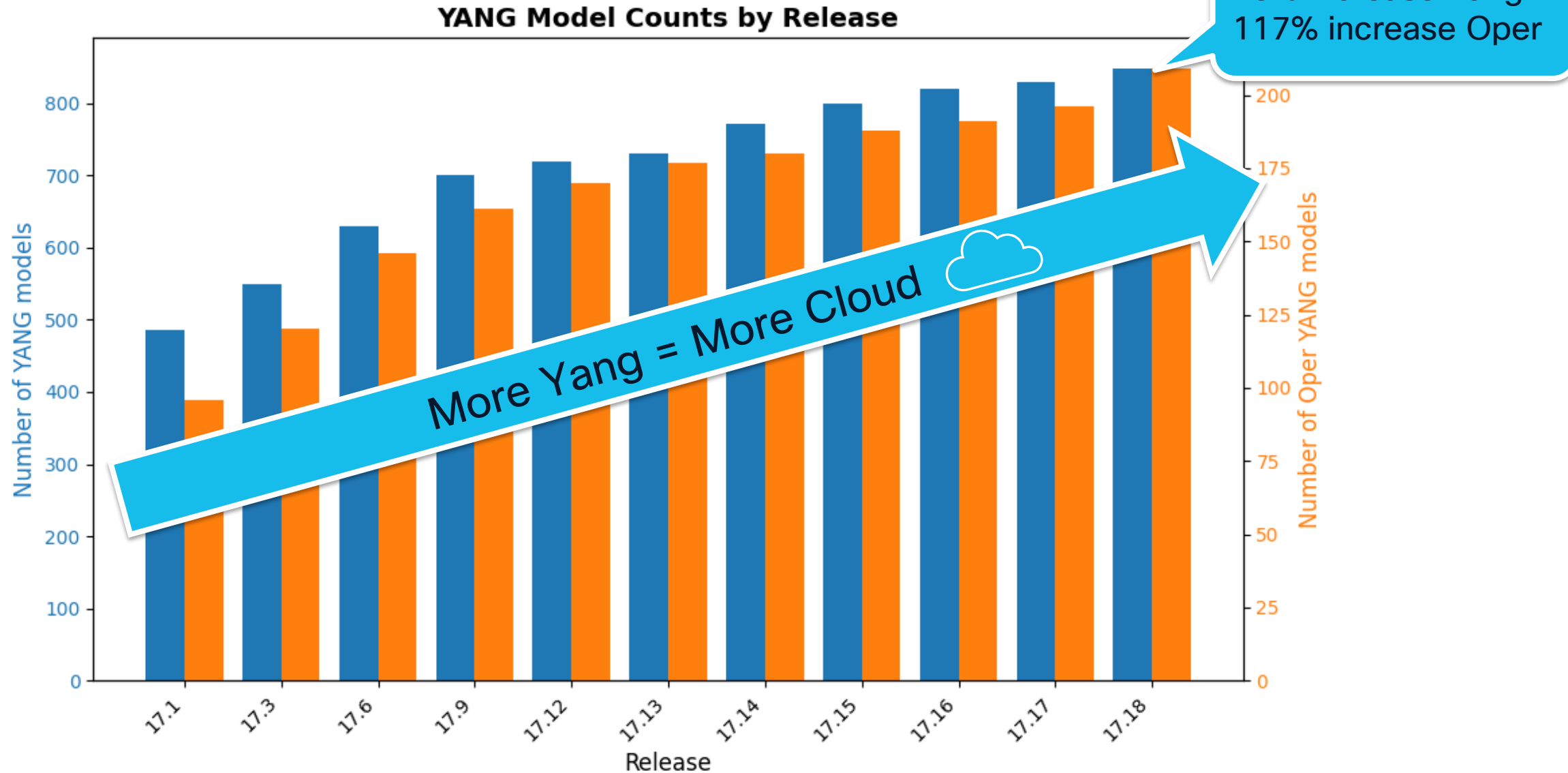
print("✅ VLAN 20 configured on Gi1/0/1 successfully!")
```



I want to
configure
VLAN20 on
Gig1/0/1

</>

Programmability: the Yang evolution



IOS-XE version 17.15 YANG summary

Many additional YANG models added 17.15+ to enable cloud & on-prem controller use cases. For example:

including features and use cases related to:

- RESET button management
- Uplink Autoconfig
- Config Updater
- RPC for port bounce
- Model to invoke (via RPC) Blinking of LEDs
- LED Management
- SYSLOG
- LSP (Local Status Page)
- Layer-2 oper models
- MTR
- Ping
- Tracert
- Wake on LAN (WOL)
- Dashboard Throughput test
- New HTTP endpoint for CSRF token from NGINX
- TDL read-only for shard access
- Support IPv6 when configuring 'flow file-export'
- nginx web server listen in VRF_GLOBAL
- Limit the number of required TDL websocket exec contexts to one
- Show romvar switch all | sec MODEL_NUM
- Cisco-IOS-XE-poe-oper
- Cisco-IOS-XE-cdp-oper
- Cisco-IOS-XE-lldp-oper
- Show running-config | inc tlv-list
- Show etherchannel summary | inc LACP
- Copy running-config startup-config
- Install {add|remove|activate}
- Cisco-IOS-XE-environment-oper
- Add EEE capability and operational status
- File-based telemetry
- Cisco-IOS-XE-flow
- Cloud Connectivity Health & Management



IOS-XE in the cloud

Building on simplified cloud management with IOS-XE



One unified OS for cloud and on-prem



Options for migration or Day 0 cloud management



Cloud simplicity with advanced IOS XE features

Industry Leading Enterprise Switching Portfolio

✓ C9200CX

✓ C9500H¹

✓ C9350 Smart Switches

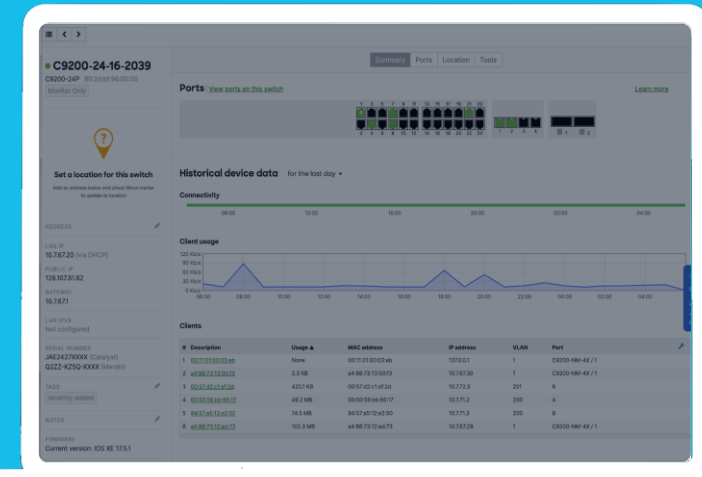
✓ C9200/L

✓ C9300/L/X/LM

✓ C9610 Smart Switches²



Unified Cloud Platform



Cisco Meraki Dashboard

¹Current support for C9500-48Y4C, C9500-24Y4C, C9500-32C and C9500-32QC (not currently C9500X)

²Support for C9610 is expected in a future release

Maintain operational flexibility with cloud management

Configuration Source: Cloud



UNLOCK FULL CLOUD SIMPLICITY

Configurations are performed in the cloud and managed using the dashboard UI

Configuration Source: Device



RETAIN ADVANCED CONTROL

Configurations are managed via traditional methods and performed local to the device

FLEXIBLE OPTIONS FOR MANAGING YOUR DEVICES FROM THE CLOUD

Configuration source: cloud

The full cloud experience with management and configurations performed in the cloud

- Support for automated 'show' CLI commands for advanced troubleshooting
- Leverage the intuitive user interface to build configurations that are performed directly from the Meraki cloud at scale.

The screenshot shows the 'Add devices to network' configuration page in the Meraki dashboard. At the top, a progress bar indicates three steps: 1. Select network (completed with a checkmark), 2. Configure IOS-XE devices (current step, highlighted in blue), and 3. Summary. Below the progress bar, the section 'Device management and configuration source' is visible. Under the sub-header 'C9200/C9300 devices', there are two radio button options. The first option, 'Cloud configuration', is selected and highlighted with a blue border; its description is 'Configuration is sourced from the Meraki Dashboard.' The second option, 'Device configuration', is unselected and has a 'Beta' label next to it; its description is 'Configuration remains local to the device.' At the bottom left is a 'Cancel' link, and at the bottom right are 'Back' and 'Next' buttons.

9200/9200L/9200CX/9300/9500H as of 17.18.1

Configuration source: **device**

Cloud scale visibility with localized configurations and the full IOS XE feature set

- Non-destructive onboarding preserves configurations, which are managed and performed local to the device via traditional methods.
- CLI read/write feature-set supported in dashboard
- Optional configuration back up in the cloud.

The screenshot shows a web interface titled "Add devices to network". At the top, there is a progress bar with three steps: 1. Select network (marked with a checkmark), 2. Configure IOS-XE devices (highlighted in blue), and 3. Summary. Below the progress bar, the section "Device management and configuration source" is visible. Under the heading "C9200/C9300 devices", there are two radio button options: "Cloud configuration" (with the subtext "Configuration is sourced from the Meraki Dashboard.") and "Device configuration" (with a "Beta" label and the subtext "Configuration remains local to the device."). The "Device configuration" option is selected and highlighted with a blue border. At the bottom of the form, there are "Cancel", "Back", and "Next" buttons.

9200/9200L/9200CX/9300/9500H as of 17.18.1

Combined with advanced features powered by IOS-XE

What's New

IOS XE 17.18.1 (beta) brings advanced capabilities to the cloud through the introduction of advanced routing and high availability features. Additional cloud expansion features deliver value to enterprise customers through the introduction of simplified support for troubleshooting, monitoring, and configuration management tasks.

Cloud CLI

Access an embedded cloud terminal within the Meraki dashboard.

Expanded Support

Support for new hardware models and expanded support for cloud features.

Advanced Routing

Advanced capabilities like BGP and VRF are now supported in the cloud dashboard

High Availability

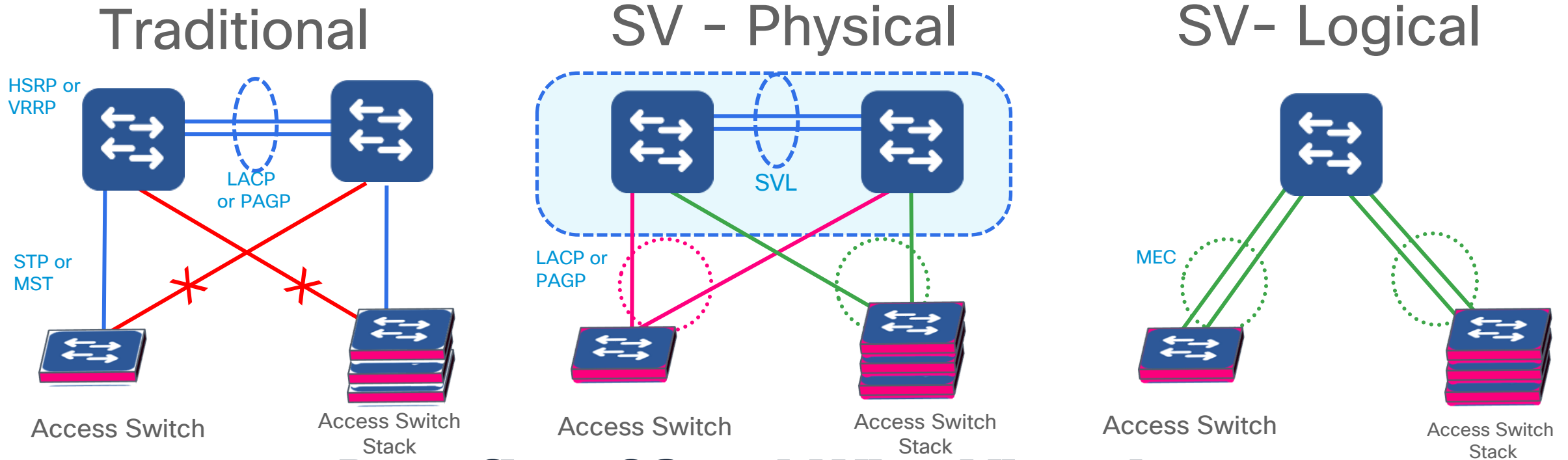
In-Service Software Upgrades, Virtual Stacking for C9500, and more.

GA: IOS XE 17.15.4

Beta: IOS XE 17.18.1

High availability

StackWise Virtual topology comparisons



Benefits of StackWise Virtual

Simplify Operations by Eliminating STP, FHRP and Multiple Touch-Points

Double Bandwidth & Reduce Latency with Active-Active Multi-chassis EtherChannel (MEC)

Minimizes Convergence with Sub-second Stateful and Graceful Recovery (SSO/NSF)

Introducing support for StackWise Virtual from the cloud

Simplify configuration management by presenting two physical switches as one logical entity

Lower the risk associated with a looped topology while reducing operational failure points

Maintain HA with support stateful switch failover (SSO) by ensuring minimal downtime during failures or maintenance

Create Stack

Stack name

Hourglass Twins

Q Search

Name

- ☒ Ash Twin
- ☒ Ember Twin

Configure your StackWise Virtual pair

To successfully provision Catalyst 9500 switches as a StackWise Virtual pair, select switch ports below to set up SVL and DAD links.

⚠ Please ensure you have physically connected the ports selected below before proceeding

Stack name Hourglass Twins

Members **Ash Twin**, **Ember Twin**

SVL links

Select between 2 and 8 ports on each switch to establish the SVL link. Note that any existing switch port config will be overwritten for ports selected here.

Ash Twin

Ember Twin

1 × 2 ×

1 × 2 ×

DAD link

Select 1 port to establish the DAD link. Note that any existing switch port config will be overwritten for the port selected here.

Ash Twin

Ember Twin

3

3

☒ I acknowledge that by clicking 'Configure' I have physically connected the ports selected for SVL and DAD links.

Cancel **Configure**

Introducing In-Service Software Upgrades from the cloud

ISSU allows users to upgrade switch stacks while the network continues to forward packets

Minimize network disruptions and downtimes with simplified scheduling

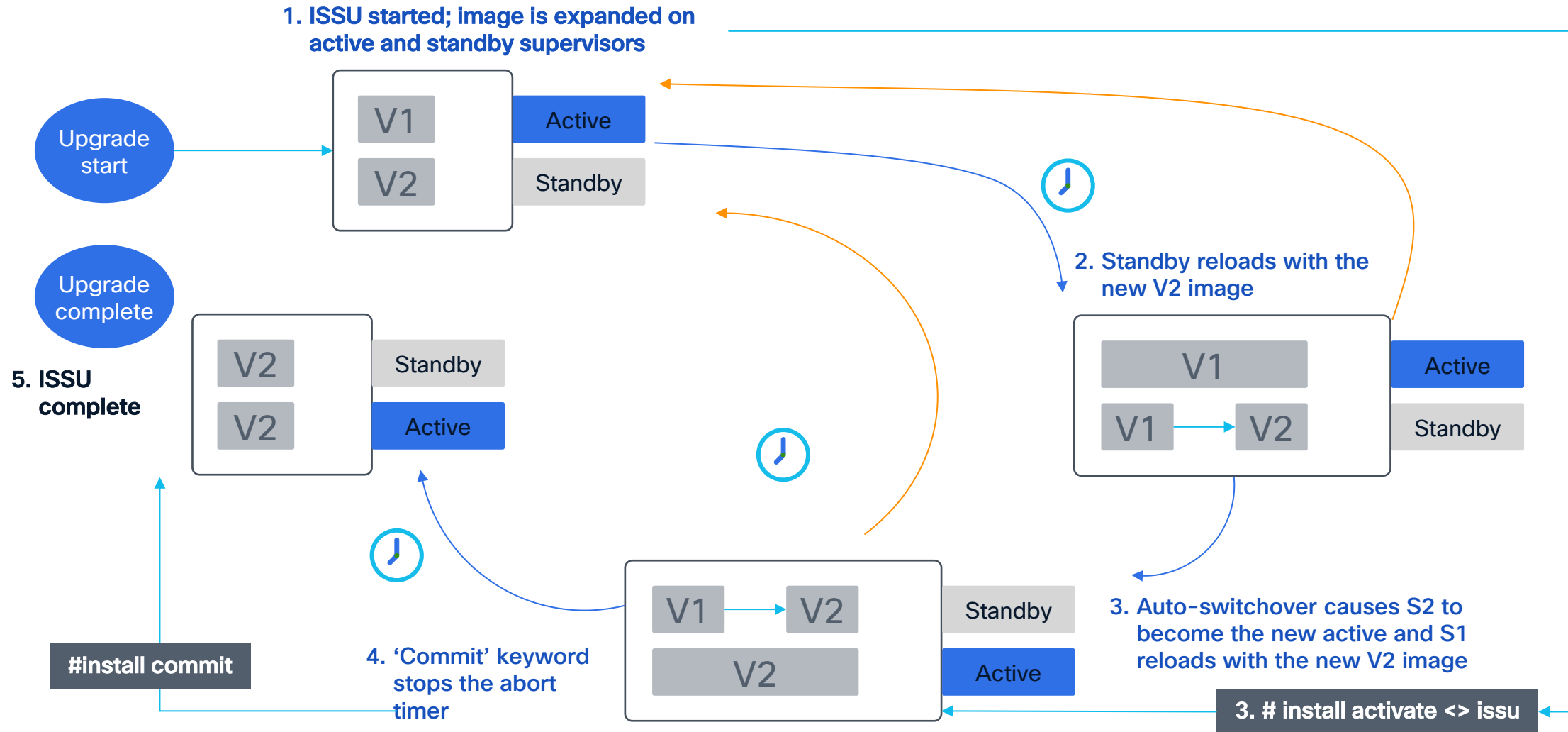
Deploy new services and features faster with remote execution

Only for C9500H currently

The screenshot shows the Meraki management console interface. On the left is a sidebar menu with options: Global Overview, Organization (Meraki Launchpad), Network (Sao Paulo - Cloud Campus Fabric), Secure Connect, Network-wide, Assurance, Security & SD-WAN, Switching, Wireless, Insight, Organization, Security (marked New), Automation, and Access Manager (marked New). The main content area is titled 'Staged upgrades' with tabs for 'Groups' and 'Sequence'. A modal dialog titled 'Schedule firmware change' is open. It asks 'When should this firmware be installed?' and includes a note: 'Upgrade times may be staggered depending on the number of devices changing firmware.' There are two radio buttons: 'Perform the upgrade now' (selected) and 'Schedule the upgrade for:'. The scheduling option shows a date field with '03/28/2025', a time dropdown with '11:00', and '(network local time)'. Below this is a section titled 'ISSU' with the text: 'When enabled, this setting will apply exclusively to the eligible switches withn the StackWise Virtual pairs.' There is a checked checkbox labeled 'Attempt ISSU when available'. At the bottom right of the dialog are 'Back' and 'Next' buttons.

ISSU introduced with 17.18.1 (beta)

Cisco Catalyst 9500 ISSU workflow refresher



Introducing Rapid Per-VLAN STP+ from the cloud

RPVST+ provides faster convergence to minimize downtime and ensure resilience in dynamic environments

Allows efficient load balancing across multiple different VLANs

Critical for maintaining stable L2 topologies in dense campus deployments

Switch settings

VLAN configuration

Management VLAN ⓘ

1

STP configuration

☒ Enable Rapid Spanning Tree (RSTP) ⓘ

STP bridge priority ⓘ

Switches/Stacks	Bridge priority
Default	32768

[+ Set the bridge priority for another switch or stack](#)

Quality of service ⓘ

#	VLAN	Protocol	Source port ⓘ	Destination port ⓘ	Trust incoming DSCP
---	------	----------	----------------------------	---------------------------------	---------------------

STP configuration

STP configuration mode

☒ Enable Spanning Tree

Select Spanning Tree mode for Catalyst switches:

☐ Enable Multiple Spanning Tree (MST)

☒ Enable Rapid per-VLAN Spanning Tree (RPVST+)

ℹ Operating network with a mix of RPVST+ and RSTP may cause unexpected issues, please refer to [Documentation](#) for best practices for operating mixed STP environments.

☐ Disable Spanning Tree

STP bridge priority ⓘ

Switches/Stacks	Bridge priority	VLAN list	Actions
Default	32768		
Rocky_and_Bullwinkle	8192	1-4094	

[+ Set the bridge priority for another switch or stack](#)

Advanced routing

Introducing **Border Gateway Protocol** from the cloud

Multiple configuration options including full stack dynamic routing (SD-WAN + LAN) and simplified iBGP/eBGP routing

Flexible configurations including per switch and peer-group templates, plus support for common policy objects

Support for full API programmability and open compatibility with third-party vendors

The screenshot displays the Cisco SD-WAN configuration interface for BGP Routing. The main panel shows the 'Local Networks' section with a table of BGP Routers. A callout box highlights the 'BGP Routing' configuration page, which includes tabs for 'General', 'BGP Filters', and 'ASN'. The 'General' tab shows the 'BGP Routers' table, and the 'ASN' tab shows the 'Autonomous System Numbers (ASN)' table.

BGP Routing - General Tab

Enable	Switch name	Model	ASN	Active peers	Advertised routes
☒	Bob	C9300-24UX	65500	0	1

BGP Routing - ASN Tab

ASN	Description	BGP routers
65500		1

Supported Hardware: C9500, C9300X, C9300, C9300L, C9300LM, C9200CX, MS390
Beta: IOS XE 17.18.1

Introducing VRF deployment from the cloud

Easily create isolated route domains without additional hardware and enhance fault isolation

Strengthen security with scalable macro-segmentation, limiting lateral movement of threats

Simplify network management by eliminating the need for ACLs on every SVI and reducing oversized route tables

The screenshot displays the Cisco Cloud Managed Network (CMN) interface, specifically the 'Routing & DHCP' section. A modal window titled 'Edit BLUE_VRF' is open, showing configuration details for a new VRF. The modal includes fields for 'VRF name' (BLUE_VRF), 'Description' (IoT), 'Route distinguisher' (52:106), and 'Route target' (52:106). Below the modal, a table lists the VRF configuration details, including the interface, name, VRF, subnet, and IP address. The table also shows the status of the VRF (e.g., 'Routed') and the associated interface (e.g., '80 VLAN').

Switch or switch stack	Interface	Name	VRF	Subnet	IP
☐ Doug	80 VLAN	eighty	BLUE_VRF	10.80.80.0/24	10.80.80.254
☐ Rocky_and_Bullwinkle	80 VLAN	BLUE VLAN 80	BLUE_VRF	10.80.80.0/24	10.80.80.253
☐ Bob	Bob / 13	Bobs routed port	BLUE_VRF	10.88.88.0/24	10.88.88.252
☐ Bob	Bob / 14	Bobs 2nd routed port	BLUE_VRF	10.89.89.0/24	10.89.89.252
☐ Doug	0 Loop	0	BLUE_VRF	10.252.252.252/32	10.252.252.252
☐ Doug	20 VLAN	Uplink Vlan 20	Default	10.20.20.0/24	10.20.20.2

Below the modal, a 'VRF' section shows a list of VRFs with associated interfaces and a search bar. The table lists the VRF configuration details, including the name, description, route distinguisher, route target, and networks. The table also shows the status of the VRF (e.g., 'Routed') and the associated interface (e.g., '80 VLAN').

Name	Description	Route distinguisher	Route target	Networks
☐ Default	—	—	—	—
☐ BLUE_VRF	IoT	52:106	—	—
☐ GREEN_VRF	PCI	52:108	—	—
☐ RED_VRF	Evil Printers and Fax Machines	52:107	—	—

VRF structure within Dashboard

VRF Profiles

Q Search

+ Add VRF Profile

☐	ID ▾	Name	Route Distinguisher	Route Target	Associated Networks	
☐	1	VRF Red	64513:1	64513:1	HQ-Campus-Denver , Branch-Tokyo	 
☐	1	VRF Green	65500:100	65500:100	HQ-Campus-Denver, HQ-Campus-Phoenix	 

Rows per page

2 < 1 2 ... 10 >



Defined at the Organisation



Implemented at the Network



Building block for complex topologies

Add VRF Profile

Name

WirelesslyWired_PROD

Route Distinguisher

65501:10

Route Target Export

65501:10

Route Target Import

65501:100

+ Add Route-Target

Cancel

Save

Introducing Routed Ports from the cloud

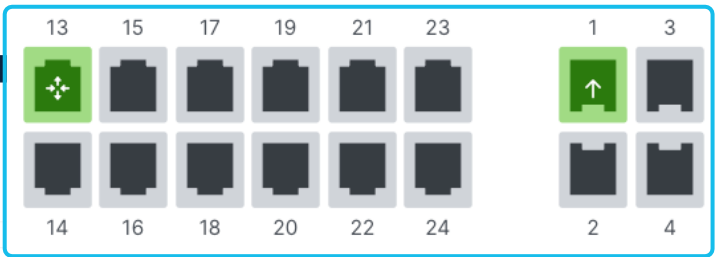
Reduce convergence time while simplifying network management

Routed peer to peer links including east/west and north/south traffic

Minimise VLAN ID consumption while joining separate networks

Reduce fault domains for Layer2/STP

New port icon



Routing & DHCP

SWITCH OR SWITCH STACK: Select... IP ADDRESS: Select...

Interfaces

Search... 9 Interfaces

Switch	VLAN	Name	Subnet	
☐	CAMPUS01-CORE	10	Corp-Data	172.16.10.0/24
☐	CAMPUS01-CORE			172.16.10.254
☐	CAMPUS01-CORE			False
☐	CAMPUS01-CORE			False
☐	CAMPUS01-CORE			Server
☐	CAMPUS01-CORE			Enabled

Static routes

Search... 1 Static route

Switch	VLAN	Name	Subnet	
☐	CAMPUS01-CORE			

Multicast routing

Search... 1 Static route

Update 1 Ports

Selected Switch / Port: 1 ^

Bob/13

Interface mode

☐ Switch port ☒ Routed port

☒ Navigate to configure routed port

Name

Transit Network

Tags

Port status

☒ Enabled

Link negotiation

Auto negotiate

EEE ⓘ

☐ Enabled

Port schedule

Unscheduled

PoE

☒ Enabled

Port isolation

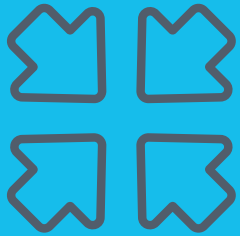
☐ Enabled

Cancel Update

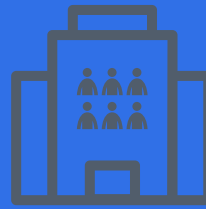
Beta: IOS XE 17.18.1

Securing a cloud campus

Why do we need micro-segmentation?



minimize exposure in
an organisation



provide multi-tenancy
in a secure way



maintain compliance
and pass security
audits



quarantine malicious
or compromised
devices



implement a zero-
trust framework

Adaptive policy



Organization-Wide intent-based policy



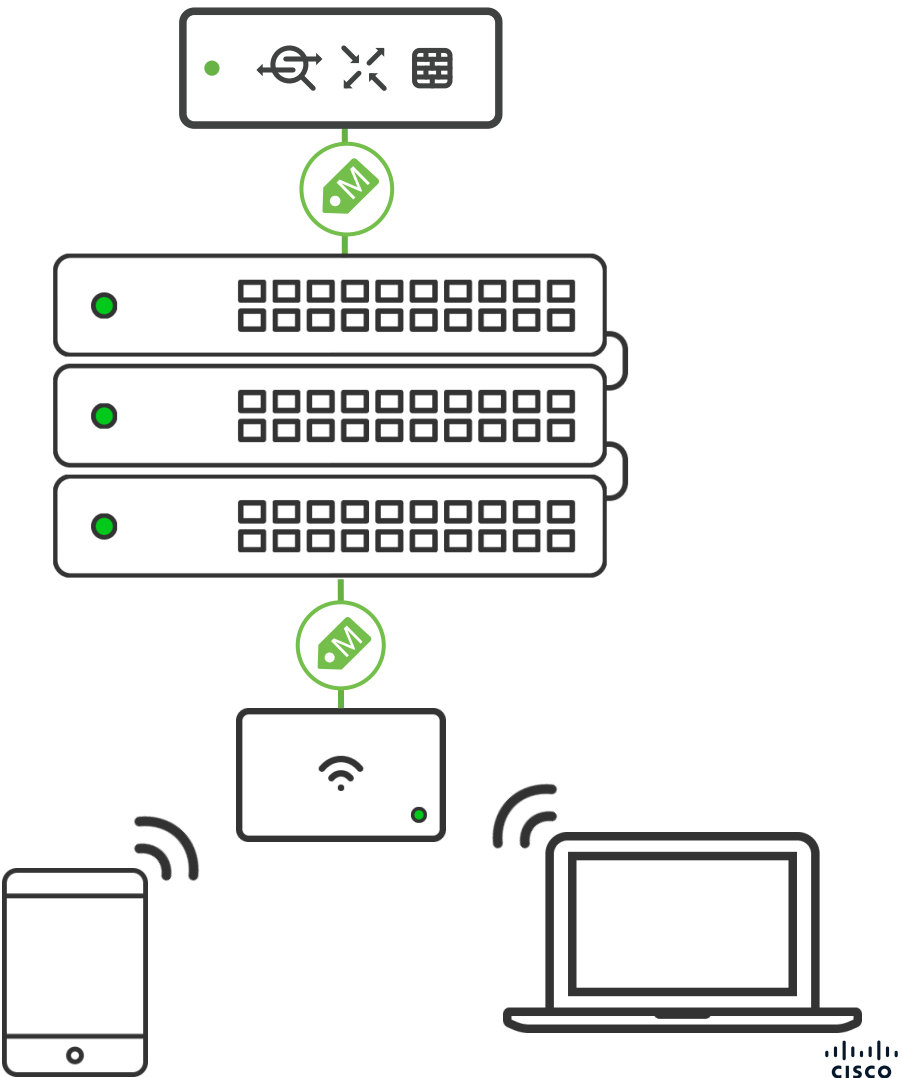
Utilizing inline Security Group Tags (SGTs)



Context shared over the data-plane

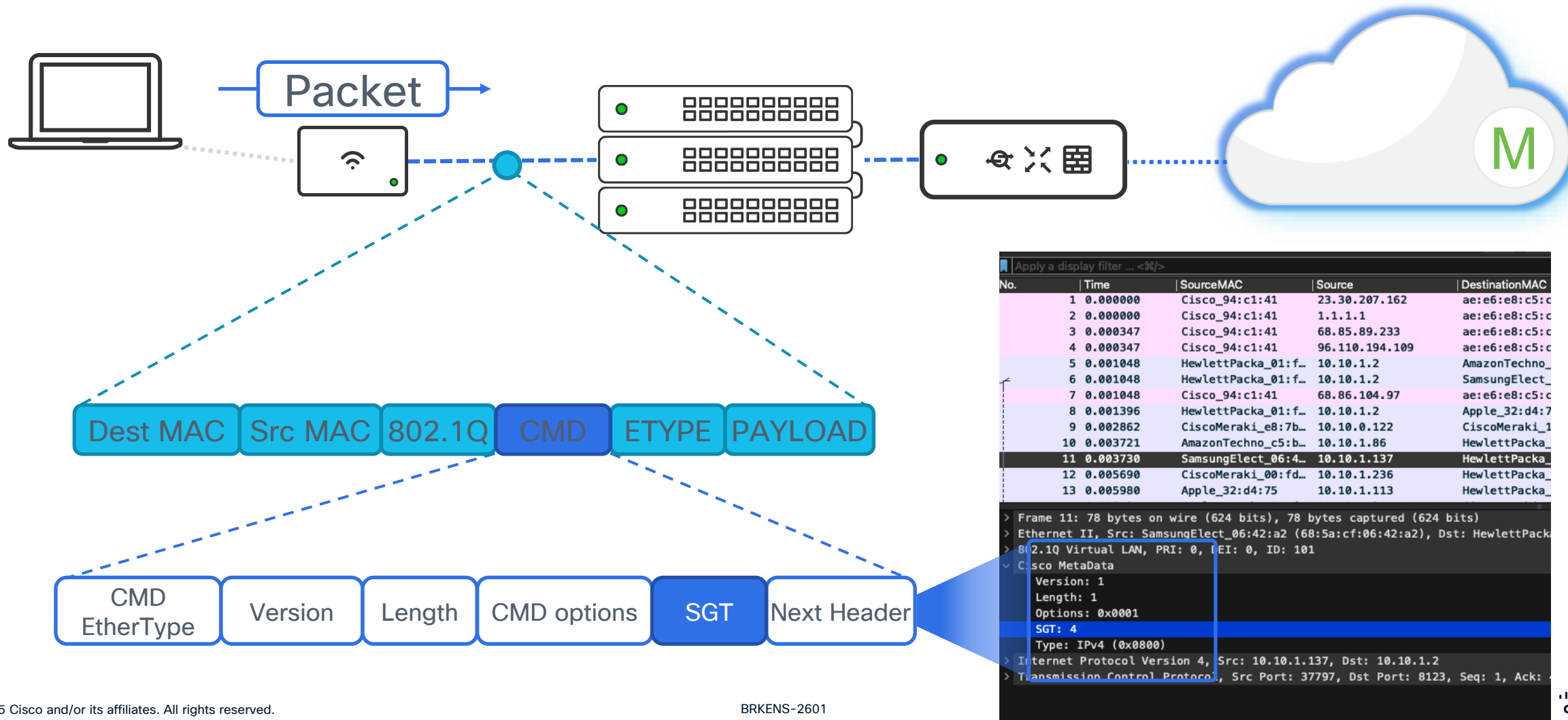


IP and topology agnostic security providing consistent policy for wired and wireless access



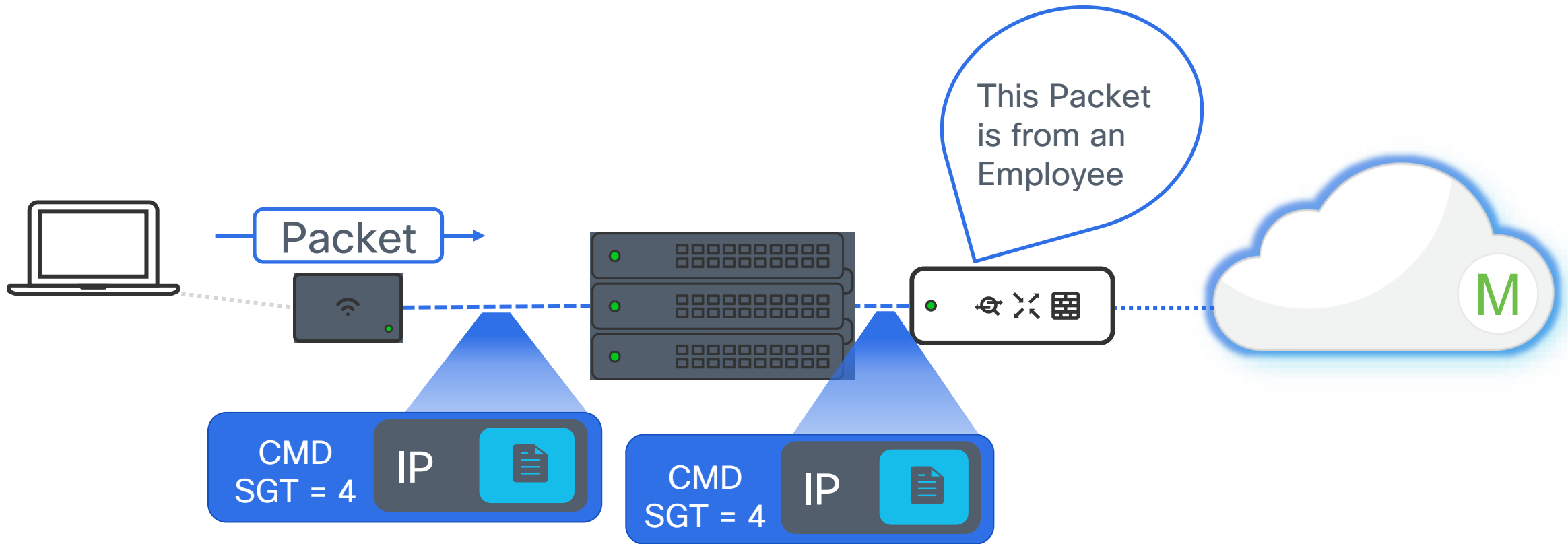
What are SGTs?

SGT = Scalable Group Tags, aka Secure Group Tags)

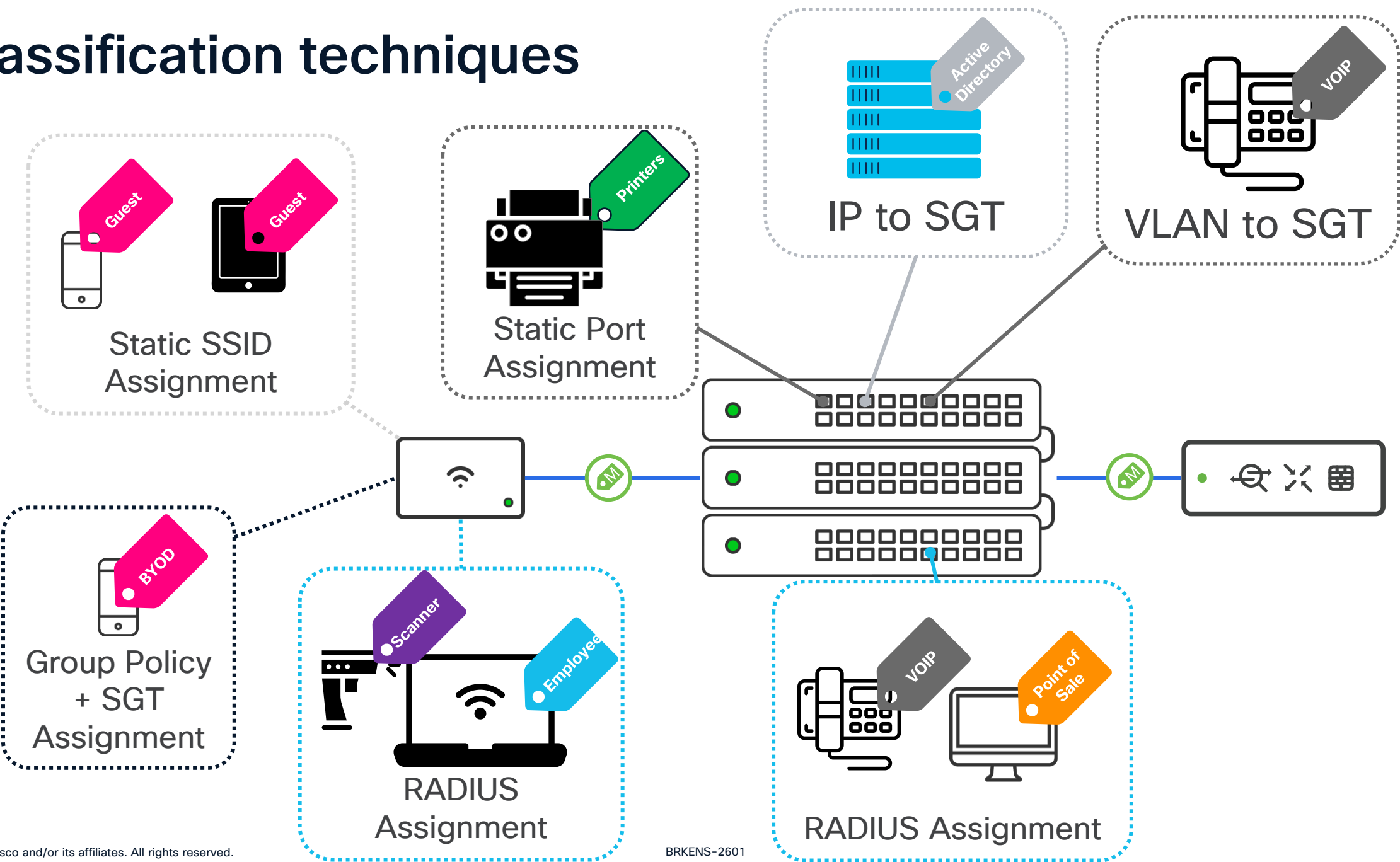


Scalable identity and context

Sharing security group information over the data plane, in every packet.



Classification techniques



One consistent policy

Define groups for your network.

Infrastructure (2) and Unknown (0) are added automatically.

Adaptive Policy

[Policies](#)[Groups](#)[Custom ACLs](#)[Networks](#)

6 results [+ Add group](#)

☐	Name	SGT Value	Description	Policy Objects	
☐	Contractor	40	Contractor Group	—	
☐	Employee	10	Employee group	—	
☐	Guest	20	Guest group	—	
☐	Infrastructure	2	Created by Meraki, the Infrastructure group is used by Meraki devices for internal and dashboard communication	—	
☐	IOT	30	IOT Group	—	
☐	Unknown	0	Created by Meraki, the Unknown group applies when a policy is specified for unsuccessful group classification	—	

One consistent policy

Create any custom ACL's to define specific access beyond allow/deny.

Adaptive Policy

Policies

Groups

Custom ACLs

Networks

Q Search

IP version

1 result

+ Add custom ACL

☐	Name	Description	IP version	Rules	
☐	Management	—	any	allow tcp src: any, dst: 22 tcp established: Enabled log: Enabled allow tcp src: any, dst: any tcp established: Enabled log: Enabled	

One consistent policy

For each source group, define the destination group and the access that is allowed.

If there is no SGT policy, the default behaviour is to allow-all.

Adaptive Policy

Policies Groups Custom ACLs Networks

Total policies
18

Allow policies
6

Deny policies
11

Groups
6

ACLs
1

Filters 18 results + Add policies

Destination Groups 6

	Contractor	Employee	Guest	Infrastructure	IOT	Unknown
Contractor						
Employee						
Guest						
Infrastructure						
IOT						
Unknown						

6

Source Groups

+

-

i

SGT port assignment

Switchports can be configured with a static SGT group directly.

Update 1 Ports

Name

GigabitEthernet1/0/1

Tags

Port status

☒ Enabled

Link negotiation

Auto negotiate

EEE ⓘ

☐ Enabled

Port schedule

Unscheduled

PoE

☒ Enabled

Type

☐ Trunk

☒ Access

Access policy ⓘ

Open

VLAN

default - 1

Voice VLAN

RSTP

☒ Enabled

STP guard

Disabled

Adaptive policy group

10: Employee

SGT via any RADIUS server for wired port

Switch ports connecting to intelligent devices that can run a 802.1X stack can be configured for authentication and dynamic SGT assignment based on identity.

Update 1 Ports

Selected Switch / Port

1

Name

GigabitEthernet1/0/1

Tags

Port status

☒ Enabled

Link negotiation

Auto negotiate

EEE ⓘ

☐ Enabled

Port schedule

Unscheduled

PoE

☒ Enabled

Type

☐ Trunk ☒ Access

Access policy ⓘ

ISE

VLAN

default - 1

Voice VLAN

SGT assigned to SSID

Guest SSID that don't have 802.1X enabled can simply be assigned a common SGT for all devices.

Client IP and VLAN NAT mode with content filtering

☒ Meraki AP assigned (NAT mode)

Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with the Internet.

Content filtering ⓘ

Enabled

Disabled

Custom DNS servers ⓘ

e.g. 192.168.0.0

☐ External DHCP server assigned

Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or from shared printers, and wireless cameras.

VLAN tagging ⓘ

Disabled

Assign group policies by device type

Enabled

Disabled

Adaptive policy group

Bridge mode, NAT mode, MCG mode only

20: Guest ▼

SGT via any RADIUS server for wireless SSID

Wireless SSIDs can also be configured with WPA2/3 Enterprise with RADIUS authentication for dynamic SGT assignment.

This can work well too with CoA and posture. A client that needs to be quarantined can have its SGT modified.

The screenshot shows a configuration page for a wireless SSID. The title is "Security" with a subtitle "WPA2 Enterprise with 0 RADIUS servers". There are five radio button options:

- ☐ Open (no encryption)
Any user can associate
- ☐ Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption
- ☐ Password
Users must enter a passphrase to associate ⓘ
- ☐ MAC-based access control (no encryption)
my RADIUS server ▼
RADIUS server is queried at association time
- ☒ Enterprise with
my RADIUS server ▼
User credentials are validated with 802.1X at association time

The "Enterprise with" option is selected and highlighted with a red rounded rectangle.

SGT via any RADIUS server

An SGT is just a RADIUS av-pair that is sent to the network device in the Access-Accept message

Must be hex of SGT decimal value

Can be as simple as 00

```
cisco-av-pair:cts:security-group-tag={SGT value in HEX}-{revision number}
```

iPSK Default

Radius-Called-Station-ID **CONTAINS** Tornado-AP_PSK

× DefaultPSK4Clients

+

TestClient

× ▾

+

Result

Class	CACS:adcd880600000000386d43c6:ww-ise/374370439/1664
cisco-av-pair	cts:security-group-tag=0fa0-00
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

←

= 4000

Adaptive Policy with full API access

API Index

API Reference

Overview

API

Platform

configure

actionBatches

adaptivePolicy

acls

POST Create Organization Adaptive Policy Acl

GET Get Organization Adaptive Policy Acls

GET Get Organization Adaptive Policy Acl

PUT Update Organization Adaptive Policy Acl

DELETE Delete Organization Adaptive Policy Acl

organizations

configure

adaptivePolicy

acls

Get Organization Adaptive Policy Acl

Operation Id: getOrganizationAdaptivePolicyAcl

Description: Returns the adaptive policy ACL information

GET /organizations/{organizationId}/adaptivePolicy/acls/{aclId}

Request Parameters

Path

organizationId required | string

Organization ID

aclId required | string

Acl ID

```
adaptivepolicy.py
1 import meraki
2 import json
3
4 dashboard = meraki.DashboardAPI()
5
6 organization_id = '123456'
7
8 response = dashboard.organizations.getOrganizationAdaptivePolicyPolicies(
9     organization_id
10 )
11
12 print("Pretty printing each JSON object in the list:")
13 for item in response:
14     pretty_json = json.dumps(item, indent=4)
15     print(pretty_json)
16     print("-" * 20) # Separator for clarity
```

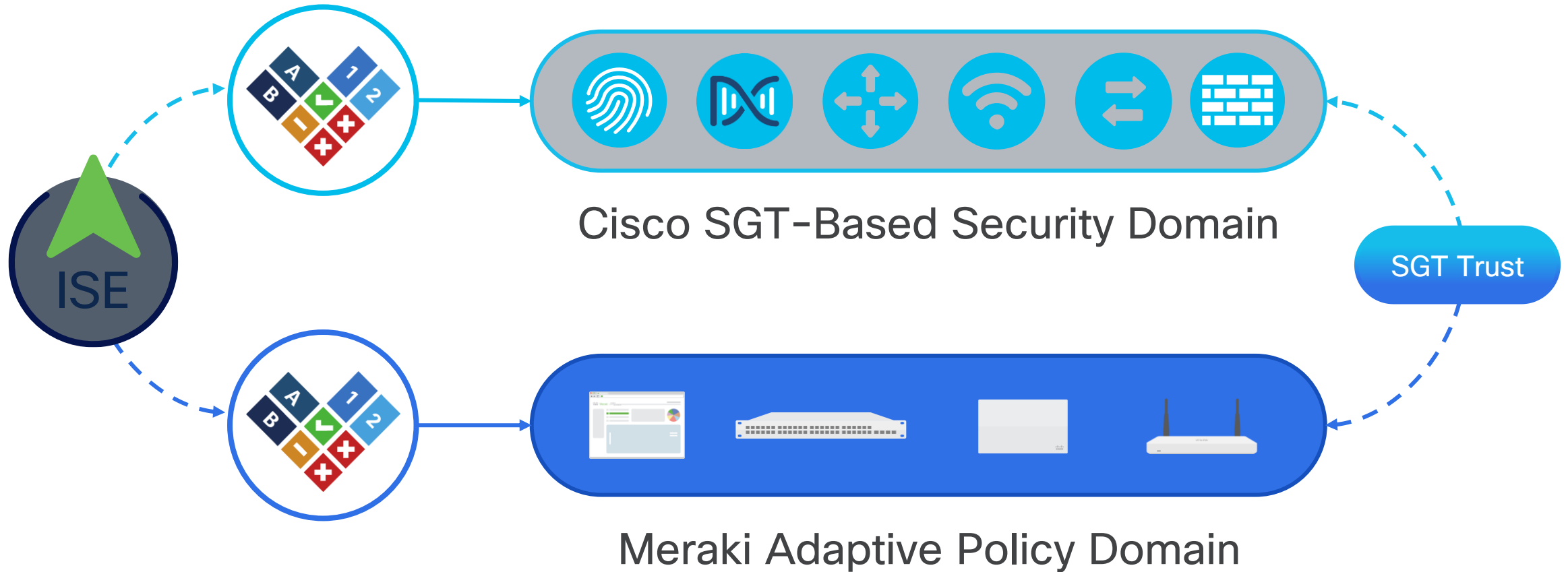
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
(.venv) (base) ljewell@LJEWELL-M-JP4D meraki % /Users/ljewell/Documents/meraki/.venv/bin/python
{"adaptivePolicyId": "667095694804254940",
 "sourceGroup": {
   "id": "667095694804260542",
   "name": "Employee",
   "sgt": 10
 },
 "destinationGroup": {
   "id": "667095694804260542",
   "name": "Employee",
   "sgt": 10
 },
 "acls": [],
 "lastEntryRule": "allow",
 "createdAt": "2025-06-03T04:18:27Z",
 "updatedAt": "2025-06-03T04:18:27Z"
}
```

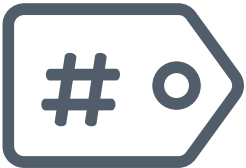


Fully integrated and common policy

Cloud Campus Adaptive Policy integrates into Cisco's common policy framework.



Scaling considerations



60 x SGTs



3600 Policies



113 ACEs Per Policy



8000 IP to SGT Maps

Destination Groups 6

	Contractor	Employee	Guest	Infrastructure	IOT	Unknown
Contractor	✓	✗	✗	✗	✗	✗
Employee		✓		✗	✓	✓
Guest	✗	✗	✗	✗	✗	✗
Infrastructure						
IOT	✓	✓				
Unknown						

Source Groups 6

+

-

i

Cloud managed campus fabric

Cloud-managed campus fabric overview



Multi-Network Cloud-Managed
EVPN-VXLAN Fabric



Focused on brownfield migration



Flexible deployment and staging



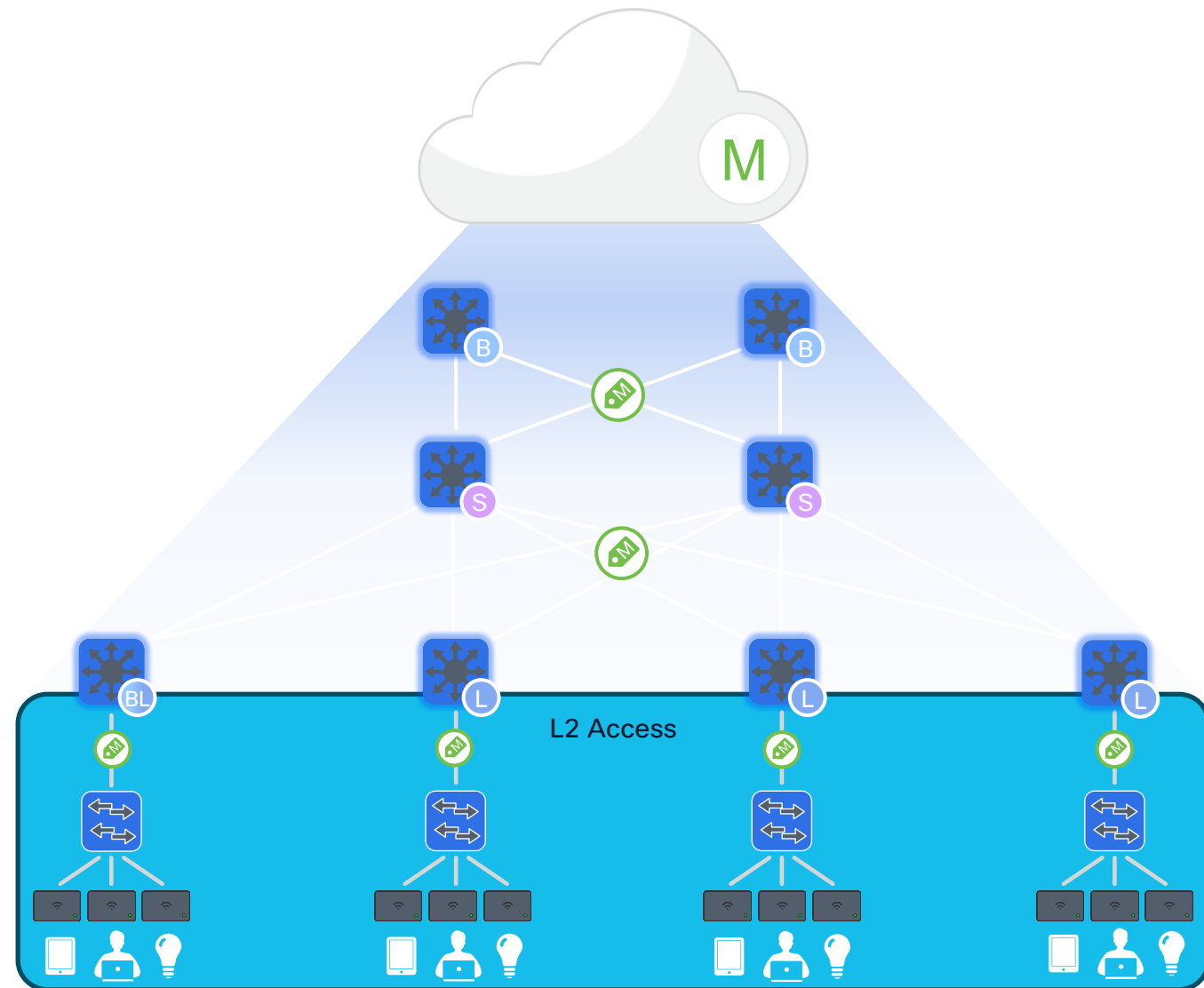
Securing the network with
Adaptive Policy



Optimised L2 extension

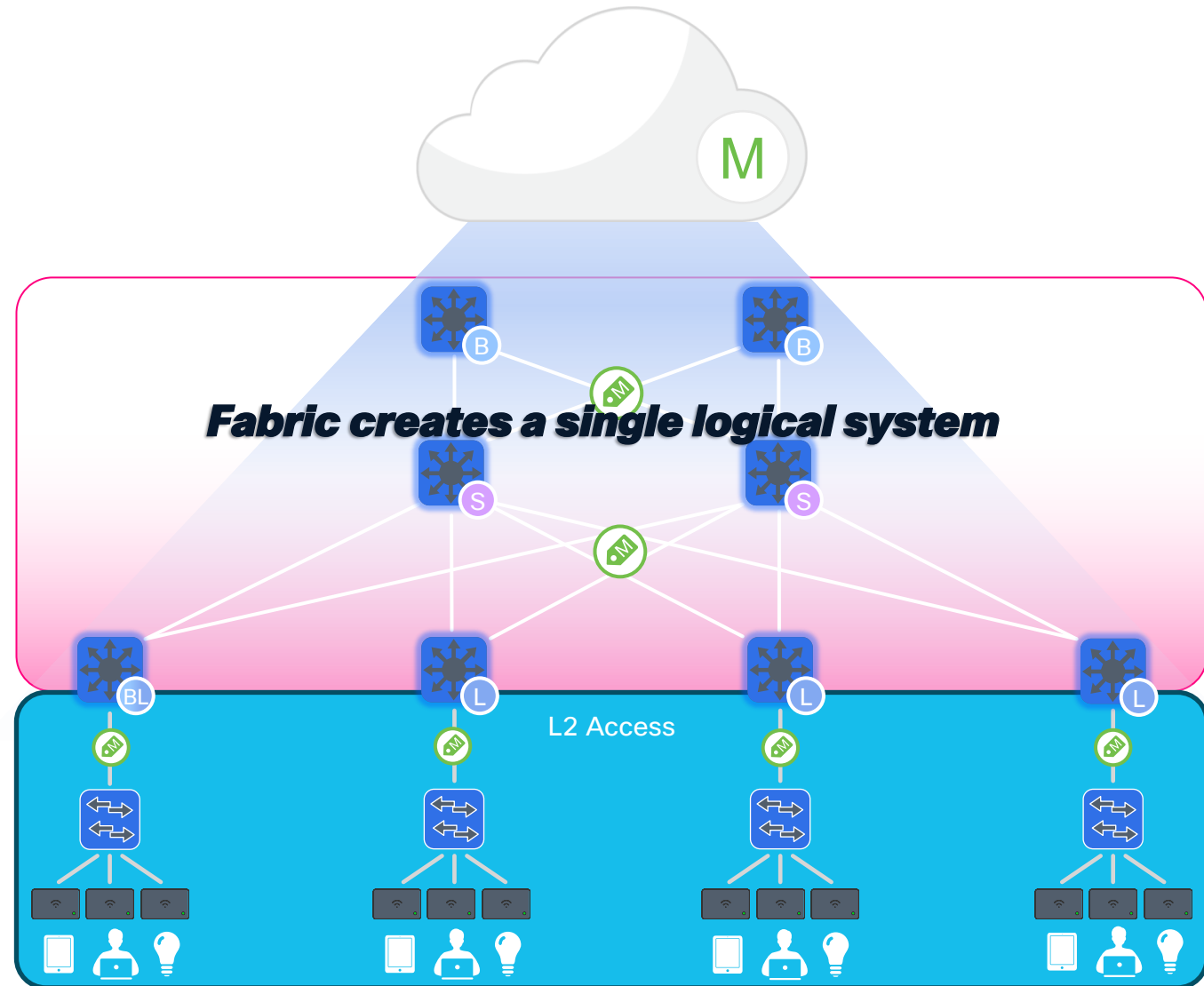


Day-2 Operational Assurance

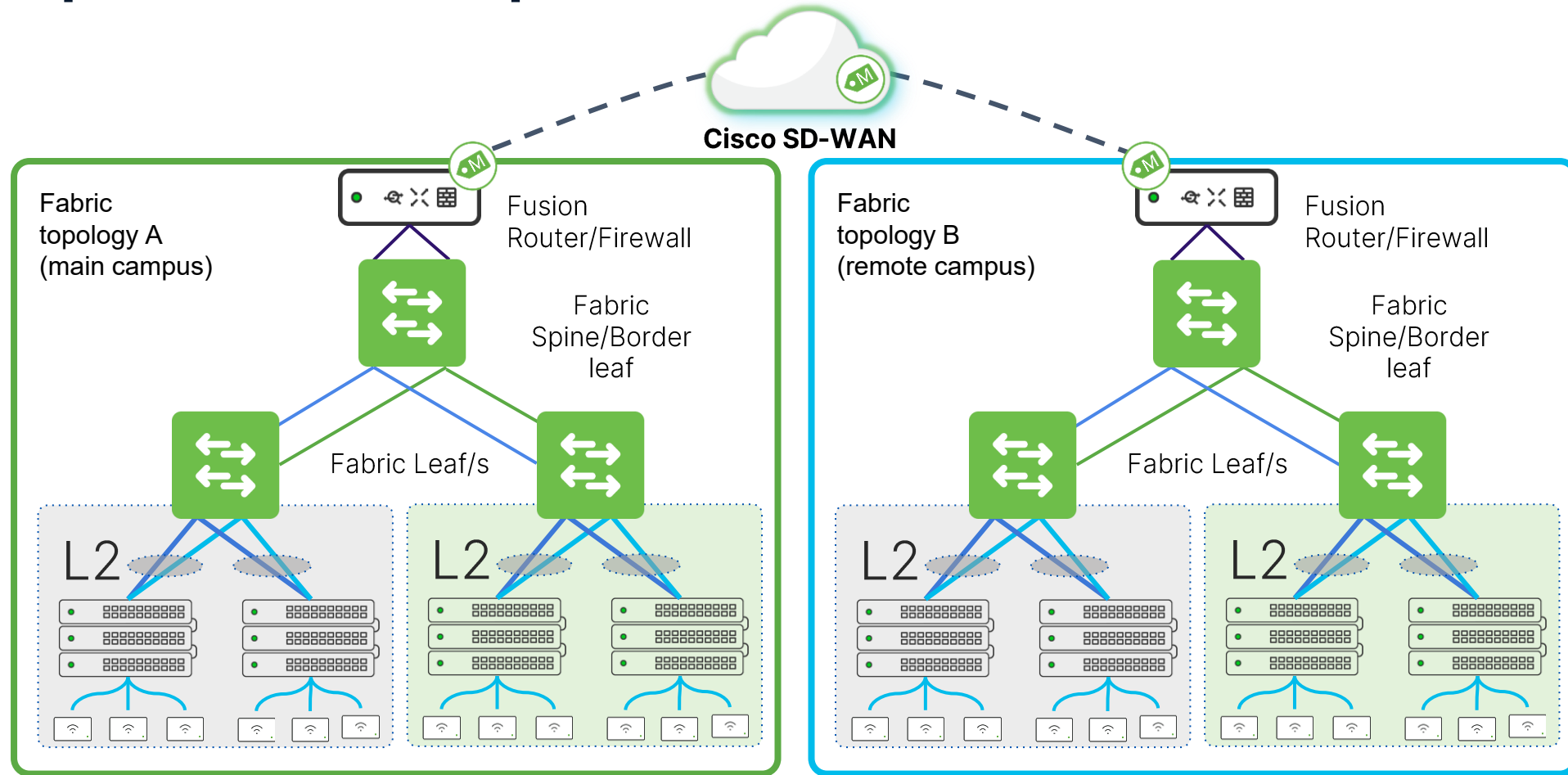


Why cloud managed Campus Fabric?

- Scalability
- Mobility
- Security
- Reachability



Cloud optimised campus fabric



Focus on brownfield with seamless migration

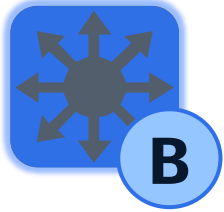
Standards-based BGP-EVPN Fabric

Optimized L2 mobility through Anycast Gateways

Adaptive Policy For micro-segmentation and ZTNA

Leverage Existing Hardware Where Possible (390/9300/9500)

Fabric roles and model support



Border

- Routing into and out of the fabric
- **eBGP / OSPF / Static Routing**
- **Example:** northbound peering to a firewall for internet connectivity

Need this to get out of the fabric.



Spine (RR)

- BGP Route Reflector (RR) and high bandwidth aggregation
- Provides Leaf interconnectivity
- **Example:** Core/Distribution in a 3-tier topology

Connect the leaf nodes together



Leaf (VTEP)

- Virtual Tunnel End Points (VTEP)
- Default Anycast Gateway Host
- BGP Route-reflector client
- **Example:** Distribution/access in a 3-tier topology

Provides multiple default gateways across the fabric to emulate Layer-2 VLAN

Fabric roles and model support



Border



Spine (RR)



Leaf (VTEP)

Campus fabric supports assigning one or multiple roles to a switch
Common combinations of roles are:

- 1. **Border-Spine:** Topologies that would historically have a collapsed core + distribution (e.g. Layer3 + Fiber aggregation / Layer2 handoff)
- 2. **Border-Leaf:** topologies where external route peering occurs along-side direct client connectivity (e.g. lab network, research, vendor)

All 3 roles must be present in a topology to deploy the fabric.

Model	Role		
	Border	Spine	Leaf
9500H	✓	✓	✓
9300X	✓	✓	✓
9300 / MS390	✓	✓	✓
9300L / LM (MVP+)	✗	✗	✓

What is a BGP EVPN-VXLAN fabric?

Connectivity out of fabric

eBGP/OSPF/Static routes

BGP Control Plane

BGP Route-reflectors

Distributed anycast gateway for IP mobility

L3 Gateways

Common Layer2 south of the anycast gateway

VXLAN
Tunnels
provides
overlay
between
fabric nodes

Wireless Client VLAN 130

Wired Client VLAN 120

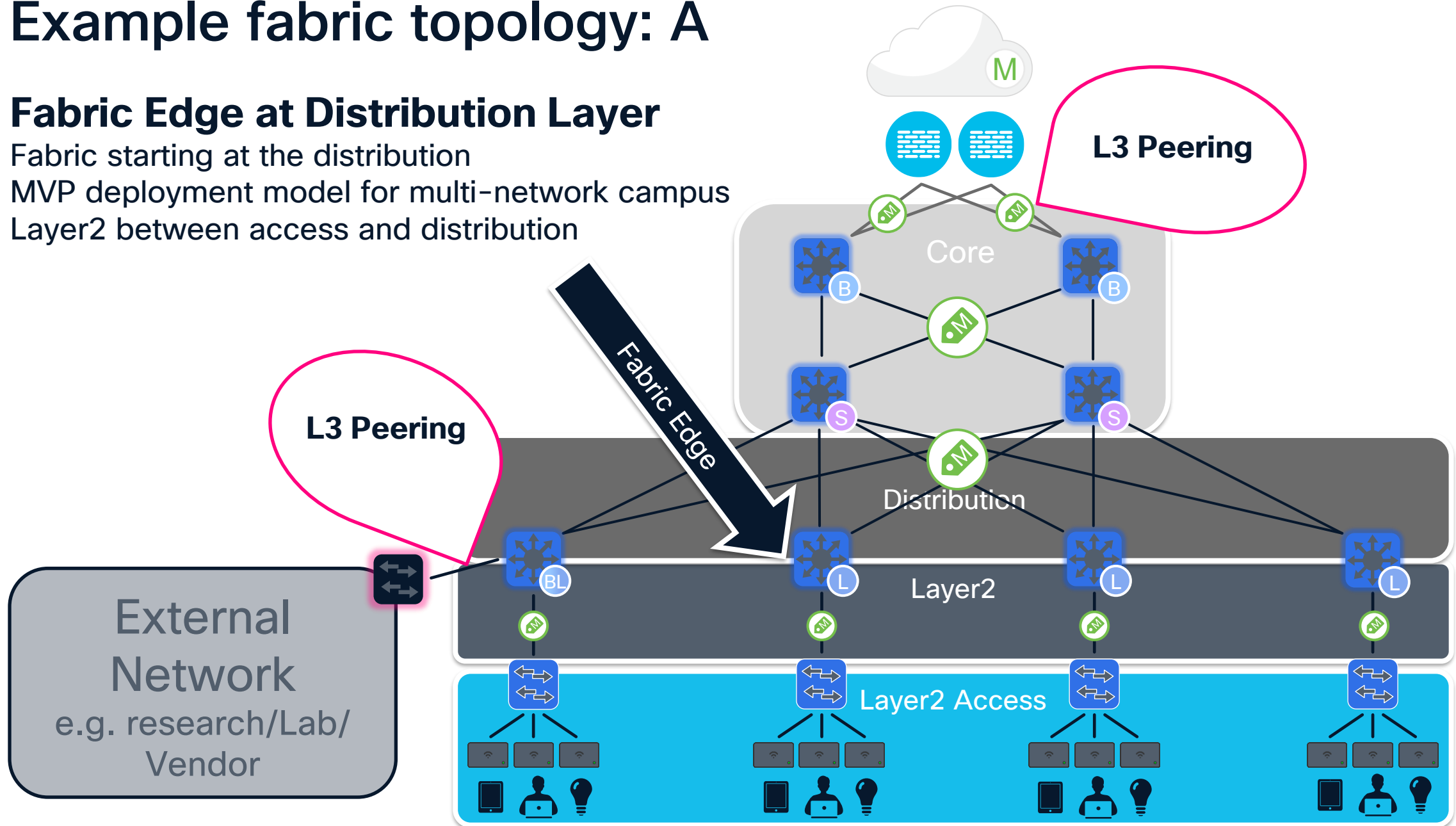
Example fabric topology: A

Fabric Edge at Distribution Layer

Fabric starting at the distribution

MVP deployment model for multi-network campus

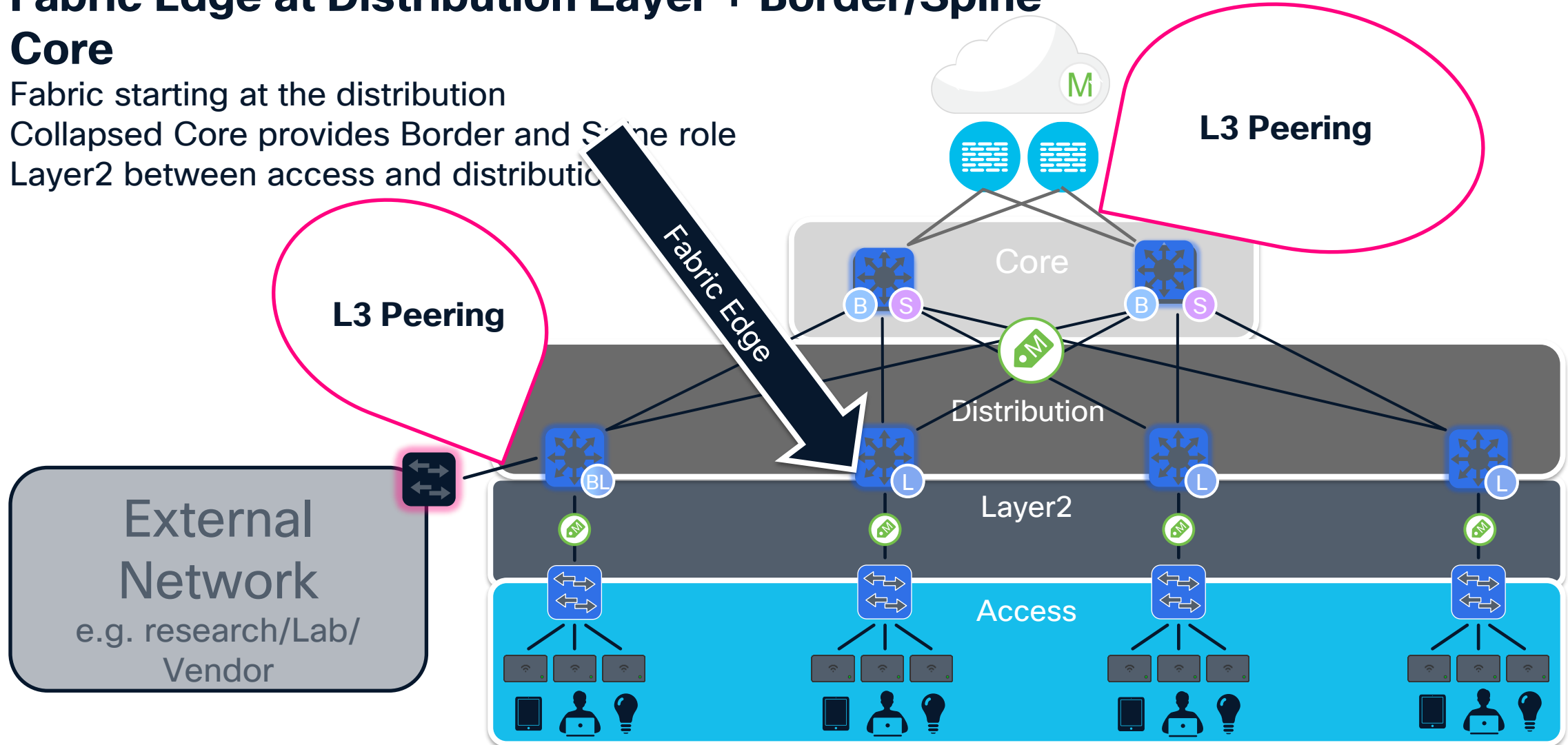
Layer2 between access and distribution



Example fabric topology: B

Fabric Edge at Distribution Layer + Border/Spine Core

Fabric starting at the distribution
Collapsed Core provides Border and Spine role
Layer2 between access and distribution



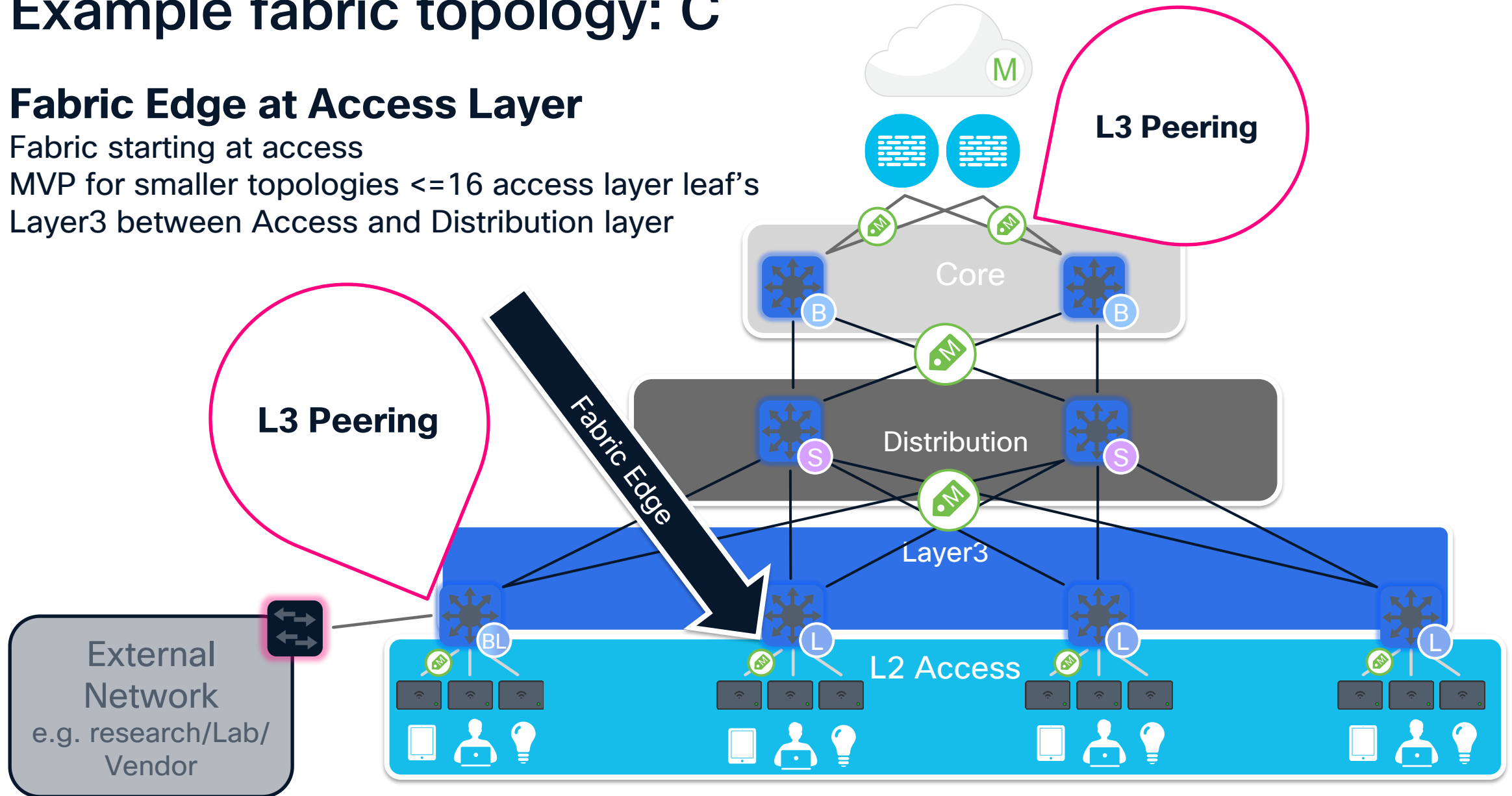
Example fabric topology: C

Fabric Edge at Access Layer

Fabric starting at access

MVP for smaller topologies ≤ 16 access layer leaf's

Layer3 between Access and Distribution layer



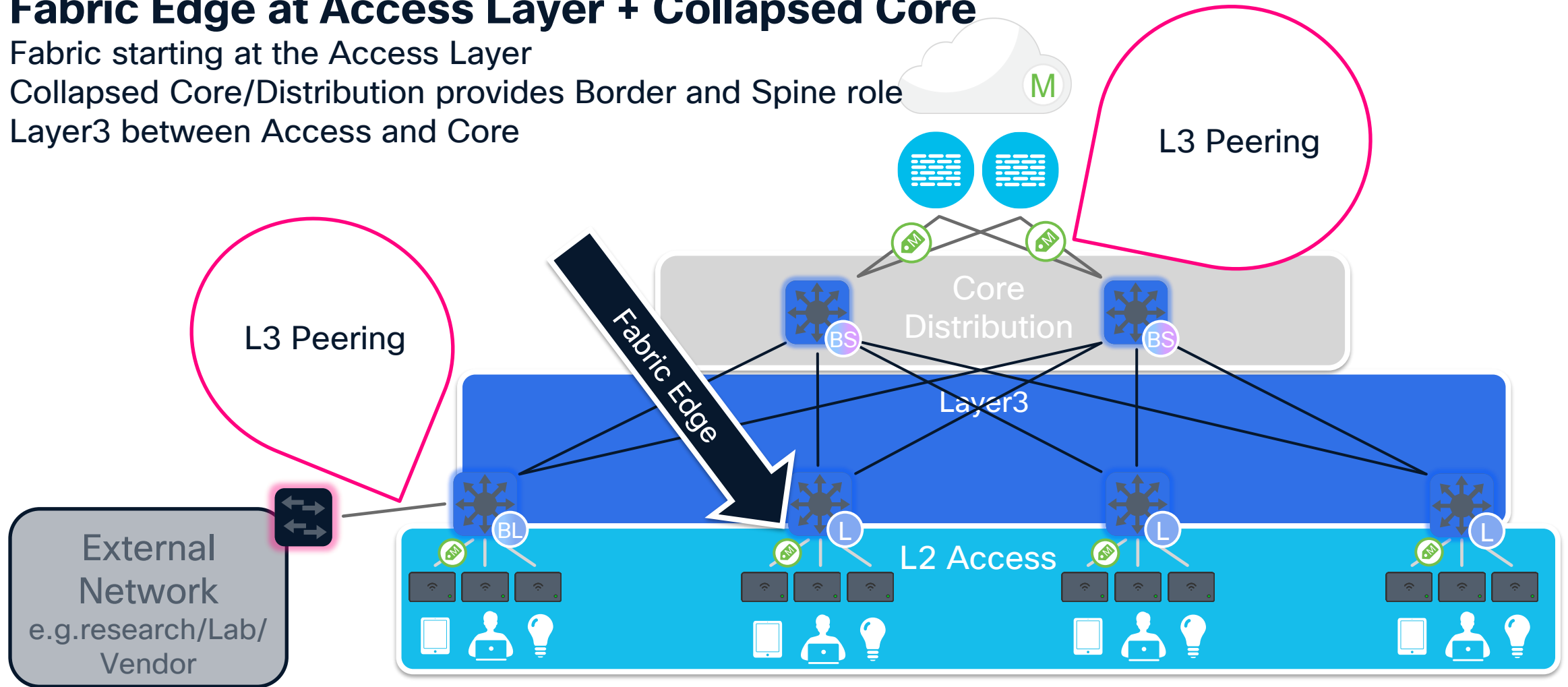
Example fabric topology: D

Fabric Edge at Access Layer + Collapsed Core

Fabric starting at the Access Layer

Collapsed Core/Distribution provides Border and Spine role

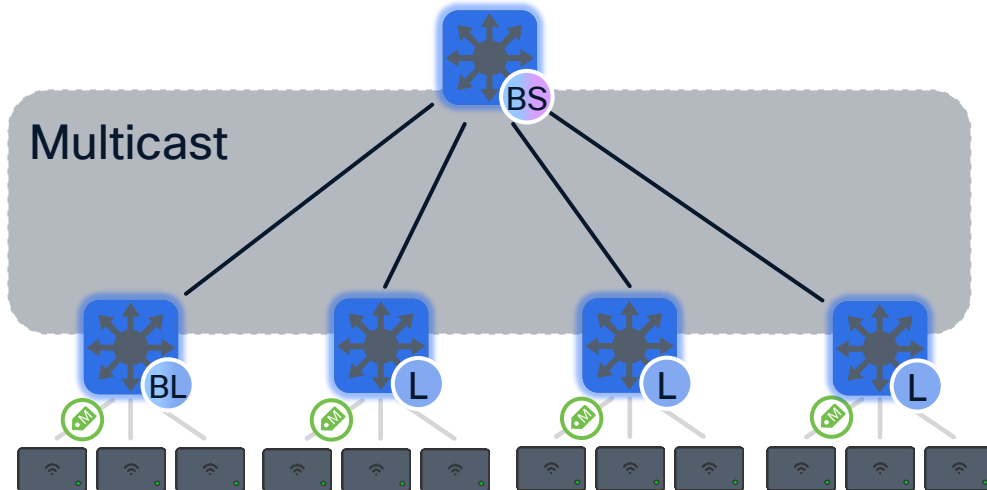
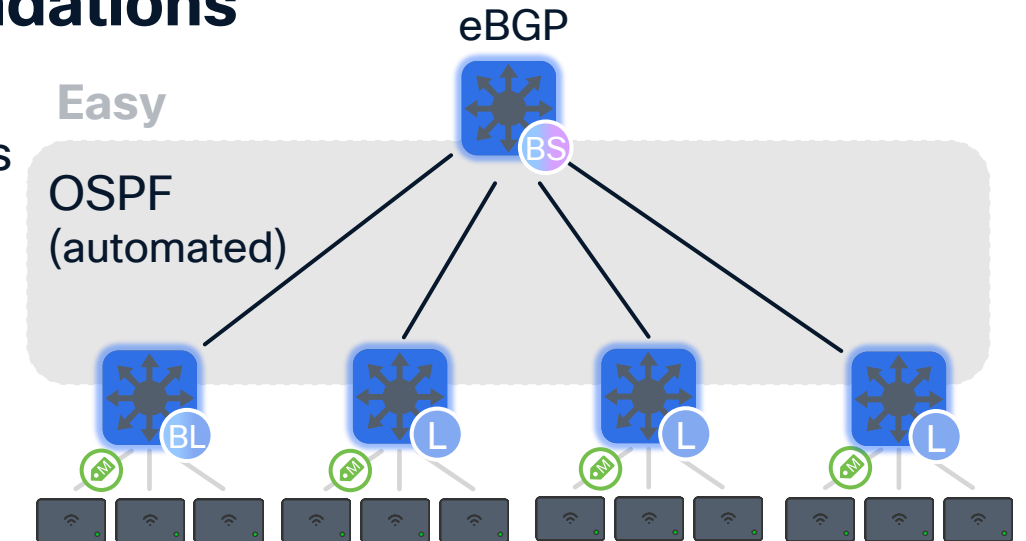
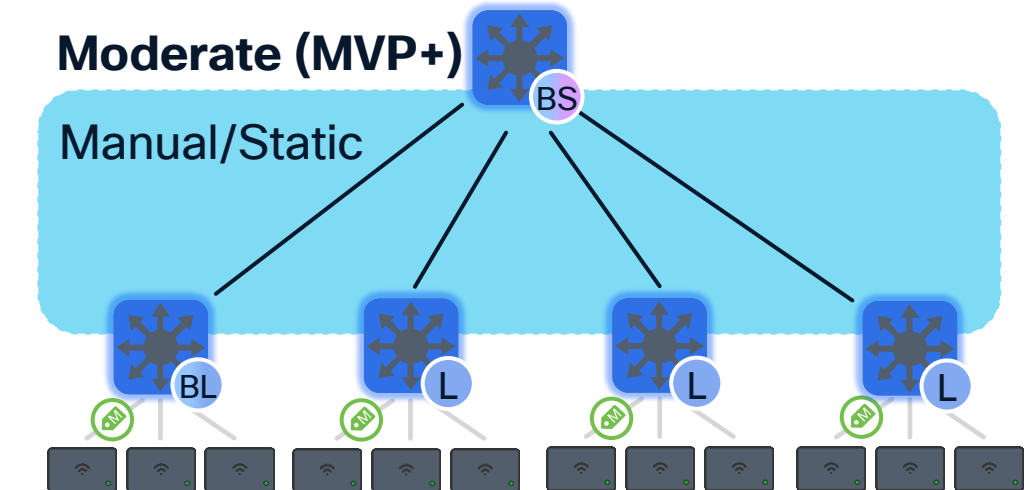
Layer3 between Access and Core



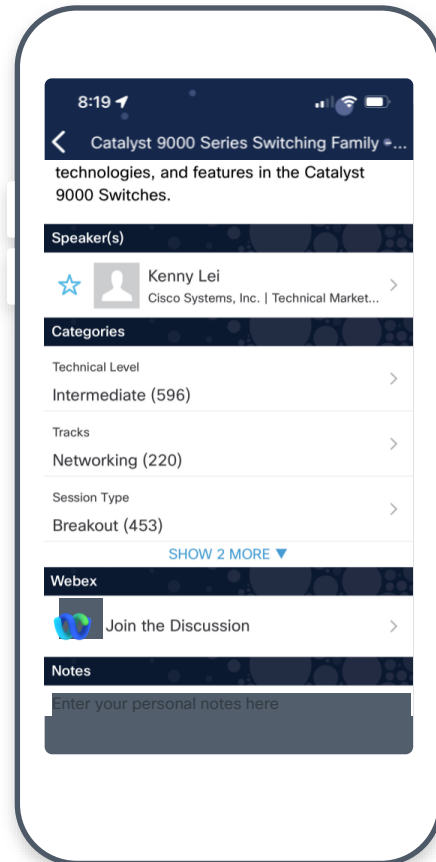
Underlay network requirements & recommendations

Fabric Pre-deployment network recommendations

- Reduce trunks to only necessary VLANs prior to migration
- Move to R-PVST+ for less impact to STP topology changes
- Target routed ports for any new leaf installations
- Post-deployment operate in brownfield underlay architecture (L2 SVI based) until segments are migrated then convert to routed uplinks between Leaf/Spine/Border



For more information



BRKENS-1402: Designing Access and Core Switching Architectures with Meraki.

Brennan Martin
Nico Darrow

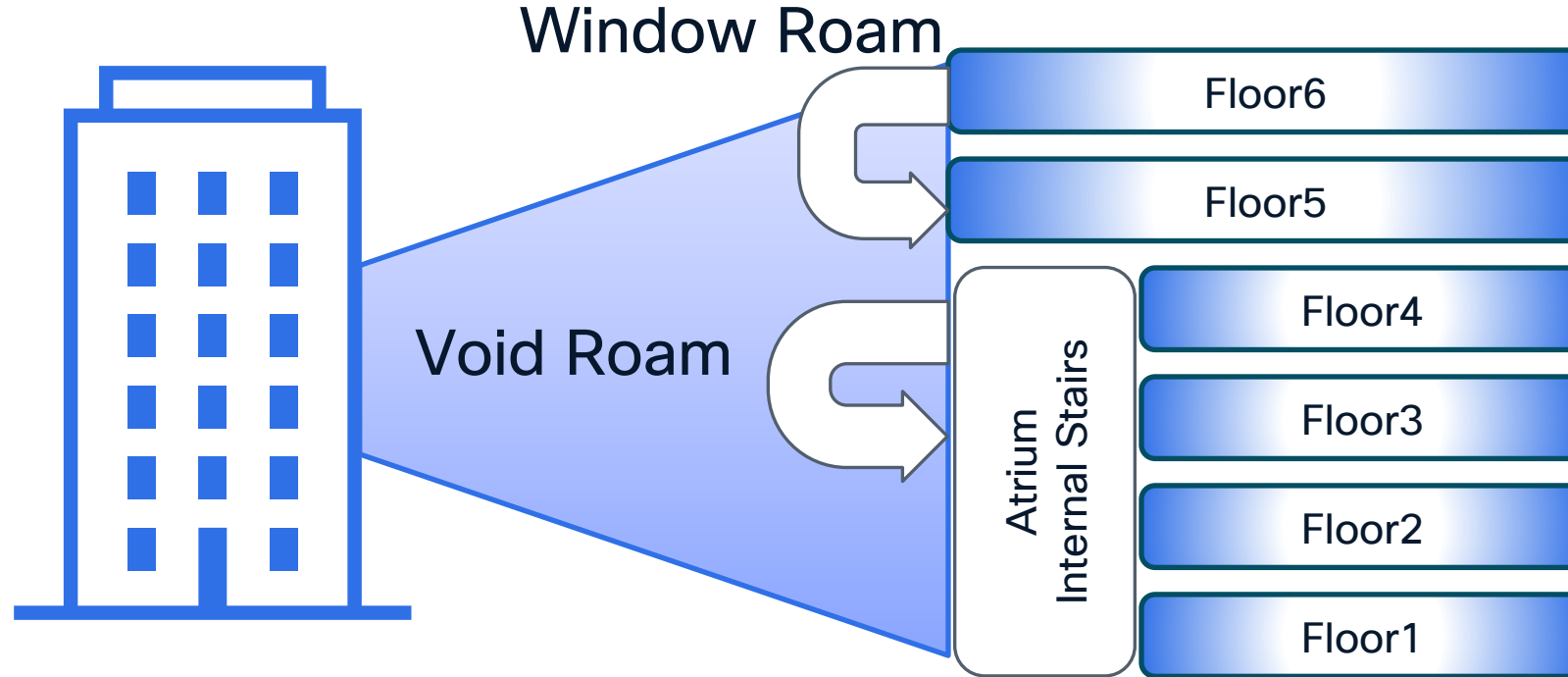


Dashboard deployment demo

Wireless in a Cloud Campus

Inter-floor roaming in a multi-floor building

- Clients determine when and where to roam.
- Windows, atriums and internal stairs can result in inter-floor roams.
- VLAN/subnet allocated per floor due to building size can result in an IP change.
- Clients can perceive this as poor wireless.

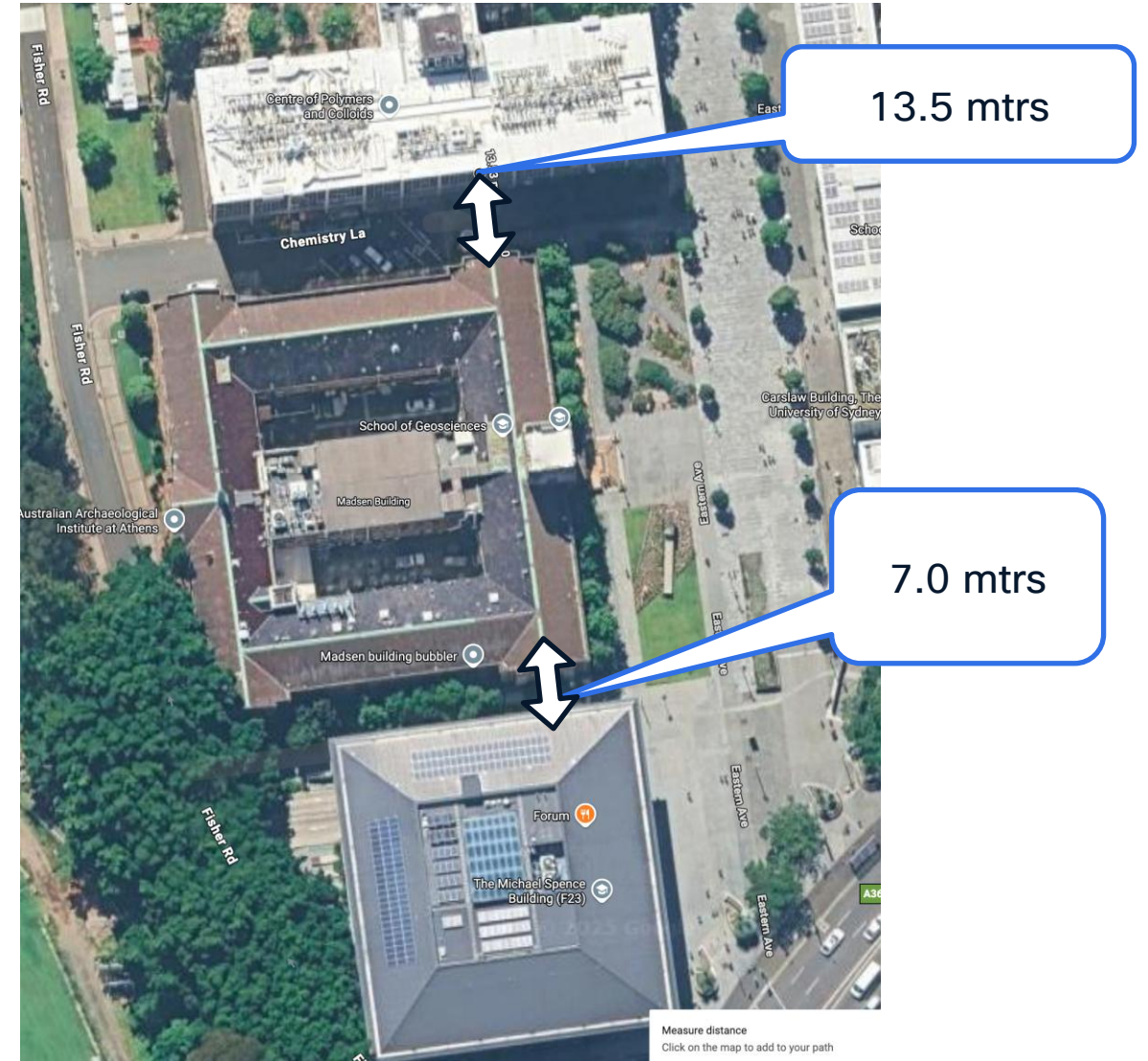


Inter-building roaming in a campus

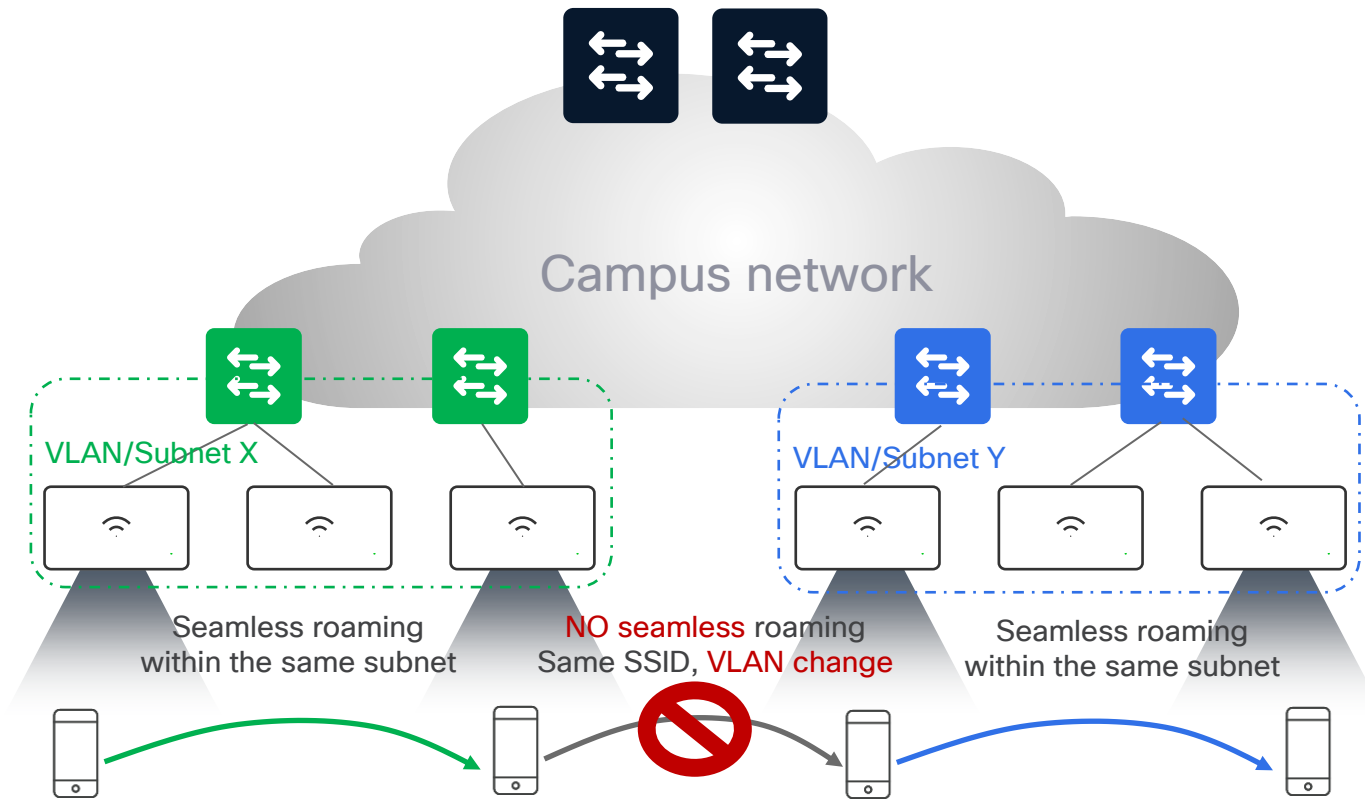
Campus buildings can be very close to each other.

Example:

- Camperdown Campus in Sydney
- Madsen building (F09)
- 13.5 mtrs from Chemistry Building (F11)
- 7.0 mtrs from Michael Spence Building (F23)
- With same SSID, roaming is very likely between buildings



Roaming in a campus



Seamless Roaming:

- Need to keep IP address (and policy) across APs
- Same client VLAN/subnet on wired side

Design Questions:

- Can I span the VLAN?
- What would be the implications?

Seamless roaming capacity planning

Distribution Layer

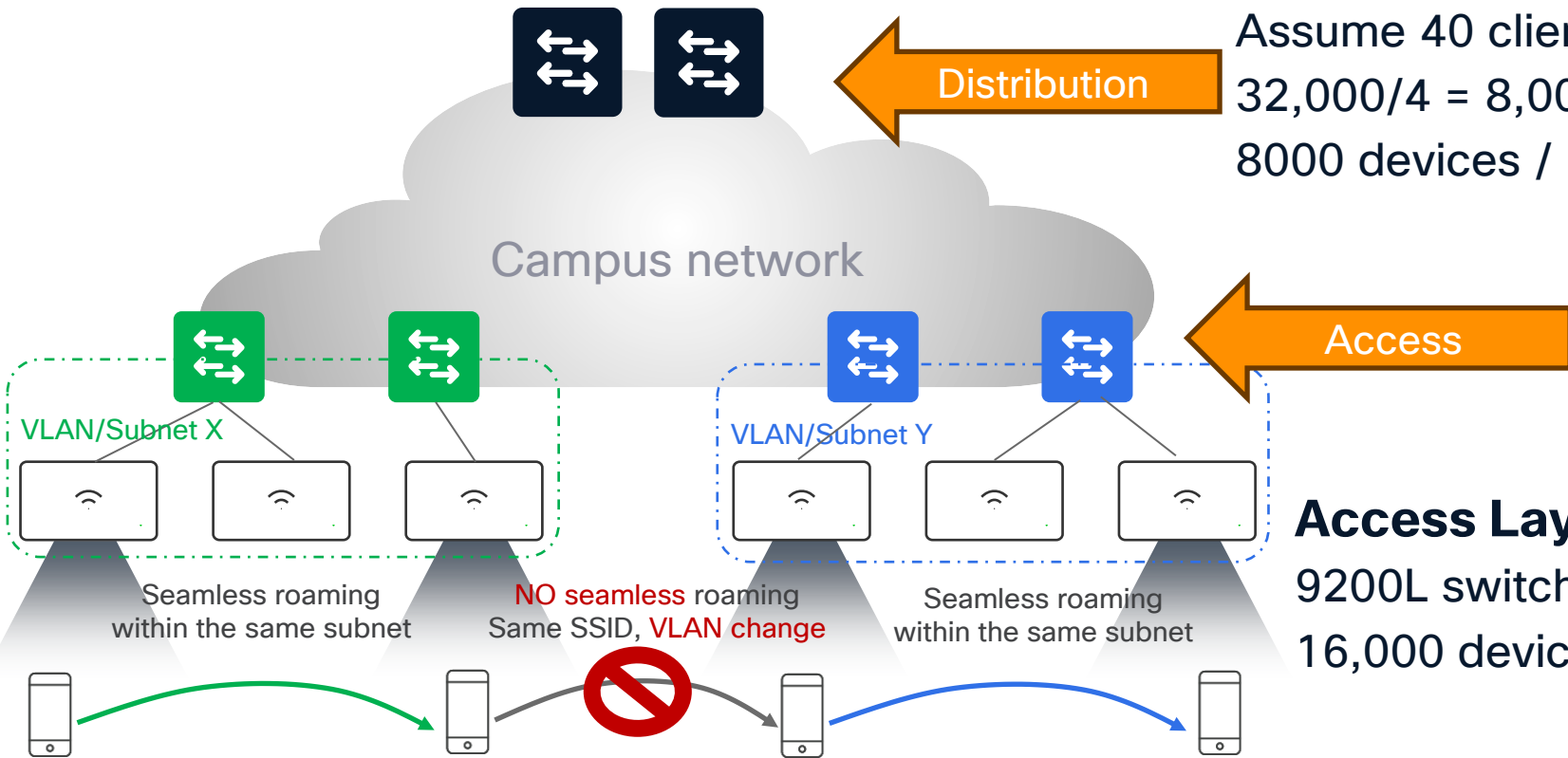
9300 switch supports 32,000 ARP entries

One device uses 1 x IPv4 + 3 x IPv6 = 4 entries

Assume 40 clients per AP

$32,000 / 4 = 8,000$ devices

$8000 \text{ devices} / 40 \text{ per AP} = \mathbf{200 \text{ APs}}$



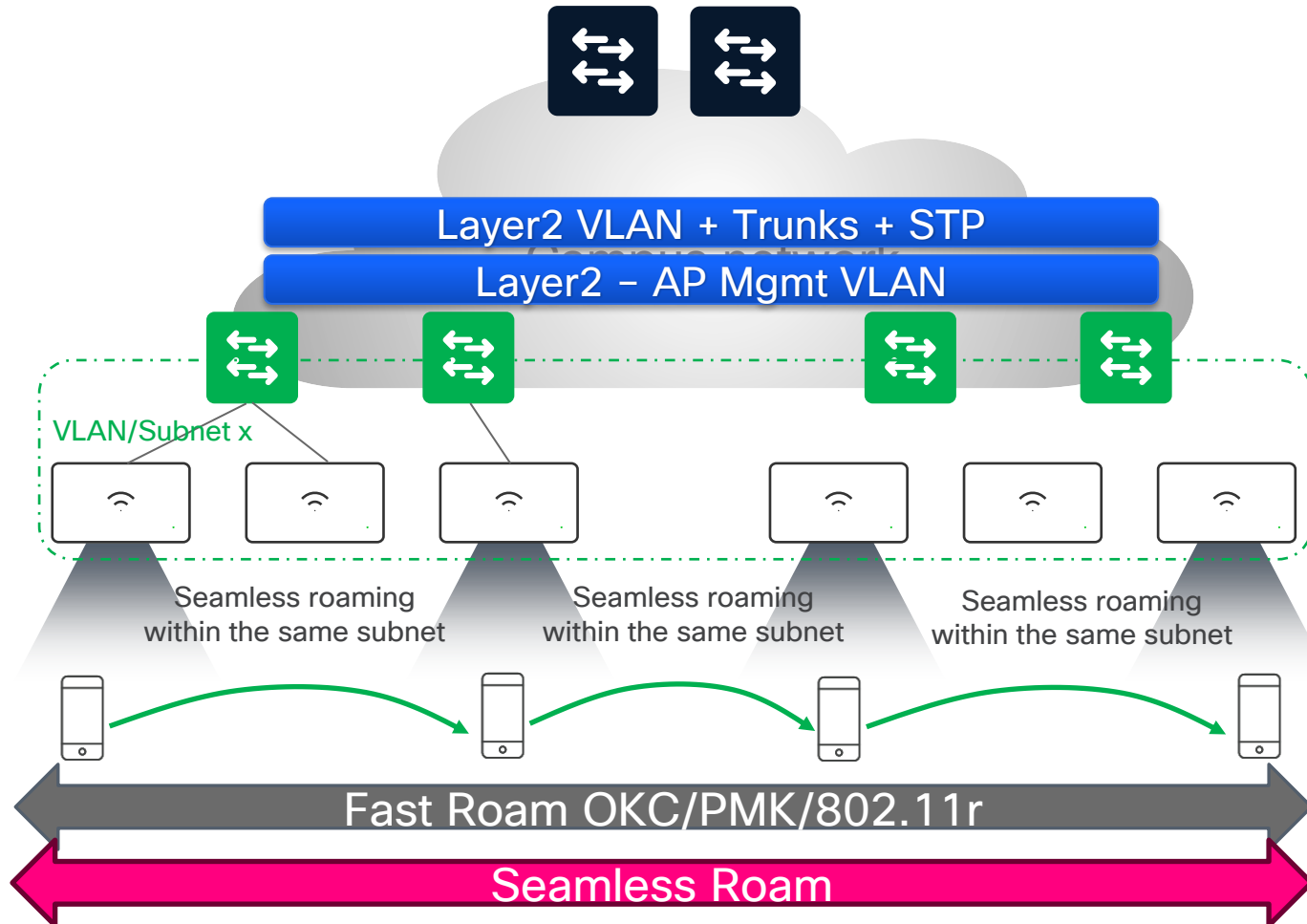
Access Layer

9200L switch supports 16,000 MAC entries

$16,000 \text{ devices} / 40 \text{ per AP} = \mathbf{400 \text{ APs}}$

Option1: VLANs

Easy to deploy but there are scalability and performance considerations.

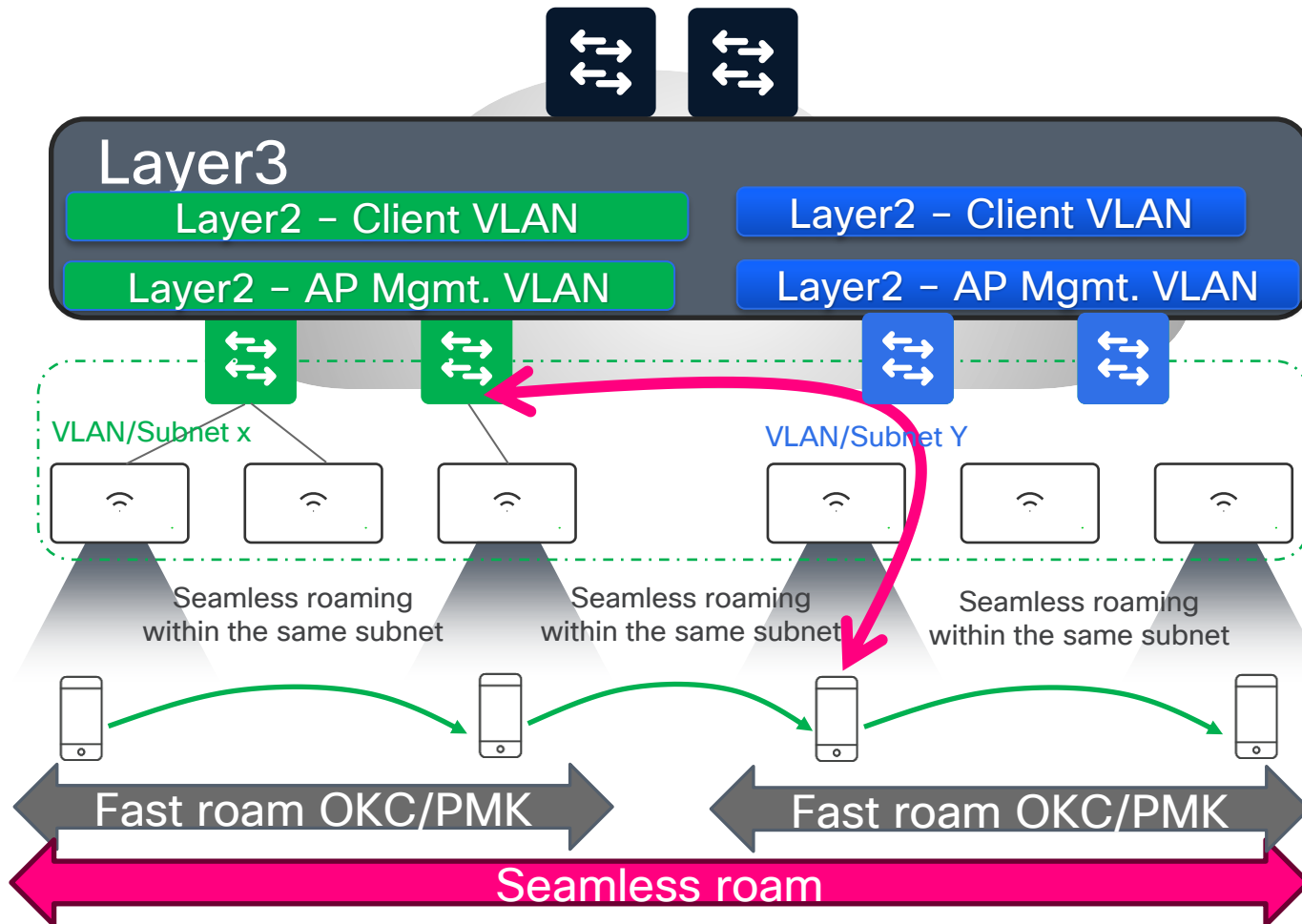


How can you create the L2 overlay?

- Spanning VLAN
- Need to consider the type of layer 2 and Layer 3 switches and their MAC/ARP tables size, the impact of spanning tree (SPT), the DHCP scope design, etc.
- How big can be the L2 broadcast domain? 200 APs, 8k clients as a reference
- To scale you need seamless roaming across L3 boundaries > L3 roaming
- Can simply just add VLAN to AP trunk

Option2: Distributed layer 3 roaming (DL3R)

Solves the seamless roaming problem but no 802.11r support (at scale).



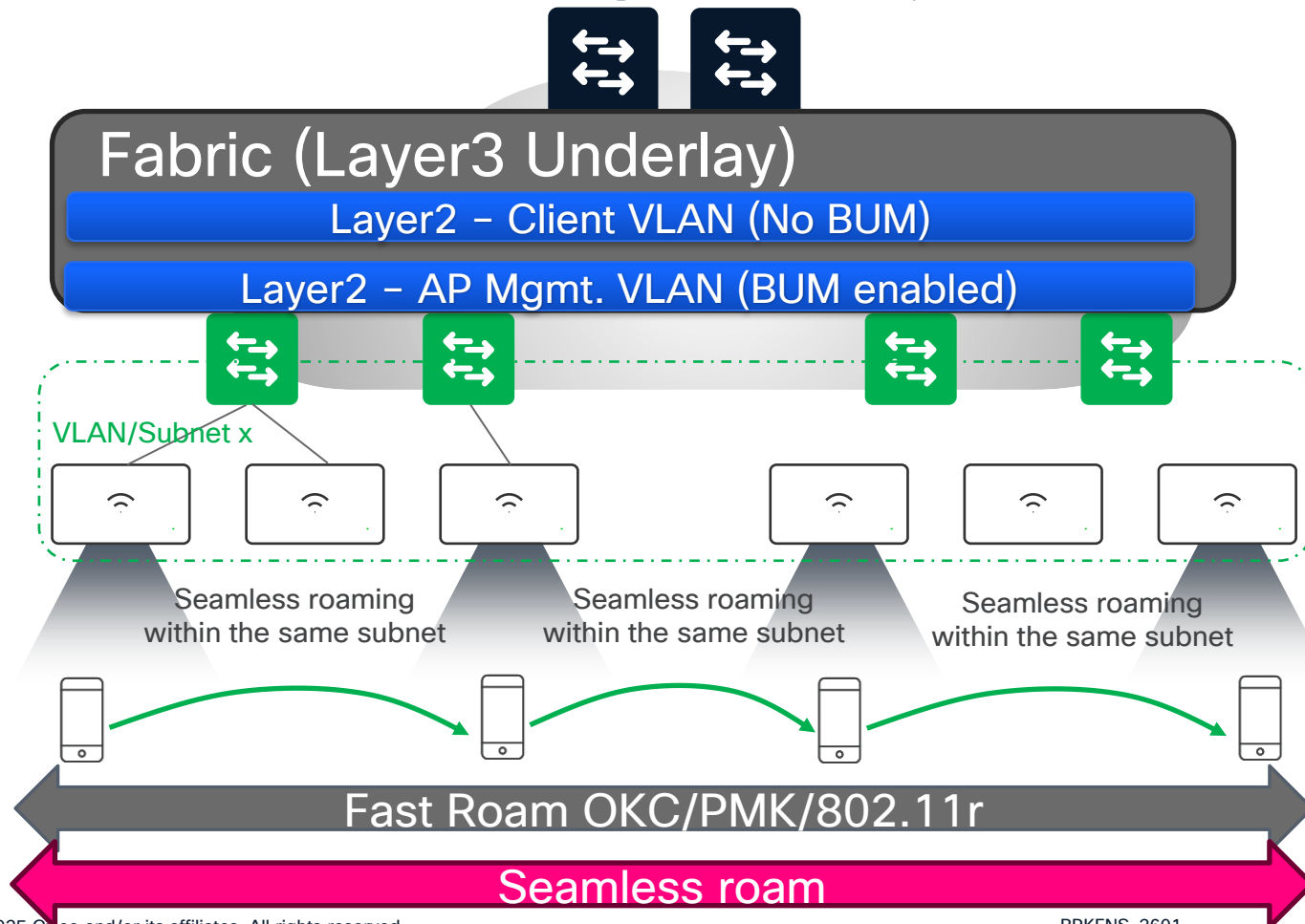
What can DL3R provide?

- AP management VLAN defines the fast-roaming boundary
- Client VLANs can be Layer3 separated
- Client will be tunneled back to anchor AP to keep their IP and roam is seamless
- Lack of 802.11r is a limiting factor

Option3: Fabric

Solves the seamless roaming and Fast Roaming with 802.11r but can introduce a little more latency (<100ms) due to Fabric.

Recommended for campus sites <1,000 APs



What can a Fabric provide?

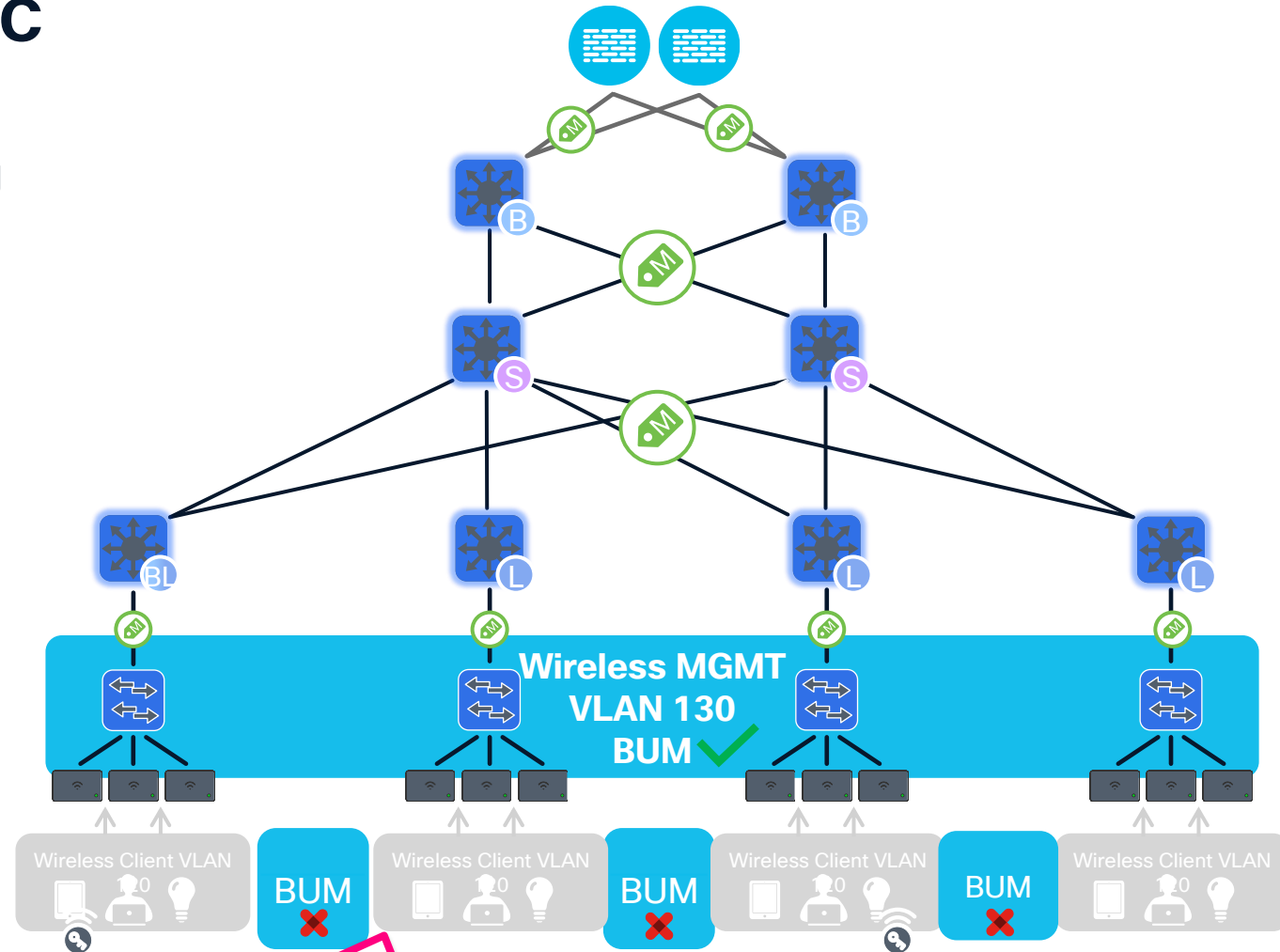
- Supports 802.11r Fast Roaming across Layer3 boundaries
- 1,000 AP limit per Meraki Network
- Enable Broadcast, Unknowns and Multicast (BUM) on Management VLAN which limits max AP to 200-300 AP per fast roaming domain
- Disable Broadcast, Unknown and Multicast on client VLAN
- <100ms latency will be introduced which is acceptable for video

Distributed wireless in fabric

Fabric support for distributed wireless

- **Fast Roaming Database:** APs maintain a roaming database within the management Layer 2 segment.
- **Fast Roaming Requirements:**
 1. Use broadcast flooding (DAG + BUM replication) on management VLAN for seamless roaming.
 2. PMK - Fast roam back to same AP
 3. OKC - non-standard Windows + Android
 4. Disable Dynamic Layer3 Roaming and enable 802.11r for Apple + Android
 5. Fabric roaming latency target < 100ms

Fast Roaming = Clients roaming quickly enough to support real time applications e.g. VoIP or Video



BUM: Broadcast, Unknown and Multicast

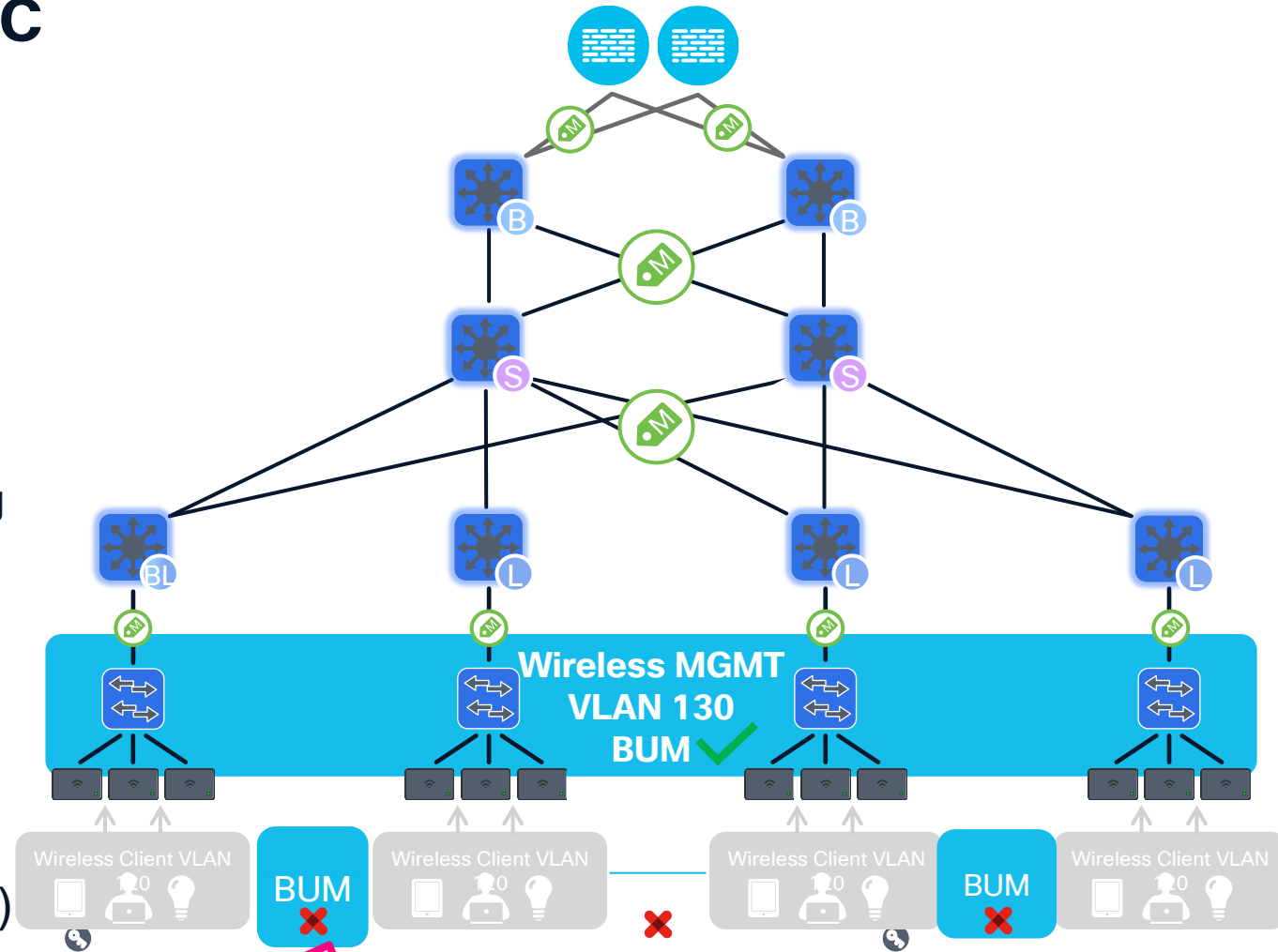
DAG: Default Anycast Gateway

BRKENS-2601

Distributed wireless in fabric

Fabric support for distributed wireless

- **Large Environments:** For many wireless clients, use anycast gateways and disable BUM traffic replication for wireless client segments.
- **Fast-Roaming Database:** APs maintain a roaming database within the management Layer 2 segment.
- **Client Association/Roaming:** When a client associates or roams, APs send "magic-ARP" packets to speed up endpoint discovery upstream.
- **SGT Propagation:** Security Group Tag (SGT/CMD) propagation to Layer 2 and forwarding over VXLAN (GPO) is performed inline by default.



BUM: Broadcast, Unknown and Multicast

DAG: Default Anycast Gateway

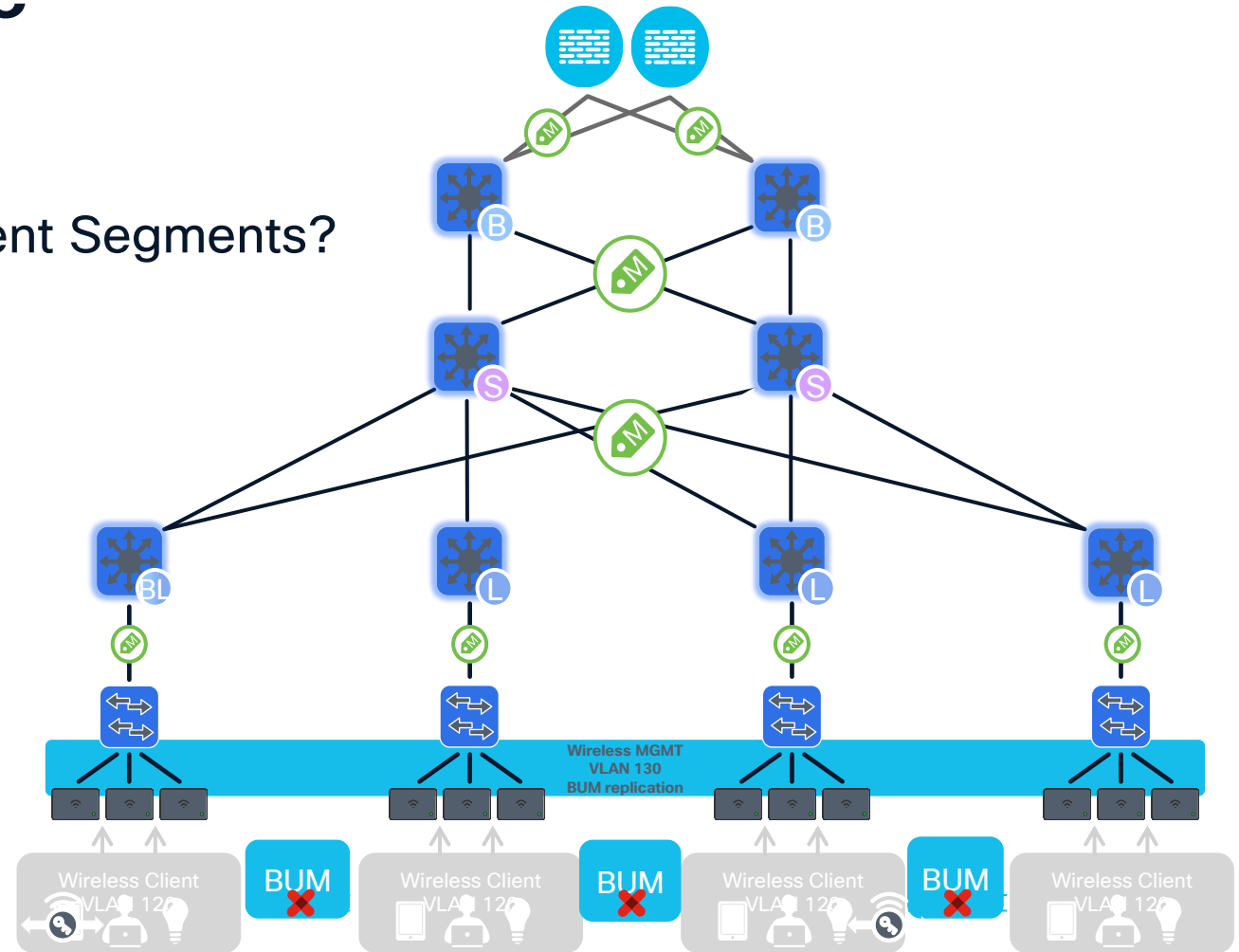
Distributed wireless in fabric

Fabric support for distributed wireless

Why disable BUM replication on Wireless Client Segments?

Disabling **BUM** replication on the client subnet will maintain L2 mobility in the topology and increase scaling by:

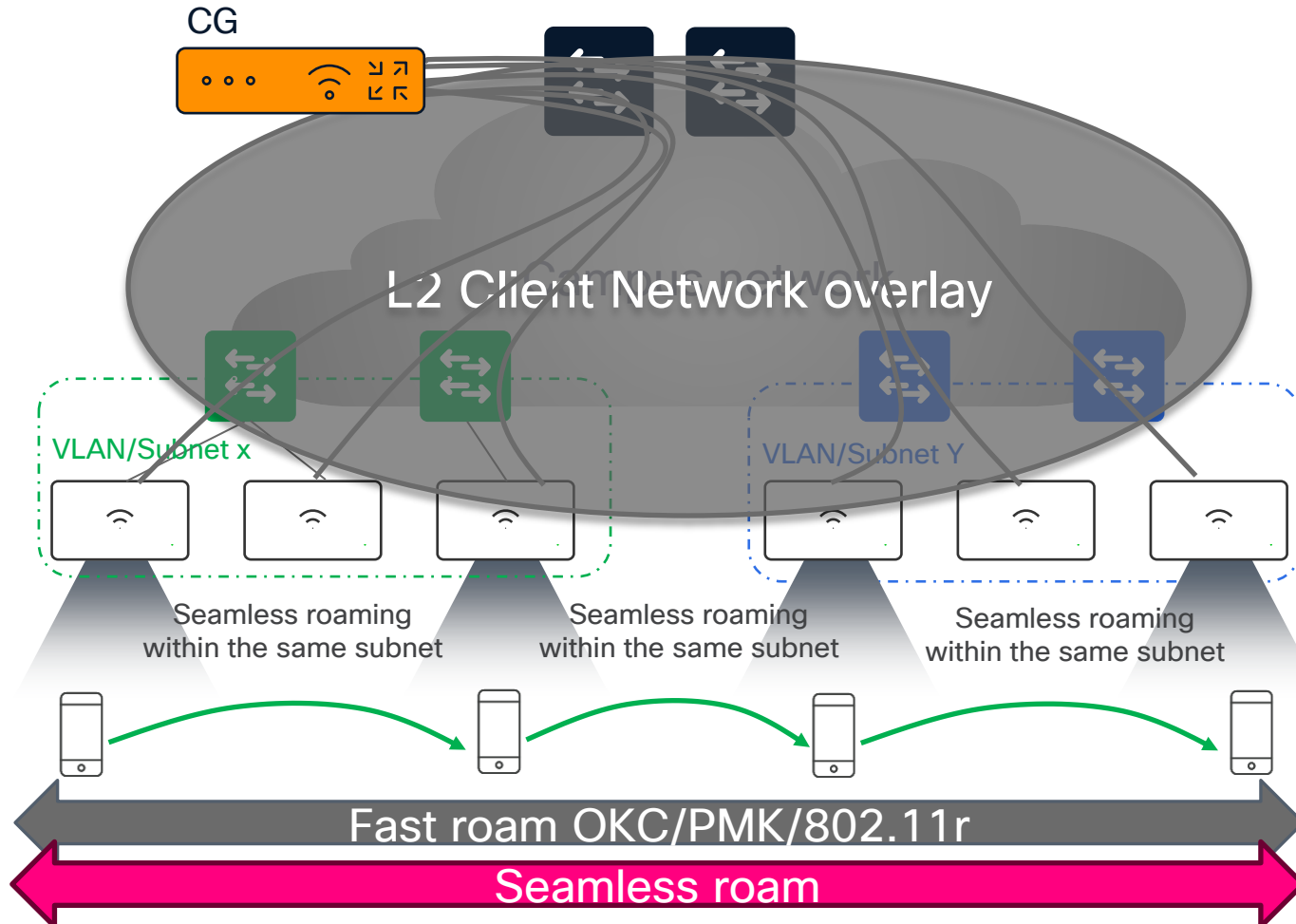
- Limiting impacts to wireless OTA performance in chatty TTL=1 Multicast / broadcast packet replication
- Reducing unnecessary downstream MAC learning and BUM processing



Option4: Campus gateway

Provides both seamless and fast roaming with 802.11r with its own fabric.

Recommended for large campus sites <5,000 APs



What can a Campus Gateway provide?

- Bigger scale for a large campus
- Supports 50k clients and 5k AP
- Seamless roaming + Fast roaming
- mDNS Gateway
- AAA proxy
- Bridge and tunnel SSID

Who should you consider a Campus Gateway?



Services @scale

- Roaming across L3 boundaries
- Fast Roaming across a large domain (> 200/300 APs)
- mDNS Gateway function



Wired Network Design

- Want to simplify VLAN/Subnet design at the access layer
- Want to simplify DHCP scope design
- Don't want to touch the underlay wired design



Policy

- Single policy (QoS, ACL, etc.) enforcement point for wireless traffic
- Single NAS to be configured in AAA server
- Simple way to handle BUM traffic



Performance

- Optimized for North-South traffic
- Centralized aggregator is not a bottleneck
- No latency impact for the “trombone” network effect

CG wireless in fabric

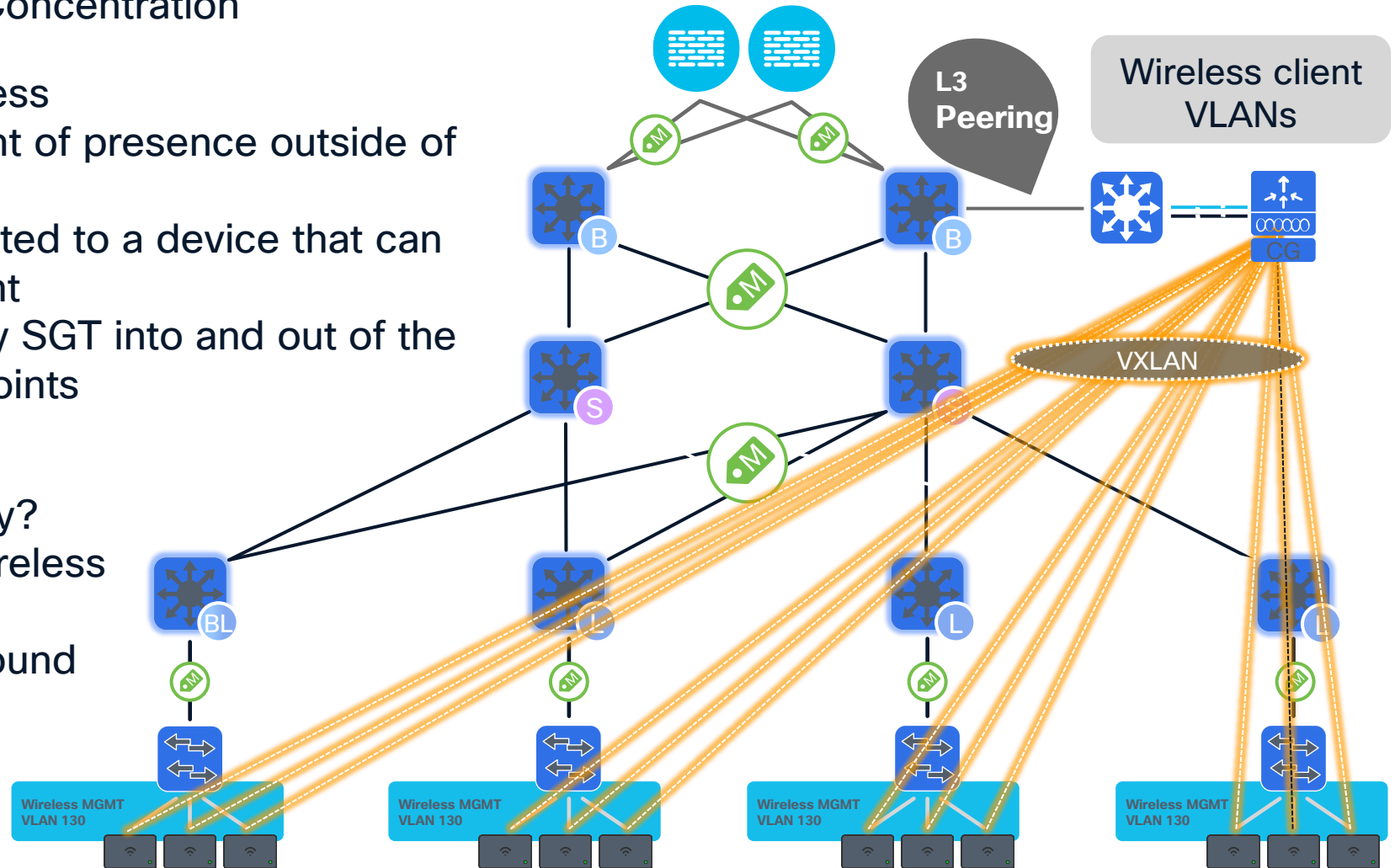
Campus Gateway Wireless Concentration

Fabric with centralized wireless

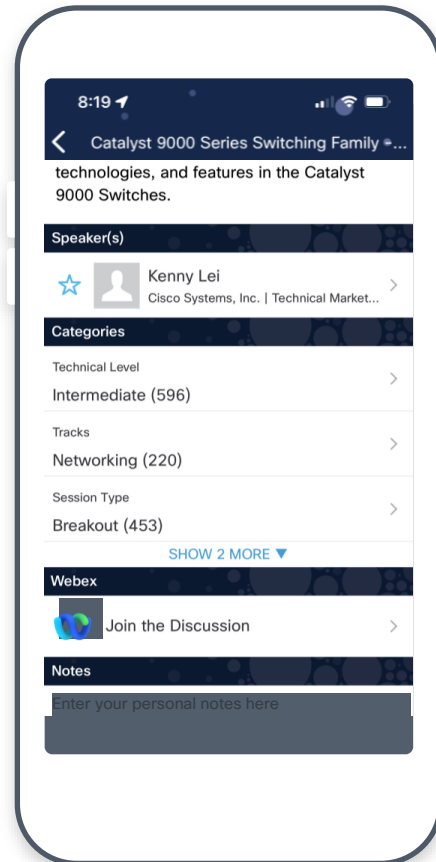
- Moves the endpoint's point of presence outside of the fabric
- The CG should be connected to a device that can support the endpoint count
- SGT propagation will carry SGT into and out of the fabric from wireless endpoints

Why use the campus gateway?

- Higher scale for campus wireless
- Seamless roaming
- Simplification of AP northbound switchport configurations

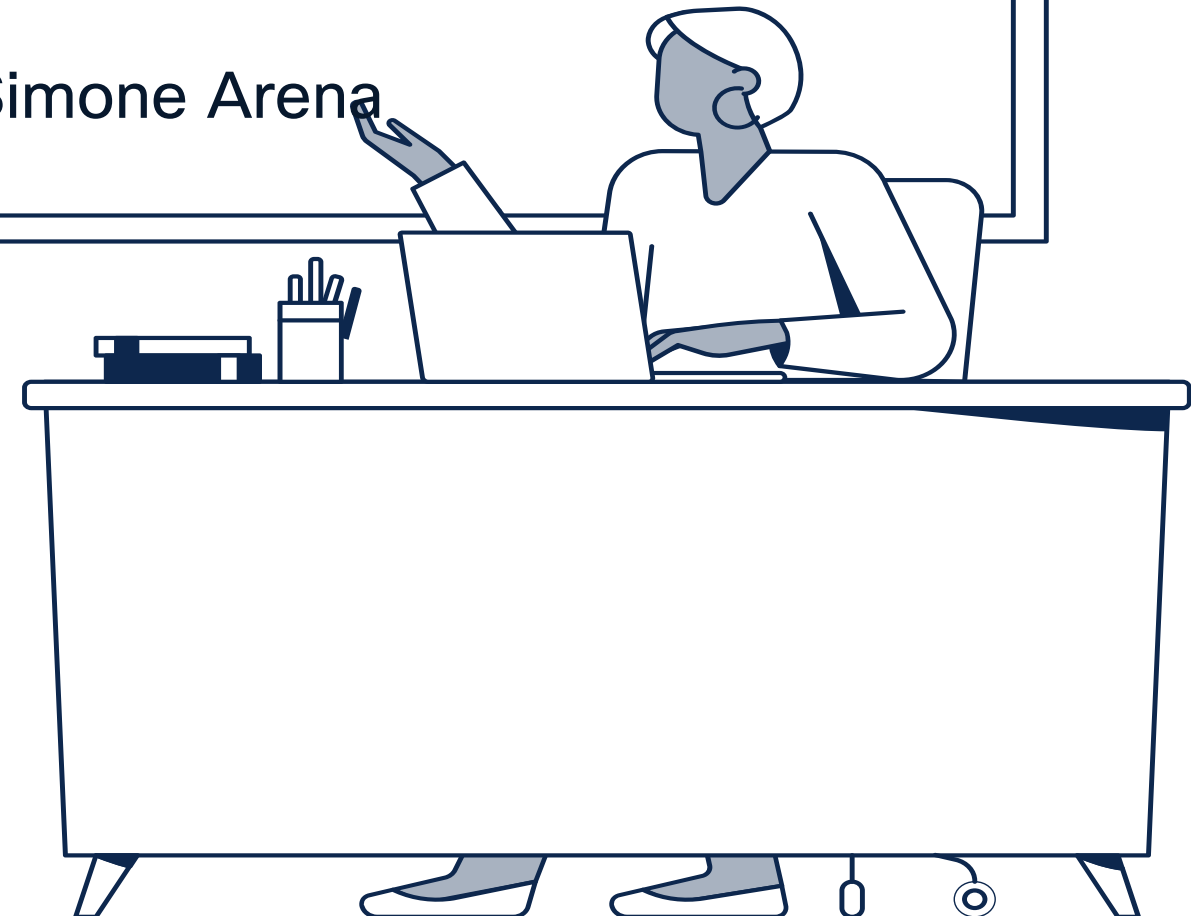


For more information

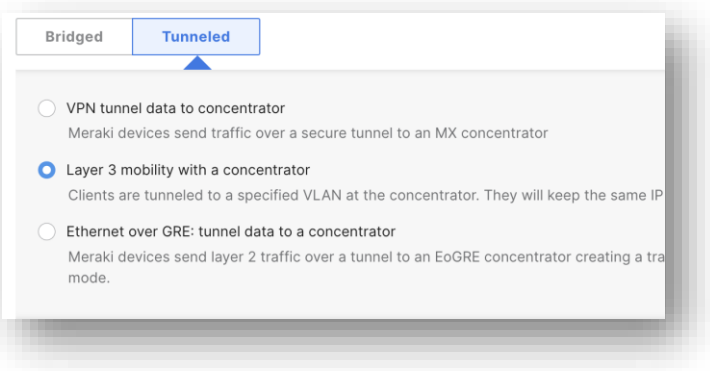


BRKEWN-2046: Design and Deploy Cisco Cloud Managed Enterprise Wireless Networks

Simone Arena



What about tunneled mode with MX?



For each SSID on an AP it consumes one VPN tunnel
Many customers use 3+ SSID

MX-Series

	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450	C8455-G2-MX
Maximum Site to Site VPN Tunnel Count	50	50	75	200	500	1,000	3,000	5,000	5,000
Recommended Maximum Site to Site VPN Tunnel Count	50	50	75	100	250	500	1,000	1,500	3,500

Not recommended for large campus deployments

Campus wireless roaming options

*OKC limited support (mainly Windows + Android)

VLAN

- Layer2 roams only
- Can use AP trunks for Layer2 roams
- STP convergence can be long
- Backup link blocking
- Large fault domain
- CAM/ARP limitation on the switch
- 802.11r – 50ms

DL3R

- Same AP management VLAN required
- Layer3 roaming
- No 802.11r
- Only OKC* + PMK (roam back) fast roams
- Slower roams due to RADIUS Auth latency (400ms+)

Fabric

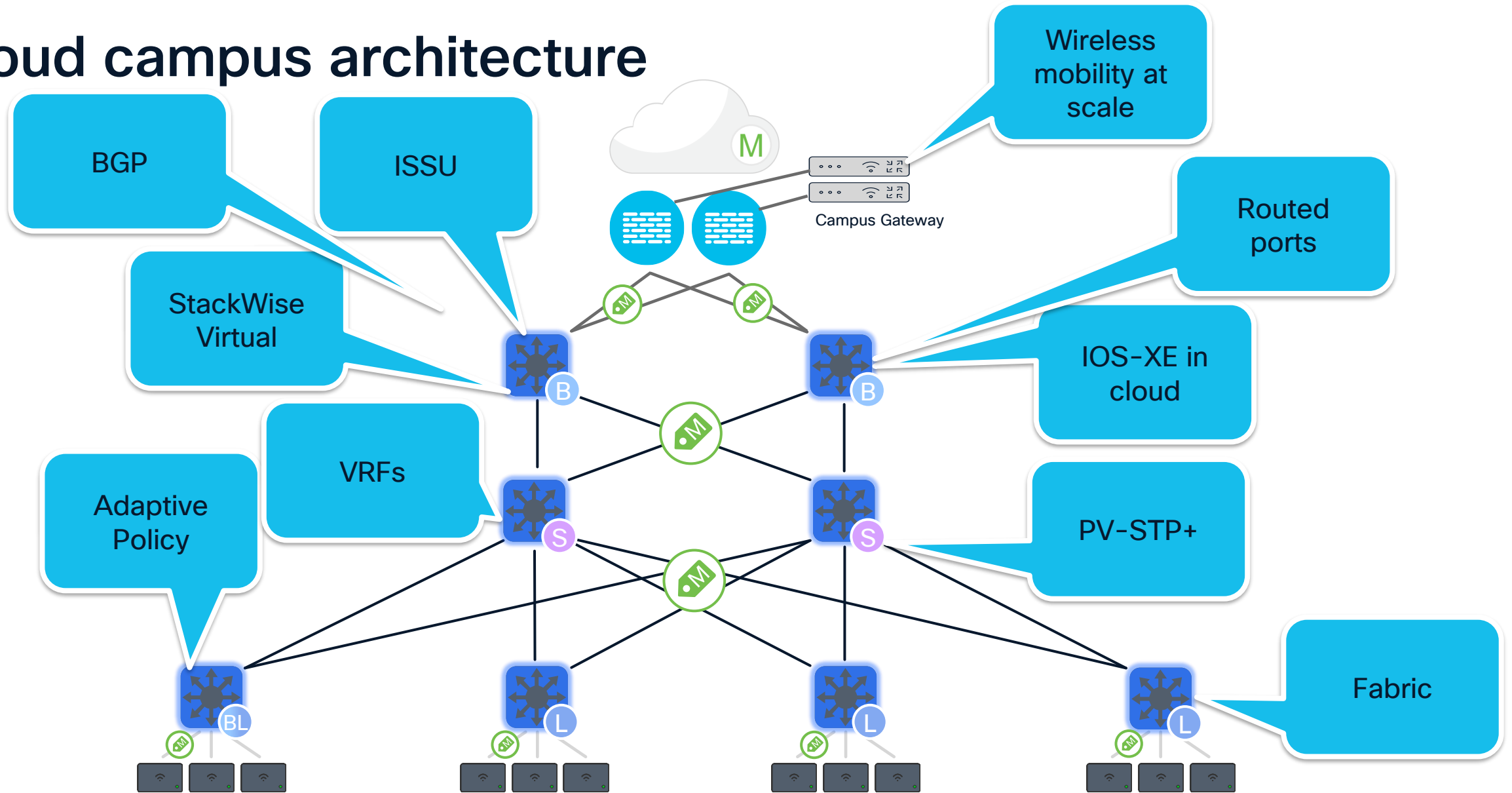
- Management VLAN required per fast roam domain
- 802.11r – 50ms
- Seamless roaming
- Fast roaming per < 200-300 AP
- Roaming latency <100ms
- 1,000 AP per network limit

CG

- No AP Management VLAN restrictions
- 802.11r – 50ms
- 5,000 AP
- Seamless roaming
- Fast Roaming

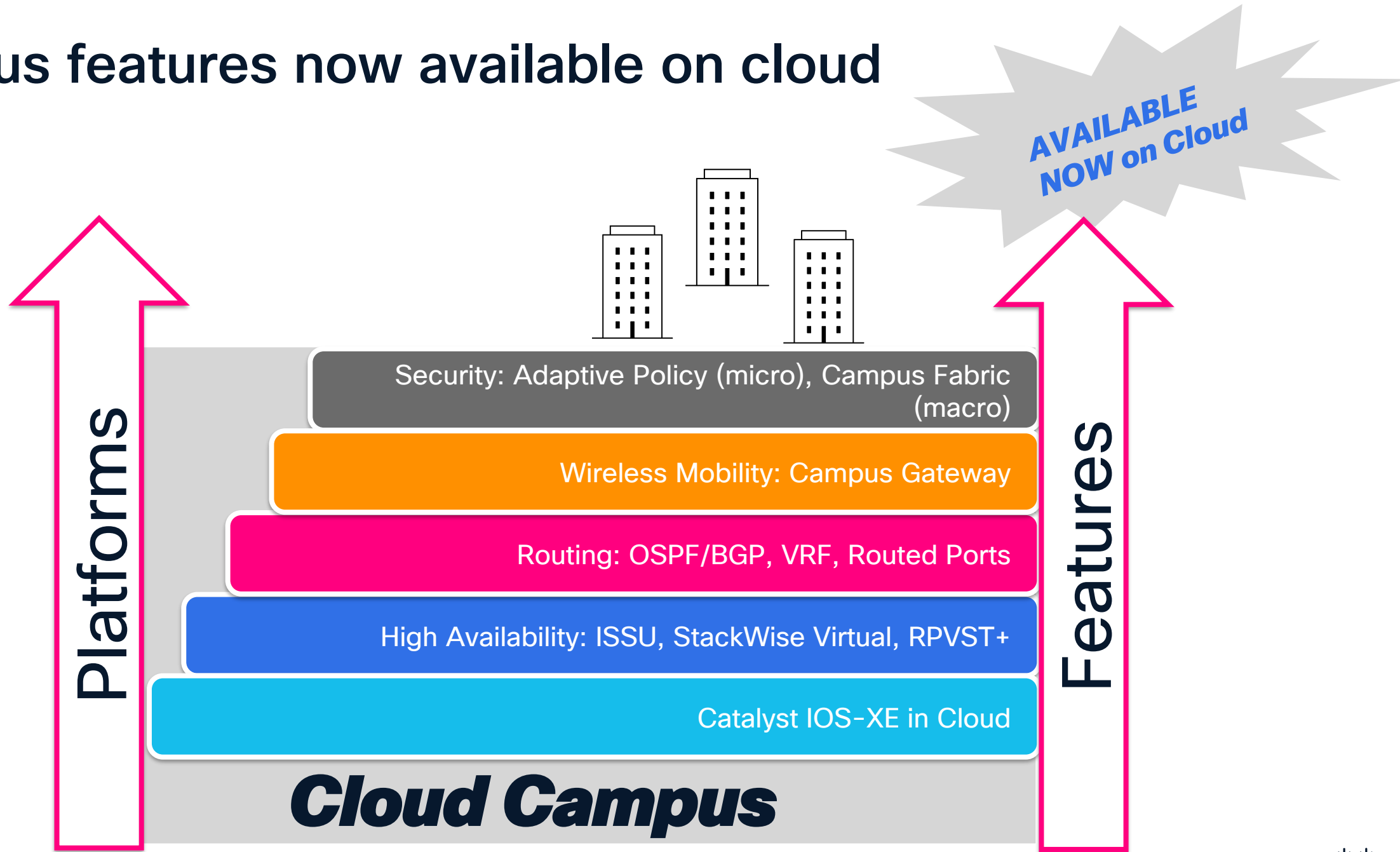
Campus cloud architecture summary

Cloud campus architecture



Full automation with a cloud management platform.

Campus features now available on cloud



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !



Cloud-managed Enterprise Switching

IOS XE 17.18.1

Advanced Routing

Routed Ports

Loop-free Routed Access

VRF Lite

Scalable Macro Segmentation

BGP

Flexible, Open Dynamic Routing

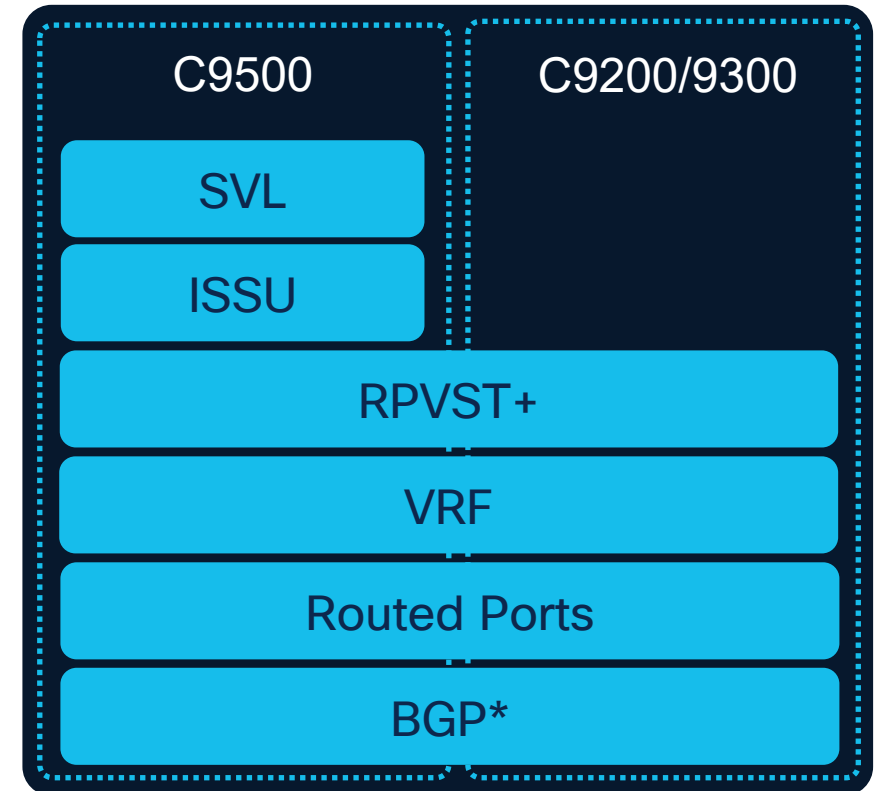
High-Availability

Rapid PVST+

Enhanced L2 Loop Prevention

StackWise Virtual (SVL)
ISSU

Sub-second downtime
firmware upgrades



*BGP supports on C9200CX, MS390, C9300 and C9500