Introduction to
Campus Network Design and Multilayer Architectures

Jakub Matela - Technical Solutions Architect

BRKENS-1500

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install 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 February 28, 2025.

Who am I?

Jakub Matela

Technical Solutions Architect

jamatela@cisco.com

I'm a Technical Solutions Architect (TSA) at Cisco, part of the EMEA Enterprise Networking team. I joined Cisco in 2016.

Since 2021, I have been leading Cisco's Enterprise Networking Switching, Software-Defined Access, and Catalyst Center technologies in EMEA Sales.

I am dedicated to enabling the field, partners, and customers in their transition to intent-based networking, leveraging Software-Defined Access and Cisco Catalyst Center.

Based in Krakow, Poland, I graduated from AGH University of Science and Technology with a Master's in Electrical Engineering and hold a CCIE in Enterprise Infrastructure.

What this session is NOT

This session is NOT intended as a Deep-Dive or CVD!

The goal is to understand *basic reasons* & *rationale* for each Campus design ☺

Please also review:

- TBD

Other Related Sessions:

- Designing Highly Available Networks using Catalyst 9000 Series Switches - BRKENS-2095
- Enterprise Campus Design: Multilayer Architectures and Design Principles - BRKCRS-2031
- Building for the Campus of the Future - BRKENS-2599

www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

Campus Architecture – Series Agenda

Design Fundamentals

1. Campus Design Fundamentals
2. Campus Design Principles
3. Campus Foundational Services

Design Considerations

4. Platform Design Considerations
5. Campus Design Best Practices
6. Campus integration with other PINs

Session Agenda - BRKENS-1500

Design Fundamentals

1 Campus Design Fundamentals

- What is “Campus”?
- Place in Network (PIN)

2 Campus Design Principles

- Multi-Layer Model
  - Hierarchical Design
- Access Layer
- Distribution Layer
- Core Layer

3 Campus Foundational Services

- Layer 1 physical layer & links
- Layer 2 switching protocols
- Layer 3 routing protocols

Design Considerations

4 Platform Design Considerations

- Chassis Considerations (Performance)
- Cabling Considerations (Speed)
- Feature Considerations (Scale)
  - L2 Features
  - L3 Features
  - Quality of Service (QoS)

5 Campus Design Best Practices

- LAN High Availability
- LAN Security
- Virtual Networking

Session Agenda - BRKENS-2500

Design Fundamentals

1 Campus Design Fundamentals

- What is “Campus”?
- Place in Network (PIN)

2 Campus Design Principles

- Multi-Layer Model
  - Hierarchical Design
  - 1,2,3 & 4+ Tiers
- Access Layer
  - Baseline, Extended Access, Routed Access
- Distribution Layer
  - Baseline, Collapsed Core, Collapsed Distro
- Core Layer
  - Baseline, Interconnect, Edge

3 Campus Foundational Services

- Layer 1 physical layer & links
- Layer 2 switching protocols
- Layer 3 routing protocols
- ECMP, LAG & Load balancing

Design Considerations

4 Platform Design Considerations

- Chassis Considerations (Capacity)
- Cabling Considerations (Speed)
- Feature Considerations (Scale)
  - L2 (Unicast & Multicast)
  - L3 (Unicast & Multicast)
  - Security (AAA & ACL)
  - Quality of Service (QoS)
  - NetFlow (AVC & XDR)

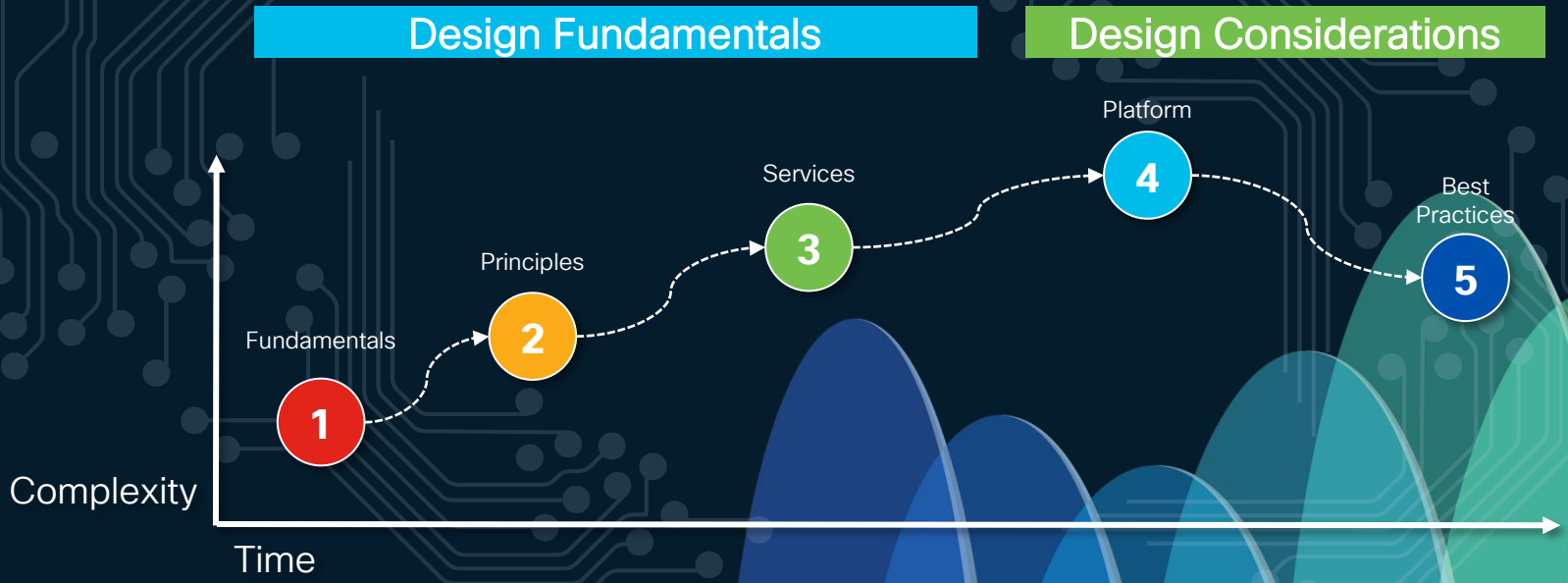
5 Campus Design Best Practices

- LAN High Availability
  - SSO/NSF, Stack/SVL, mLAG, FHRP
- LAN Security
  - NAC, Access Control, FHS, ZTNA
- Virtual Networking
  - MPLS, LISP, EVPN

6 Campus integration with other PINs

- Wireless Integration
- Firewall Integration

Session Agenda

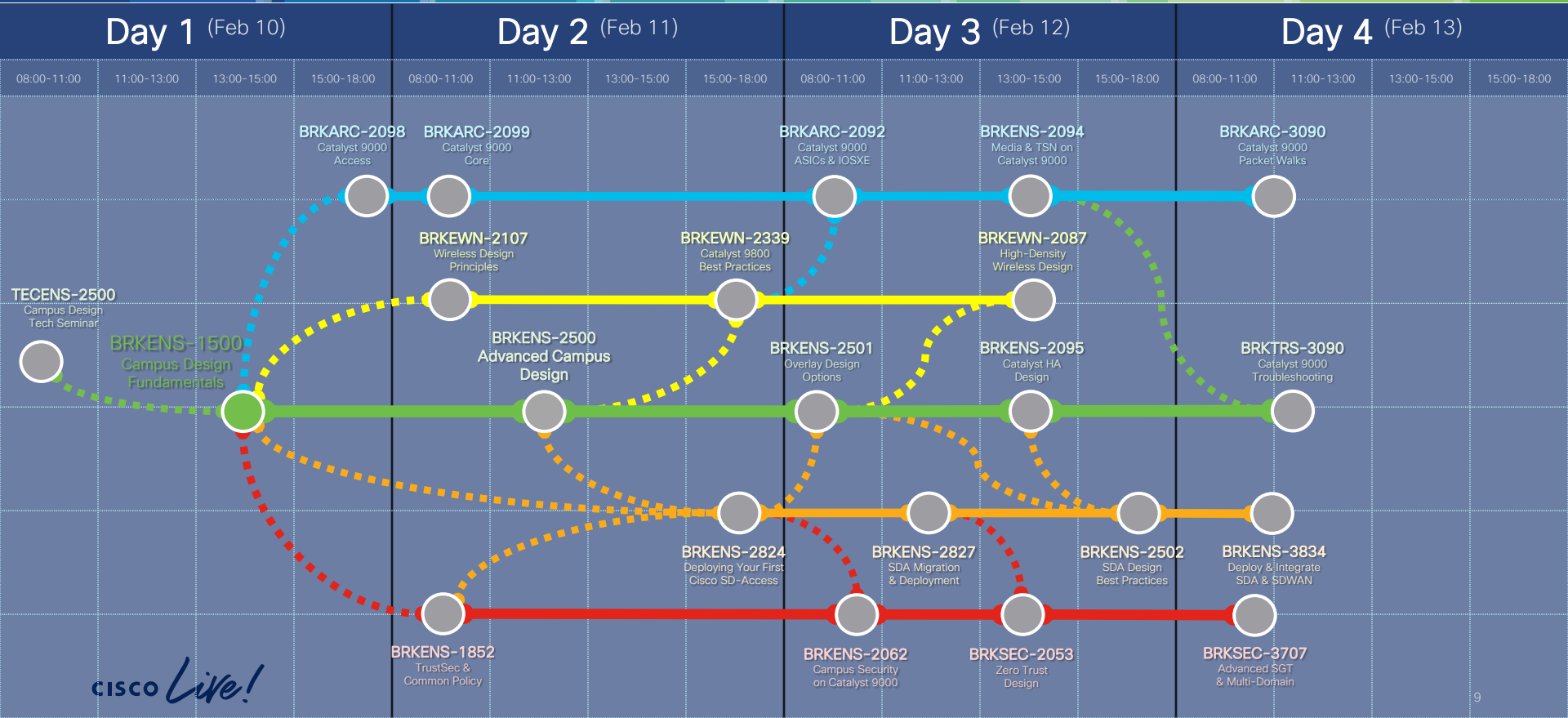


Cisco Campus Architecture

Cisco Live Amsterdam 2025 - Session Map

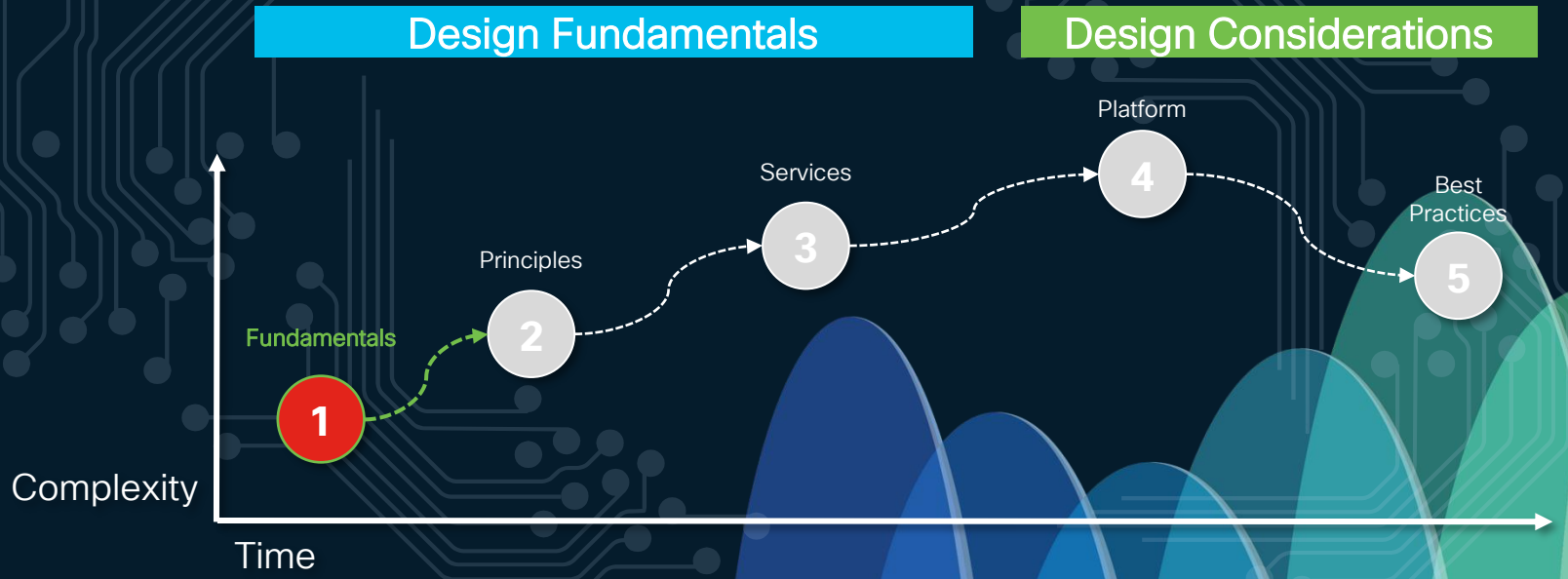
Sessions are available Online @ CiscoLive.com

You Are Here



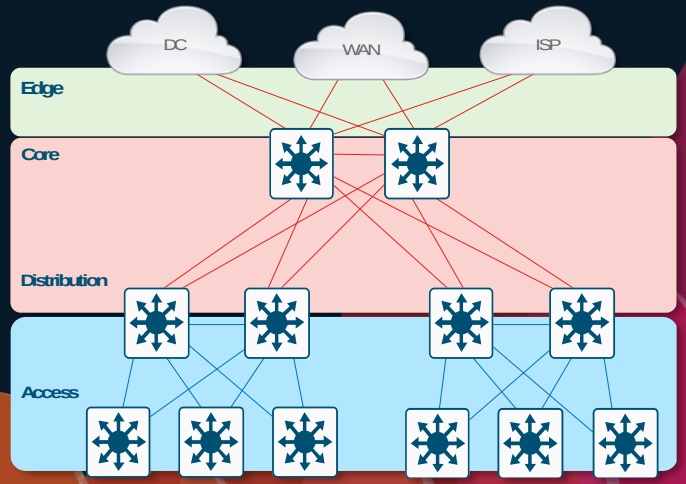
cisco Live!

Session Agenda



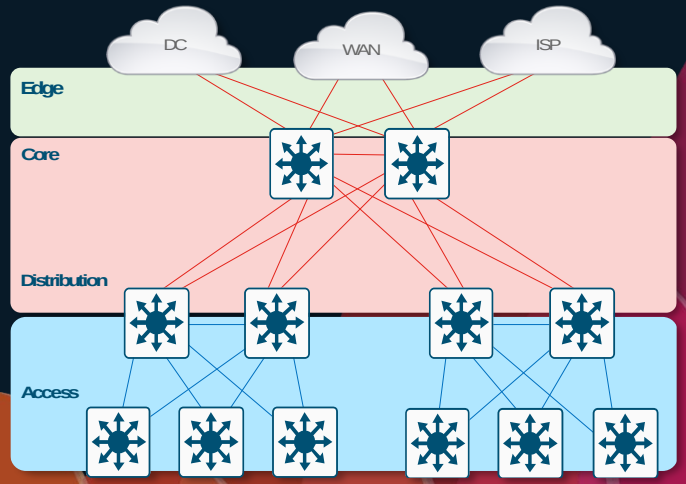
Design Fundamentals

- **What is “Campus”?**
- **Place in Network** (PIN)



Design Fundamentals

- **What is "Campus"?**
- **Place in Network** (PIN)



What is a “Campus”?

A basic **Merriam-Webster** definition of a Campus is:

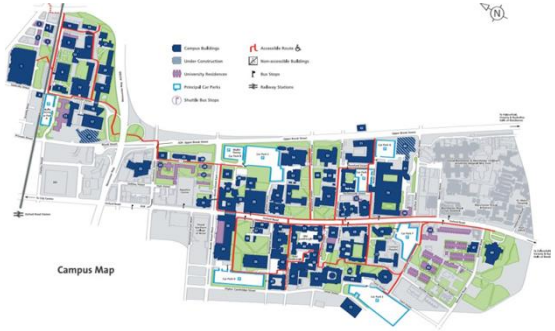
A group of one or more buildings, and surrounding grounds, where people and their belongings work together.

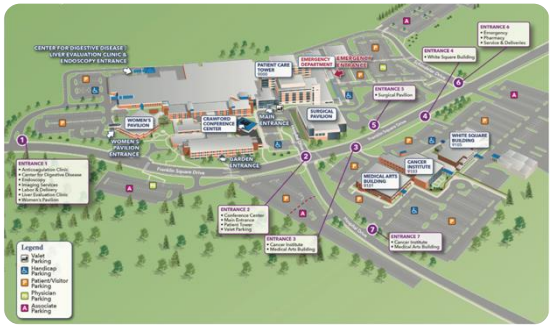
Common examples are **Corporate** & **Government Offices**, **Hospitals**, **Schools**, **Transportation**, **Manufacturing** & more.

Using this – it’s clear a Campus Network is focused on:

- ☑ **People** (*Users, Vendors, etc.*)
- ☑ **People's devices** (*PCs, Phones, Printers, etc.*)
- ☑ **Local geographic area** (*LAN, WLAN or MAN, etc.*)
- ☑ **Access other domains** (*WAN, ISP, DC & Cloud, etc.*)

This includes **many different network technology areas** (*Wired, Wireless, Security, QoS, Management, etc.*)





Campus is focused on **User Access**

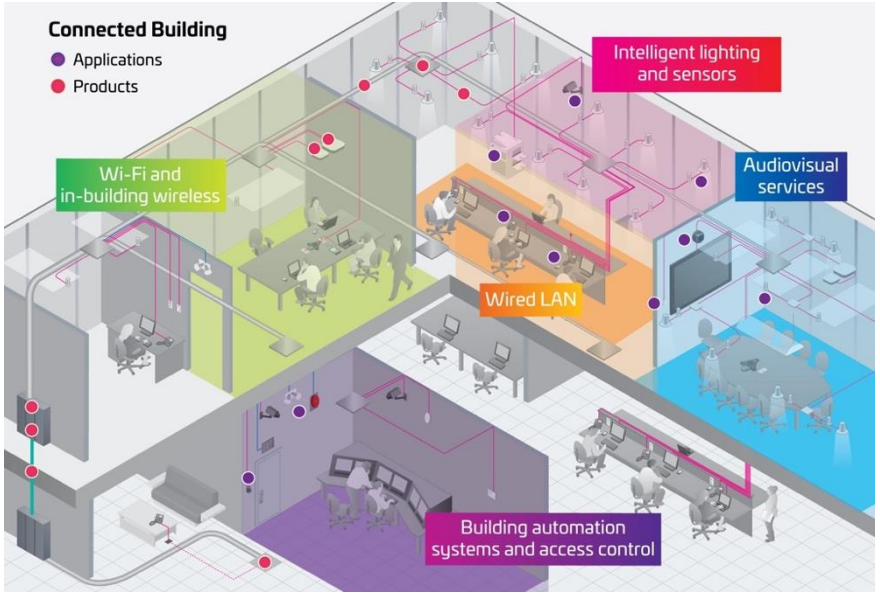
Campus = Geography

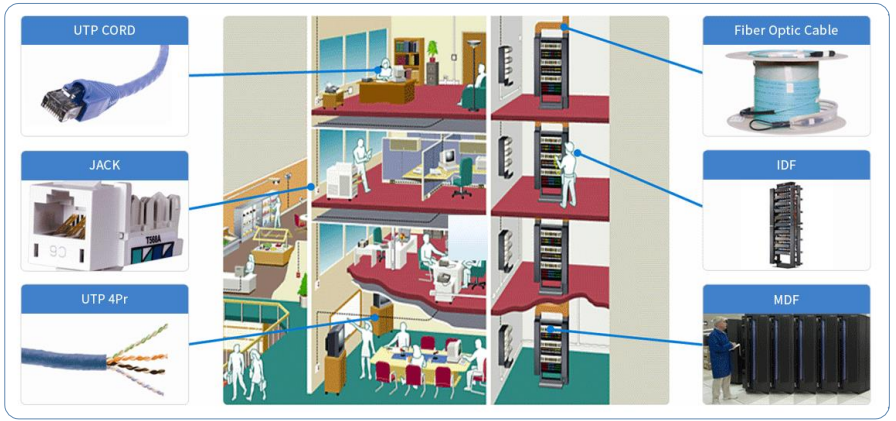
Buildings are spread out. Multiple floors per building

www.cisco.com/c/en/us/solutions/cisco-on-cisco/enterprise-networks.html

Campus Networks

Building MDF/IDF & Wiring Closets





MDF = Main Distribution Framework (Core & Edge)
IDF = Intermediate Distribution Framework (Distro & Access)

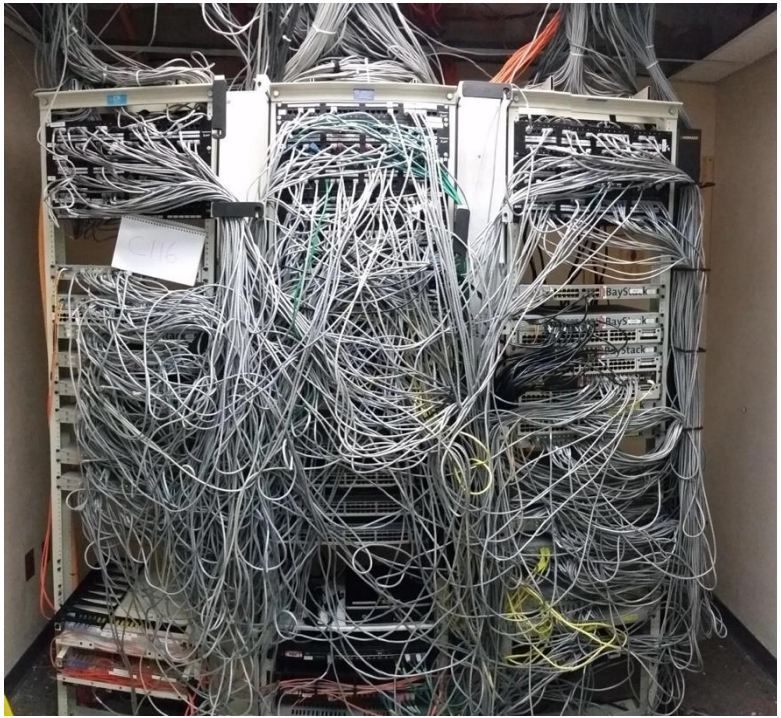
www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html

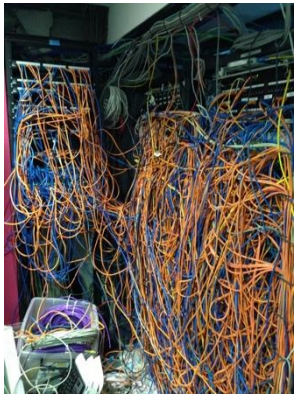
Campus ≠ Data-Center

One or few large buildings nearby. Usually a single floor.

www.cisco.com/c/en/us/solutions/cisco-on-cisco/enterprise-networks.html

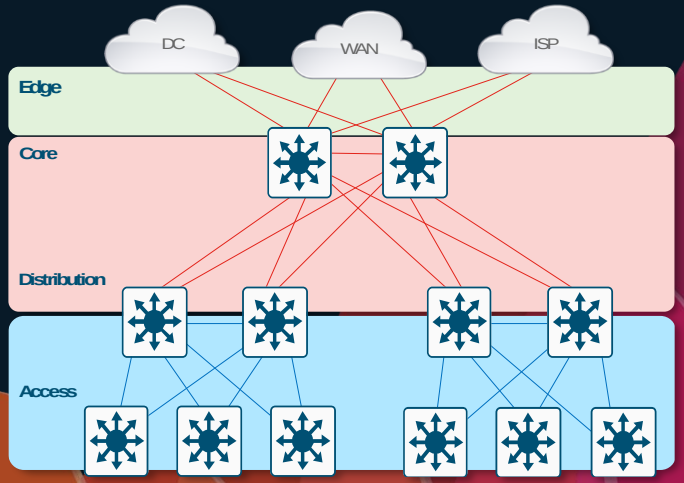
Campus Networks - Real Life



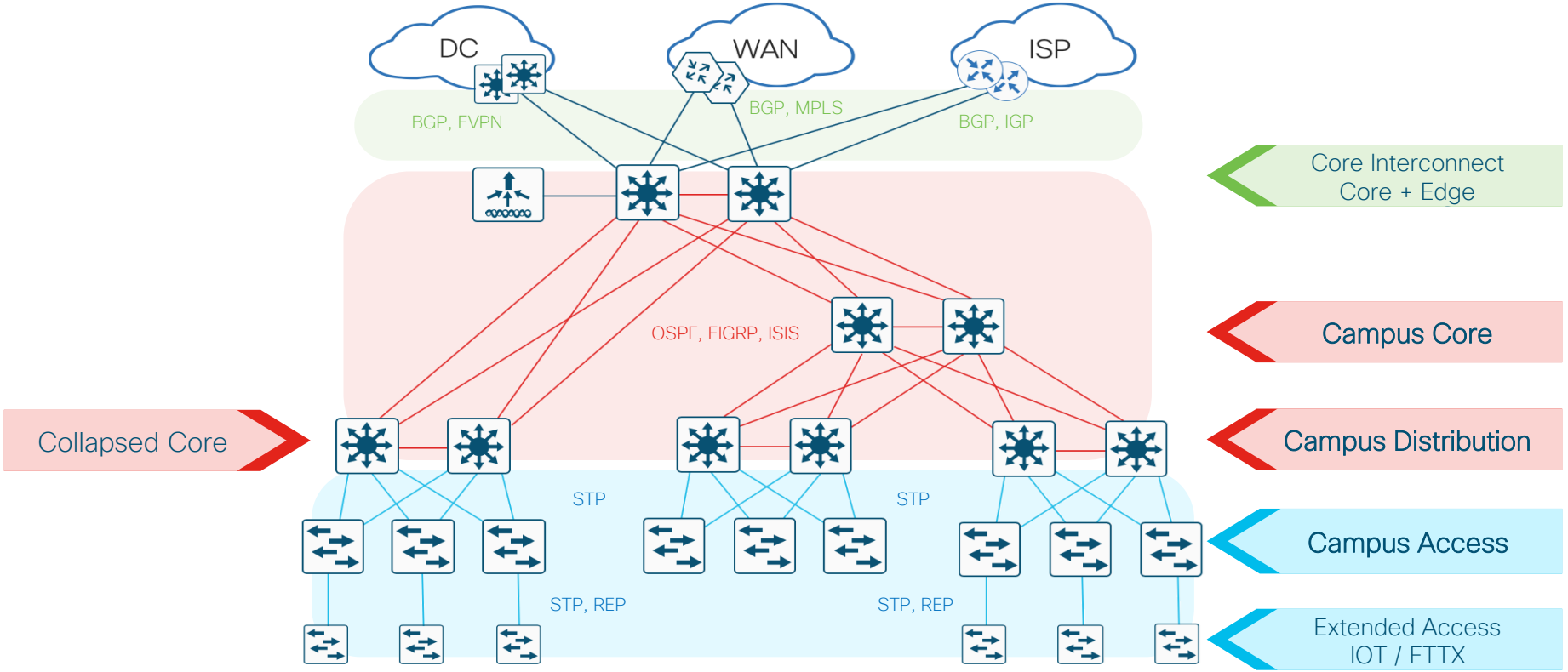


Design Fundamentals

- **What is "Campus"?**
- **Place in Network** (PIN)



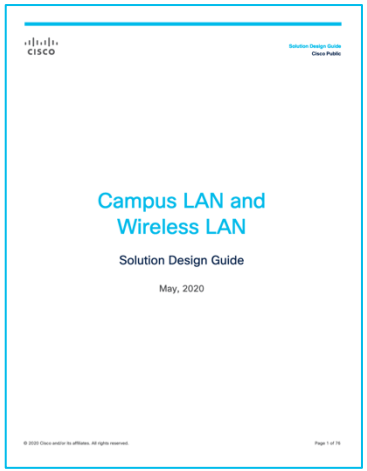
Campus PINs & Topology

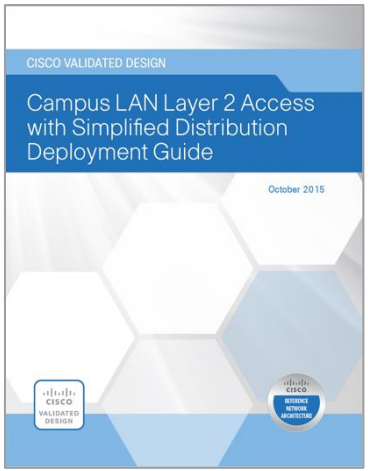


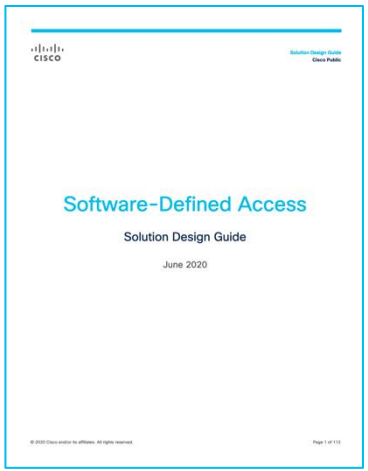
Where do I start?

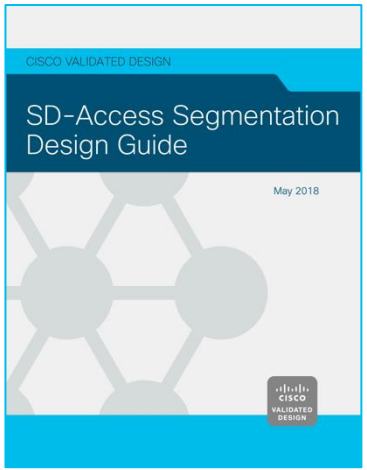
Cisco Validated Designs

...provide a framework for design and deployment guidance based on common use cases.





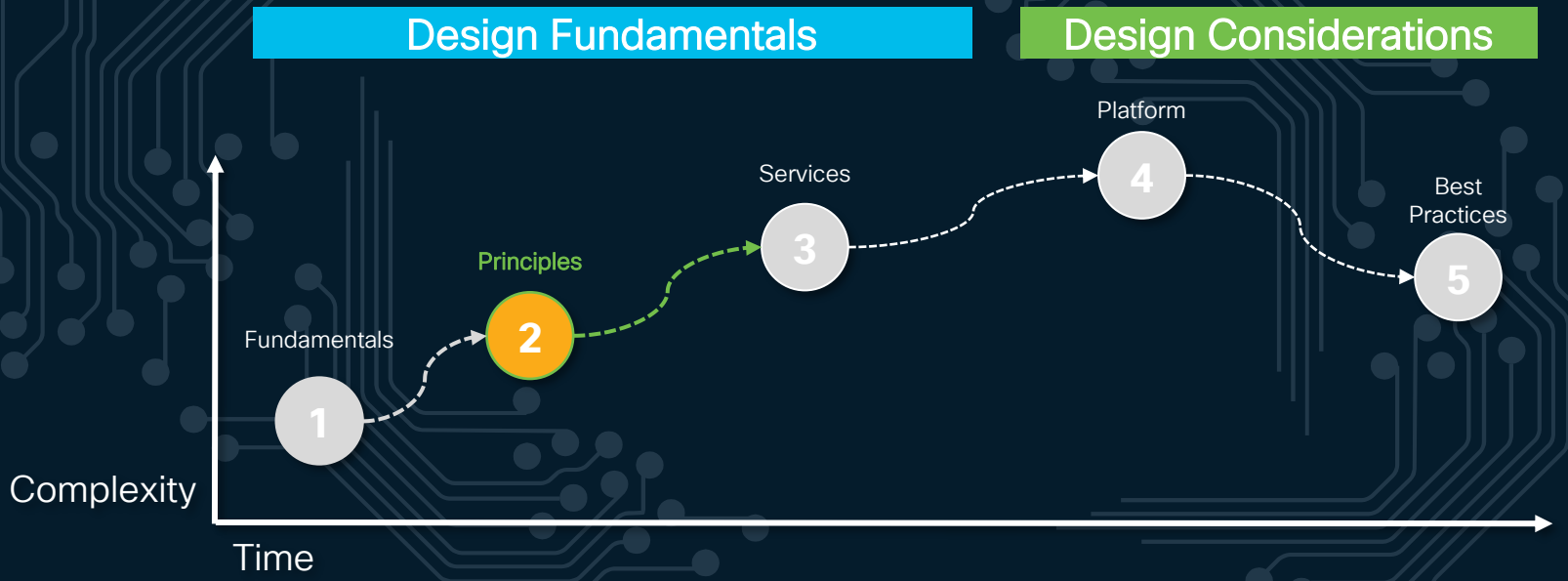




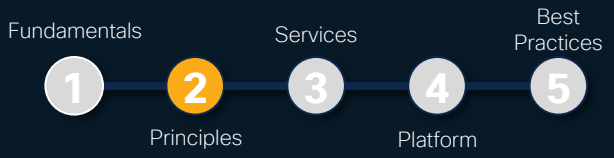
Design Zone: www.cisco.com/go/designzone

Design Zone for Campus: www.cisco.com/go/cvd/campus

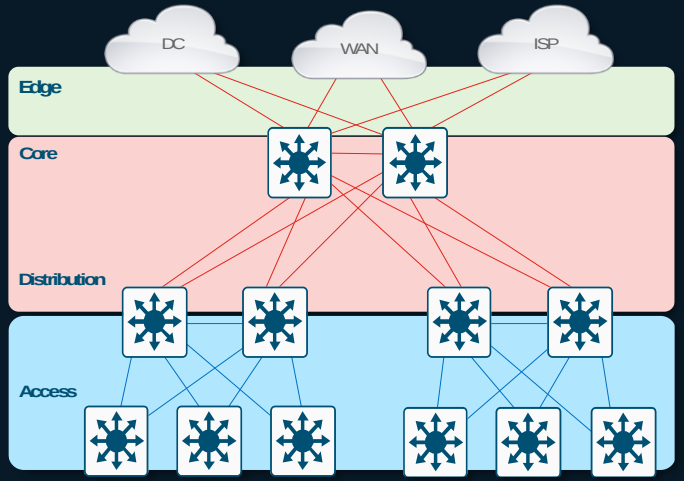
Session Agenda



Design Principles

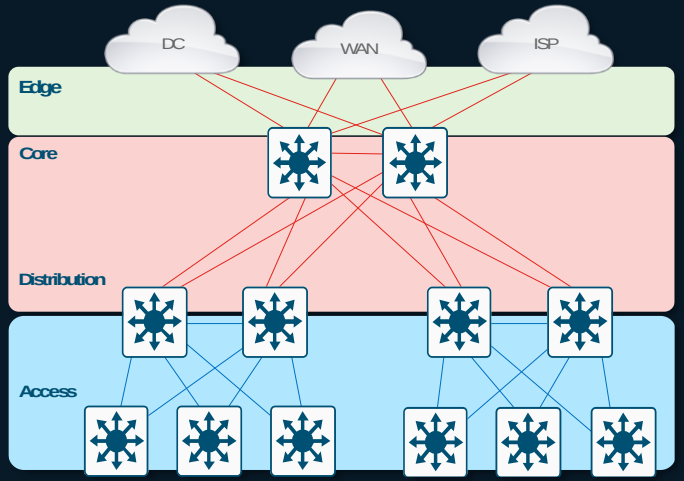


- **Multi-Layer Model**
- **Access Layer**
- **Distribution Layer**
- **Core Layer**

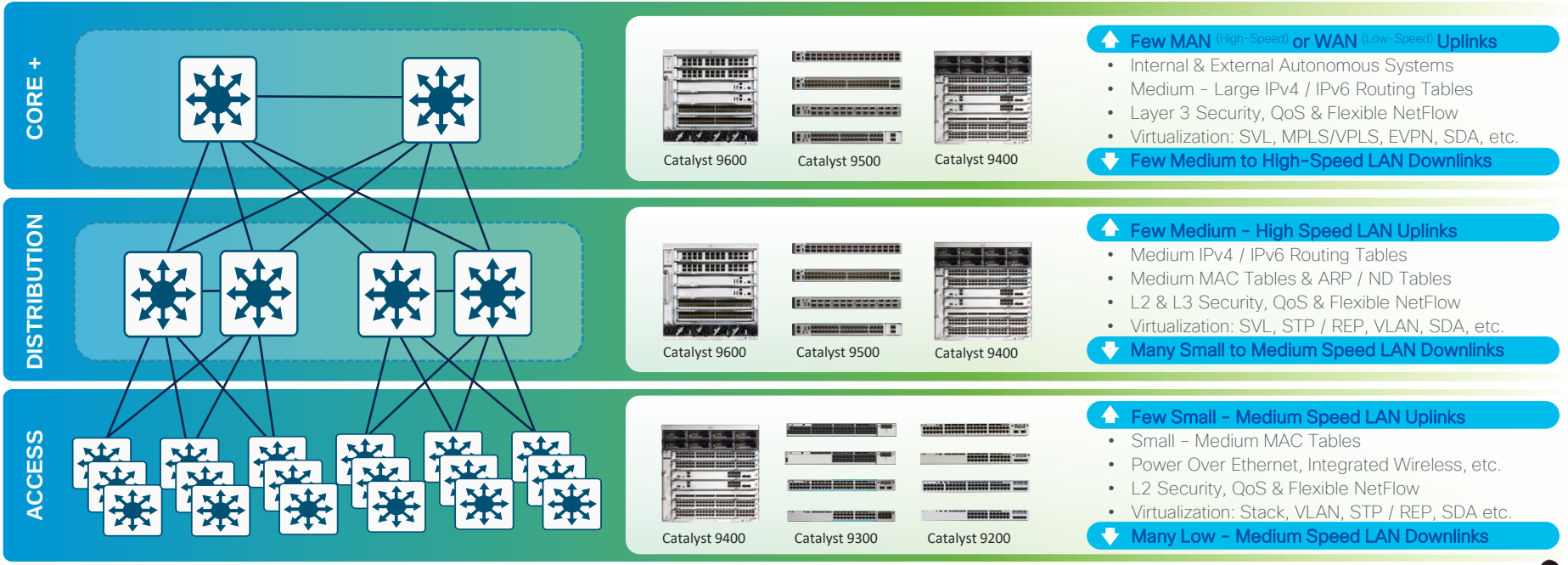


Design Principles

- **Multi-Layer Model**
  - **Campus Multi-Layer**
  - **Hierarchical Design**
- **Access Layer**
- **Distribution Layer**
- **Core Layer**



Campus Multi-Layer Model



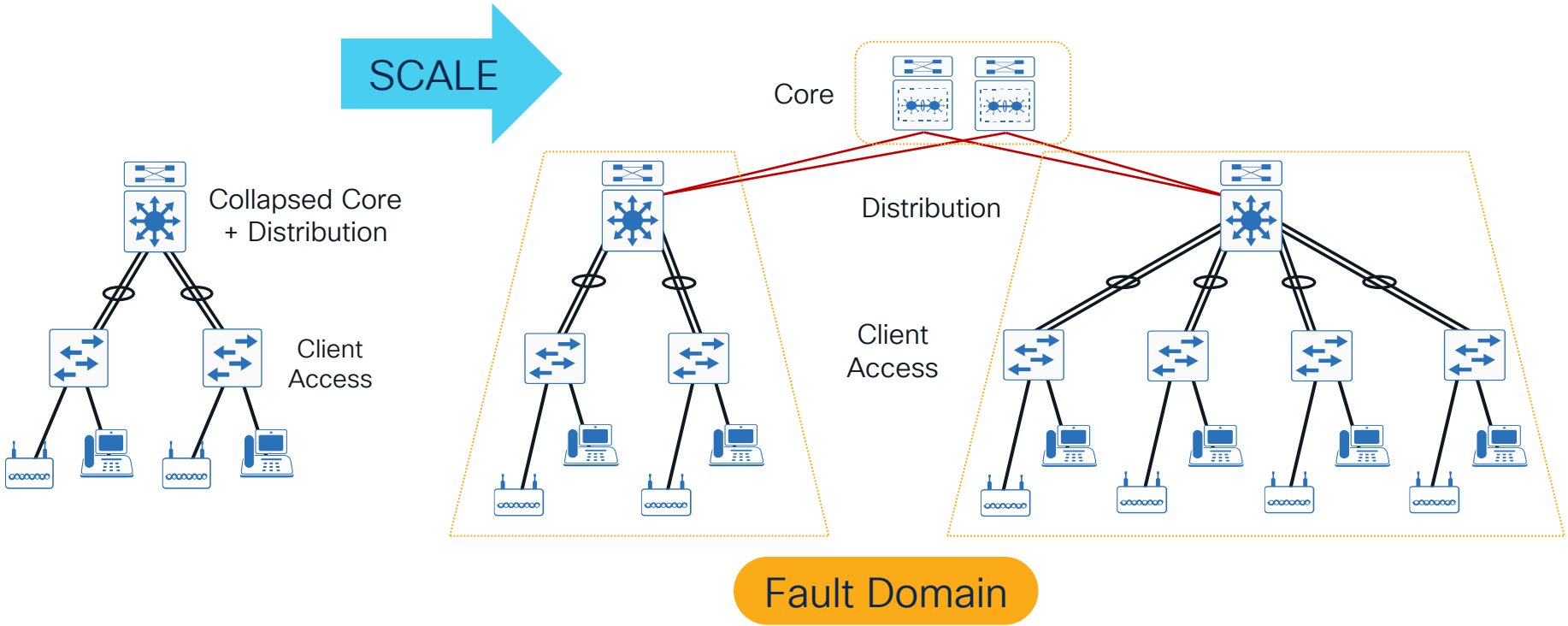
Always 3 “Logical” Layers

- Each layer provides a specific set of functions
- Each layer has a specific set of requirements

If you ‘collapse’ layers
your device needs
to support
all ‘**logical**’ functions

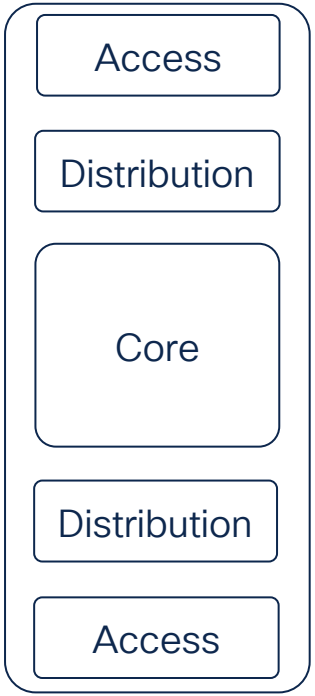
Campus Design Fundamentals

Hierarchical design model – Scalability & Stability

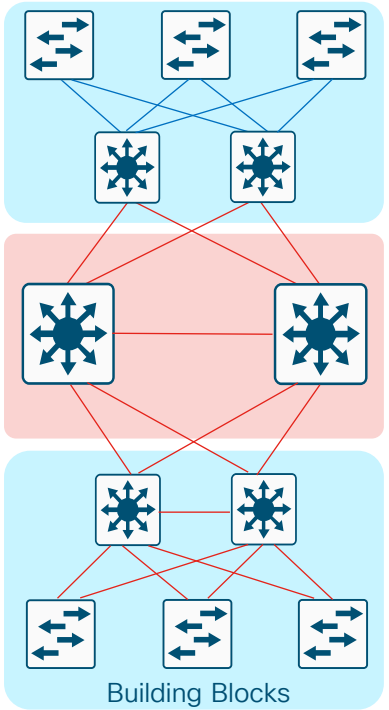


Hierarchical Network Design

Without a Rock Solid Foundation the Rest Doesn't Matter



- Offers hierarchy—each layer has specific role
- Modular topology—building blocks
- Easy to grow, understand, and troubleshoot
- Creates small fault domains— clear demarcations and isolation
- Promotes load balancing and redundancy
- Promotes deterministic traffic patterns
- Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
- Utilizes Layer 3 routing for load balancing, fast convergence, scalability, and control



Alternative Designs in Multilayer architecture

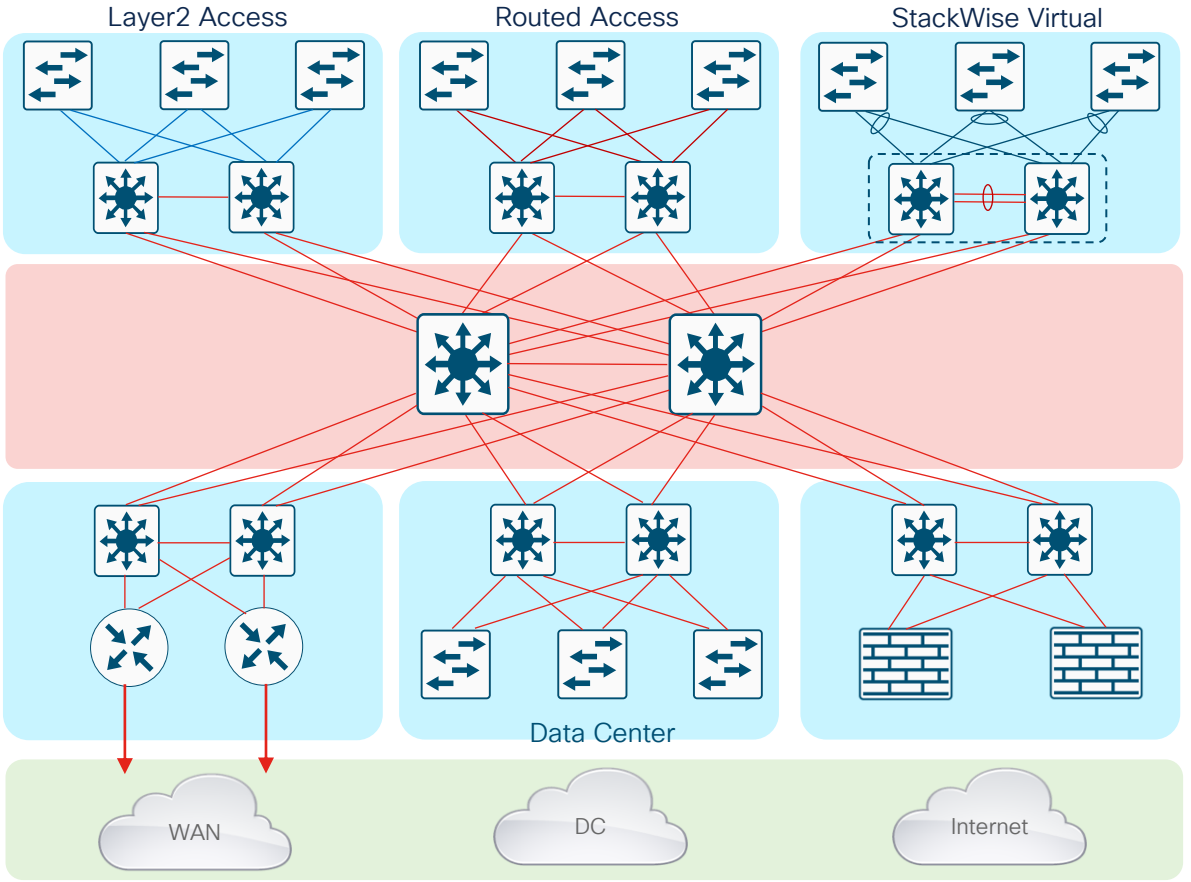
Access

Distribution

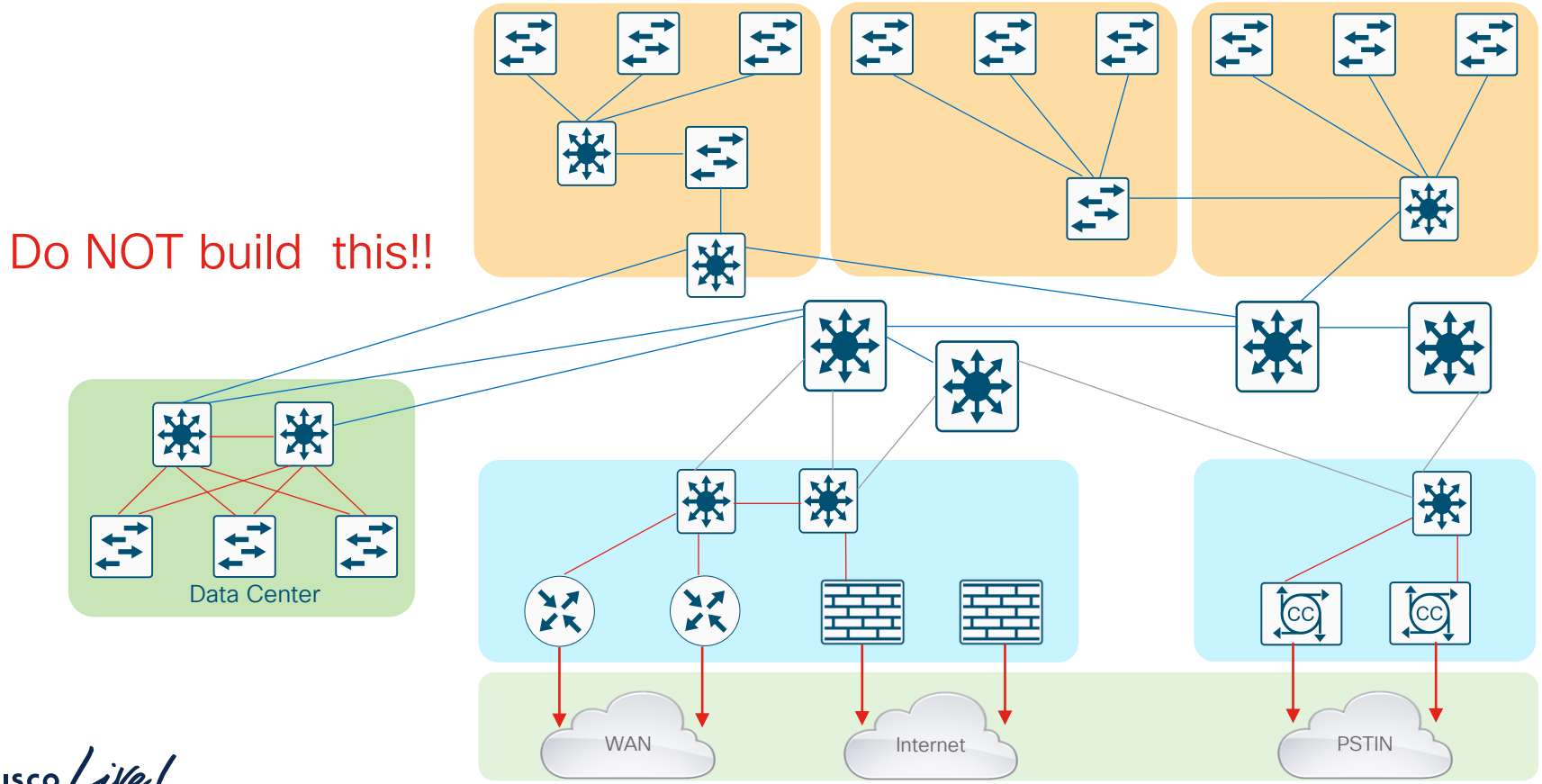
Core

Distribution

Access

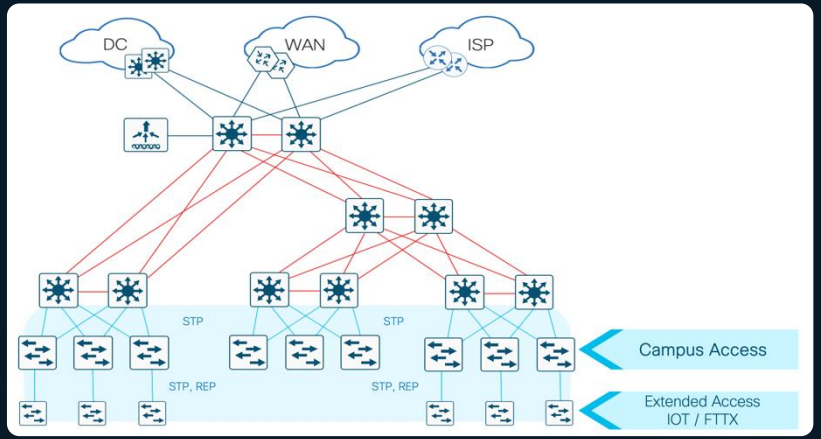


Multilayer Architecture DON'Ts

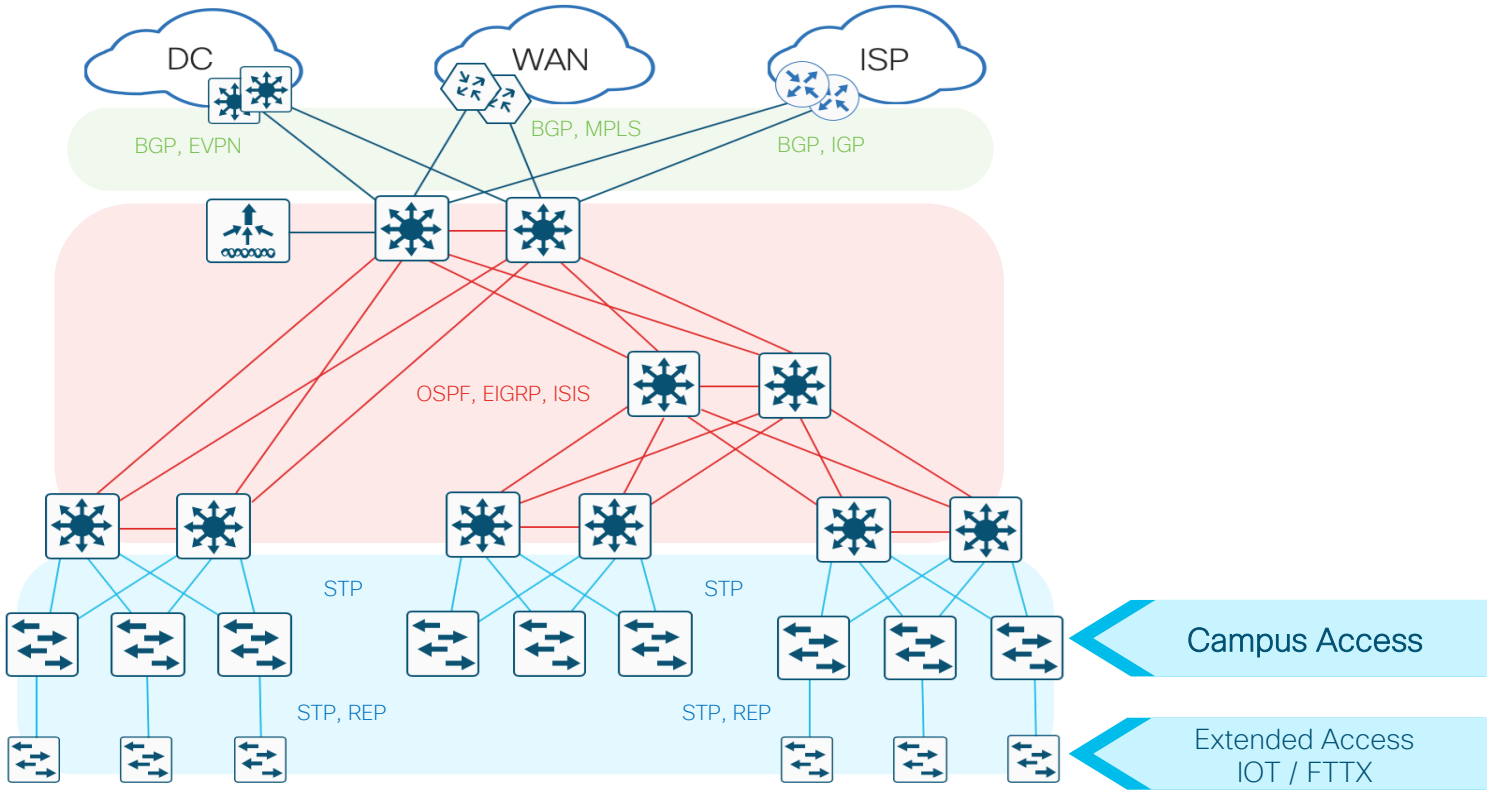


Design Principles

- Multi-Layer Model
- Access Layer
  - Baseline
  - Oversubscription ratio
- Distribution Layer
- Core Layer



Campus PINs & Topology



Campus Access (Baseline)

The **Access PIN** (Tier 1) focuses on connecting Users & Devices, or an Extended Access (if applicable), to the Distribution layer

- Other names: IDF, Wiring Closet
- Common in all Campus & Branch networks

Main purpose is to connect users to network

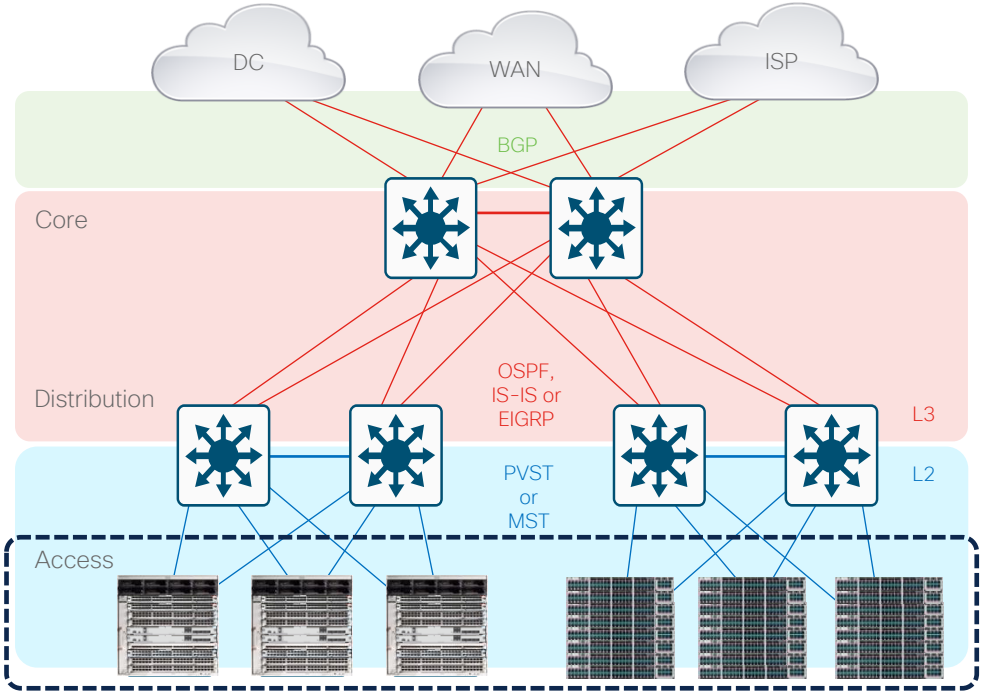
Tends to be **L2 switched** (north & south)

- North: VLAN, 802.1Q, STP, MAC, IGMP Snooping
- South: AAA, STP, Portfast, Storm-Control

Tends to use multiple L2 features & services

- Access Security (e.g. 802.1x, VACLs, PACLs, etc)
- Access QoS (e.g. L2 CoS, Classification & Marking)
- Access NetFlow (e.g. AVC, FNF, EPA & ETA)

Tends to require low-med L2 & feature scale



Extended Access (IOT / FTTX)

The **Extended Access PIN** (Tier 1) is an extension of the Access, to connect multiple Access layers (areas) to the Distribution layer

- Other names: High-End Access, IOT, FTTX
- Common in Very-Large Campus or Large Branch

Main goal is to extend the size and scale of the Access layer and connect more hosts

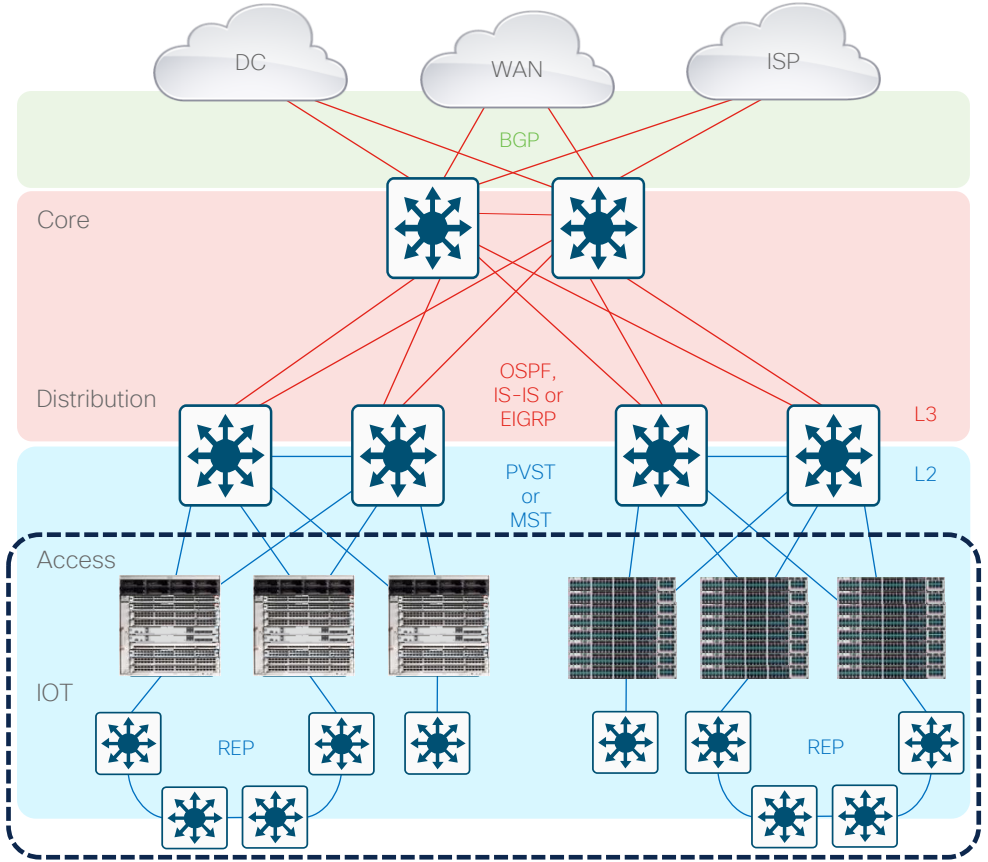
Tends to be **L2 switched** (north & south)

- North: VLAN, 802.1Q, STP/REP, MAC, IGMP Snooping
- South: AAA, STP/REP, Portfast, Storm-Control

Tends to use multiple L2 features & services

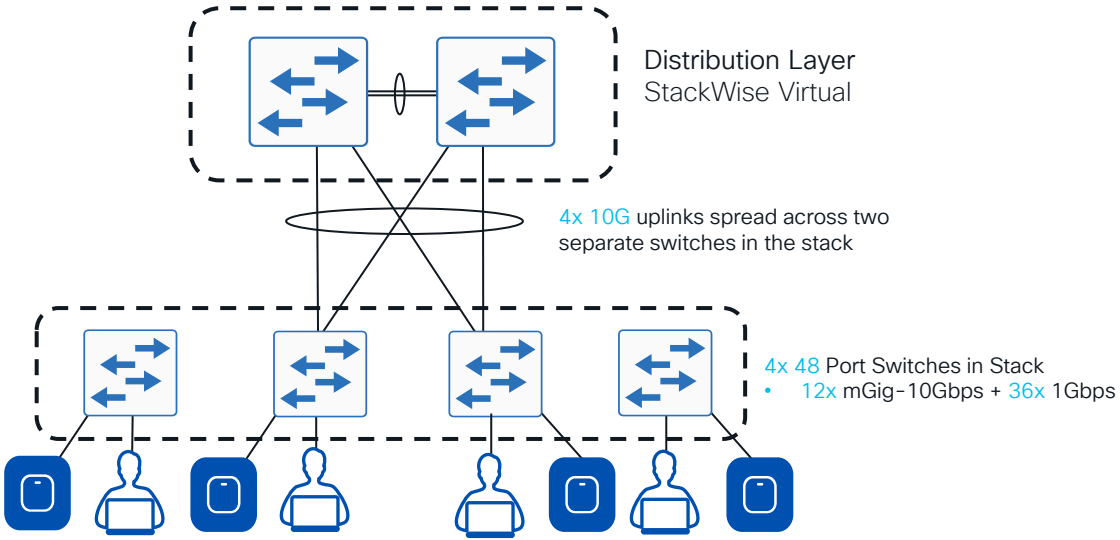
- Access Security (e.g. 802.1x, VACLs, PACLs, etc)
- Access QoS (e.g. L2 CoS, Classification & Marking)
- Access NetFlow (e.g. AVC, FNF, EPA & ETA)

Tends to require med-high L2 & feature scale



Campus Design Fundamentals

Access Layer – Oversubscription Ratios



Soft recommendation for Access to Distribution ≤ 20:1

Access Uplinks: 40 Gbps

Potential Downlinks:

48 x 10 Gbps

\+ 144 x 1 Gbps

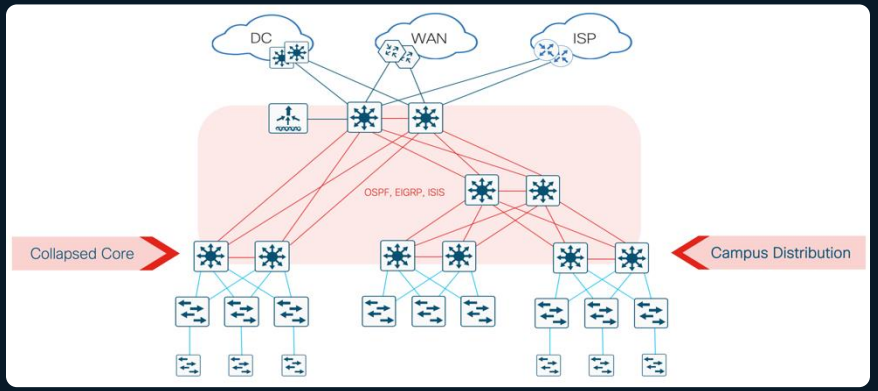
SUM: 624 Gbps

Oversubcription ratio:

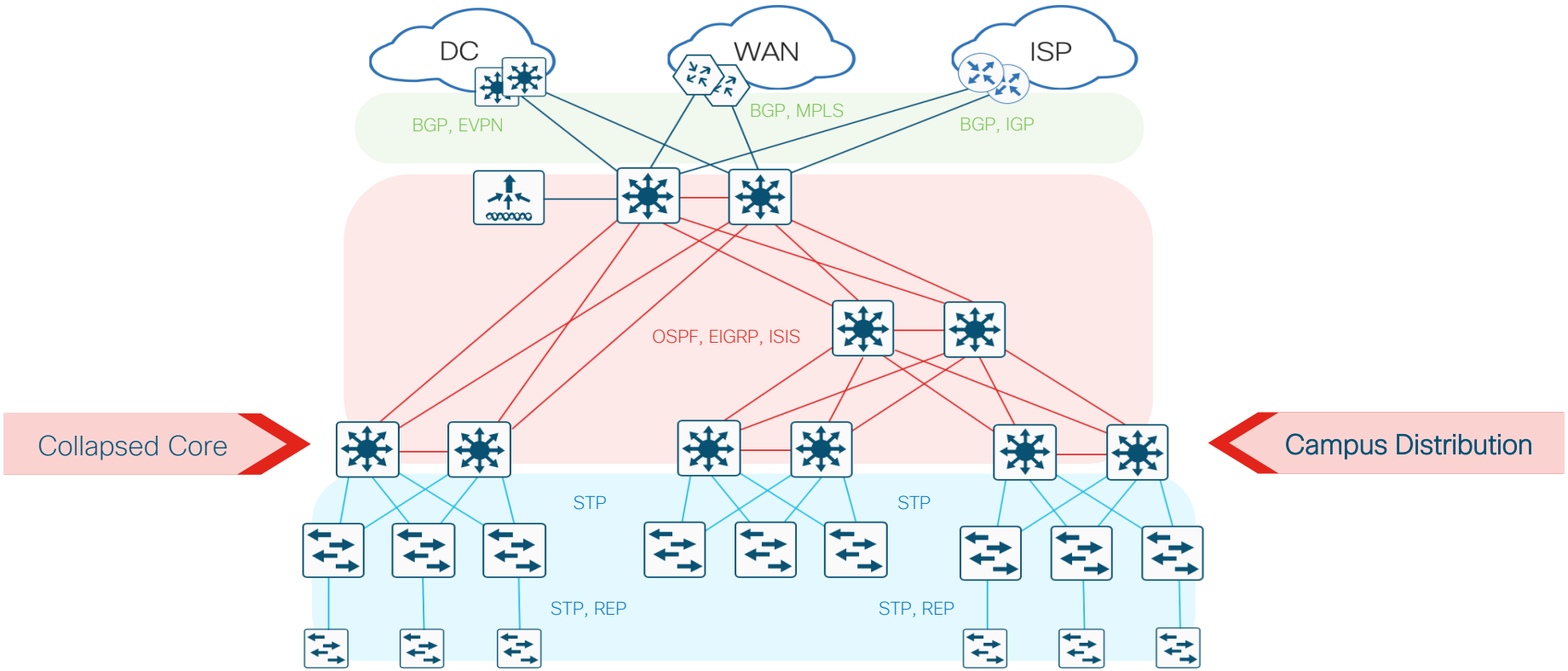
~15.6 : 1

Design Principles

- Multi-Layer Model
- Access Layer
- Distribution Layer
  - Baseline
  - Oversubscription ratio
  - Different setups
- Core Layer



Campus PINs & Topology



Campus Distribution (Baseline)

The **Distribution PIN** (Tier 2) focuses on connecting multiple Access layers and the Core layer.

- Other names: Collapsed Core, Aggregation, IDF
- Common in Small to Large Campus

Main purpose is to “distribute” connectivity (fan-out) from the Core/WAN to the Access

- Reduces need for high port-density in Core layer
- Also applicable to L3 Routed Access

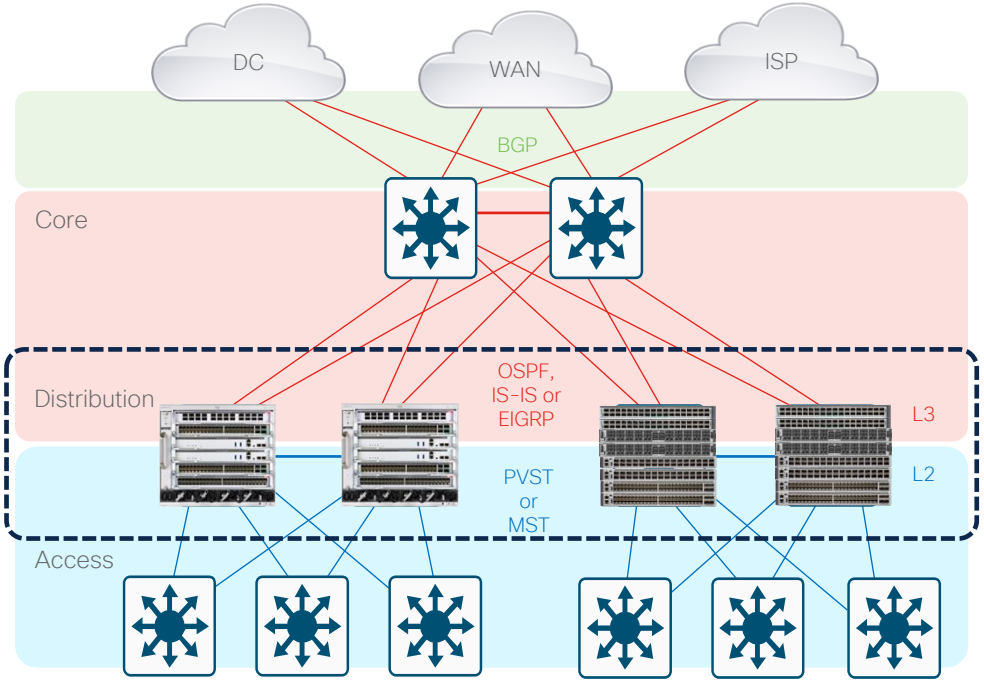
Tends to be both **L3 routed** (north) and **L2 switched** (south)

- North: SVI, HSRP/VRRP, ARP/ND, IGP, PIM
- South: VLAN, 802.1Q, STP, MAC, IGMP

Tends to use multiple L2 & L3 features

- Access Security (e.g. IPDT/SISF, VACLs, PACLs, etc)
- Access QoS (e.g. NBAR, Classification & Marking)
- Access NetFlow (e.g. AVC, FNF, EPA & ETA)

Tends to require med-high L2/L3 & feature scale



Campus Distro + Ext. Access

The **Distribution + Ext. Access PIN** (Tier 2+) focuses on connecting multiple Access layers, including an Extended Access (IOT/FTTX) layer, to the Core layer.

- Other names: Distribution, BDF
- Common in Very-Large Campus or Large Branch

Main purpose is to "distribute" connectivity (fan-out) from the Core/WAN to the Access + Ext. Access

- Reduces need for high port-density in Core layer

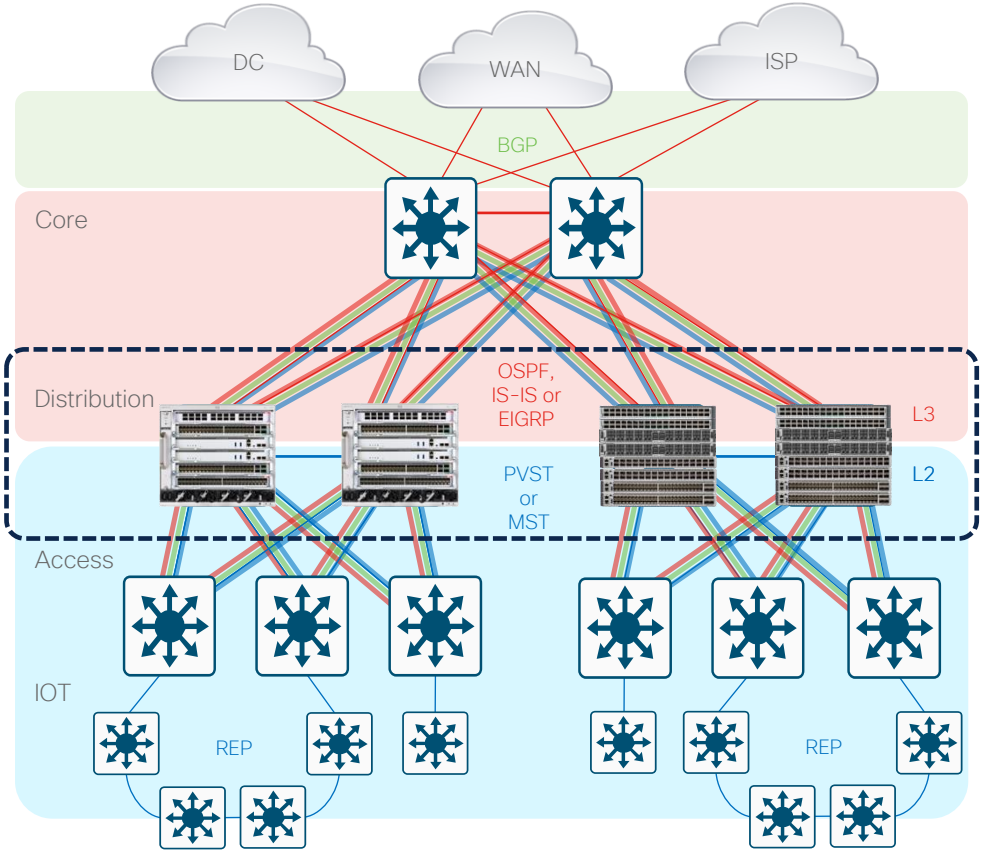
Tends to be both **L3 routed** (north) and **L2 switched** (south)

- North: VRF, SVI, HSRP/VRRP, ARP/ND, IGP, PIM
- South: VLAN, 802.1Q, STP, MAC, IGMP

Tends to use multiple L2 & L3 features

- Access Security (e.g. IPDT/SISF, VACLs, PACLs, etc)
- Access QoS (e.g. NBAR, Classification & Marking)
- Access NetFlow (e.g. AVC, FNF, EPA & ETA)

Tends to require highest L2/L3 & feature scale



Campus Collapsed Core

The **Collapsed Core** (Tier 2) focuses on connecting multiple Access layers and the WAN/Edge layer.

- Other names : Distribution, BDF
- Common in Small Campus or Medium Branch

Main purpose is to collapse Core & Distribution layers

- Mostly for small(er) sites, with low(er) port density
- Similar attributes & requirements as Core + Distribution
- Also applicable to L3 Routed Access

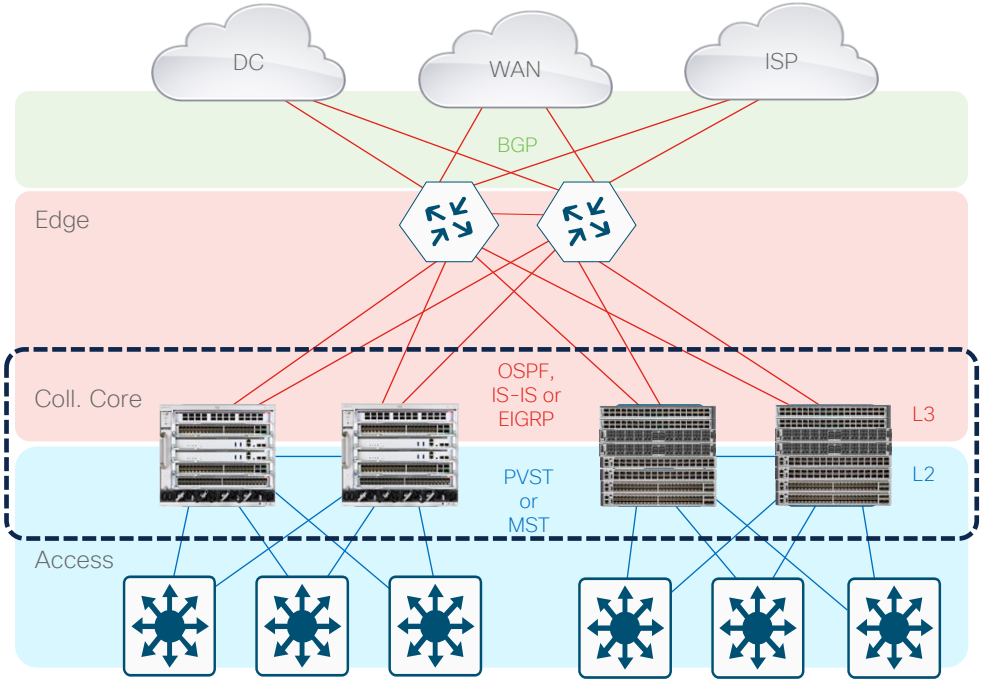
Tends to be both **L3 routed** (north) and **L2 switched** (south)

- North: SVI, HSRP/VRRP, ARP/ND, IGP, PIM
- South: VLAN, 802.1Q, STP, MAC, IGMP

Tends to use multiple L2 & L3 features

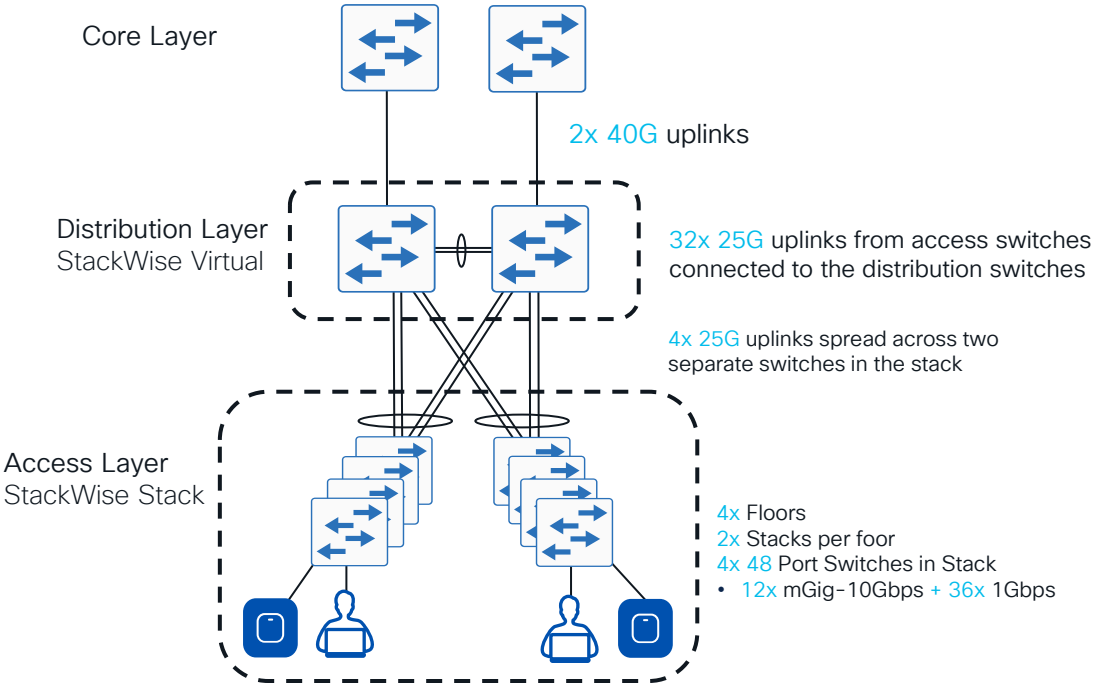
- Access Security (e.g. IPDT/SISF, VACLs, PACLs, etc)
- Access QoS (e.g. NBAR, Classification & Marking)
- Access NetFlow (e.g. AVC, FNF, EPA & ETA)

Tends to require high L2/L3 & feature scale



Design Fundamentals

Distribution Layer – Oversubscription Ratios



Soft recommendation for Distribution to Core ≤ 4:1

Distribution Uplinks: 80 Gbps

From Access Layer:

4 x 2 x 4 x 25 Gbps

SUM: 800 Gbps

Oversubcription ratio:

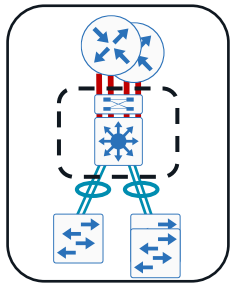
10 : 1

Design Fundamentals

Distribution Layer – different setups

Two tier remote site:

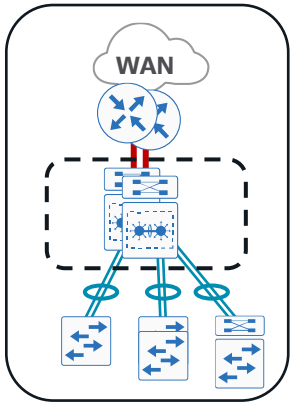
- Aggregates LAN Access Layer and connects to WAN routers



Collapsed Core:

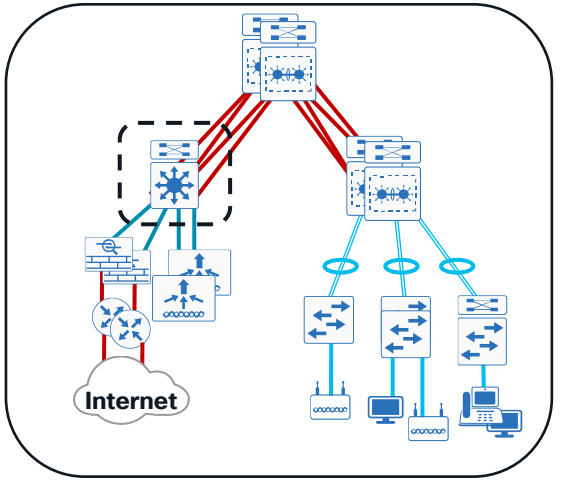
Two tier campus LAN and WAN Core

- LAN Access Layer aggregation
- Central connect point for all services



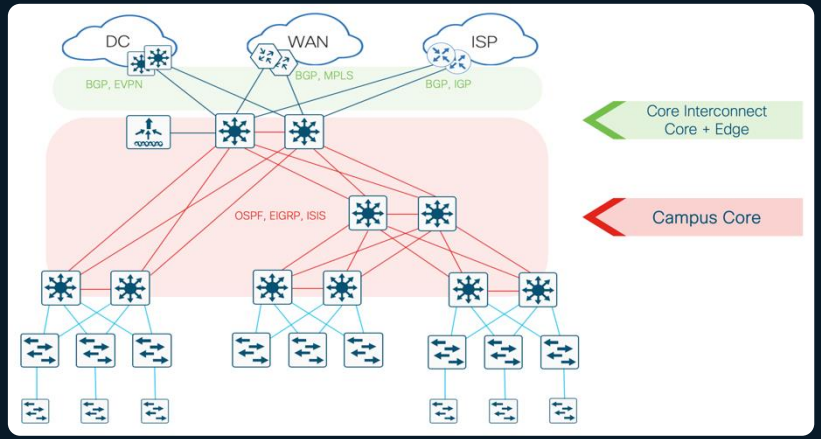
Large LAN Services Block:

- Connection point for services
- Drives modular building block design

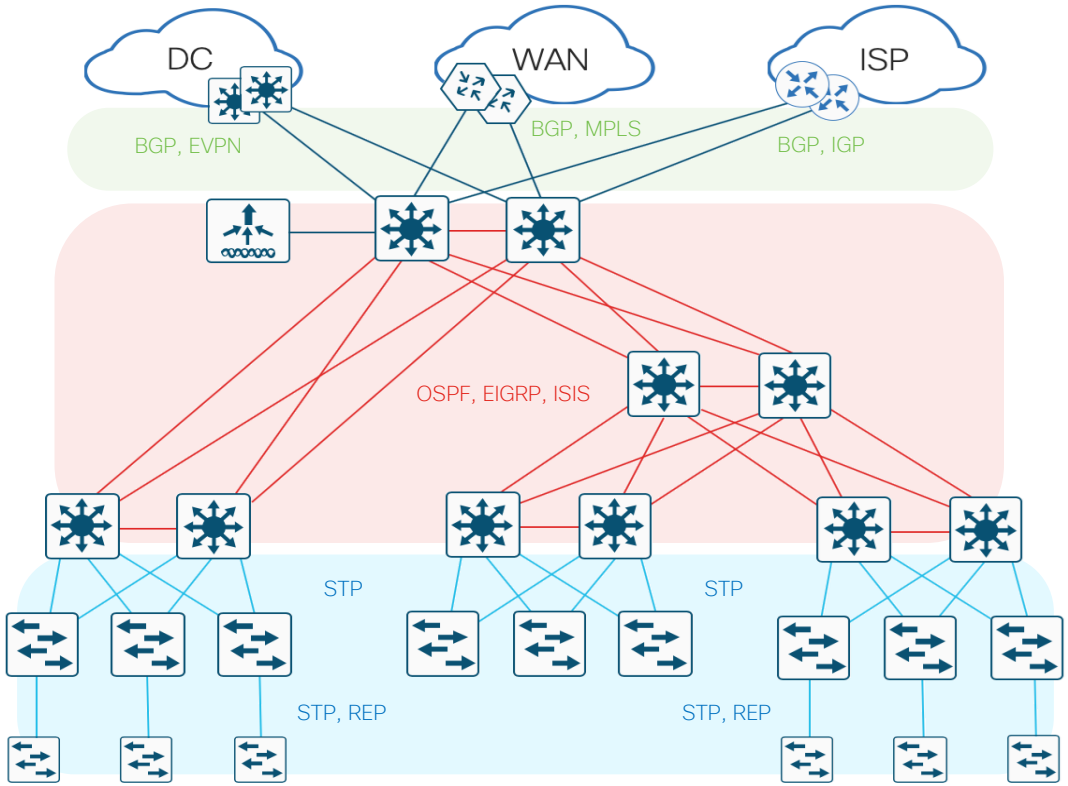


Design Principles

- Multi-Layer Model
- Access Layer
- Distribution Layer
- Core Layer
  - Baseline
  - Do I need it?



Campus PINs & Topology



Core Interconnect
Core + Edge

Campus Core

Campus Core (Baseline)

The **Core PIN** (Tier 3) focuses on connecting multiple Distribution layers to an Interconnect (if applicable) and/or other network domains

- Other names: MDF, BDF
- Common in Medium & Large Campus

Main goal is a simple, high-bandwidth, L3 transport between other network layers

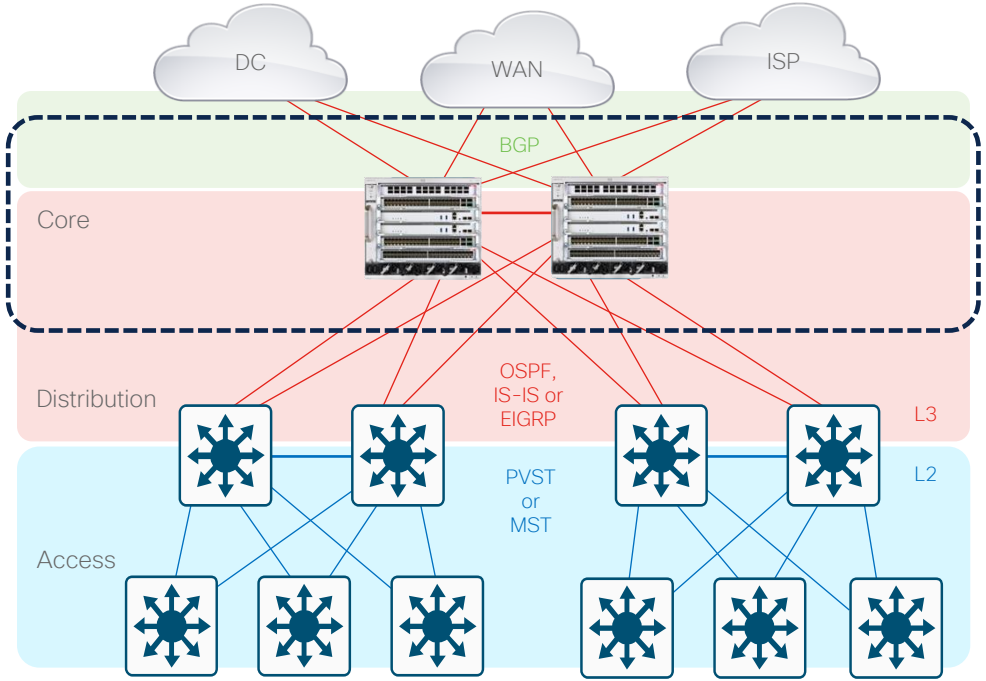
Tends to be **L3 routed** (north & south)

- North: BGP or IGP (ABR), PIM + MSDP
- South: OSPF, IS-IS or EIGRP, PIM

Tends to use minimal L3 features

- Limited ACLs (e.g. inter-area route-maps, remote access)
- Limited QoS (e.g. many-to-one WRED, aggregate policers)
- Limited NetFlow (e.g. inter-area, aggregate flows)

Tends to require high L3 forwarding scale

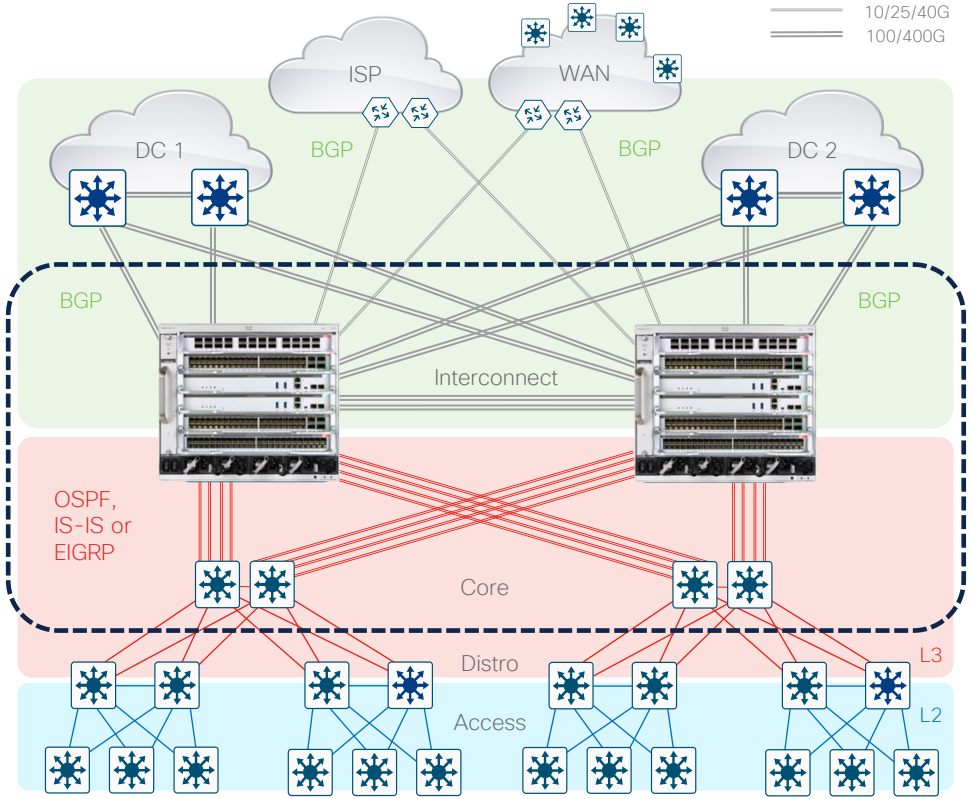


Campus Core Interconnect

The **Interconnect PIN** (Tier 4) is an extension of the Core, used to connect multiple Core layers (areas) and/or other network domains.

- Other names: Backbone, Super Core, MAN, DCI
- Common in Large & Very-Large Campus

- Main goal is to distribute the bandwidth and density requirements of multiple Core layers
  - Similar attributes & requirements as Core PIN
- Tends to be **L3 routed** (north & south)
  - North: BGP or IGP (ABR/ASBR), PIM + MSDP
  - South: OSPF, IS-IS or EIGRP, PIM
- Tends to use minimal L3 features
  - Limited ACLs (e.g. inter-area route-maps, remote access)
  - Limited QoS (e.g. many-to-one WRED, aggregate policers)
  - Limited NetFlow (e.g. inter-area, aggregate flows)
- Tends to require higher L3 scale

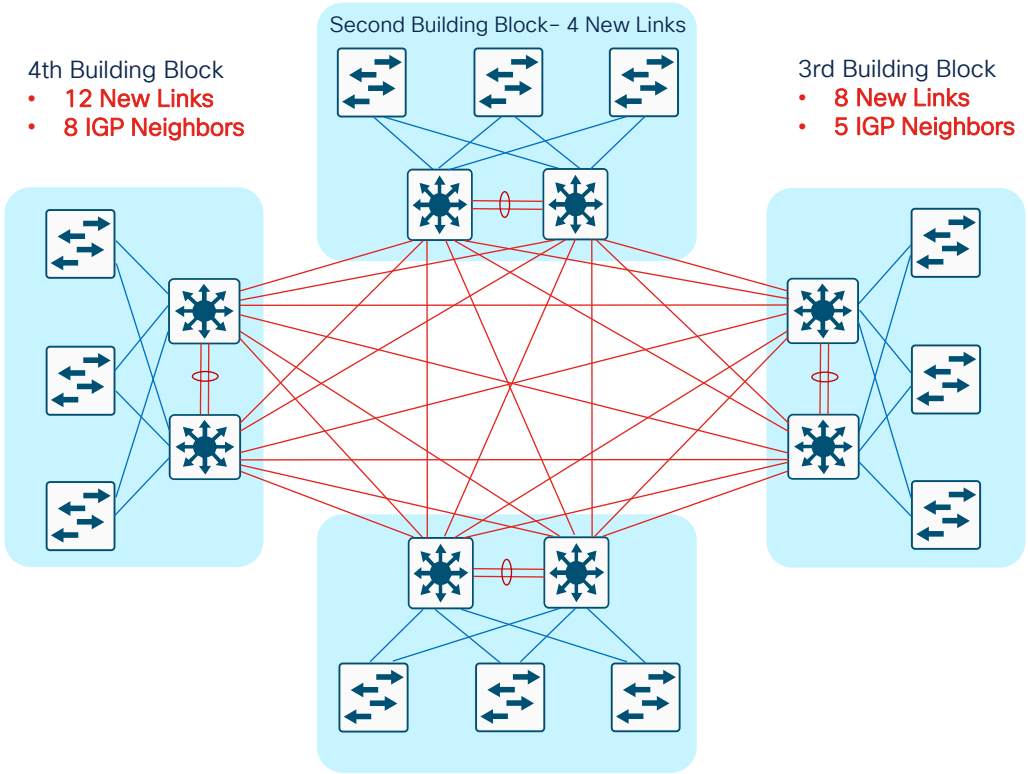


Do I need a Core Layer?

It's Really a Question of Scale, Complexity, and Convergence

No Core (2-Tier)

- Fully-meshed distribution layers
- Difficult to add new blocks
- More physical cabling (2n-2)
- Routing complexity
  - More routing peers
  - More ECMP paths

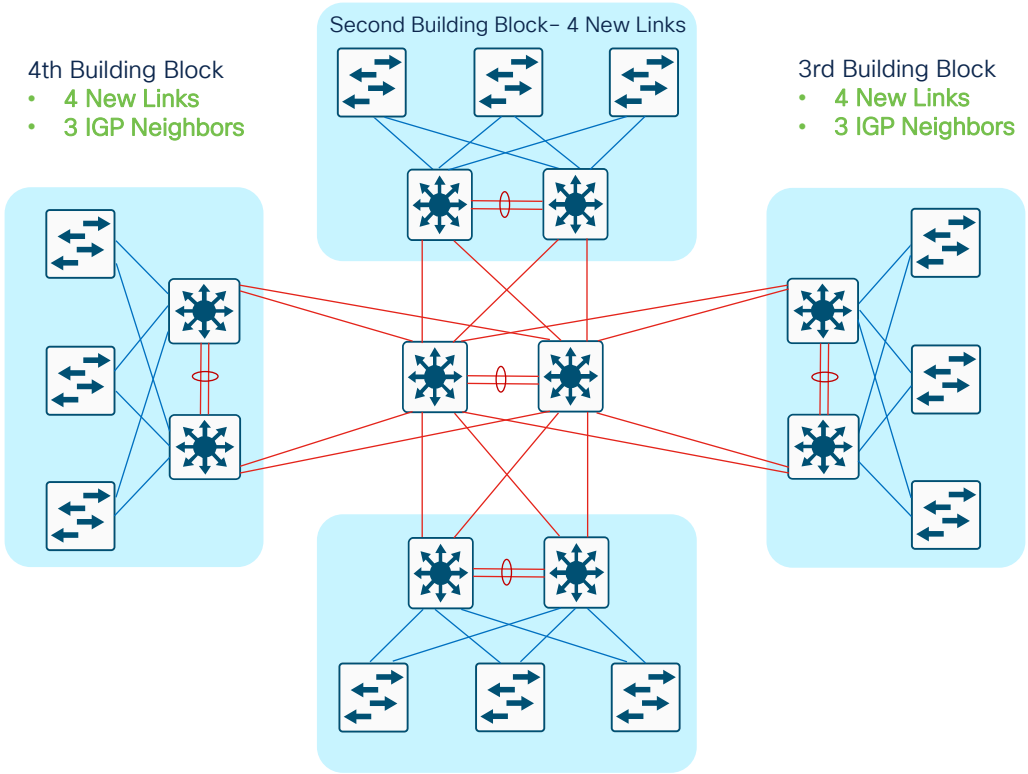


Do I need a Core Layer?

It's Really a Question of Scale, Complexity, and Convergence

Dedicated Core (3-Tier)

- Easier to add a block
- Fewer links in the Core
- Easier bandwidth upgrade
- Fewer routing peers
- Fewer ECMP paths
- Best for convergence



Campus Core + Edge (SP/WAN)

The **Core-Edge PIN** (Tier 4) focuses on connecting multiple Campus areas to remote domains (SP/WAN) and/or to the Internet.

- Other names: Edge Device, Internet Edge
- Common in Medium to Very-Large Campus

Main purpose is to collapse Core & Edge layers

Tends to be **L3 routed** (north & south)

- North: MP-BGP + Inter-AS, NAT/PAT, PIM + MSDP
- South: BGP or IGP (ABR/ASBR), PIM + MSDP

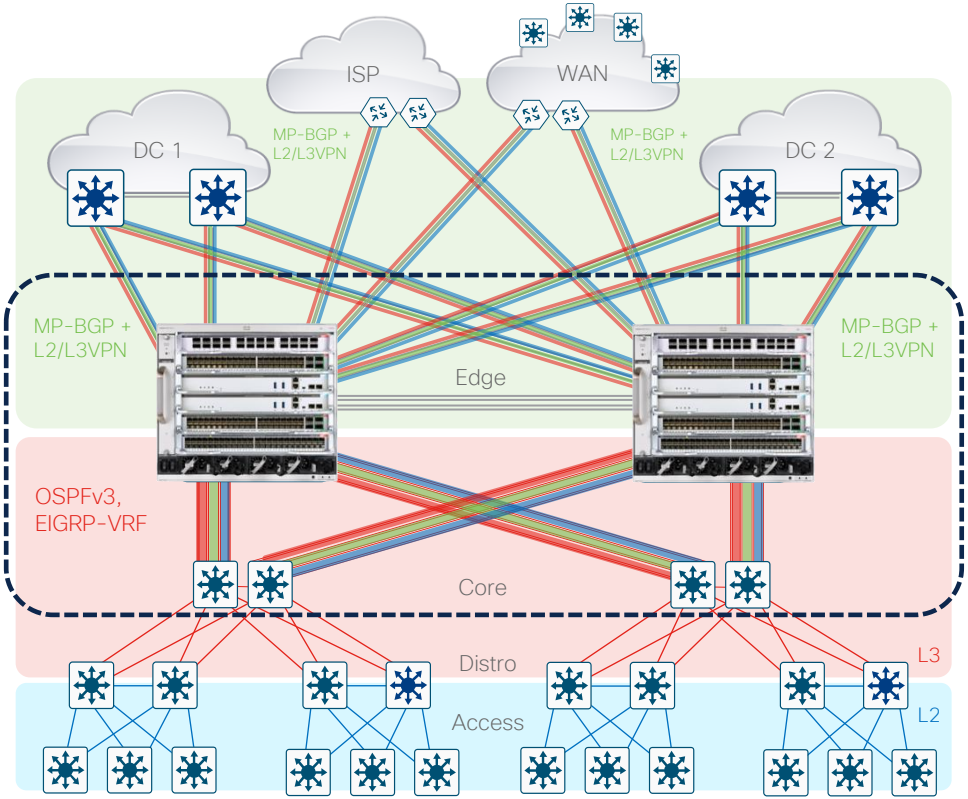
Tends to use **Virtualization** & **Tunnels**

- VRF-Lite, MPLS/VPLS, SR, MVPN
- GRE/MGRE, IPsec, DMVPN
- QinQ, L2oMGRE, OTV, EVPN

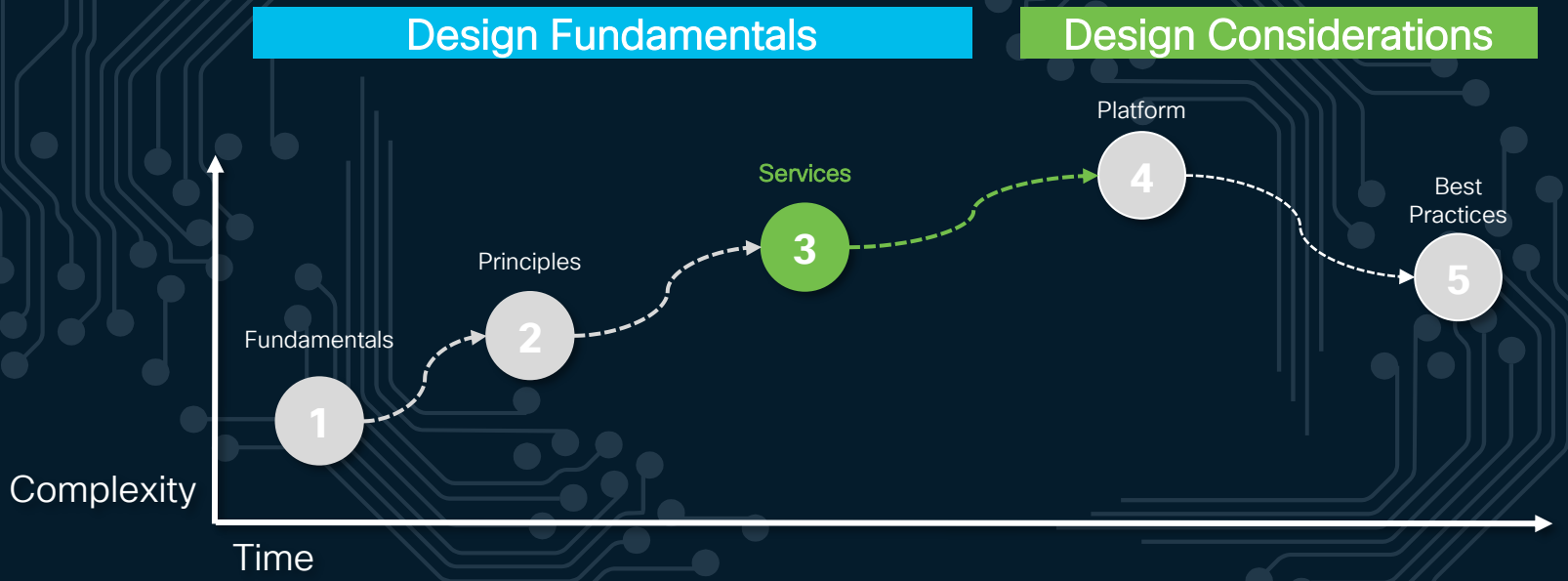
Tends to use multiple L3/VRF features

- Edge Security ACLs (e.g. RACL, CBAC, ZBFW)
- Hierarchical QoS (e.g. Class-based Queuing, Shaping)
- Policy Based Routing (e.g. WAAS & WCCP)
- WAN NetFlow (e.g. L3/VRF FNF, WAN ETA)

Tends to require highest L3/VRF & feature scale

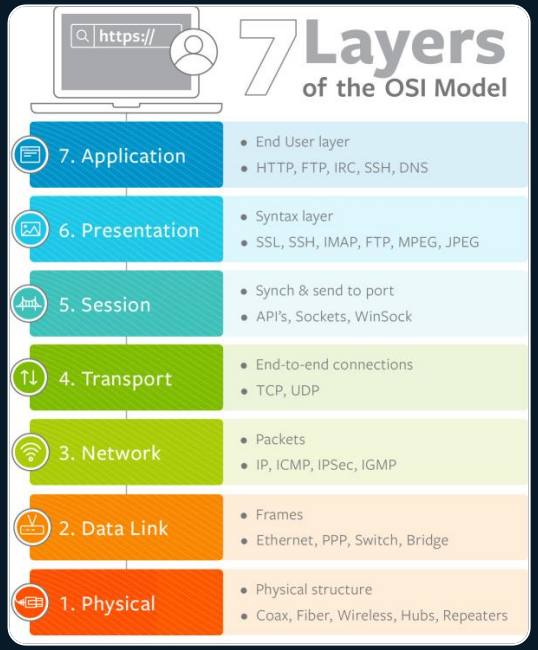


Session Agenda



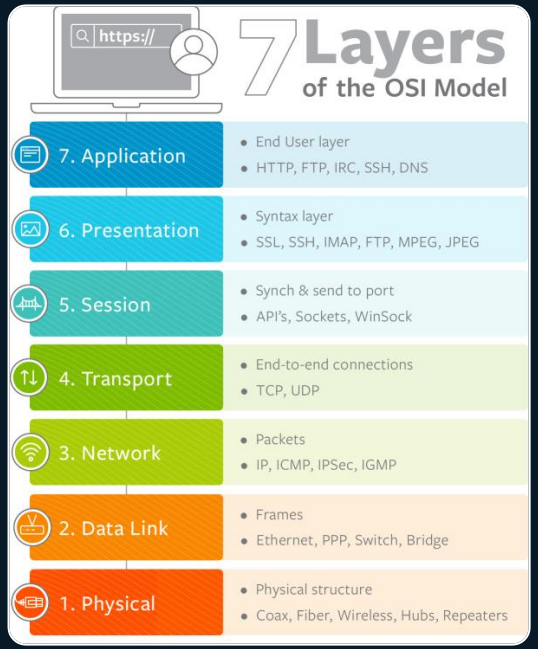
Campus Services

- **Layer 1 physical layer & links**
- **Layer 2 switching protocols**
- **Layer 3 routing protocols**



Campus Services

- **Layer 1 physical layer & links**
  - **Media type**
  - **UDLD**
  - **EtherChannel**
- **Layer 2 switching protocols**
- **Layer 3 routing protocols**



Copper vs. Fiber Media

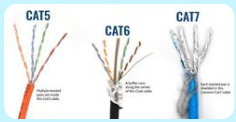
www.cisco.com/c/en/us/products/interfaces-modules/transceiver-modules/

Category 5, 6 and 7

Unshielded (UTP) | Shielded (STP)

RJ45 (Access to Endpoints)

Cat6A (Offset Wires) Cat5E (Flush Wires)



Category	Frequency	Distance	Data Rate	Shielding
5E	100-350 MHz	100m	1000 Mbps	UTP or STP
6	250-550 MHz	1G – 100m 10G - 50m	1 Gbps 10 Gbps	UTP or STP
6A	500-550 MHz	100m	10 Gbps	UTP or STP
7	600 MHz	100m	10 Gbps	Shielded only

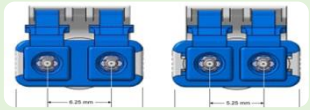
10M 100M 1G 2.5G 5G 10G

NBASE-T ALLIANCE

OM3, OM4 and OM5

Multi-Mode (MMF) | Single-Mode (SMF) | Wave-Division Multiplex (WDM)

SFP (Access and Distribution) **QSFP** (Core and Edge)

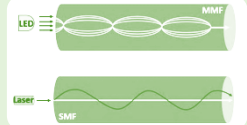


SFP-LC LC Duplex mSFP Mini LC Duplex

MPO12 12 Fibers MPO24 24 Fibers

Multimode
- Short distance cable runs (less than 1000ft.)
- High bandwidth support
- Higher cable cost
- Lower electronics cost
- Easier to terminate due to larger core size

Single Mode
- Long distance cable runs (greater than 1000ft.)
- Highest bandwidth support
- Lower cable cost
- Higher electronics cost
- Harder to terminate due to smaller core size

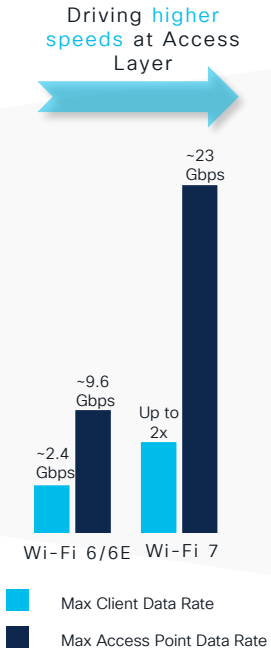


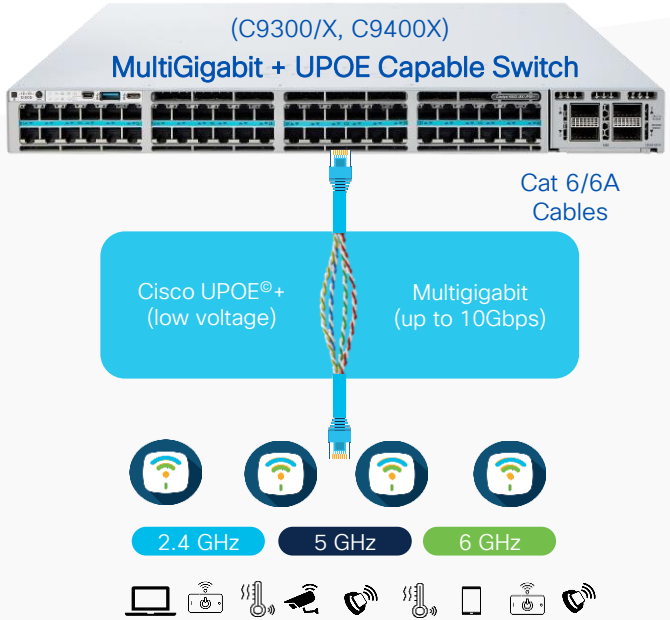
100M 1G 10G 25G 40G NEW 50G NEW 100G 200G NEW 400G

www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat9000-panduit-cables-wp-cte-en.html

Higher Speeds driving Multi-Gigabit Access

Future Proof with Speed and More Power Over Ethernet





Up to 10G speed

60W UPOE

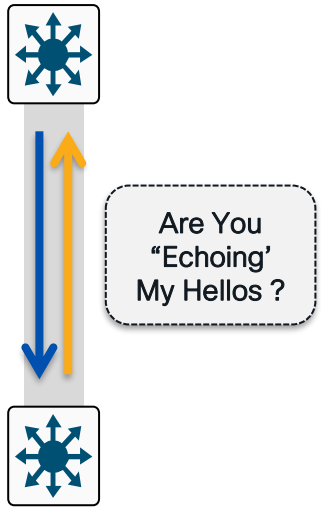
Dual 10G ports* (LACP & PoE Redundancy)

*CW9178I Model

Unidirectional Link Detection (UDLD)

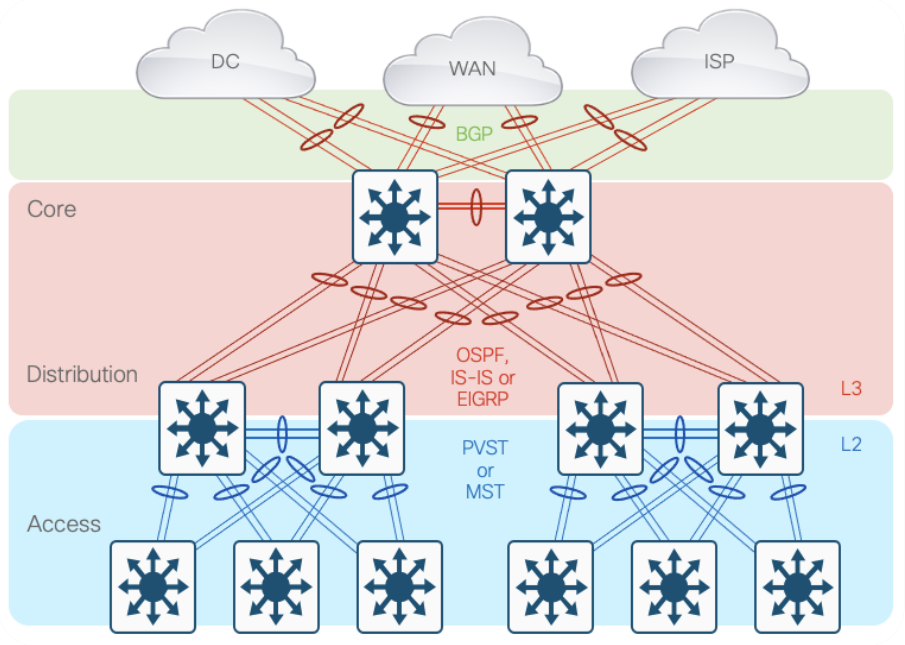
Protecting Against One-Way Communication

- UDLD protects against one-way communication or partially failed optics, and the effect it could have on L2 protocols like STP
- Primarily used on fiber optic links where patch or cable errors cause link up/up – with mismatched transmit/receive pairs
- Each switch port configured for UDLD will send UDLD protocol packets (L2) containing the port's own device/port ID
  - The neighbor's device/port IDs seen by UDLD on that port
- Neighboring ports should see their own device/port ID (echo) in the packets received from the other side
- If the port does not see its own device/port ID in the incoming UDLD packets (for a specific duration) – then the link is considered unidirectional and is put into errdisable



EtherChannels

Reduce Complexity/Peer Relationships



- More links = more protocol peer relationships (and associated overhead)
- EtherChannels allow you to reduce peers by creating single logical interface to peer
- When single link-failure in a bundle:
  - OSPF running on a Cisco IOS-based switch will reduce link cost and reroute traffic
  - EIGRP may not change link cost and may overload remaining links

Campus + EtherChannel

Using **EtherChannel** focuses on combining multiple physical links into a single logical link

- Other names: Portchannel, Link-Aggregation (LAG)
- Common in Medium & Large Campus

Main goal is to increase bandwidth, and provide link-level redundancy between network layers

- Mostly for large(r) sites, with high(er) port density
- Similar attributes & requirements as existing PIN(s)

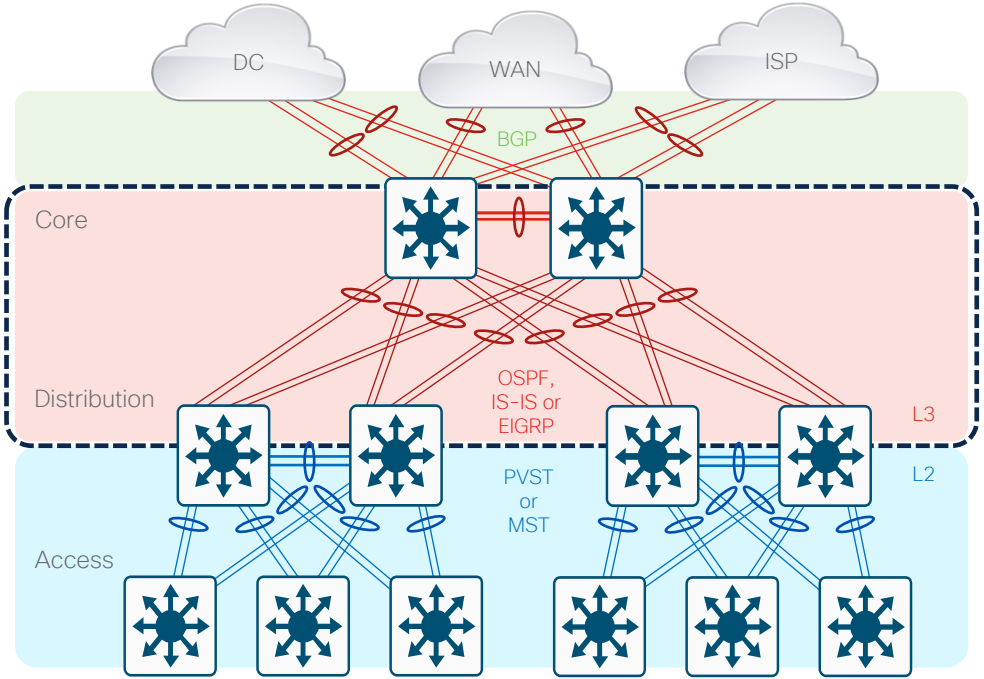
Can be used for both L2 & L3 links (north & south)

- North: BGP or IGP, PIM
- South: STP or REP, IGMP/MLD

Tends to require special L2/L3 features

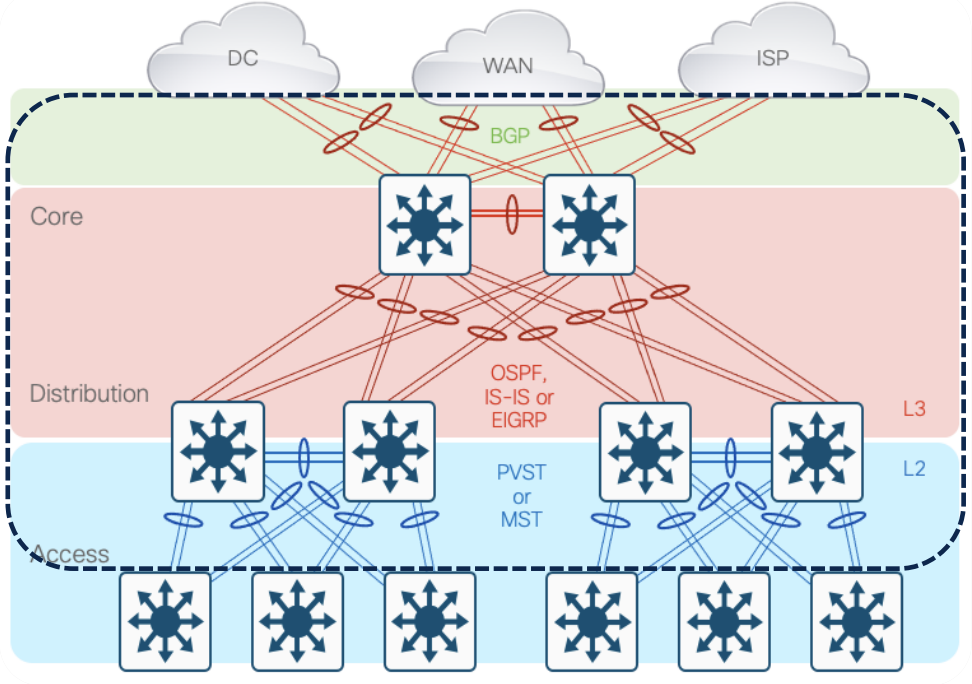
- Portchannel ACLs (e.g. L2/L3 RACL)
- Portchannel QoS (e.g. L2/L3 aggregate policers)
- Portchannel NetFlow (e.g. L2/L3 FNF)

Tends to require less L2/L3 forwarding scale



L2/L3 Ether Channel Config – Best Practices

- Typically deployed in distribution to core, and core to core interconnections
- Used to provide link redundancy—while reducing peering complexity
- Tune L3/L4 load balancing hash to achieve maximum utilization of channel members
- Deploy in powers of two (two, four, or eight)
- 802.3ad LACP for interop if you need it

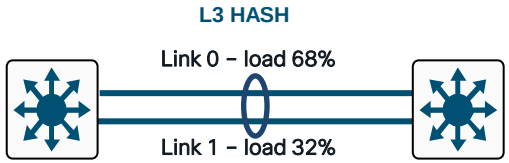


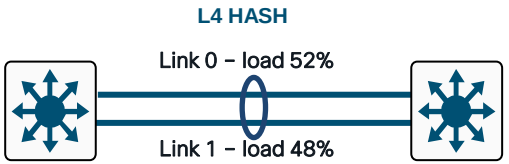
Ether Channel load balancing

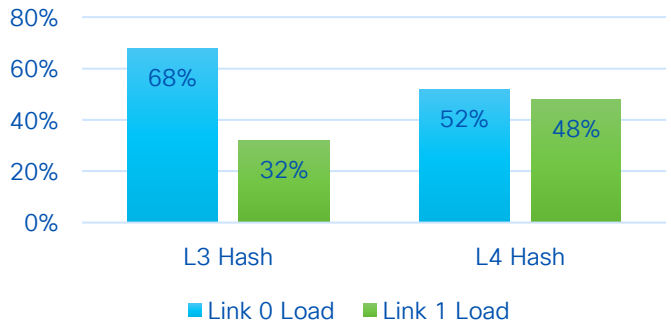
Use as much information as possible

- Cisco switches let you tune the hashing algorithm used to select the specific EtherChannel link.
- You can use the default source/destination IP information, or you can add an additional level of load balancing to the process by adding the L4 TCP/IP port information as an input to the algorithm.

```
switch(config)#port-channel load-balance ?
  dst-ip                  Dst IP Addr
  dst-mac                 Dst Mac Addr
  dst-mixed-ip-port       Dst IP Addr and TCP/UDP Port
  dst-port                Dst TCP/UDP Port
  extended                Extended Load Balance Methods
  src-dst-ip              Src XOR Dst IP Addr
  src-dst-mac             Src XOR Dst Mac Addr
  src-dst-mixed-ip-port   Src XOR Dst IP Addr and TCP/UDP Port
  src-dst-port            Src XOR Dst TCP/UDP Port
  src-ip                  Src IP Addr
  src-mac                 Src Mac Addr
  src-mixed-ip-port       Src IP Addr and TCP/UDP Port
  src-port                Src TCP/UDP Port
```



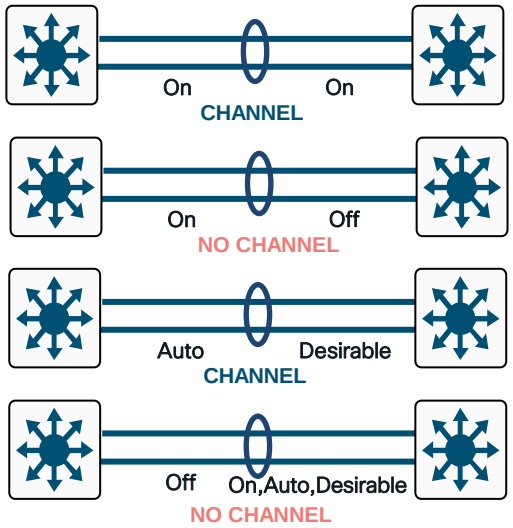




Understanding Ether Channel

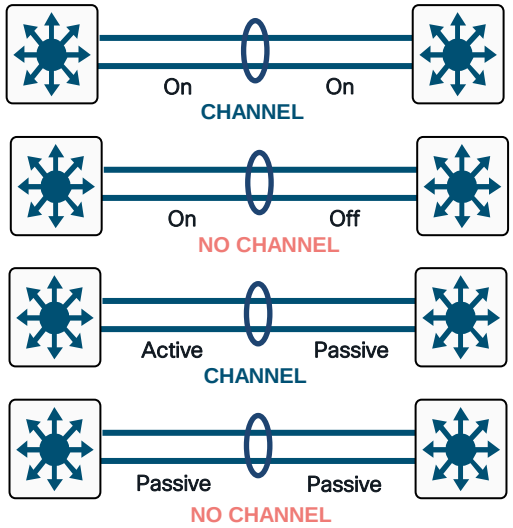
Link Negotiation Options–PAgP and LACP

Port Aggregation Protocol



On: always be a channel/bundle member
Desirable: ask if the other side can/will
Auto: if the other side asks I will
Off: don't become a member of a channel/bundle

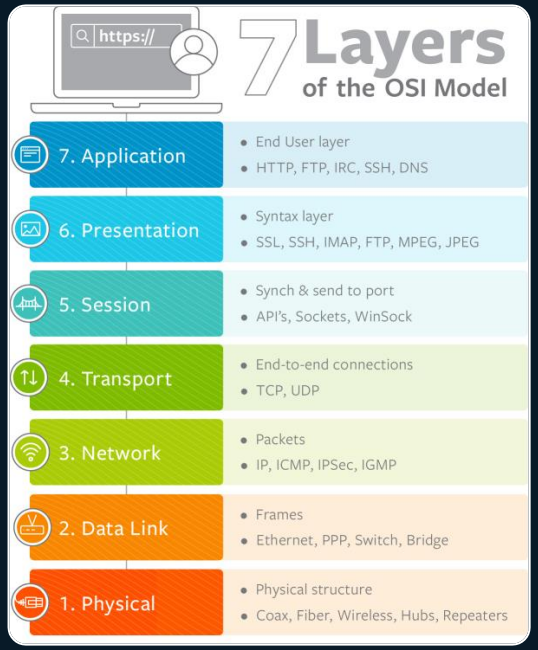
Link Aggregation Protocol



On: always be a channel/bundle member
Active: ask if the other side can/will
Passive: if the other side asks I will
Off: don't become a member of a channel/bundle

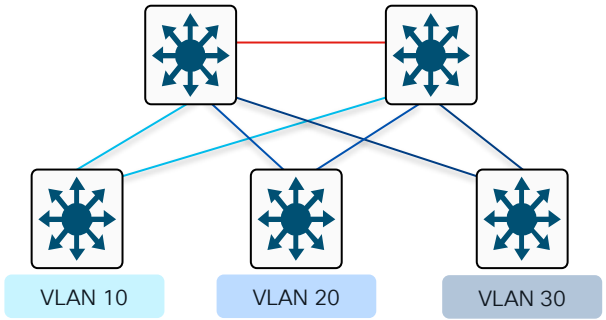
Campus Services

- **Layer 1 physical layer & links**
- **Layer 2 switching protocols**
  - **STP**
  - **Trunks**
  - **VTP/DTP**
- **Layer 3 routing protocols**

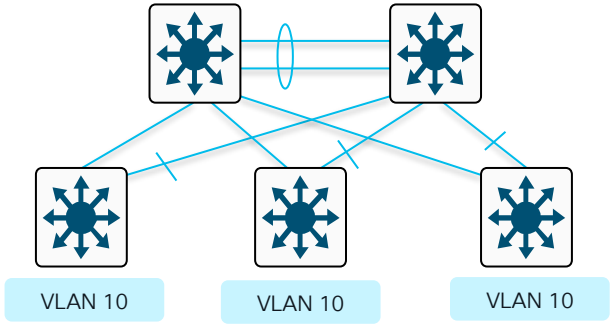


Multilayer Network Design

Layer 2 Access with Layer 3 Distribution



- Each access switch has unique VLANs
- No Layer 2 loops
- Layer 3 link between distribution
- No blocked links

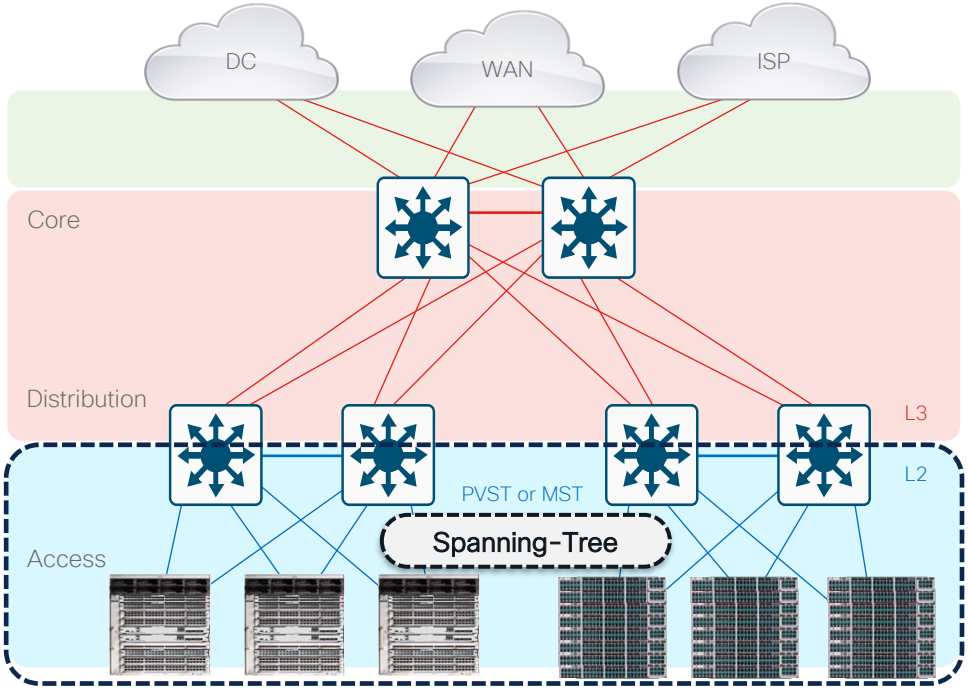


- At least some VLANs span multiple access switches
- Layer 2 loops
- Layer 2 and 3 running over link between distribution
- Blocked links

L2 Spanning Tree

Best Practices

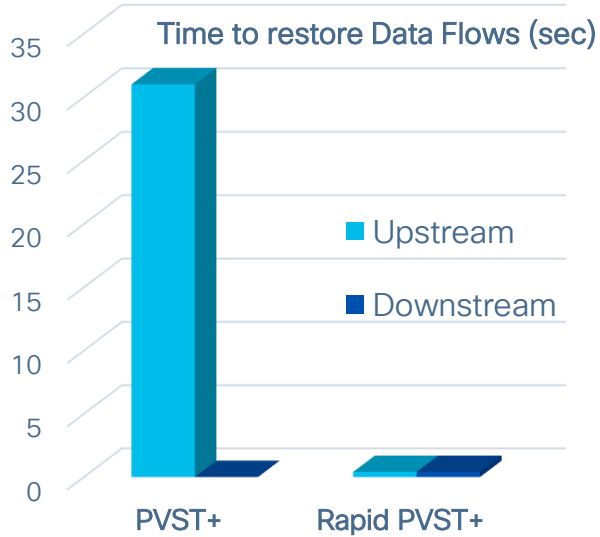
- Only extend VLANs across Access & Distribution layers when you must!
- Use PVST for best convergence
  - Rapid-PVST+ (RPVST) is default
- Use MST for best scale
  - Required to protect against access loops
  - Required to protect against operational accidents (misconfig or hardware failure)
  - Take advantage of Spanning Tree toolkit



Optimizing L2 Convergence

PVST+, Rapid PVST+ or MST

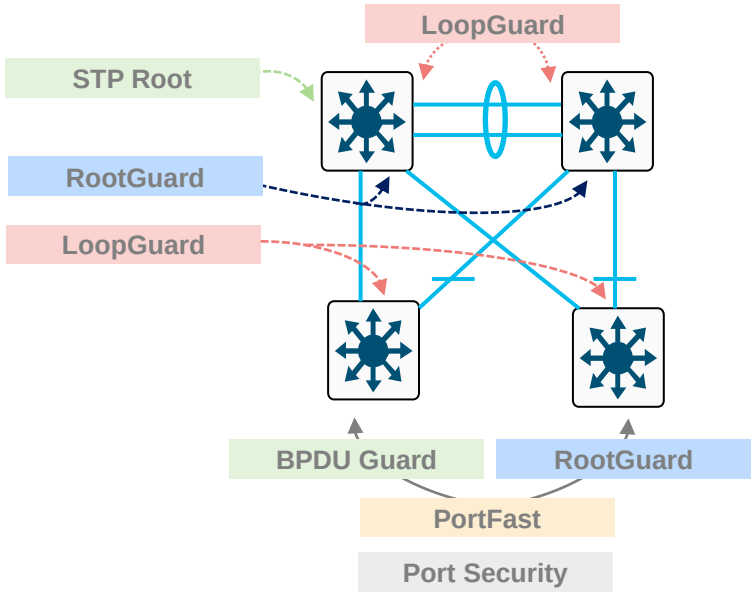
- Rapid-PVST+ greatly improves the restoration times for any VLAN that requires a topology convergence due to link UP
- Rapid-PVST+ also greatly improves convergence time over backbone fast for any indirect link failures
- PVST+ (802.1d)
  - Traditional spanning tree implementation
- Rapid PVST+ (802.1w)
  - Scales to large size (~10,000 logical ports)
  - Easy to implement, proven, scales
- MST (802.1s)
  - Permits very large scale STP implementations (~30,000 logical ports)
- Not as flexible as rapid PVST+



Layer 2 Hardening

Spanning Tree Should Behave the Way You Expect

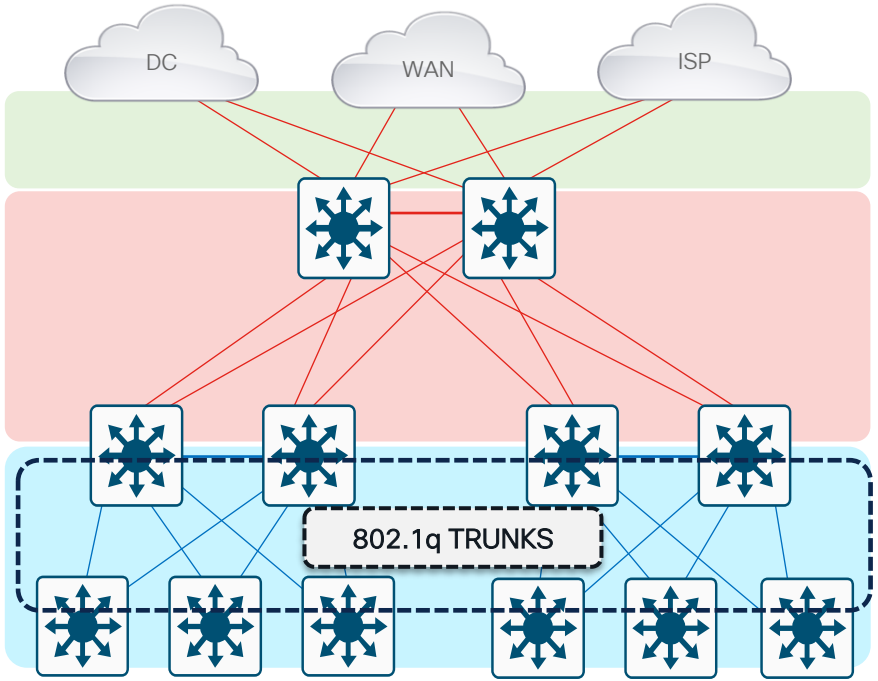
- Place the root where you want it
  Root primary/secondary macro
- The root bridge should stay where you put it
  - RootGuard
  - LoopGuard
  - UplinkFast
  - UDLD
- Only end-station traffic should be seen on an edge port
  - BPDU Guard
  - RootGuard
  - PortFast
  - Port-security



L2 Trunk Configuration

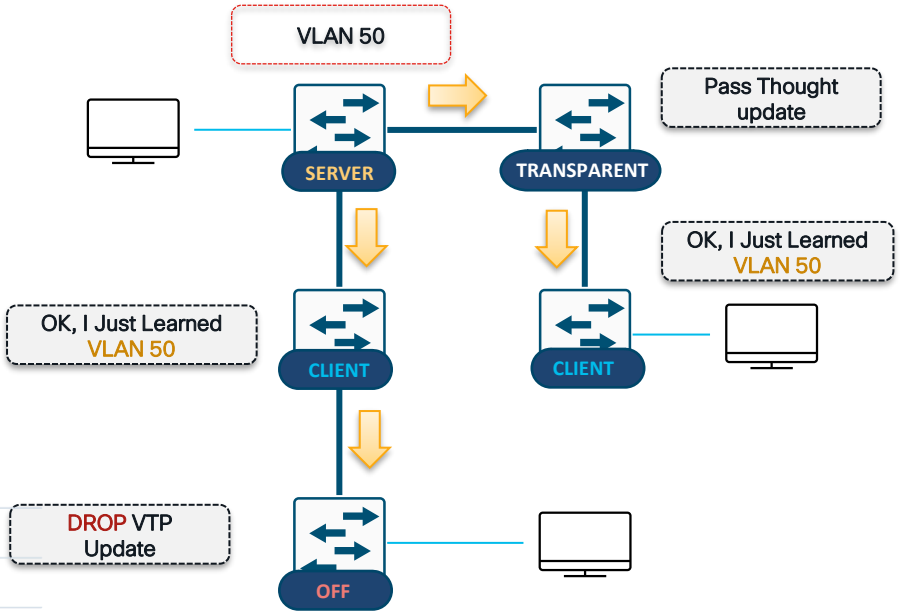
Best Practices

- Typically deployed on interconnection between
  access and distribution layers
- Use VTP transparent mode to decrease potential for operational error
- Hard set trunk mode to ON and encapsulation negotiate off for optimal convergence
- Change the native VLAN to something unused to avoid VLAN hopping
- Manually prune all VLANS except those needed
- Disable on host ports*

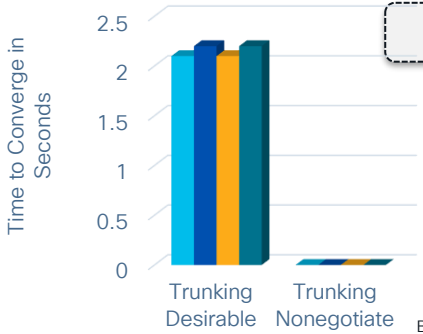


Virtual Trunk Protocol (VTP)

- Centralized VLAN management
- VTP server switch propagates VLAN database to VTP client switches
- Runs only on trunks
- Four modes:
  - Server: updates clients and servers
  - Client: receive updates– cannot make changes
  - Transparent: let updates pass through
  - Off: ignores VTP updates

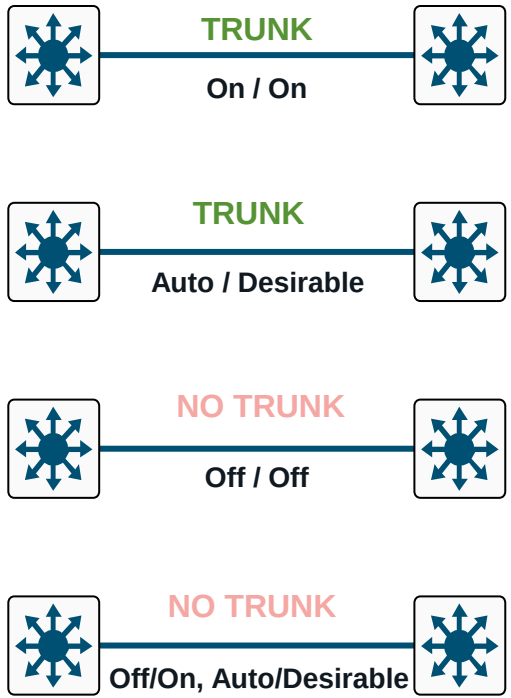


Trunk Auto/Desirable Takes Some Time



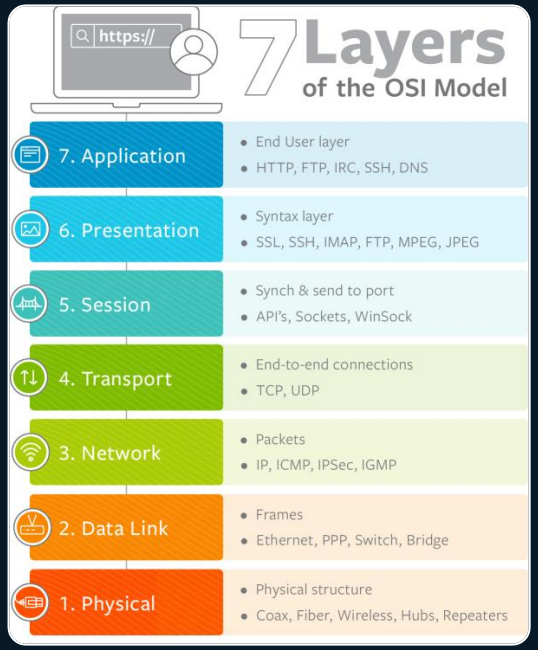
Dynamic Trunk Protocol (DTP)

- Automatic formation of trunked switch-to-switch interconnection
  - On: always be a trunk
  - Desirable: ask if the other side can/will
  - Auto: if the other sides asks I will
  - Off: don't become a trunk



Campus Services

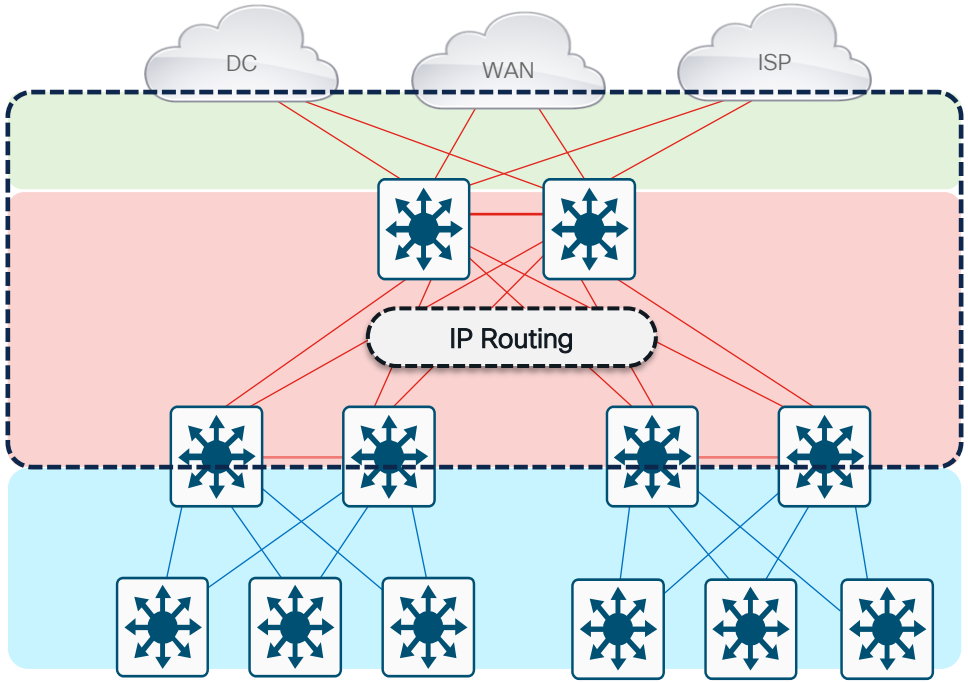
- **Layer 1 physical layer & links**
- **Layer 2 switching protocols**
- **Layer 3 routing protocols**
  - **Best practices**
  - **FHRP**
  - **Summarization**
  - **BFD**



L3 Routing Protocols

Best Practices

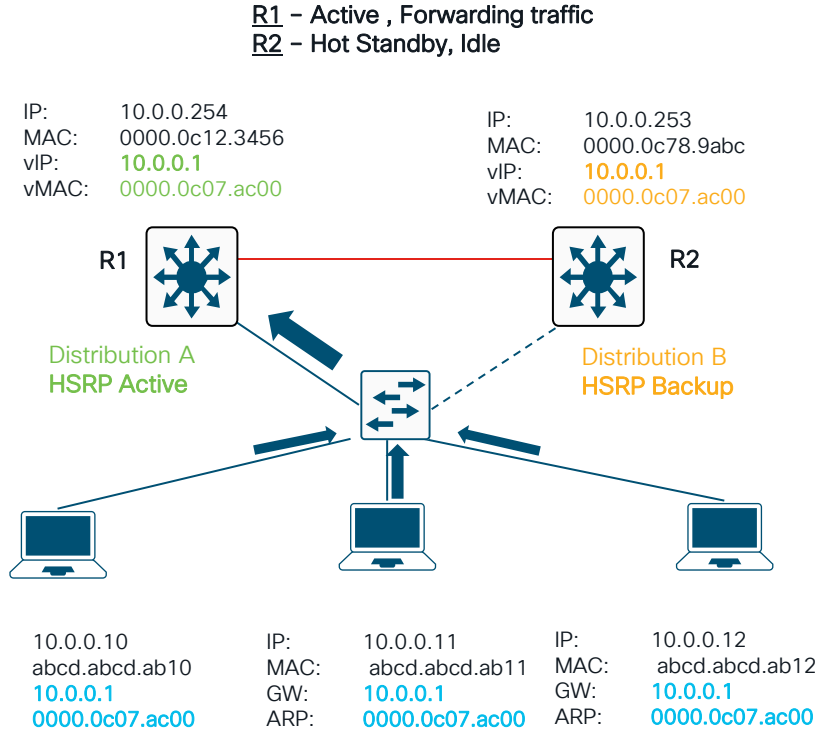
- Typically deployed in Distribution-to-Core, and Core-to-Core interconnects
- Used to quickly re-route around failed nodes or links, while providing load balancing over redundant paths
- Build Triangles - Not Squares for deterministic convergence
- Insure redundant L3 paths to avoid black holes
- Only create peers on links that you intend to use as transit



First Hop Redundancy

Hot-Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP)

- A pair of L3 routers function as one virtual router by sharing one virtual IP address and one virtual MAC address
- One L3 router is elected as “Active” and performs packet forwarding for local hosts
- The other routers are elected as “Standby” in case the Active router fails
- Standby routers stay idle and do not participate in packet forwarding
  - Use alternating Active/Standby routers for different VLANs (known as Load-Splitting)
    - www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp-v2.html
    - www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html



Redundancy and Protocol Interaction

Layer 2 and 3 - Why Use Routed Interfaces

L3 routed interface provides faster convergence than **L2 switch port** with an associated L3 SVI

1. Link Down
2. Interface Down
3. Routing Update

1. Link Down
2. Interface Down
3. Autostate
4. SVI Down
5. Routing Update

~ 8 msec loss

```
21:38:37.042 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet3/1, changed state to down

21:38:37.050 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet3/1,
changed state to down

21:38:37.050 UTC: IP-EIGRP(Default-IP-Routing-Table:100): Callback:
route_adjust GigabitEthernet3/1
```

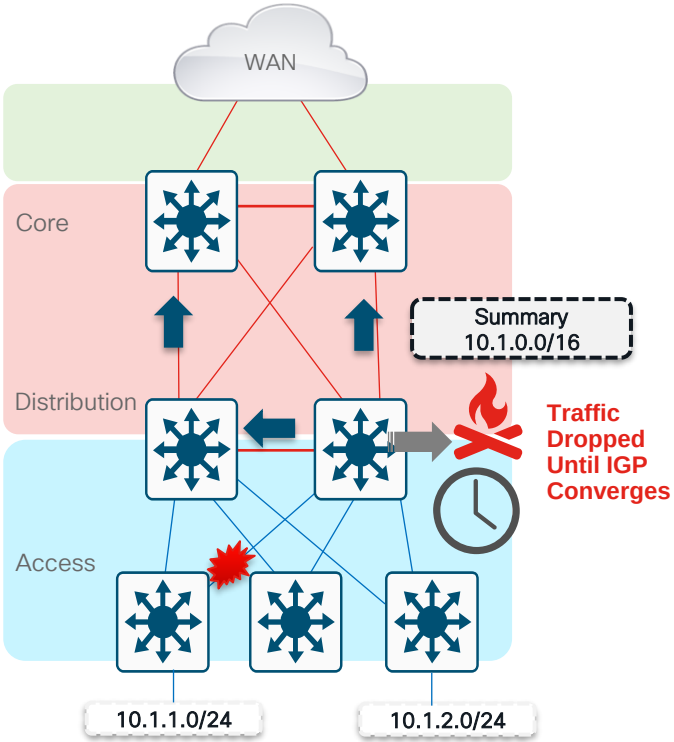
~ 150–200 msec loss

```
21:32:47.813 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet2/1, changed state to down

21:32:47.821 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet2/1, changed
state to down

21:32:48.069 UTC: %LINK-3-UPDOWN: Interface Vlan301, changed state to down

21:32:48.069 UTC: IP-EIGRP(Default-IP-Routing-Table:100): Callback: route,
adjust Vlan301
```

Why You Want to Summarize at the Distribution

Reduce the Complexity of IGP Convergence

- It is important to **force summarization** at the distribution **towards the core**
- For return path traffic an OSPF or EIGRP re-route is required
- By **limiting the number of peers** an EIGRP router must query or the number of LSAs an OSPF peer must process we can optimize his reroute
  - For EIGRP if we summarize at the Distribution, we stop queries at the core boxes for an Access layer flap
  - For OSPF when we summarize at the Distribution (area border or L1/L2 border), flooding of LSAs is limited to the Distribution: SPF now deals with one LSA not three.



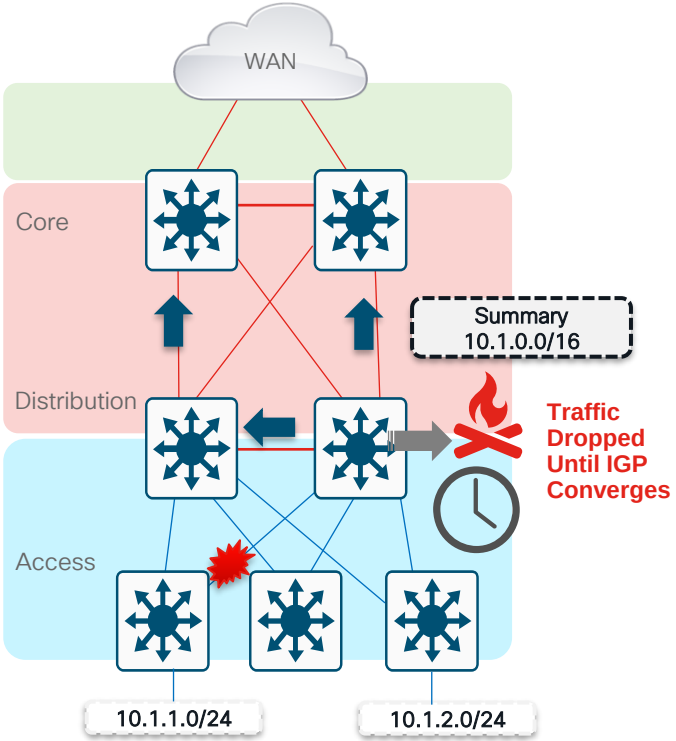
Why You Want to Summarize at the Distribution

Limit EIGRP Queries and OSPF LSA Propagation

- It is important to force summarization at the distribution towards the core
- For return path traffic an OSPF or EIGRP re-route is required
- By limiting the number of peers an EIGRP router must query or the number of LSAs an OSPF peer must process we can optimize this reroute

EIGRP Example:

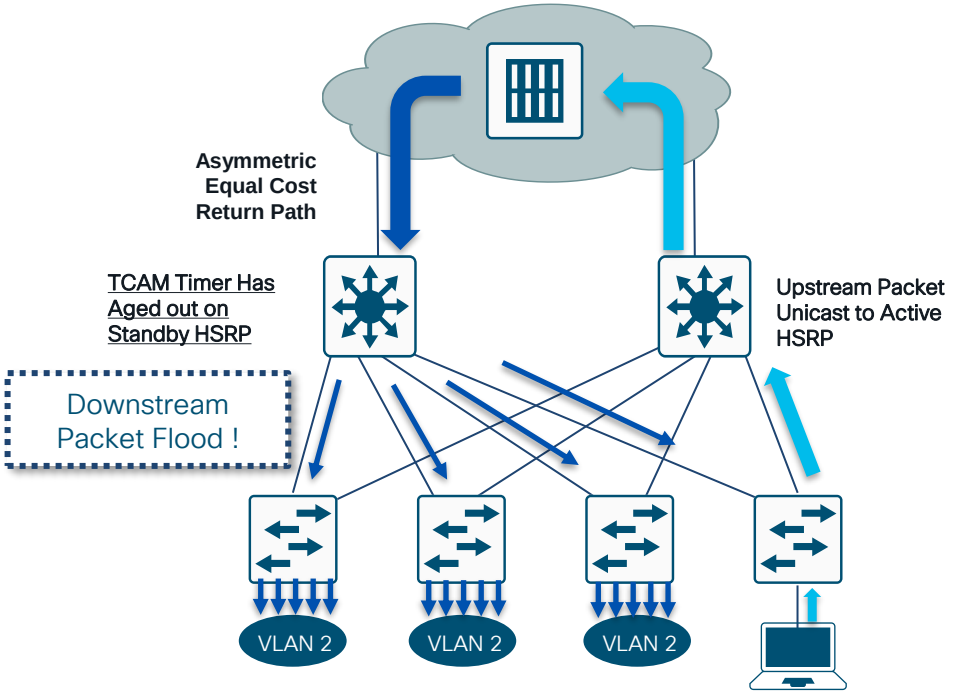
```
interface Port-channel1
 description to Core#1
 ip address 10.122.0.34 255.255.255.252
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip summary-address eigrp 100 10.1.0.0 255.255.0.0 5
```



Asymmetric Routing (Unicast Flooding)

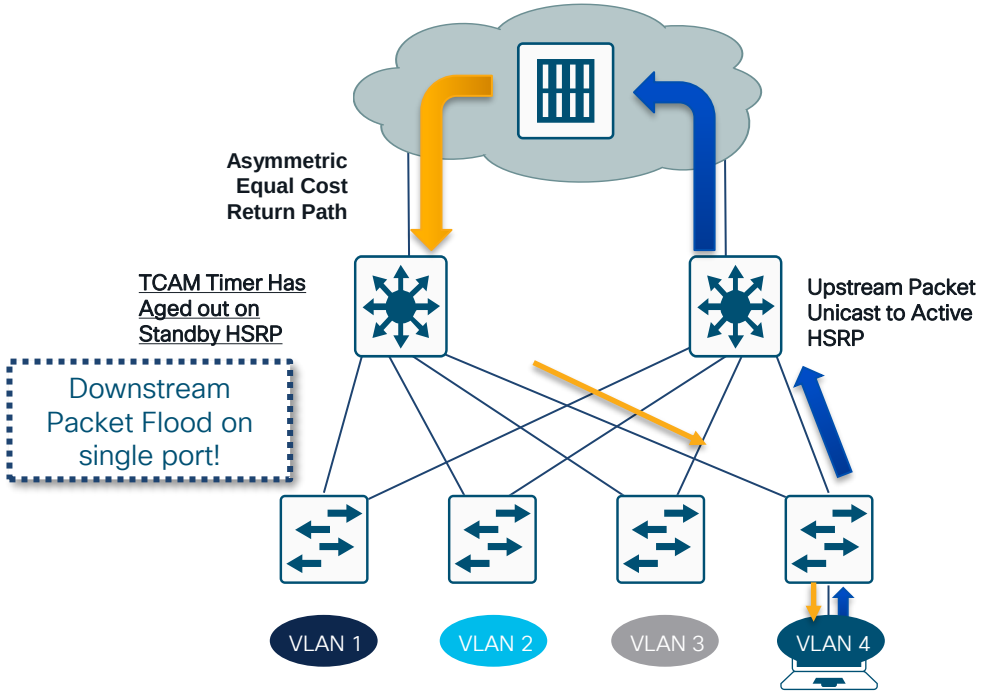
Affects redundant topologies with shared L2 access

- One path upstream and two paths downstream
- CAM table entry ages out on standby HSRP
- Without a CAM entry packet is flooded to all ports in the VLAN



Best Practices Prevent Unicast Flooding

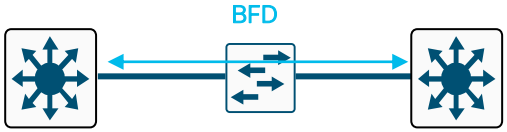
- Assign one unique data and voice VLAN to each access switch
- Traffic is now only flooded down one trunk
- Access switch unicasts correctly; no flooding to all ports
- If you have to:
  - Tune ARP and CAM aging timers; CAM timer exceeds ARP timer
  - Bias routing metrics to remove equal cost routes



Bidirectional Forwarding Detection (BFD)

- Detect faults between 2 routers
  - Fast (reaction time in milliseconds)
  - Single mechanism to signal upper-layer routing protocols (ISIS, BGP, OSFP, Static) that link is down
    - faster than the DEAD timer of that protocol
  - Works on directly-connected (single hop) routers, as well as routers separated by an L2 overlay (Metro Ethernet, MPLS, VPLS/Pseudowire, etc.)
  - Uses fast exchange of IP/UDP packets
    - port 3784 for control
    - port 3785 for echo
- Supports single-hop and multi-hop

The official recommendation for Catalyst 9000 switches
- 250ms x3 for physical interfaces
- 750ms x3 for SVI




```
interface Gig1/0/1
 ip address 1.1.1.1 255.255.255.0
 bfd interval 300 min_rx 300 multiplier 3
 ip ospf 1 area 0

router ospf 1
 bfd all-interfaces
```

Distribution Interconnection

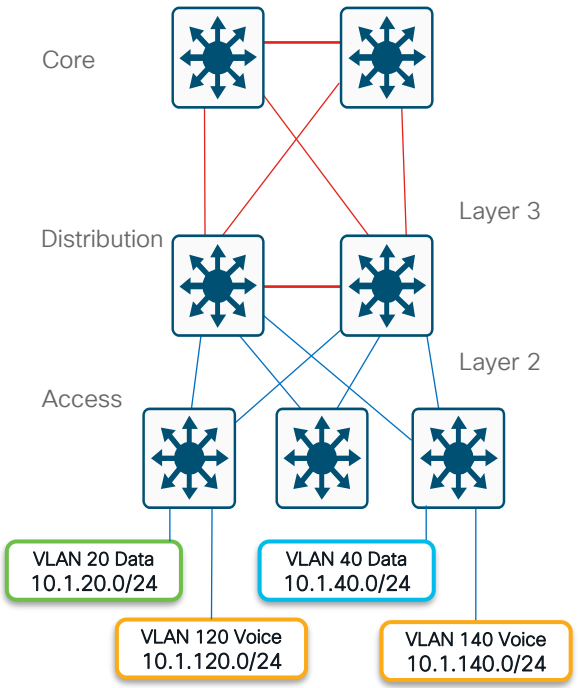
Best Practices - Summary

Core

Distribution

Access

- ✓ Summarize routes towards Core
- ✓ Limit redundant IGP peering
  - User EtherChannels
  - Passive interfaces to Access
- ✓ HSRP Active tuning
- ✓ Set Trunk mode on/no-negotiate
- ✓ Set EtherChannel mode on/auto
- ✓ STP Root tuning
- ✓ RootGuard or BPDU-Guard
- ✓ Limit protocols on Access ports:
  - Enable PortFast
  - Disable Trunking
  - Disable EtherChannel
- ✓ Use Port Security features



Layer 3 Distribution Interconnection

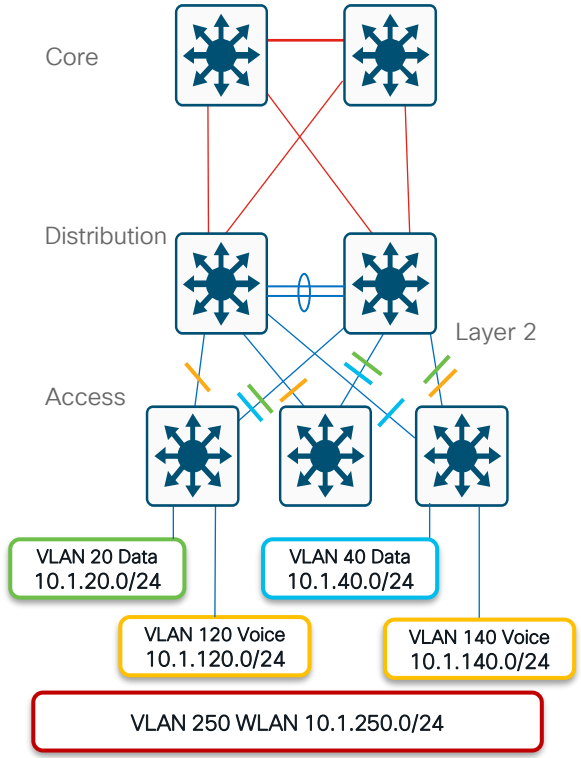
Layer 2 Access - Some VLANs Span Access Layer

Core

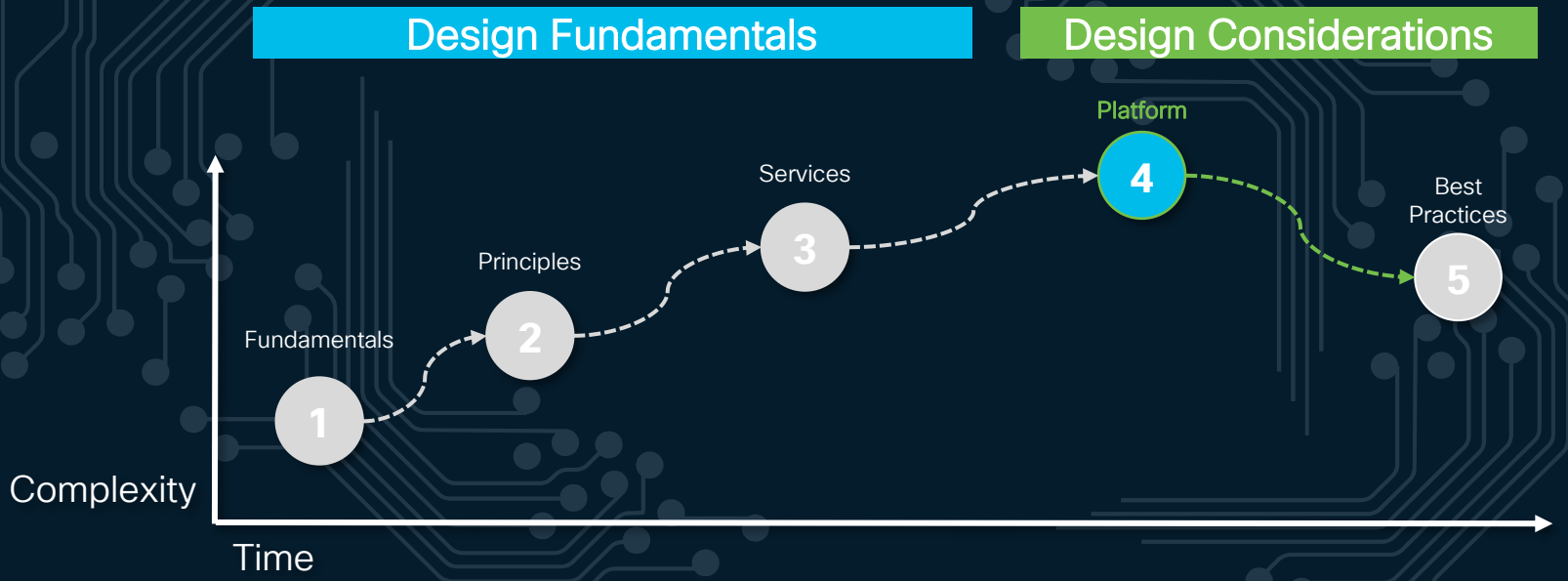
Distribution

Access

- Tune CEF load balancing
- Summarize routes towards core
- Limit redundant IGP peering
- STP Root and HSRP primary or GLBP and STP port cost tuning to load balance on uplinks
- Set trunk mode on/no-negotiate
- Disable Ether Channel unless needed
- RootGuard on downlinks
- LoopGuard on uplinks
- Set port host on access Layer ports:
  - Disable trunking
  - Disable Ether Channel
  - Enable PortFast
- RootGuard or BPDU-Guard
- Use security features

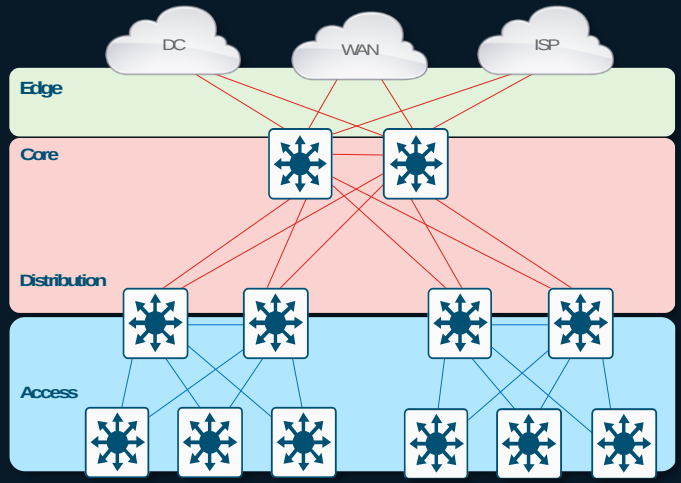


Session Agenda



Platform Design

- Chassis Considerations
- Cabling Considerations
- Feature Considerations



Design

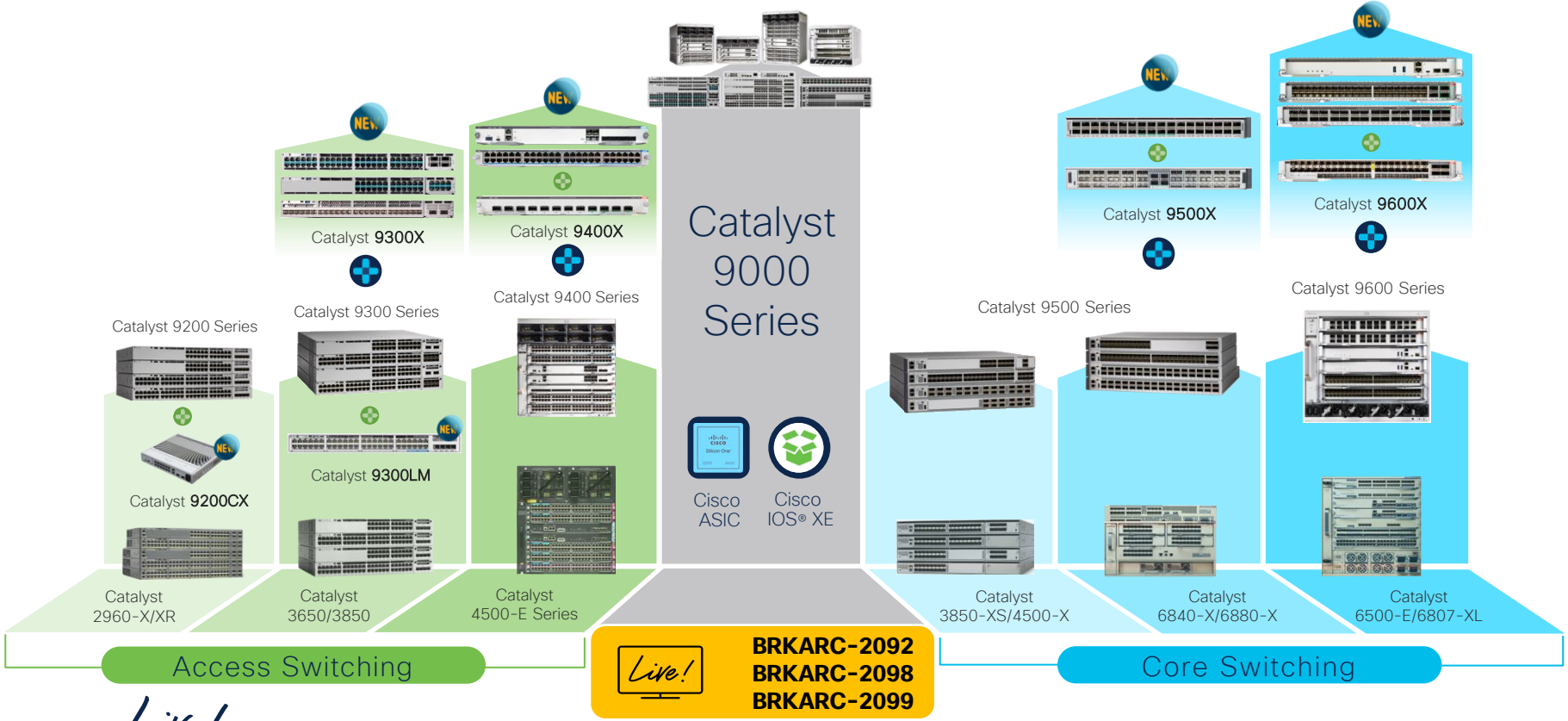
Platform Design

- **Chassis Considerations**
  - Catalyst 9k (Overview)
  - Software vs. Hardware
  - Modular vs. Fixed
- **Cabling Considerations**
- **Feature Considerations**

Cisco Catalyst 9000 Switching Portfolio

2022-2024 NEW

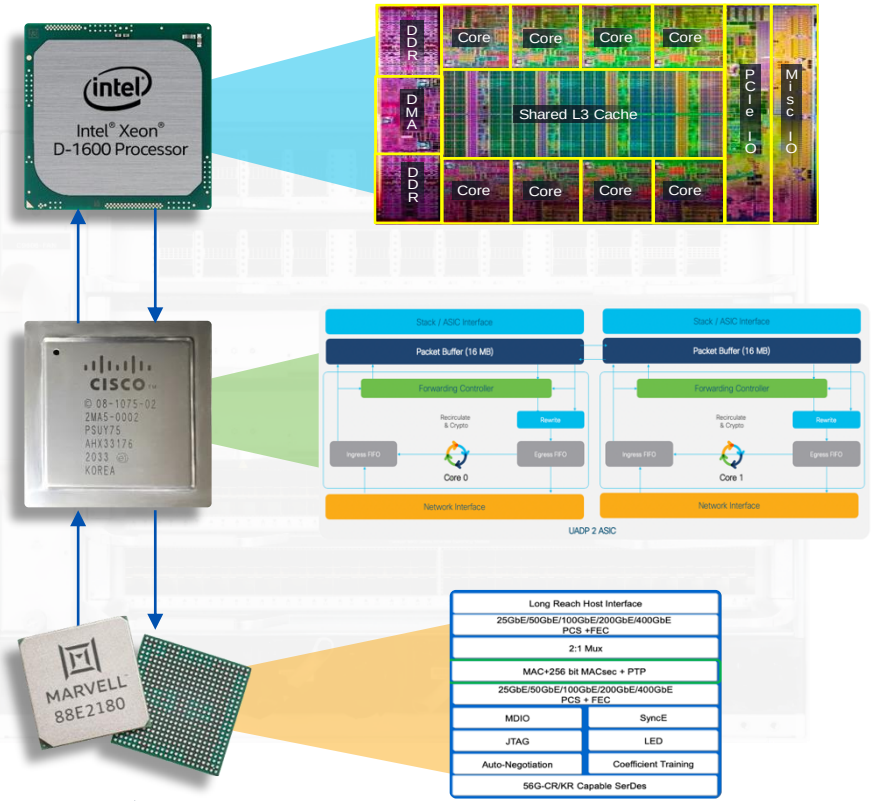
One Family from Access to Core – Common Hardware & Software



Live! BRKARC-2092 BRKARC-2098 BRKARC-2099

Software vs. Hardware

What to look at when selecting the Switch



CPU/DRAM

Where the OS "software" runs. Includes control-plane, data-plane and system-management functions.

- OS layer – IOSXE (IOSd) and Features, etc.
- System layer – FMAN, CMAN, IOMD, FED, etc.

ASIC(s) – Application Specific Integrated Circuit

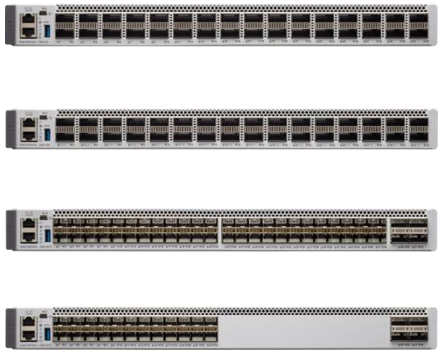
Where the "hardware" processing of traffic & services runs. Uses forwarding and state tables programmed by the software.

- Forwarding – L2, L3, ECMP, Encap, etc.
- Services – ACLs, QoS, Analytics, Encryption, etc.

Stub/PHY(s)

Transforms electrical and optical signals, splits or combines signals, and other various "physical" layer functions, such as encryption and timestamping.

Modular vs. Fixed Platforms



Modular

PROs	CONs
• More Flexible	• More Complex
• Longer Life-Cycle	• BW limit by Chassis
• Higher Port Density	• Slow(er) Dev & Test
• More Power/Cooling	• Lower MTBF
• Redundant Processors	• Higher COGs

Fixed

PROs	CONs
• Less Complex	• Less Flexible
• Swap Chassis for BW	• Shorter Life-Cycle
• Faster Dev & Test	• Lower Port Density
• Higher MTBF	• Less Power/Cooling
• Lower COGs	• Single Processor

Modular Platform Features & Benefits

Redundancy, Expansion, Efficiency & Flexibility

Highest Resiliency

Redundant Supervisors
StackWise® Virtual
Easy Upgrades with ISSU & GIR
Redundant Fans (Fan-Tray)
Redundant PSUs (1:1, N+1)

Highest Flexibility

SUP1 for Small Designs
SUP2/XL for Large Designs
Custom ASIC Scale Templates
Traditional Multi-Layer Designs
Fabric Overlay Designs

Highest Efficiency

Lowest Watts per Port
3000W Power Supplies
Titanium Rated (95%) PSUs
AC and/or DC Power
Configurable Power Priority

Longest Lifecycle

Start w/ SUP1 & few Gen1 LCs
Add Gen1 LCs as Access grows
Replace SUP1 with SUP2
Gen1 LCs get a 2X boost
Add new Gen2 LCs as Core grows

Most Port Options

Mixes of RJ45, SFP & QSFP

C9600-LC-40YL4CD
40x 50G SFP + 2x 100G + 2x 400G QSFP

C9600X-LC-32CD
32x 100G or 24x + 8x 400G QSFP

C9400-LC-48XS
48x 1/10G SFP

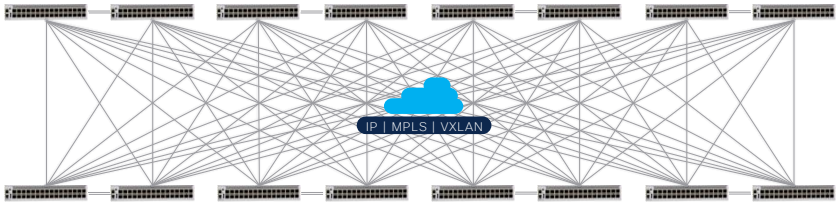
C9400-LC-48HX
48 x 10G mGig + UPOE®

Modular Design for Large Campus

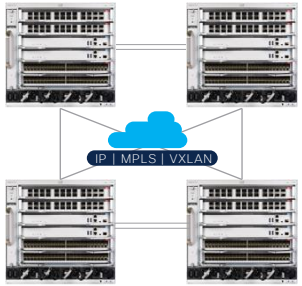
Architecture Perspective – Full Mesh vs. Hierarchical Design

Fixed System Design

- Static
- Costly
- Complex



Modular System Design



- Simple
- Scalable
- Sustainable

Modular System Benefits

Sustainable

Reduce Energy Demand
Reduce Carbon footprint
Environmental efficient

Cost

Reduce cost – CAPEX | OPEX
License & Service Management
Reduce product life-cycle TCO

Operation

Proven for large Enterprise
Day 0 – N scalable architecture
Simplified Tools and Management

Flexible

Pay-As-You-Grow model
Elastic Aggregation. Static Core.
Simple and large L2 boundaries

Resilient

Non-stop communication
Protected network performance
Reduced MTTR and MTBF

Catalyst 9200/CX, 9300/X & 9400/X

BRKARC-2098

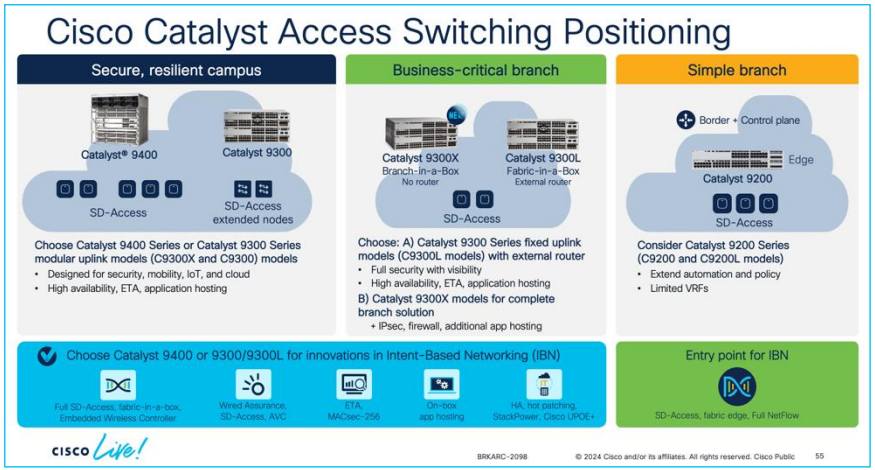
Catalyst 9000 Series Switching Family – Access

Minhaj Uddin - Leader Technical Marketing, Cisco

This session will cover the platform overview of Cisco Catalyst 9000 Series switches.

It will share the details of the Catalyst 9000 product portfolio, which will include new additions in fixed and modular access series – Catalyst 9200/CX, Catalyst 9300/X, and Catalyst 9400/X.

The session will talk about the component at the heart of these switches, which is the ASIC. It will also cover common attributes, technologies, and features in the Catalyst 9000 Series switches.



Catalyst 9500/X & 9600/X

BRKARC-2099

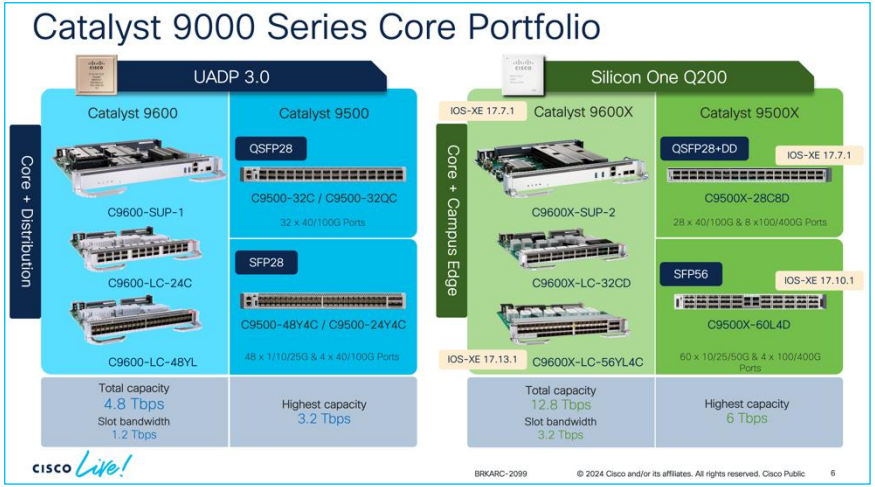
Catalyst 9000 Series Switching Family – Core & Distribution

Kenny Lei – Leader Technical Marketing, Cisco

This session will cover the platform overview of Catalyst 9000 Series core and distribution switches.

It will share the details of the Catalyst 9000 Series product portfolio, which will include new additions in fixed and modular core and distribution switching series: Catalyst 9500/X and Catalyst 9600/X.

The session will discuss the component at the heart of these switches, which is the ASIC, and it will also cover common attributes, technologies, and features in Catalyst 9000 switches.



Platform Design

- **Chassis Considerations**
- **Cabling Considerations**
  - Why 2.5, 5 & 10G?
  - Why 25G & 50G?
  - Why 100G & 400G?
- **Feature Considerations**

Copper vs. Fiber Media

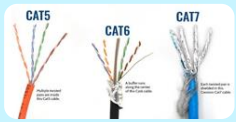
www.cisco.com/c/en/us/products/interfaces-modules/transceiver-modules/

Category 5, 6 & 7

Unshielded (UTP) | Shielded (STP)

RJ45 (Access to Endpoints)

Cat6A (Offset Wires) Cat5E (Flush Wires)



Category	Frequency	Distance	Data Rate	Shielding
5E	100-350 MHz	100m	1000 Mbps	UTP or STP
6	250-550 MHz	1G – 100m 10G - 50m	1 Gbps 10 Gbps	UTP or STP
6A	500-550 MHz	100m	10 Gbps	UTP or STP
7	600 MHz	100m	10 Gbps	Shielded only

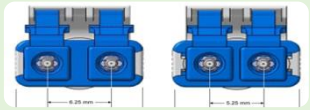
10M 100M 1G 2.5G 5G 10G

NBASE-T ALLIANCE

OM3, OM4 & OM5

Multi-Mode (MMF) | Single-Mode (SMF) | Wave-Division Multiplex (WDM)

SFP (Access & Distribution) **QSFP** (Core & Edge)

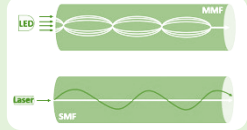


SFP-LC (LC Duplex) mSFP (Mini LC Duplex)

MPO12 (12 Fibers) MPO24 (24 Fibers)

Multimode
- Short distance cable runs (less than 1000ft.)
- High bandwidth support
- Higher cable cost
- Lower electronics cost
- Easier to terminate due to larger core size

Single Mode
- Long distance cable runs (greater than 1000ft.)
- Highest bandwidth support
- Lower cable cost
- Higher electronics cost
- Harder to terminate due to smaller core size

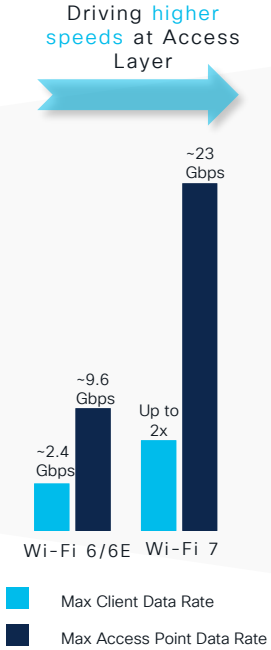


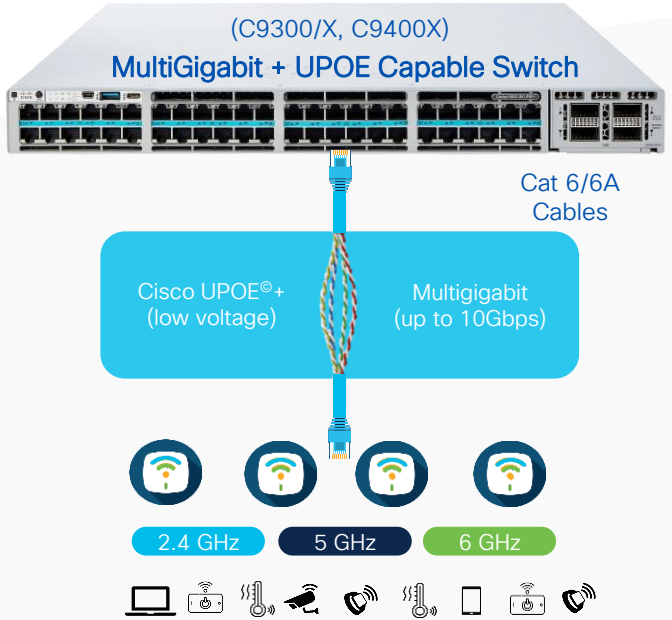
100M 1G 10G 25G 40G 50G (NEW) 100G 200G (NEW) 400G (NEW)

www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat9000-panduit-cables-wp-cte-en.html

Higher Speeds driving Multi-Gigabit Access

Future Proof with Speed and More Power Over Ethernet





Up to 10G speed

60W UPOE

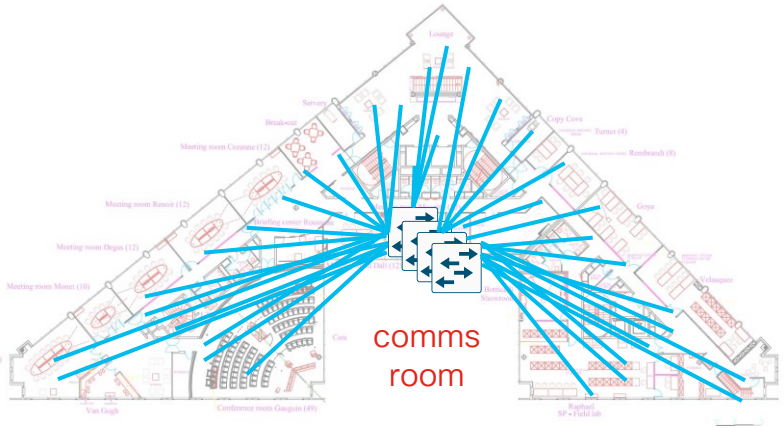
Dual 10G ports* (LACP & PoE Redundancy)

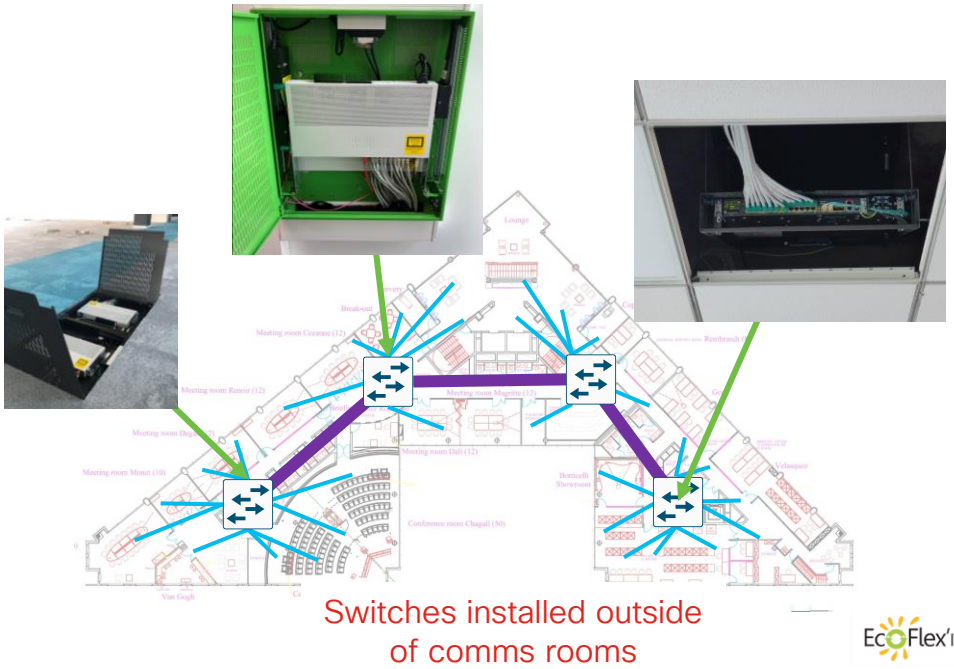
*CW9178I Model

Fiber To The Active Consolidation Point

EcoFlex'IT™

Upgrading Fiber/Ethernet cabling can be costly





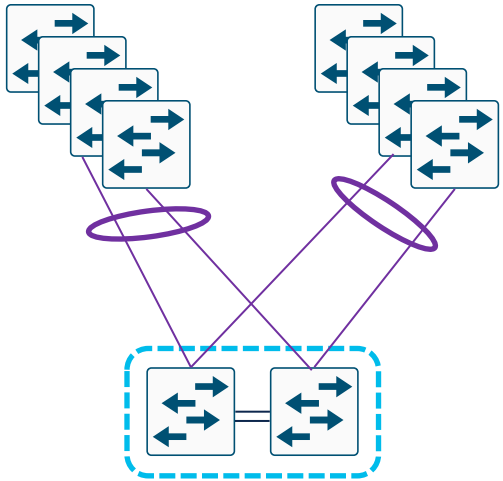
Traditional deployment

FTTACP-EcoFlex'IT™ deployment

https://osi.rosenberger.com/fileadmin/content/osi/EN/News/Whitepaper/Rosenberger_OSI_Whitepaper_FTT-ACP_EN.pdf

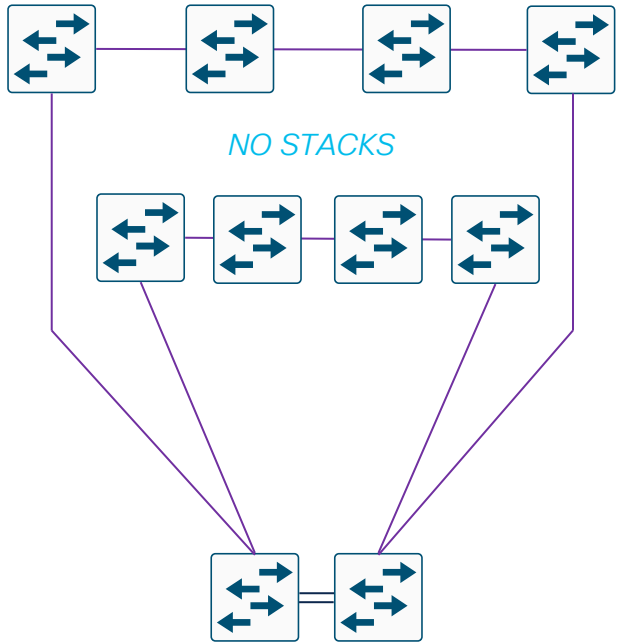
FTTACP-EcoFlex'IT™ impact...

Stack floor 1 Stack floor 2



Aggregation

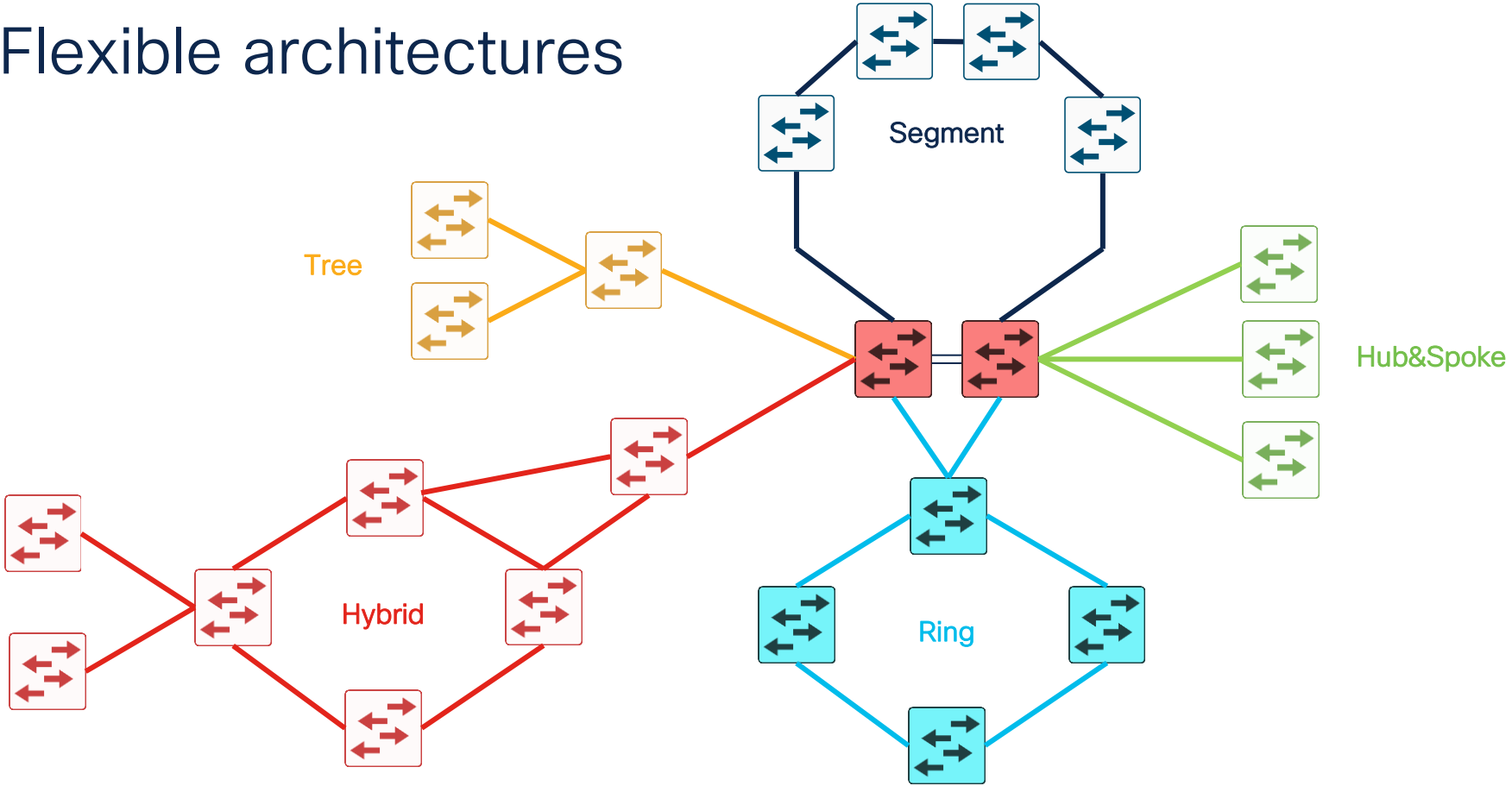
Traditional deployment



Aggregation

FTTACP-EcoFlex'IT™ deployment

Flexible architectures



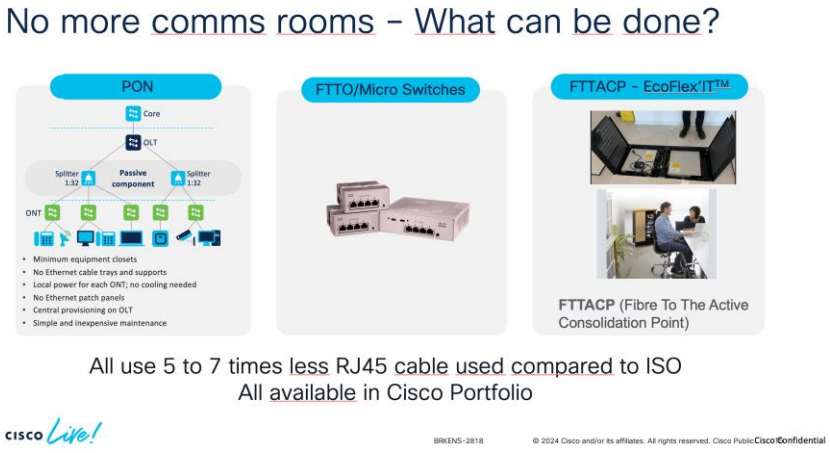
Sustainable Enterprise

BRKENS-2818

Cisco SD-Access for the Sustainable Enterprise

Jerome Durand - Technical Solutions Architect, Cisco

What if I told you that it's possible to remove comms rooms in your building floors, make associated air conditioning energy savings, increase usable surface in your premises, and drastically decrease the amount of copper wires and inherent cost. Would that trigger some appetite? What if I told you now that you can do all this and at the same time fully automate your network infrastructure, get more flexibility, and increase resiliency and security with micro-segmentation. Is this too good to be true? Come and see how Cisco SD-Access can be leveraged to improve sustainability and make building smarter.



25GE & 50GE – A Better Alternative

Provide a seamless migration path from 1/10GE SFP

Designation	Speed
L	50GE
Y	25GE
X	10GE

Catalyst 9600

C9600X-SUP2 & LC-40YL4CD

C9600-SUP1 & LC-48YL

Catalyst 9500

C9500X-60L4D

C9500-48Y4C

Catalyst 9400

C9400X-SUP2XL

C9400-SUP1XL-Y

Catalyst 9300

C9300X-NM-8Y

C9300-NM-2Y

Reduced CapEx through reuse of existing cabling

Single-Lane optics provide port densities similar to 10G

Gradual migration options with support for Dual-Rate optics

Reduced OpEx through savings in power and cooling

100GE & 400GE – A Better Alternative

Provide a seamless migration path from 40GE QSFP

Designation	Speed
D	400GE
C	100GE
Q	40GE

Catalyst 9600

C9600X-SUP2 & LC-32CD

C9600-SUP1 & LC-24C

Catalyst 9500

C9500X-28C8D

C9500-32C

Catalyst 9400

C9400X-SUP2XL

C9400-SUP1XL

Catalyst 9300

C9300X-NM-4C

C9300X-NM-2C

Reduced CapEx through reuse of existing cabling

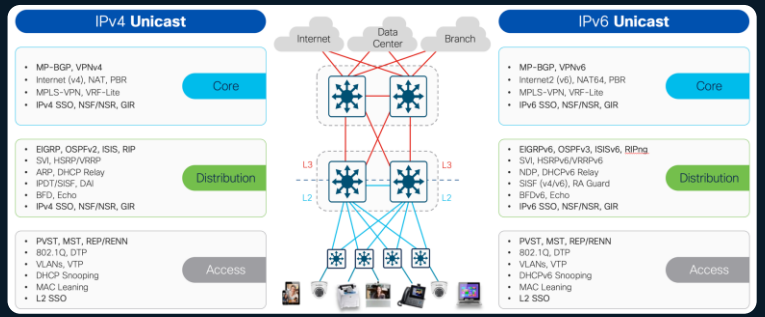
Single-Lane optics provide port densities similar to 40G

Gradual migration options with support for Dual-Rate optics

Reduced OpEx through savings in power and cooling

Platform Design

- **Chassis Considerations**
- **Cabling Considerations**
- **Feature Considerations**
  - Unicast (IPv4/IPv6)
  - **Multicast** (IPv4/IPv6)
  - Quality of Service (QoS)



Campus Networks

L2/L3 Unicast Technologies

IPv4 **Unicast**

Core

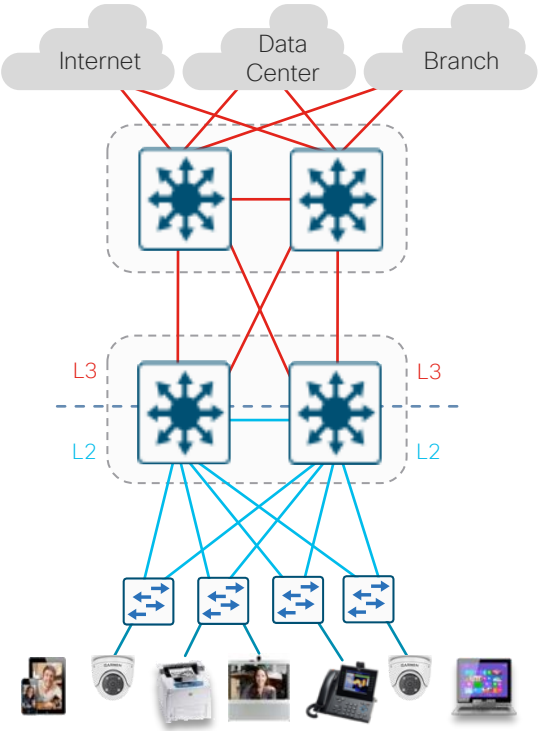
- MP-BGP, VPNv4
- Internet (v4), NAT, PBR
- MPLS-VPN, VRF-Lite
- IPv4 SSO, NSF/NSR, GIR

Distribution

- EIGRP, OSPFv2, ISIS, RIP
- SVI, HSRP/VRRP
- ARP, DHCP Relay
- IPDT/SISF, DAI
- BFD, Echo
- IPv4 SSO, NSF/NSR, GIR

Access

- PVST, MST, REP/RENN
- 802.1Q, DTP
- VLANs, VTP
- DHCP Snooping
- MAC Leaning
- L2 SSO



IPv6 **Unicast**

Core

- MP-BGP, VPNv6
- Internet2 (v6), NAT64, PBR
- MPLS-VPN, VRF-Lite
- IPv6 SSO, NSF/NSR, GIR

Distribution

- EIGRPv6, OSPFv3, ISISv6, RIPng
- SVI, HSRPv6/VRRPv6
- NDP, DHCPv6 Relay
- SISF (v4/v6), RA Guard
- BFDv6, Echo
- IPv6 SSO, NSF/NSR, GIR

Access

- PVST, MST, REP/RENN
- 802.1Q, DTP
- VLANs, VTP
- DHCPv6 Snooping
- MAC Leaning
- L2 SSO

Understanding L2 Scale

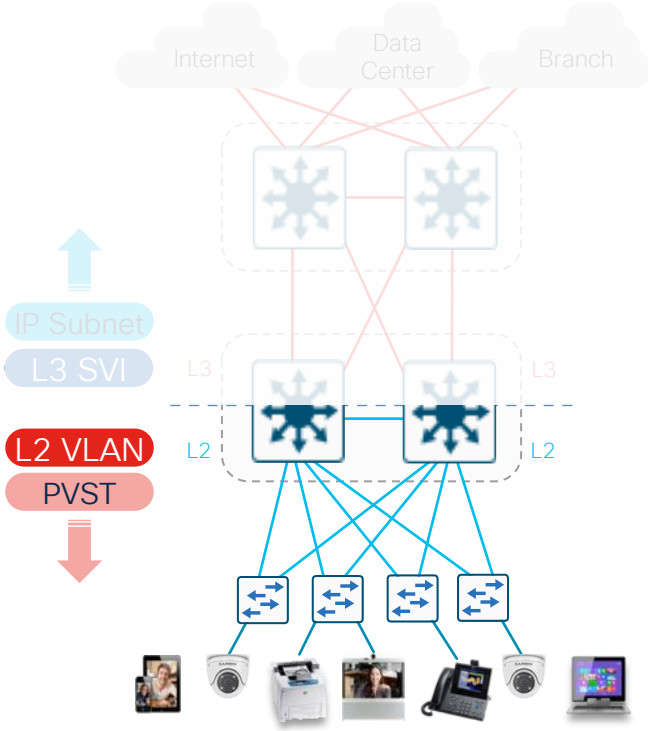
MAC Address Scale

Soft recommendation for Access to Distribution ≤ 20:1

- Each unique Endpoint (Host) will have 1x MAC address
  - Access: # Hosts = # MAC
- All MACs are learned on Distribution (STP Root)
  - Distro: Sum of # Access

1-1.5K x 20

SUM: 20-30K MACs



Campus Networks

L2/L3 Multicast Technologies

IPv4 **Multicast**

Core

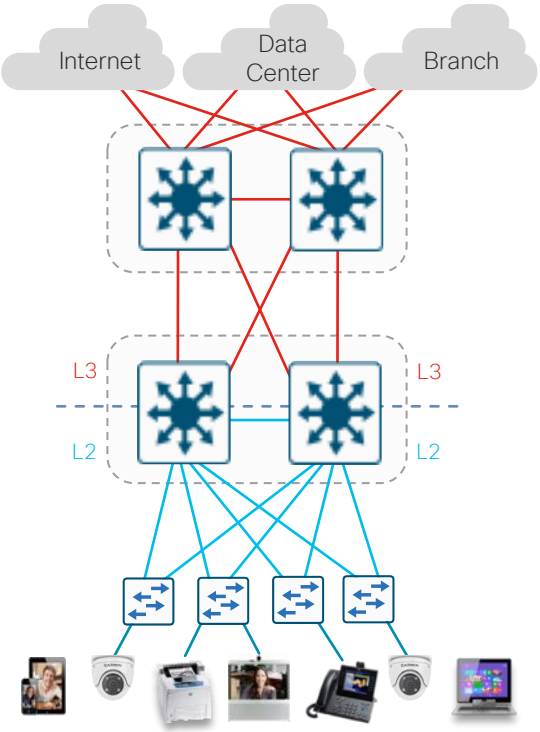
- PIM-SM, SSM and Bidir
- AutoRP, BSR RP, MSDP
- MVPN, Multicast VRF-Lite
- Multicast load splitting
- IPv4 multicast HA

Distribution

- Dual-stack IPv4 / IPv6
- PIM-SM, SSM and Bidir
- IGMPv2,v3 snooping
- Stub multicast routing
- PIM BFD
- IPv4 multicast HA

Access

- IGMP v1,v2,v3 snooping
- IPv4 multicast QoS & ACL
- IGMP v1,v2 filtering



IPv6 **Multicast**

Core

- PIM-SM and SSM
- IPv6 BSR RP
- IPv6 embedded RP
- IPv6 multicast HA

Distribution

- Dual-stack IPv4 / IPv6
- PIM-SM and SSM
- MLDv1,v2 snooping
- HW register and RPF
- HSRP-aware PIM
- IPv6 multicast HA

Access

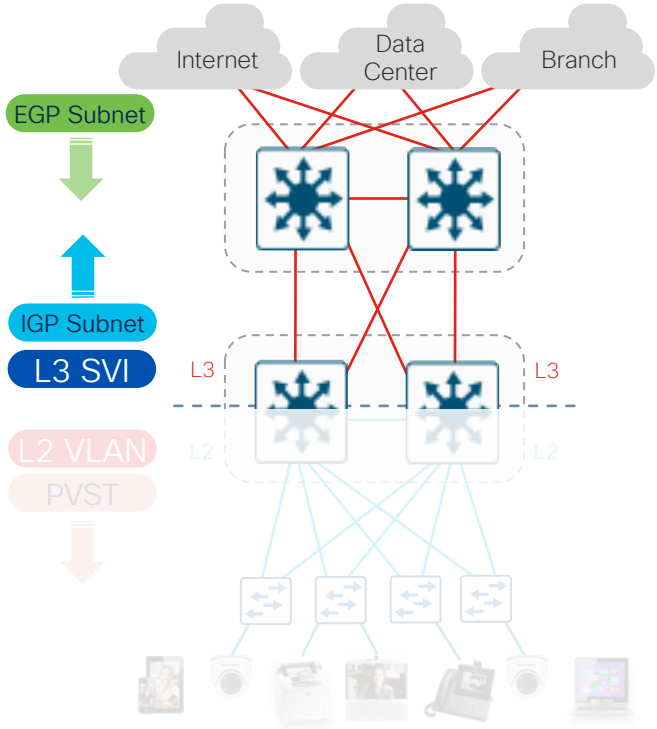
- MLD v1,v2 snooping
- IPv6 multicast QoS & ACL
- MLD v1,v2 filtering

Understanding L3 Scale

IP Route Scale

Soft recommendation for
Access to Distribution ≤ 20:1
Distribution to Core ≤ 4:1

- Each unique Endpoint (Host) will have 1x ARP (and/or 3+ NDP)
- All ARP/NDP resolve on Distribution (L3 SVI)
  - Distro: Sum of # Access = 1-3K x 20 = 20-60K
  - VLANs: 5-10 per Access = 4-5 x 20 = 100-200
- All SVI + WAN/DC (x VRF) Subnets on Core
  - Core(Site): Sum of # Distro = 10-20 x 200 = 2K-4K
  - WAN/DC: Sum of # Sites = 10-20 x 2K = 20K-40K
  - Internet: Feb. 2025 = ~990K IPv4, ~220K IPv6



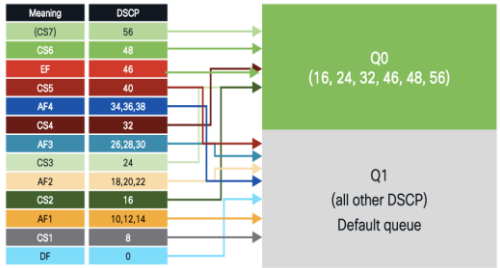
Transmit Queue Congestion

The Case for Campus QoS

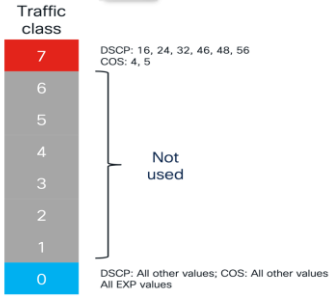
BRKENS-2096
BRKARC-2092

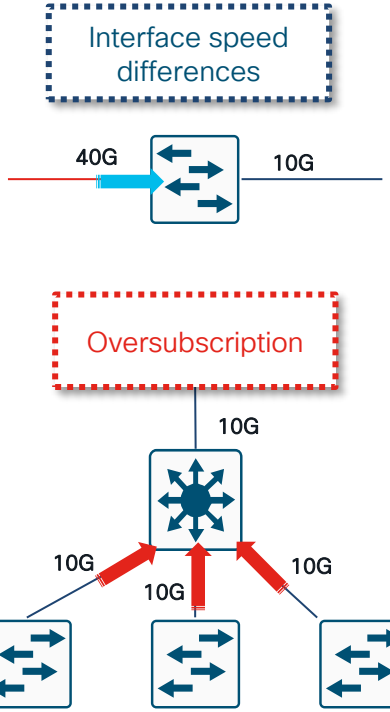
- The primary role of QoS in Campus networks is to manage packet loss
- In Campus networks – it takes only a few *milliseconds* of congestion to cause drops
- Rich media applications (audio/video) are extremely sensitive to packet drops

UADP 2.0/3.0 QoS



S1 Q200 QoS

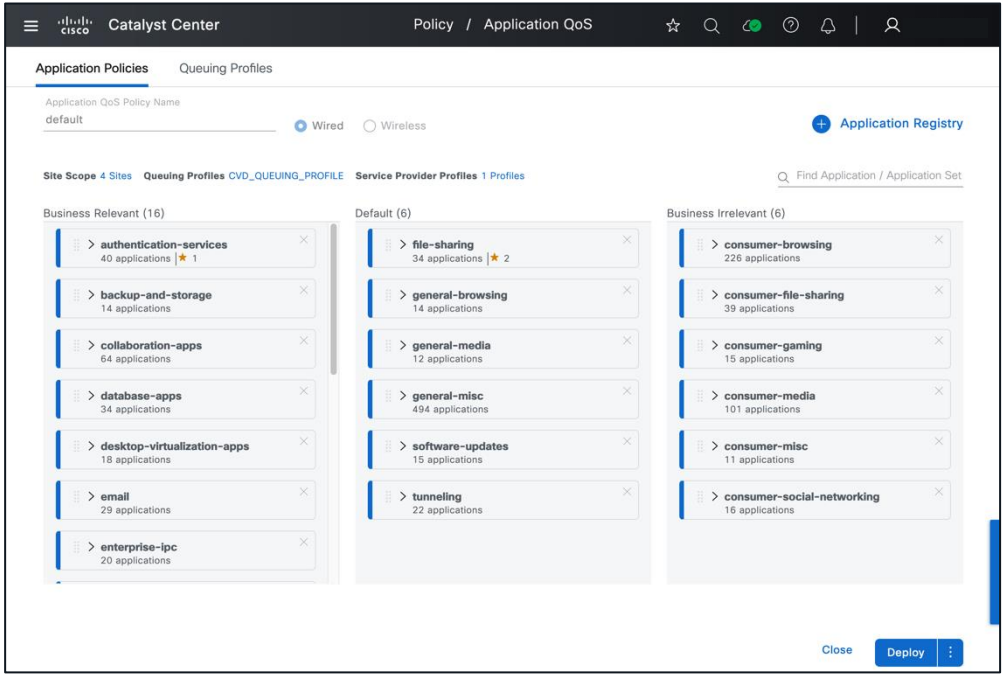




Design Fundamentals

Access Layer – Queuing with Cisco Catalyst Center Appliaction Policy

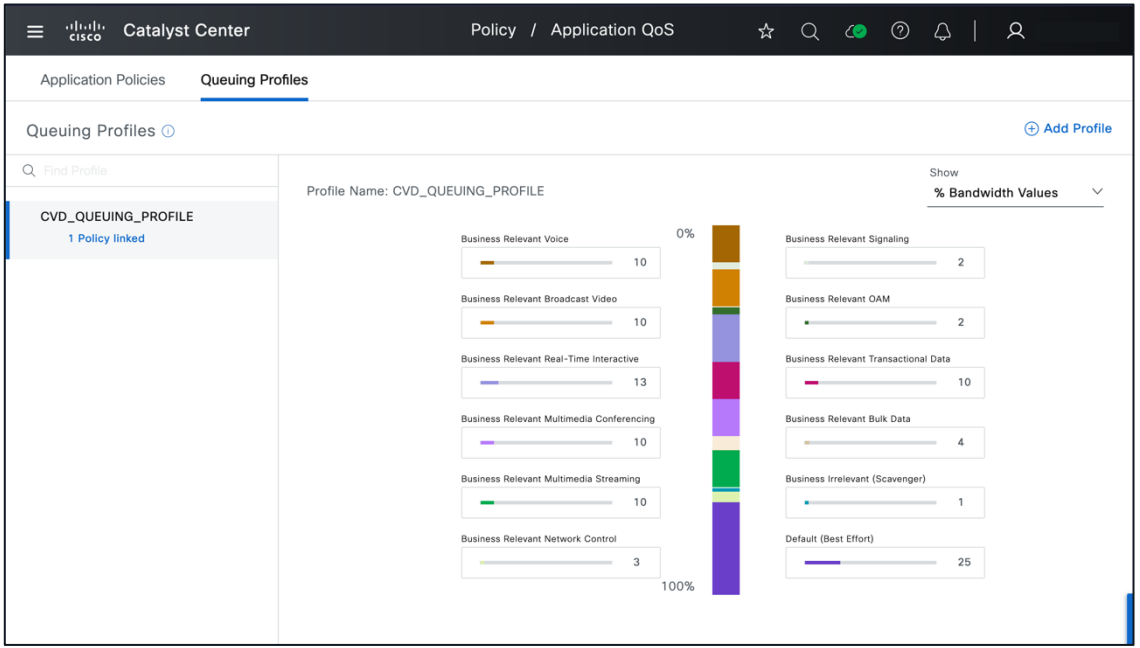
- Application Policy can be used to implement QoS
- Goes beyond default policies by deploying policies based on the “intent” of an organization



Design Fundamentals

Access Layer – Queuing with Cisco Catalyst Center Queueing Profile

- Application Policies and Queueing Profiles can be custom and could be defined per site/group of sites



Catalyst 9000 Switching QoS

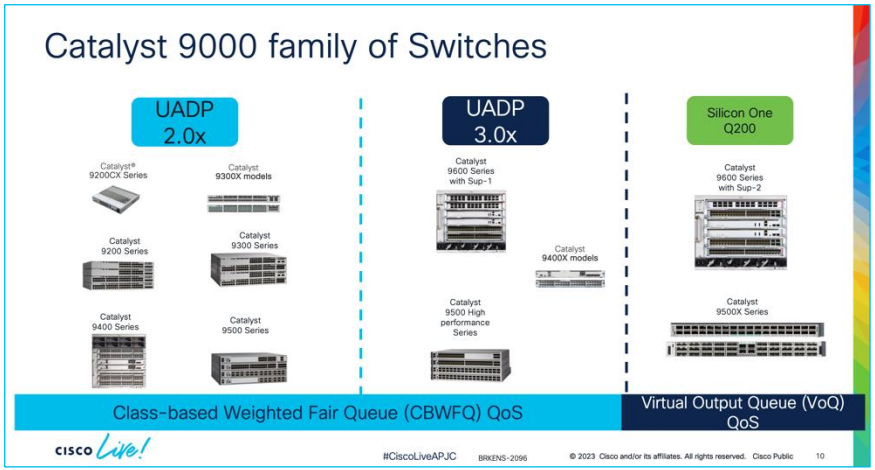
BRKENS-2096

Cisco Catalyst 9000 Switching QoS Deep Dive

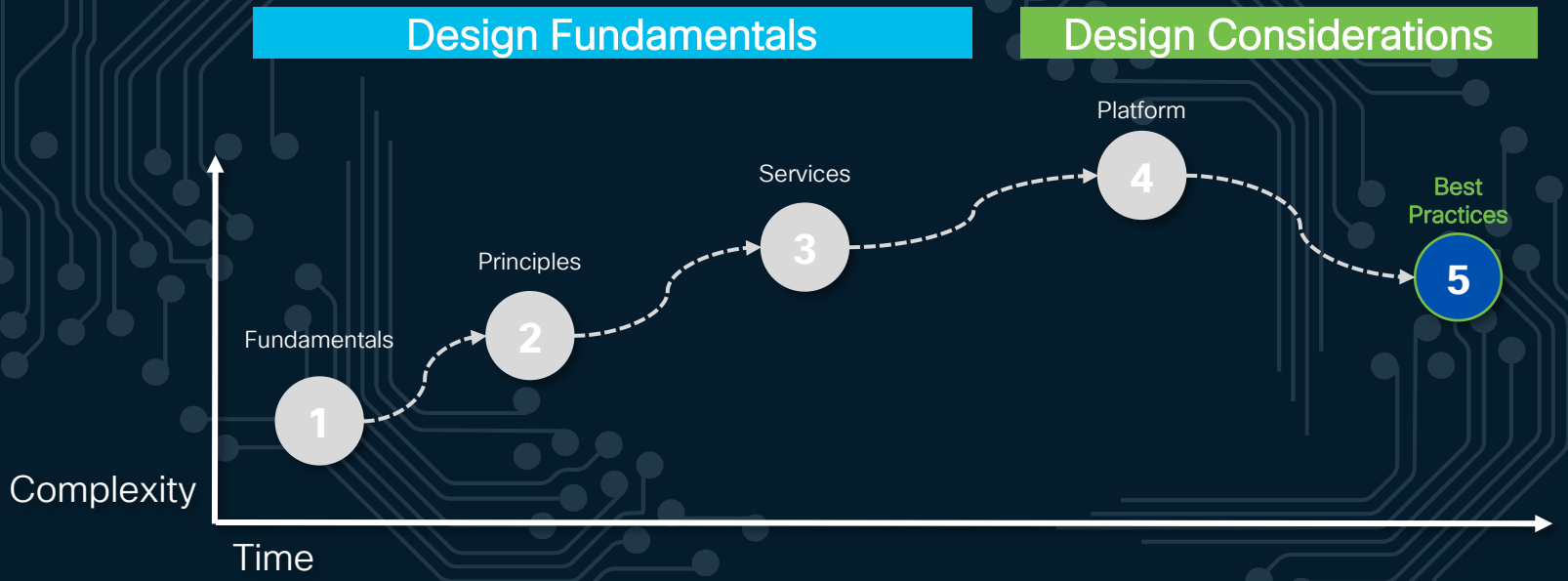
Ninad Diwakar - Technical Marketing, Cisco

This session will deep dive into the QoS model used in the Cisco Catalyst 9000 Series of switches powered by the Cisco UADP and Cisco Silicon One Q200 ASICs.

The session will cover platform-specific designs for classification, policing, and ingress and egress queueing policies which are applicable to the Catalyst 9200, 9300, 9400, 9500 and the 9600 switches. To close things off, the session will cover thought processes to be followed for migration configurations from Catalyst 6500 Series switches over to the Catalyst 9500/9600 Series switches.



Session Agenda



Best Practices

- **LAN High Availability**
- **LAN Security**
- **Virtual Networking**

Design

Best Practices

- **LAN High Availability**
  - **SSO / NSF**
  - **StackWise and StackWise Virtual**
  - **mLAG**
  - **In-Service Software Upgrades (ISSUs)**
  - **Extended Fast Software Upgrade (xFSU)**
  - **Power Redundancy**
- **LAN Security**
- **Virtual Networking**

Mission-Critical Resiliency

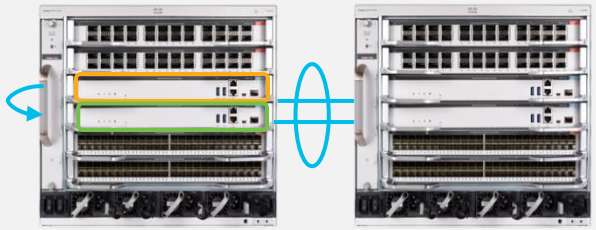
Your business stops if the network is down

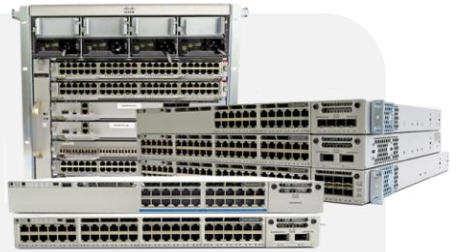
Cost of only **one hour** of downtime to an average enterprise > $300,000**

** Based on industry reports from Gartner and ITIC

Catalyst 9600

(Dual chassis w/ StackWise Virtual)





Catalyst 9300, 9400 & 9500

Architecture

StackWise® & StackWise Virtual

- Virtualized redundant systems for simplified configuration & protocols

Graceful Insertion/Removal (GIR)

- No downtime when device in maintenance mode

Operating System

Software Maintenance Upgrade (SMU)

- Minimal or no downtime patches

In-Service Software Upgrade (ISSU)

- Minimal or no traffic loss upgrade

Extended Fast Software Upgrade (xFSU) on C9300/L Stack

- < 5 sec downtime - Stack upgrade

Platform

Redundant Control & Data-Plane

- Dual Sup or Stack SSO/NSF
- SVL with Quad-SUP RPR

Redundant Power & Fans

- N+1 or Combined mode

StackPower for StackWise

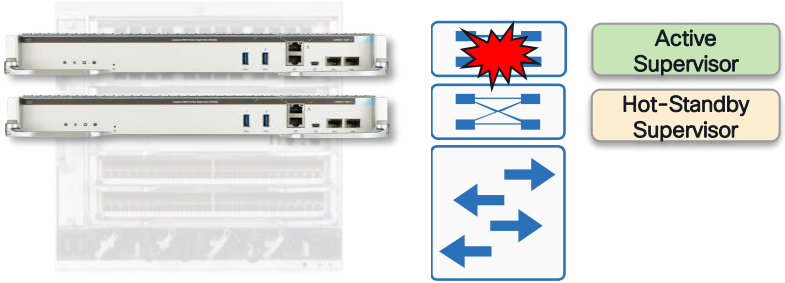
Eliminate downtime with **High Availability** designed at every level

High-Availability - SSO & NSF

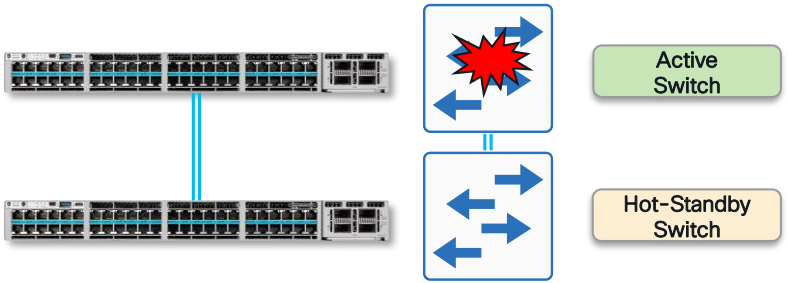
Stateful Switchover (SSO) and Non-Stop Forwarding (NSF)

- **Stateful Switchover** (SSO) synchronizes active process state and running-config, between Active & Standby supervisors or Active & Standby switches in a stack
  - Traffic loss minimized for Active supervisor or Active switch failure
- **Non-Stop Forwarding** (NSF) allows for graceful restart of L3 routing protocols

Modular Switch with **Redundant Supervisors**



StackWise Stack or **StackWise Virtual Pair**



LAN High Availability

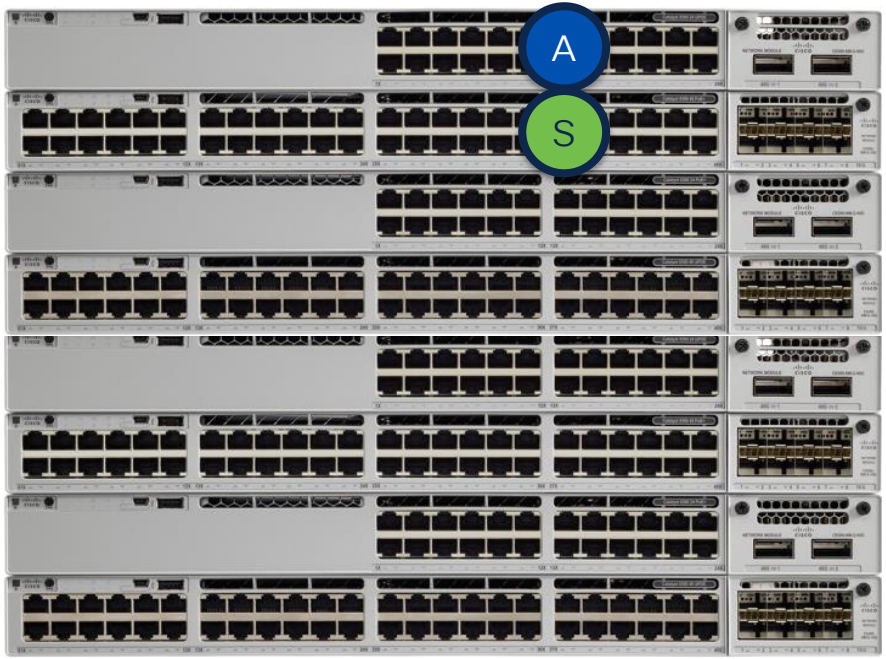
Cisco StackWise® – Access Switch Stacking


Catalyst 9300X/LM


Catalyst 9300/L


Catalyst 9200/L

SSO Active Switch responsible for:
- Management
- L2 protocols
- L3 protocols



StackWise - 80/160/360/480/1T*

Up to 8 Members

Centralized Control Plane

Distributed Data Plane

1+1 Stateful Redundancy with Active & Standby

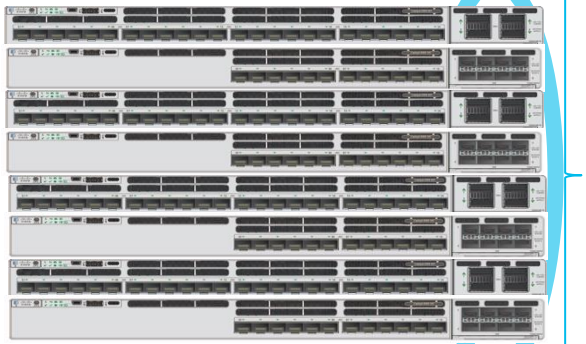
Stateful Switchover SSO/NSF

*StackWise speeds vary depending on platform choice

LAN High Availability

Switch Stacking - Catalyst 9300

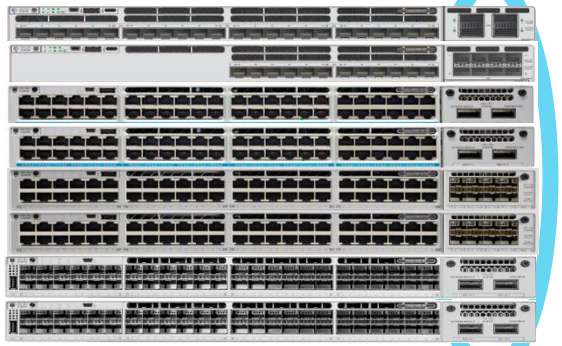
Modular Uplink
Catalyst 9300X models (10/25G Fiber)



8 switches

1T

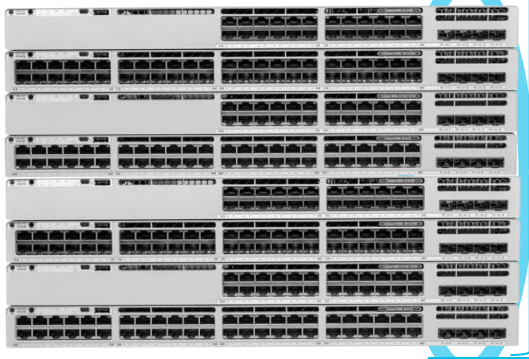
Modular Uplink
Catalyst 9300 (non -B) and Catalyst 9300X models



8 switches

480G

Fixed Uplink
Catalyst 9300L models



8 switches

320G

Stacking supported among Catalyst 9300X models and mixed stacking between Catalyst 9300 and Catalyst 9300X models

Stacking supported among Catalyst 9300L models only

9200 stacks with 9200 and 9200L stacks with 9200L

StackWise Access

The **StackWise** Access PIN focuses on combining multiple Access switches into a single virtual switch to increase access-layer port density.

- Typically, the same layer as Access (Tier 1)
- The same 'physical' topology as a multi-layer network

Main goal is to expand port density of Access layer

Same L2 protocols & features as Access

- North: VLAN, 802.1Q, STP, MAC, IGMP Snooping
- South: AAA, STP, Portfast, Storm-Control

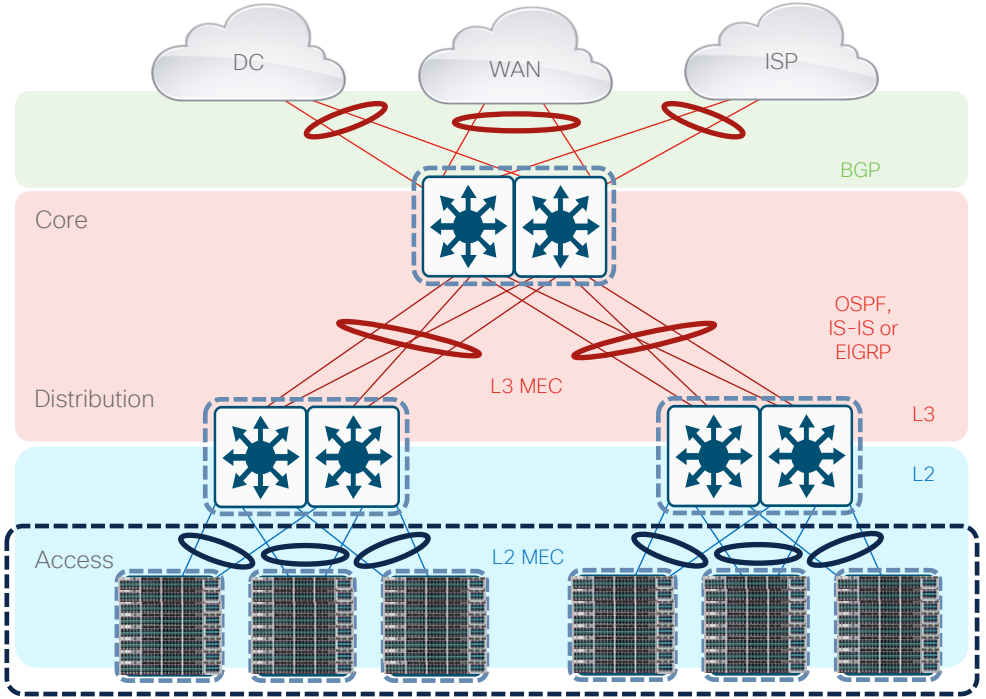
Leverages Stateful Switchover (SSO)

- Active/Standby Control-Plane (synchronized)
- Works with NSF/NSR for L3 protocols

Leverages Multi-chassis EtherChannel (MEC)

- Active/Active Data-Plane (both switches forwarding)
- L2 Portchannel (neighbor sees single neighbor)

Tends to require med-high L2 + feature scale



LAN High Availability

StackWise Virtual – Distro/Core Switch Stacking

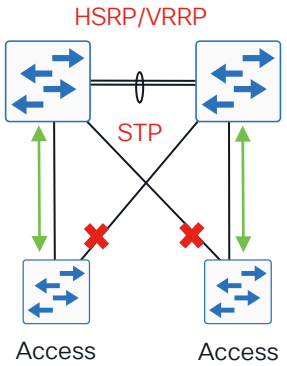

Catalyst 9600/X


Catalyst 9500/X

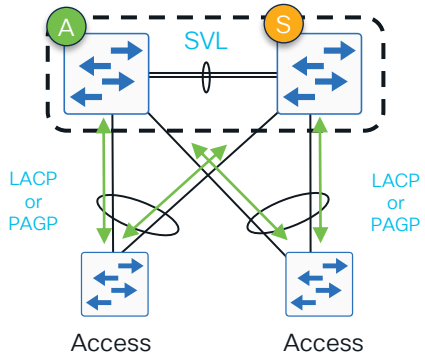

Catalyst 9400/X

SSO Active Switch responsible for:
- Management
- L2 protocols
- L3 protocols

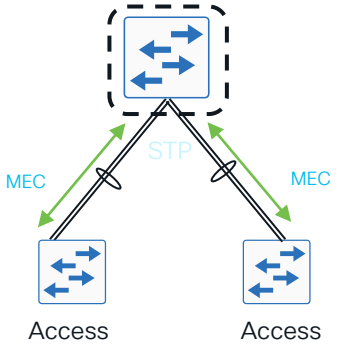
Traditional L2/L3



StackWise Virtual – Physical



StackWise Virtual – Logical



Both Active & Standby switches have Active data plane and make forwarding decisions

StackWise Virtual Technology

- Intended for **Distribution** and/or **Core** layer
- Available on **C9400**, **C9500** and **C9600**
- Formed using **Front Panel** ethernet ports

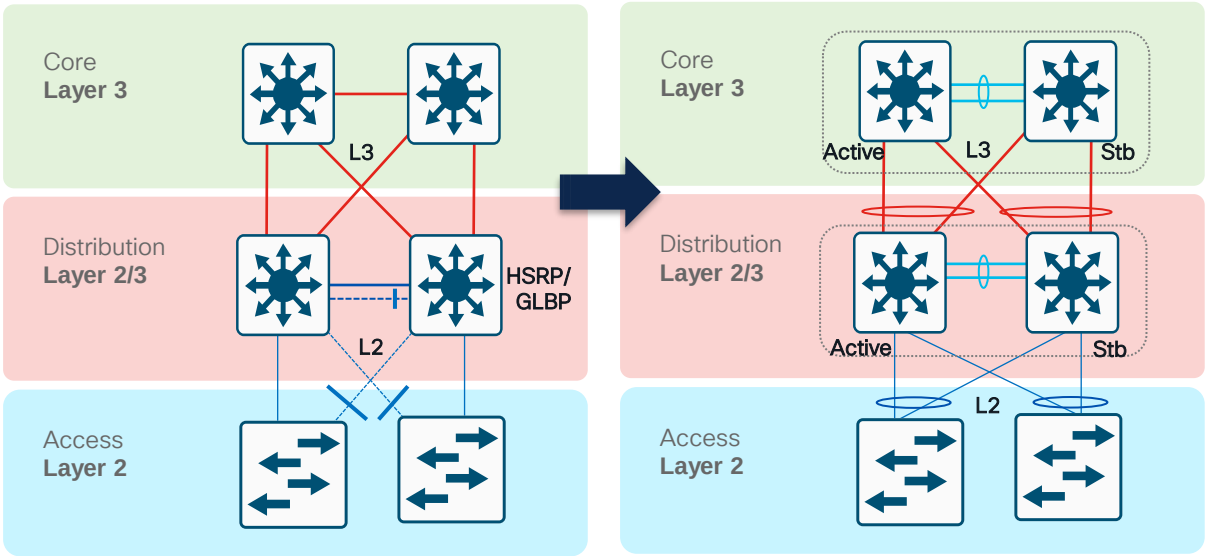

Catalyst 9600/X


Catalyst 9500/X


Catalyst 9400/X

up to 8x
10/25/50G SFP

up to 8x
40/100/400G QSFP



- 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)

StackWise Virtual Core/Distro

The **StackWise Virtual (SVL)** Core PIN focuses on combining Core and/or Distribution into a single virtual switch to connect to outside areas.

- Typically, the same layer as Distribution or Core (Tier 2-3)
- The same 'physical' topology as a multi-layer network

Main goal is to simplify and expand the Distribution and/or Core layer

Same L2/L3 protocols & features as Distro/Core

- North: SVI, ARP/ND, IGP/BGP, PIM
- South: VLAN, 802.1Q, MAC, IGMP (No STP)

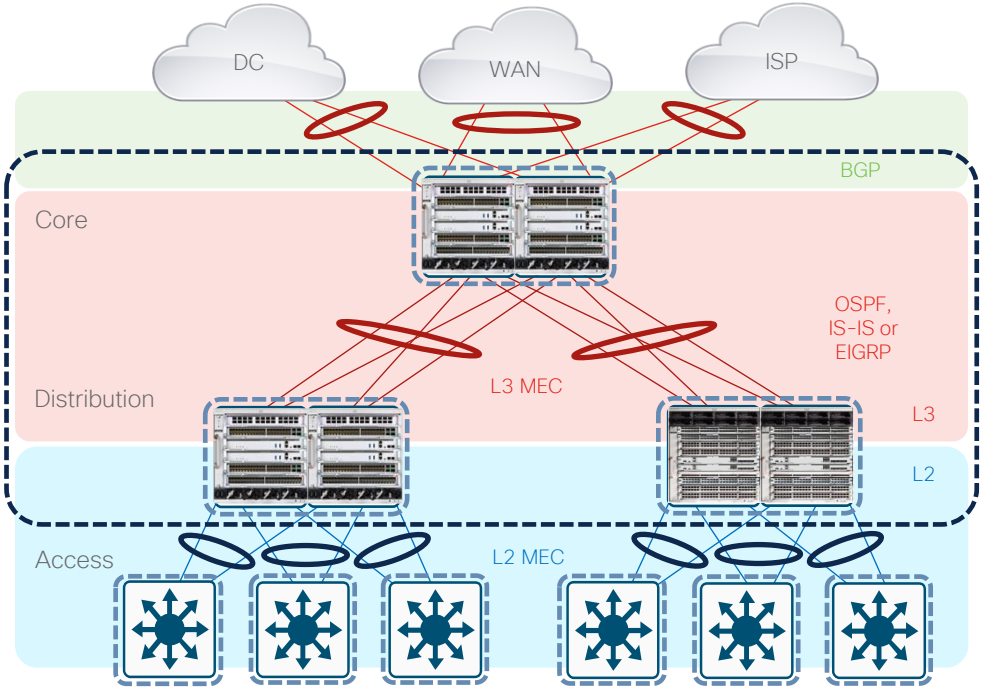
Leverages Stateful Switchover (SSO)

- Active/Standby Control-Plane (synchronized)
- Works with NSF/NSR for L3 protocols

Leverages Multi-chassis EtherChannel (MEC)

- Active/Active Data-Plane (both switches forwarding)
- L2 & L3 Portchannel (neighbor sees single neighbor)

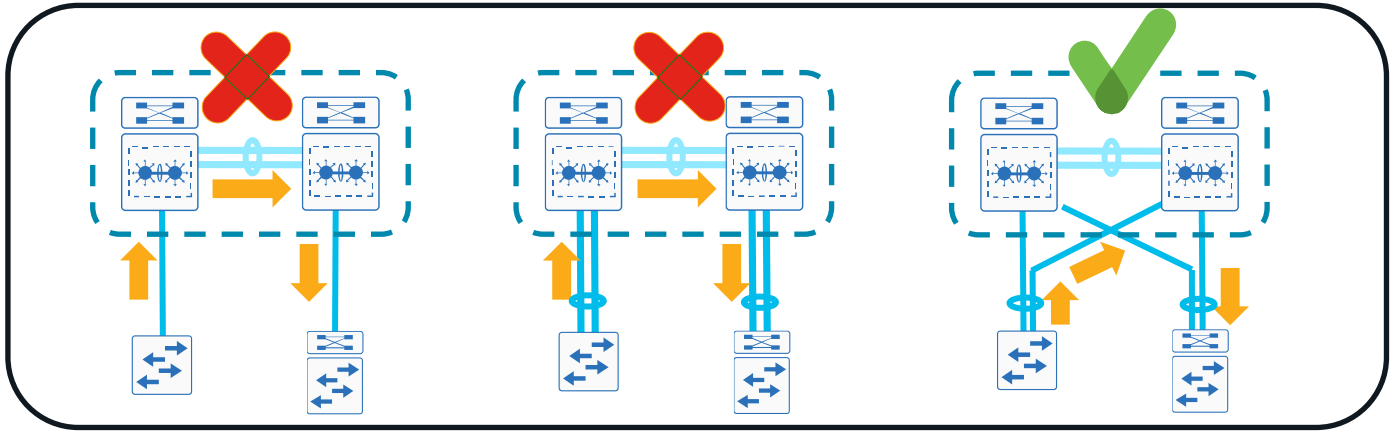
Tends to require med-high L2, L3 & feature scale



LAN High Availability

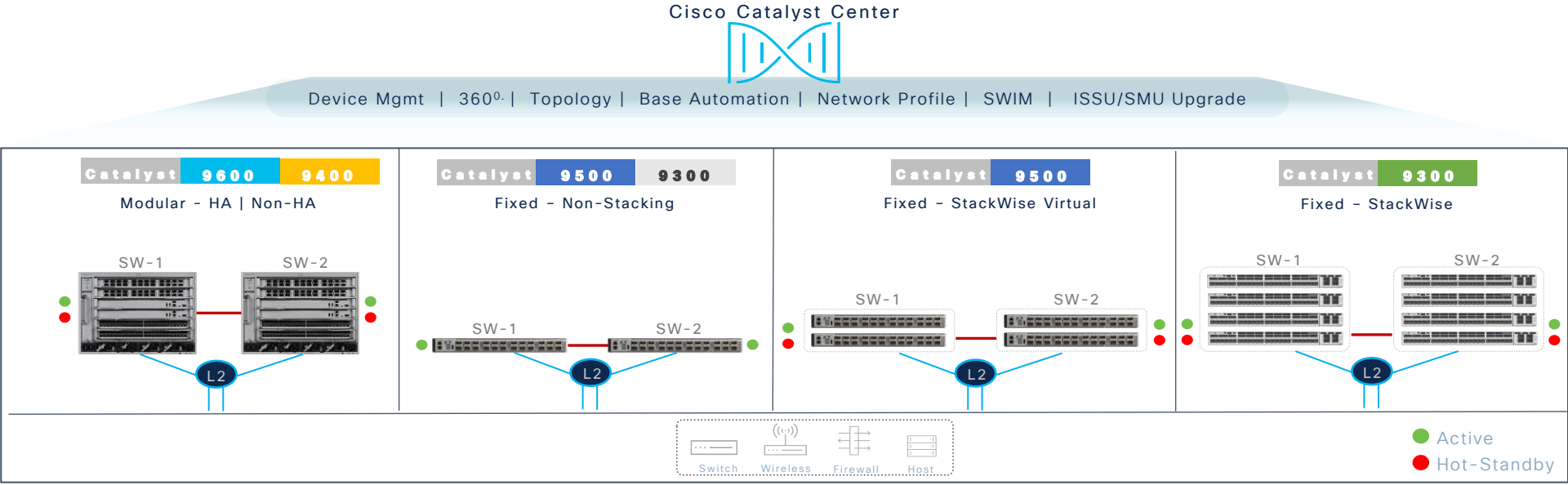
SWV/VSS: connecting distribution to access layer

- Use EtherChannel for link resiliency and load sharing
- With SWV/VSS, use multi-chassis EtherChannel and home to each switch



- Alternatively…
  With StackWise distribution layer, connect EtherChannel uplinks to multiple switches in stack

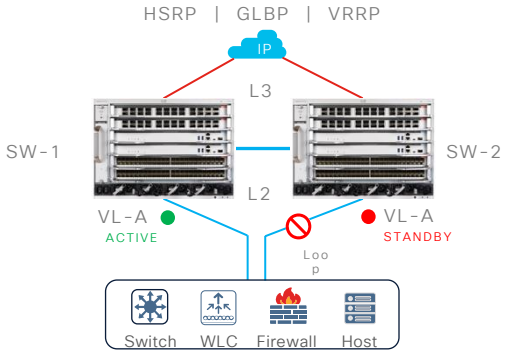
mLAG Flexible Deployment Options



- Independent Management Plane system operation from Cisco Catalyst Center
- Day-0 to day-2 complete system management application support
- Limited Layer 2 mLAG network automation and monitoring support
- Unsupported Applications : Cisco SD-Access, Wide Area Bonjour

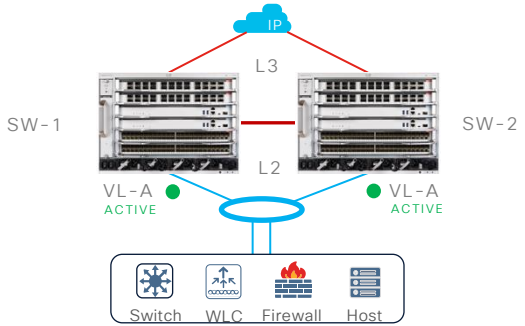
Resilient Campus Deployment Options

FHRP Based



ESI mLAG

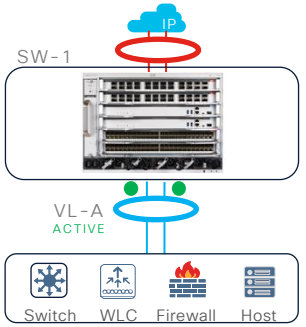
Planned Q2CY25



Ethernet Segment Identifier (ESI)
Multi-Chassi Link Aggregation (MLAG)

StackWise Virtual

Best



Best-In-Class Resiliency

Broad L3 IP gateway redundancy design alternatives

- Traditional FHRP-Based IP gateway redundancy - HSRP, GLBP and VRRP
- Industry-standard Layer 2 Multipath Network with Multi-Chassis LAG (mLAG)
- Cisco StackWise Virtual unified system for resilient, scalable and simplified networks

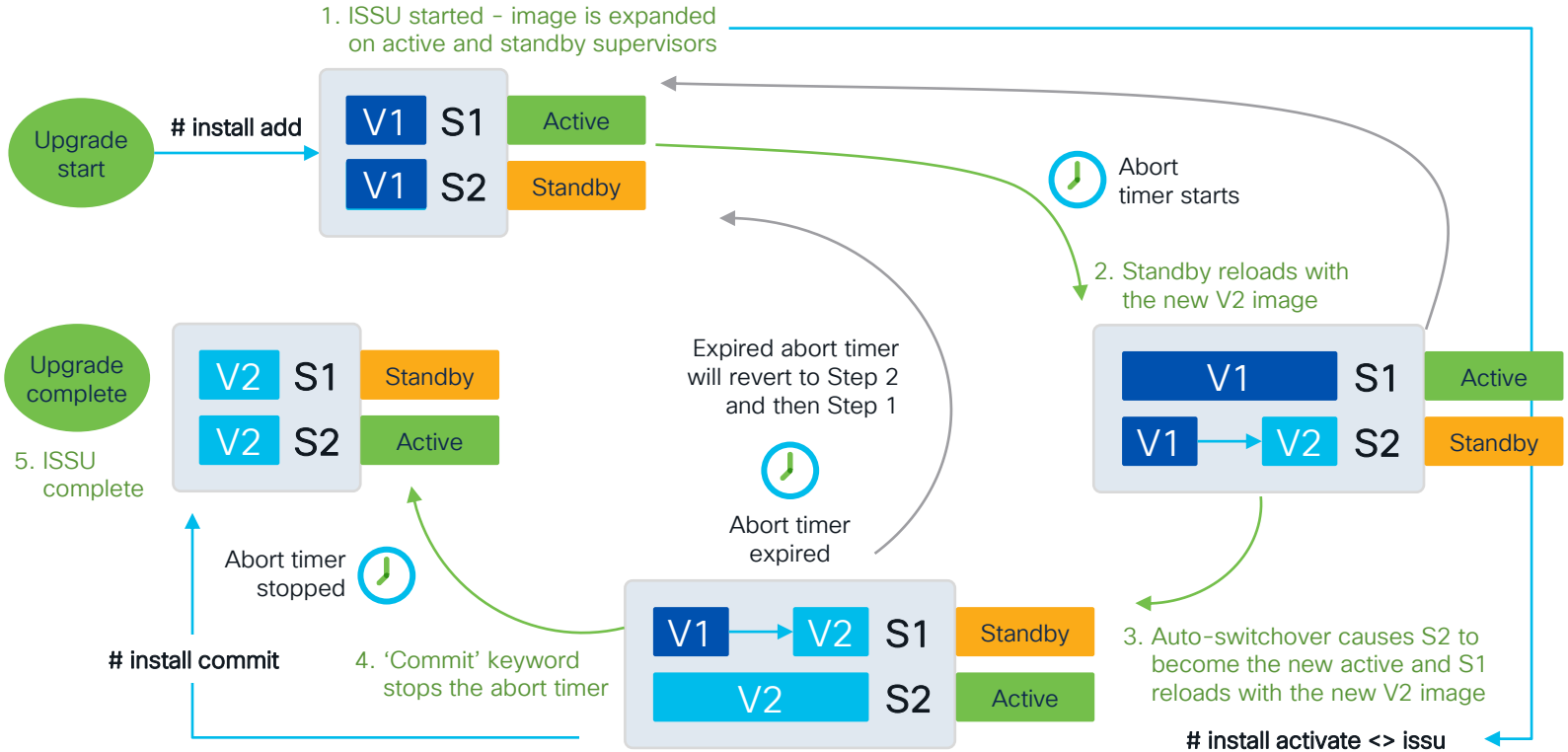
LAN High Availability

In-Service Software Upgrade (ISSU)


Catalyst 9600/X


Catalyst 9500/X


Catalyst 9400/X



LAN High Availability

Extended Fast Software Upgrade (xFSU)

C9300/L- 17.3.2

C9300X- 17.7.1

Catalyst® 9300/9300L/9300X standalone

#install add file image activate reloadfast commit

Control plane

Data plane

< 30 seconds of traffic impact

Catalyst 9300/9300L/9300X stack

#install add file image activate reloadfast commit

Active Control plane

Data plane

A

S

M

< 30 seconds of traffic impact for all ports in the stack

LAN High Availability

Extended Fast Software Upgrade (xFSU)


Catalyst 9300X/LM

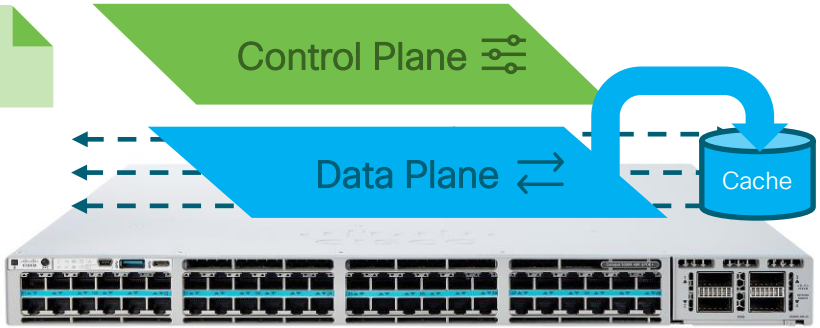

Catalyst 9300/L

NEW
- ≤ 5 Seconds - 17.15.2
- C9300X (≤ 30s) - 17.7.1
- C9300/L (≤ 30s) - 17.3.2

Command to trigger xFSU

C9300# ***install add file*** *<image>* ***activate xfsu commit***

Control Plane Upgrade
V1 ⟶ V2



Data Plane upgrade
V1 ⟶ V2

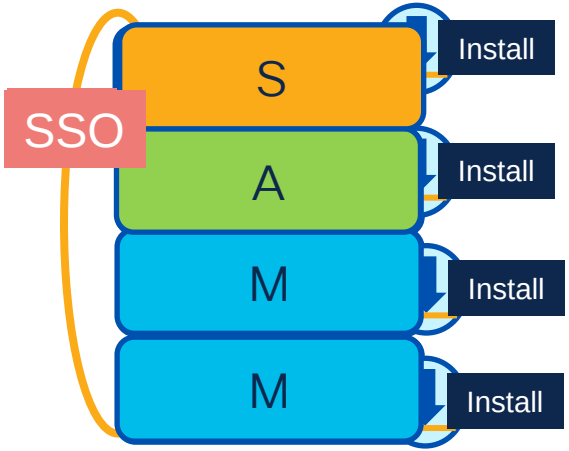
C9300 | C9300L | C9300X

Cisco xFSU minimizes downtime to less than 5 seconds (standalone or stack)

LAN High Availability

Extended Fast Software Upgrade (xFSU) on Stack

#Install add file image activate reloadfast commit



1. Install the images on all switches
2. Fast reload the standby and member switches
3. Fast reload the active switch only
4. Standby becomes the new active
5. Old Active switch becomes the new standby

Traffic Impact during the complete upgrade is less than 30 seconds

LAN High Availability

Power HA – StackPower

HA with Zero Footprint RPS

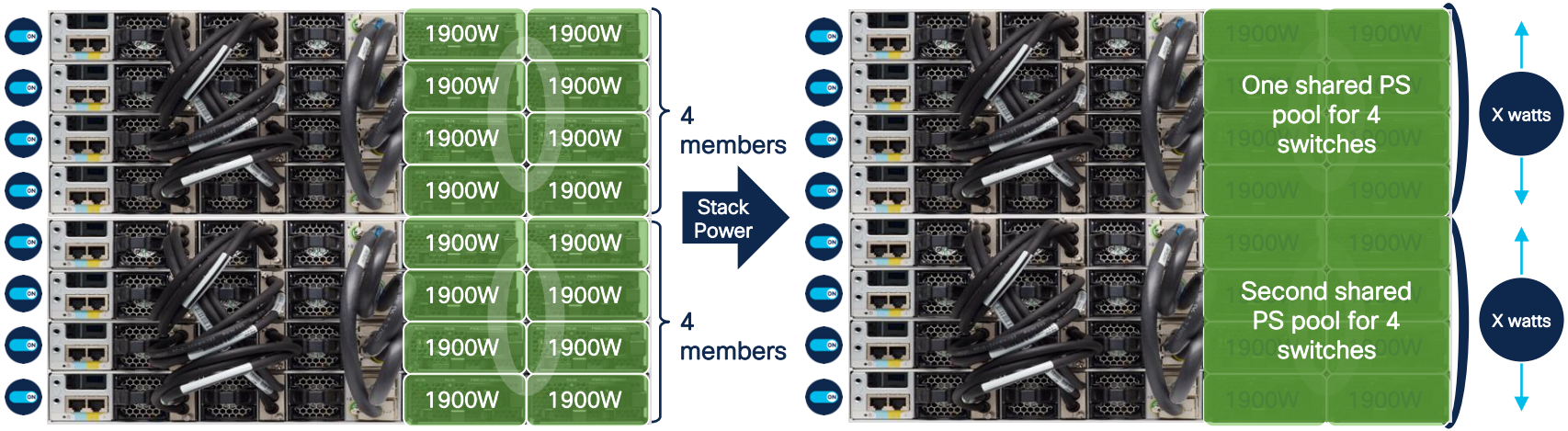
1+N Redundancy

Flexible and Efficient

Power Resiliency

LAN High Availability

Power HA – StackPower – How it works?



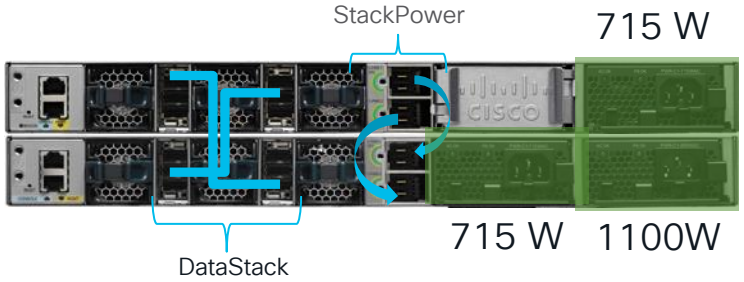
- Pools power from all Power Supplies (PS)
- All switches in StackPower share the available power in the pool
- Each switch is given its minimum power budget

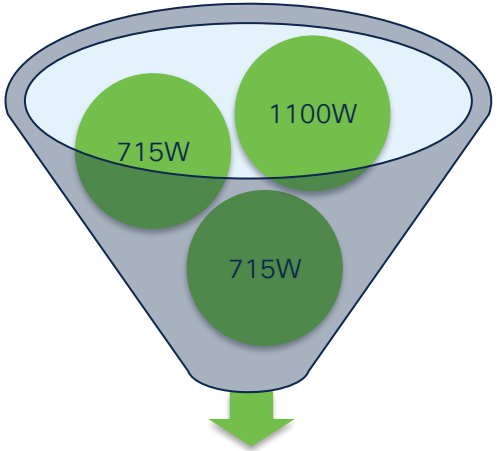
- 1+N Redundancy with inline power
- Up to 4 switches in one StackPower Ring
- Multiple Power stacks possible in one data stack

LAN High Availability

Power HA – StackPower – How it works?

- Pools Power from All PS
- All Switches in StackPower share the available Power in Pool
- Each Switch is given their Minimum Power Budget





Total Power INPUT = 2530W

LAN High Availability

Summary of Options

Platform	Switch Stacking	Supervisor Redundancy	NSF / SSO	EtherChannel	ISSU	SMUs	GIR	Power Redundancy
Cisco Catalyst 9200 Series	StackWise-160/80 with Active / Standby	–	Yes	Cross-Stack EtherChannel	No	Yes	No	Up to 2 hot-swappable power supplies per switch. PoE models operate in Combined mode. Non-PoE models operate in 1:1 redundancy mode.
Cisco Catalyst 9300 Series	StackWise-480/360 with Active / Standby For Cat 9300X: Stackwise-1T (480G when stacking with Catalyst 9300 model)	–	Yes	Cross-Stack EtherChannel	No. Supports Fast Software Upgrade (FSU) and Extended FSU (xFSU).	Yes	Yes	StackPower (up to 4 switches per stack) operating in shared or redundant mode. Cisco XPS 2200 for stacks of up to 8 switches
Cisco Catalyst 9400 Series	–	Single chassis 1:1 or cross chassis StackWise Virtual	Yes	Multichassis EtherChannel with StackWise Virtual	Yes	Yes	Yes	Hot-swappable power supplies in N+N or N+1 power redundancy modes
Cisco Catalyst 9500 Series	–	Cross chassis StackWise Virtual	Yes	Multichassis EtherChannel with StackWise Virtual	Yes	Yes	Yes	Dual 1+1 redundant power supplies.
Cisco Catalyst 9600 Series	–	Single chassis 1:1 or cross chassis StackWise Virtual	Yes	Multichassis EtherChannel with StackWise Virtual	Yes	Yes	Yes	Four power supplies which can operate in Combined or N+1 redundancy modes.

Design HA with Catalyst 9K

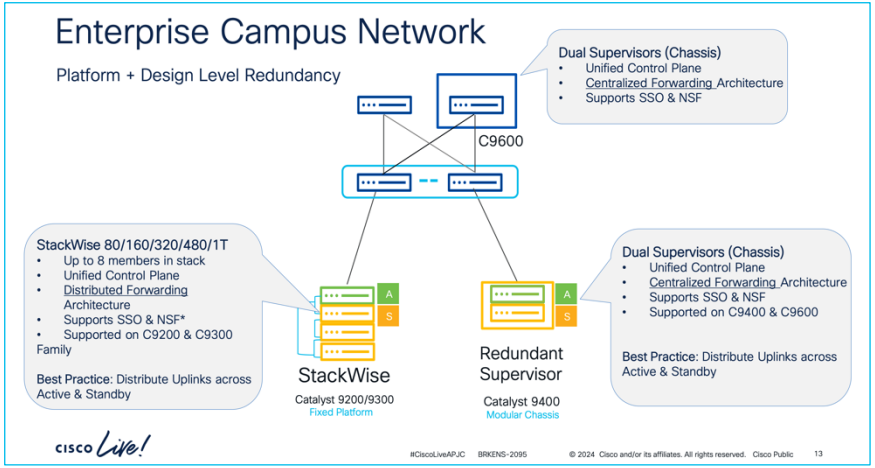
BRKENS-2095

Designing Highly Available Networks Using Cisco Catalyst 9000 Switches

Minhaj Uddin – Leader Technical Marketing, Cisco

This session will explore both new and existing high-availability features in IOS XE on Catalyst 9000 Series switching platforms.

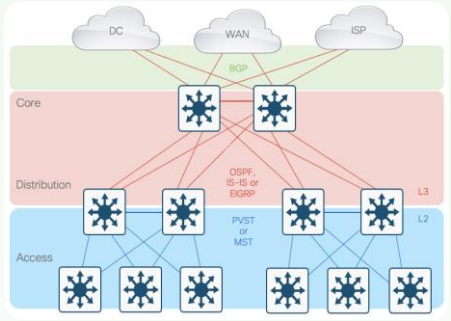
We will begin by highlighting the significance of high availability across various layers of the hierarchical network. Following this, we will delve into different levels of resiliency, including standalone platform/hardware, design, and software. The session will conclude with a summary of these capabilities, illustrated through various real-world customer use cases and requirements.



Campus Architectures

Control-Plane & Data-Plane Redundancy

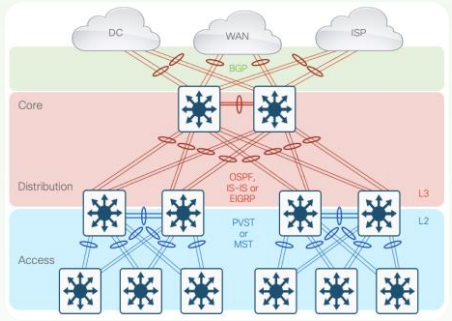
1 ECMP (L2/L3 Paths)



- Complex Topology
- More Nodes, Less Cables
- More Neighbors (+ Tuning)
- Protocol Load-Balancing (ECMP)
- Node-level Redundancy

L1 : Single Connections
L2: STP, MST, REP + ECMP (Port Cost)
L3: FHRP, IGP, BGP + ECMP(Port Cost)
More Neighbors = Requires Protocol Tuning

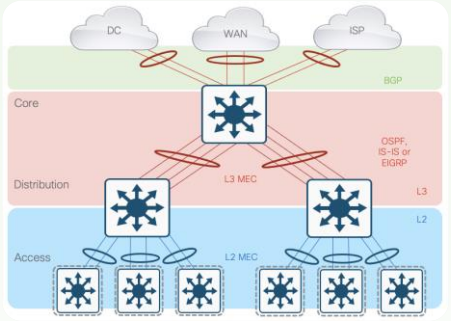
2 EtherChannel (L2/L3 LAG)



- Complex Topology
- Same Nodes, More Cables (2-8)
- Same Neighbors (+ Tuning)
- EtherChannel Load-Balancing
- Node & Link-level Redundancy

L1 : Multiple Connections
L2: STP, MST, REP + ECMP (Portchannel Cost)
L3: FHRP, IGP, BGP + ECMP (Portchannel Cost)
More Neighbors = Requires Protocol Tuning

3 StackWise (L2/L3 MEC)



- Simple Topology
- Same Cables, Less Nodes
- Less Neighbors (No Tuning)
- Multi-chassis EtherChannel (MEC)
- Layer-level Redundancy

L1 : Multiple Connections
L2: L2 MEC (No STP or REP)
L3: IGP, BGP + L3 MEC (No FHRP)
Fewer Neighbors = No Protocol Tuning

Design

Best Practices

- **LAN High Availability**
- **LAN Security**
  - **SISF**
  - **Transport Security**
  - **Endpoint Visibility and Profiling**
  - **Segmentation**
  - **XDR**
- **Virtual Networking**

The five pillars of Workplace Zero Trust Security

- Endpoint Visibility
- Secure Access
- Network Segmentation
- Endpoint Compliance
- Rapid Threat Containment

Story of a Fish Tank...

A
CASINO

A
FISHTANK
WITH A SMART
THERMOMETER

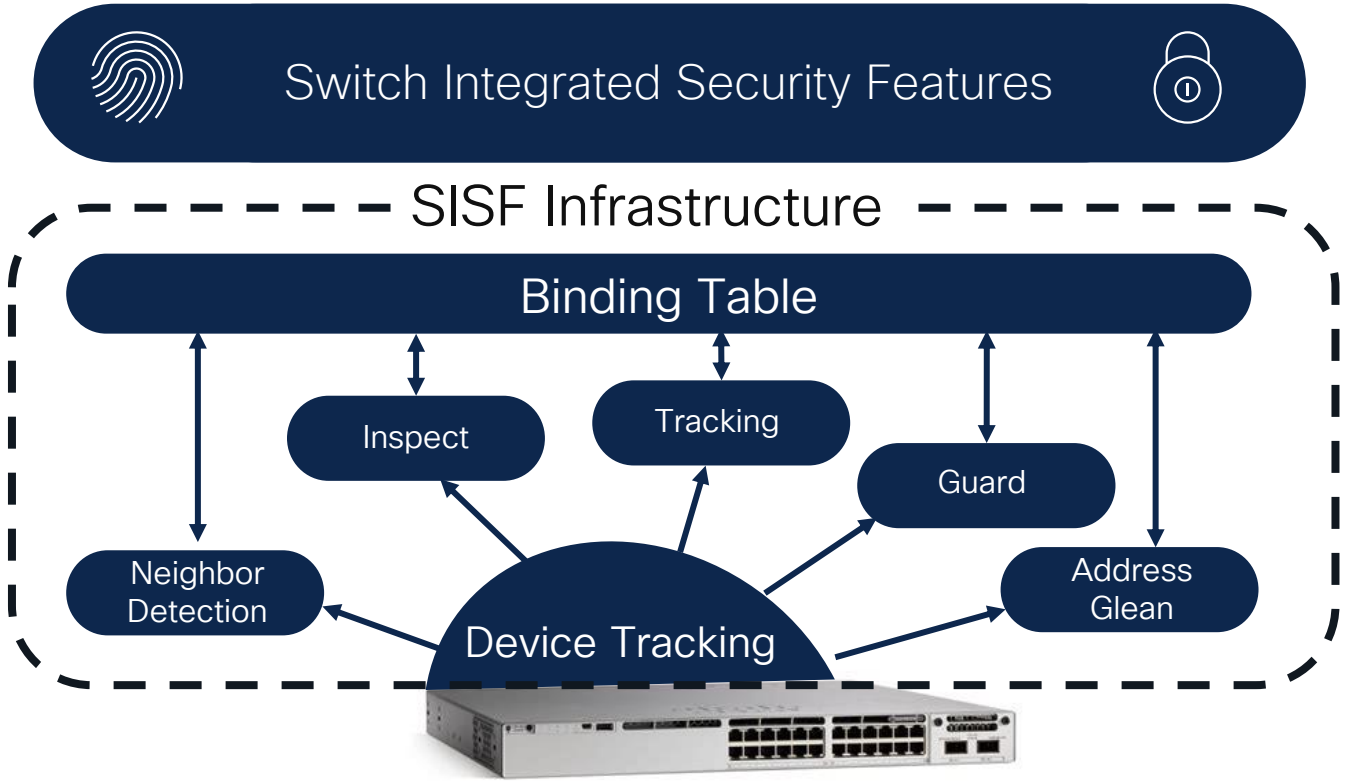
A
HACKER

...AND A LATERAL
MOVEMENT

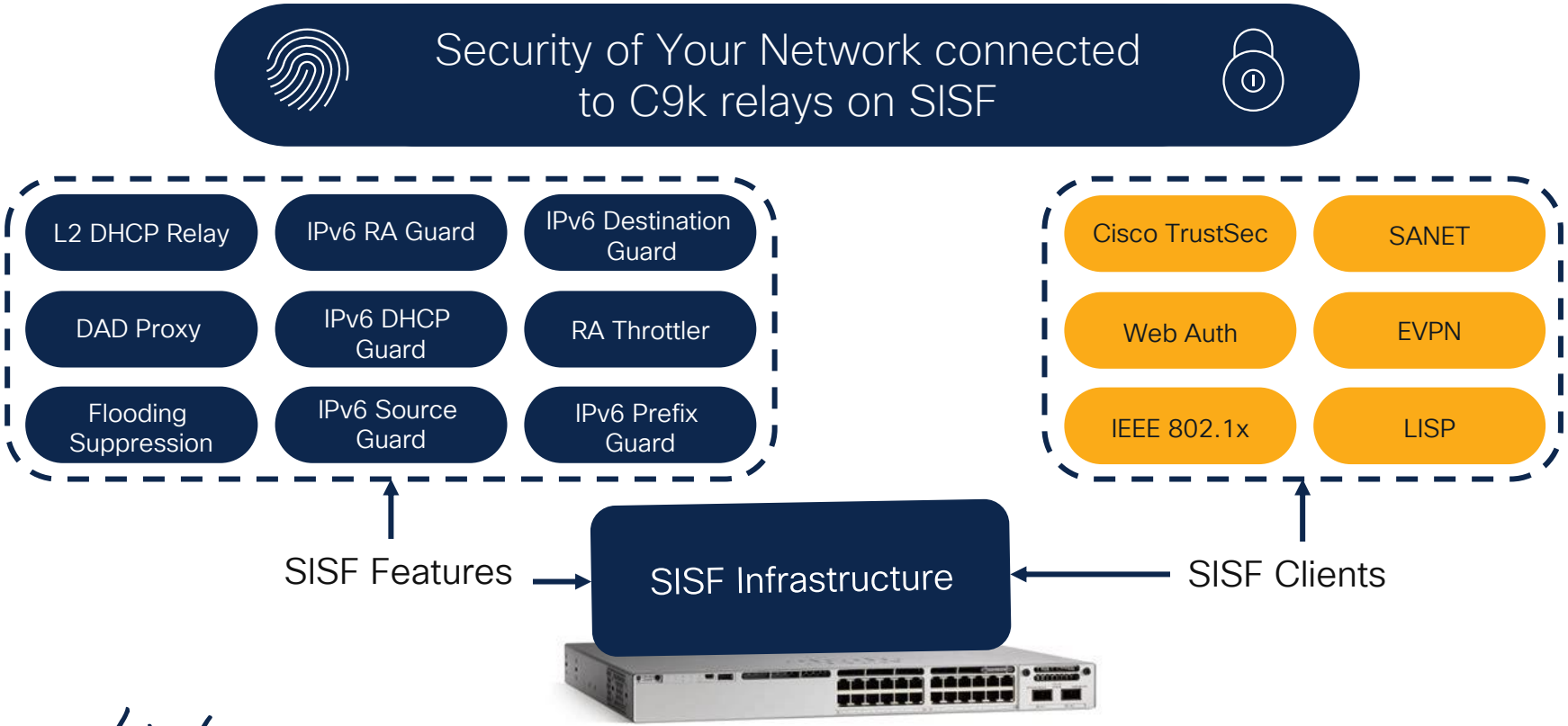
AFTERMATH

Hacker got access through the smart thermometer to the casino´s customer database and exfiltrated high-rollers data over days to a remote server

First Hop Security



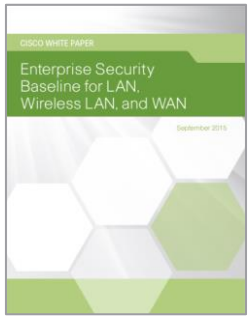
Why is First Hop Security important?



Security Best Practices

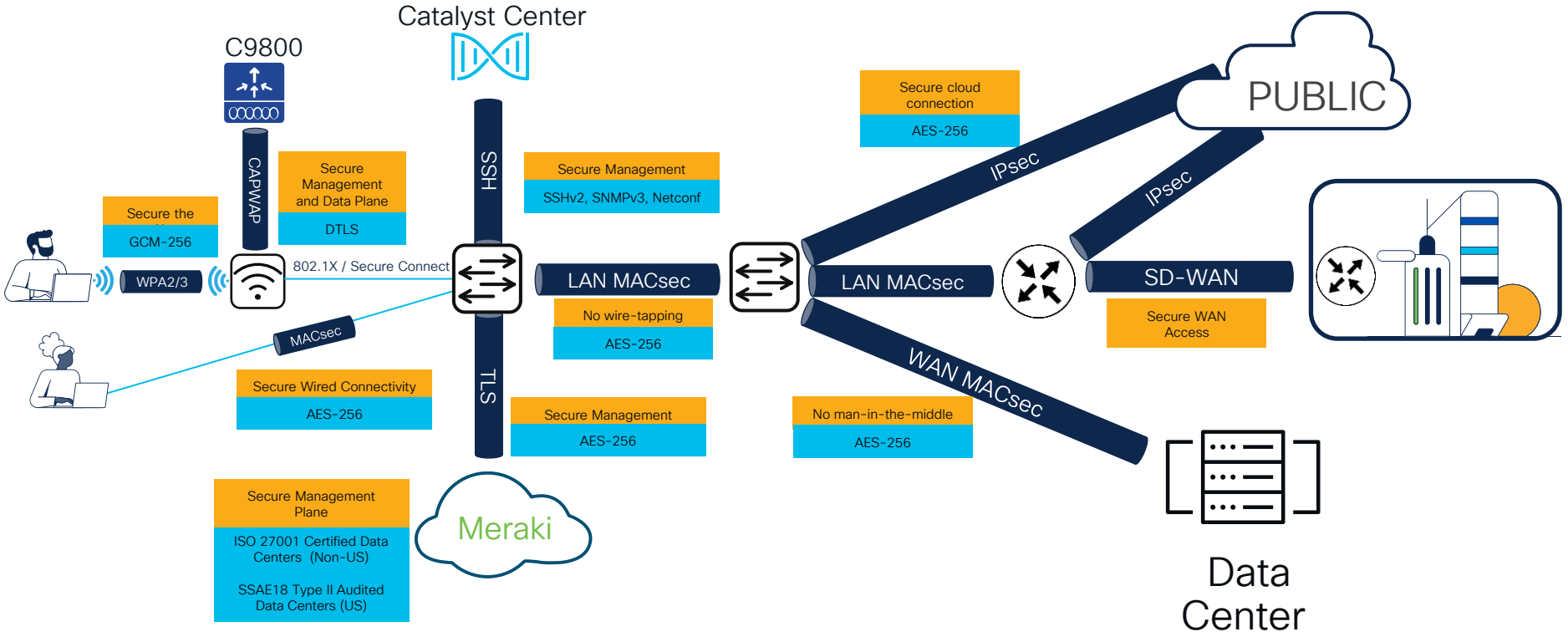
Also protects limited Hardware & Software sources

- **Cisco Umbrella** ➢ uses DNS as a security tool to identify and block threats
- **802.1x User Authentication** ➢ forces users to authenticate before allowing them on network
- **IP Source Guard / v6 RA Guard** ➢ prevents IP/MAC Spoofing and IPv6 Man-in-the-Middle attacks
- **Dynamic ARP Inspection** ➢ prevents current ARP attacks
- **DHCP Snooping** ➢ prevents Rogue DHCP Server attacks
- **Port Security** ➢ prevents CAM attacks and DHCP Starvation attacks



Transport Security

Your options

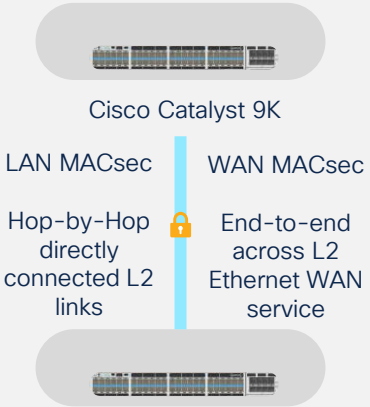


Secure Communication – examples

L2 Encryption with MACSec

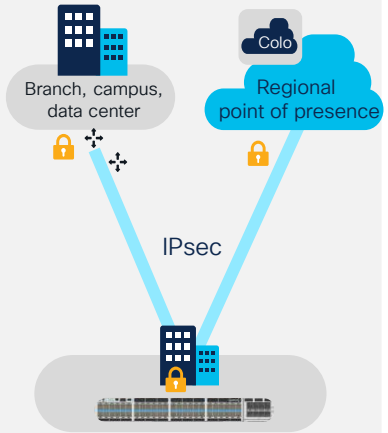
Switch-to-Host

Switch-to-Switch



L3 Encryption with IPSec

Site-to-Site

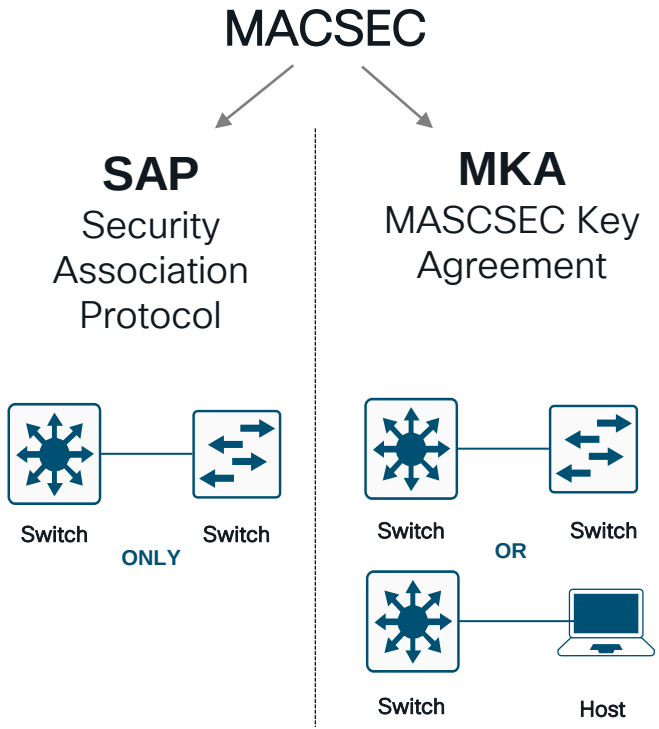


Site-to-Cloud

MacSec

Layer2 P2P Encryption

- Higher Speed compared to IP-SEC. MACSEC can reach interface Speed level.
- Encryption done at the physical layer of the ethernet port.
- MACSEC encrypts Layer 2 Frame.
- It is a hop-to-hop protocol.
- MACSEC=802.1AE. It is a Standard



End-to-End Security of Network Traffic

L2 MACSec LAN

- Hop-by-Hop Ethernet encryption per IEEE 802.1AE
- mitigate packet eavesdropping, tampering, and injection
- Keep data confidentiality & integrity
- Line-rate in C9K ASICS

WiFi Control-Plane

- CAPWAP Control encrypted by default
- DTLS Data encryption between AP and WLC

Management Plane

- Meraki tunnel per default encrypted with TLS tunnel
- Meraki SecurePort between Switch and AP
- Catalyst Center management protocols – SSH, Netconf, SNMPv3

L2 MACSec WAN

- Optimize to accommodate running over L2 public Ethernet transport.
- WAN Transparency

WiFi Data-Plane

- Optional DTLS data-plane CAPWAP encryption between AP and WLC
- WPA2/3 encryption of wireless over-the-air traffic

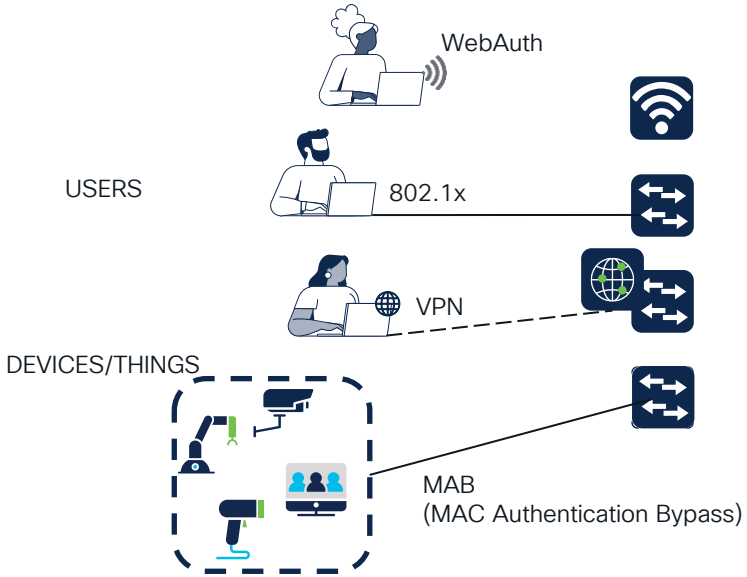
L3 IPSec

- Using C9K ASIC crypto engine
- Line-Rate up to 200G
- C9300-X and C9400X

Think about ‘HOW’ and ‘WHO/WHAT’

HOW

Authenticate



WHO/WHAT

Identify

IP add: 192.168.2.101	ID	Bob (Employee)
Unknown	WHAT	Apple iPad/IOS/11.0.1
Unknown	WHEN	10:30 AM
Unknown	WHERE	Floor-1, Amsterdam, Building 1
Unknown	Conn TYPE	Wireless
Unknown	APPS	Firefox, MS Word, Anyconnect
Unknown	HW	Serial No, CPU, memory

PROFILING

Identity Services Engine (ISE)

ISE helps you to learn ‘HOW’/‘WHO/WHAT’ and much more…

Get Endpoint Visibility

Active Probes: DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

WIFI Edge Analytics: Firmware, HW_Model, Manufacturer, OS_Version, Vendor

pxGrid: CyberVision (for Industrial endpoints)

ISE gathers context from network devices and endpoints

...and builds database of endpoints with their attributes

ISE

pxGrid

Meraki connector

Device Type	Camera	IP-Phone	Laptop	Laptop
Manufacturer	Arlo	Cisco	Apple	Lenovo
Model	Pro Wireless Cam	7980	MacBook Pro	Thinkpad 540
OS	Linux	IOS	macOS 13.0.1	Windows Enterprise

ISE classifies this data into Endpoint Profile

INTEGRATIONS

Catalyst Center

- Group-based policy
- Group-based policy analytics
- SDA Fabric Networks (LISP/EVPN)
- AI Endpoint Analytics

COMMON

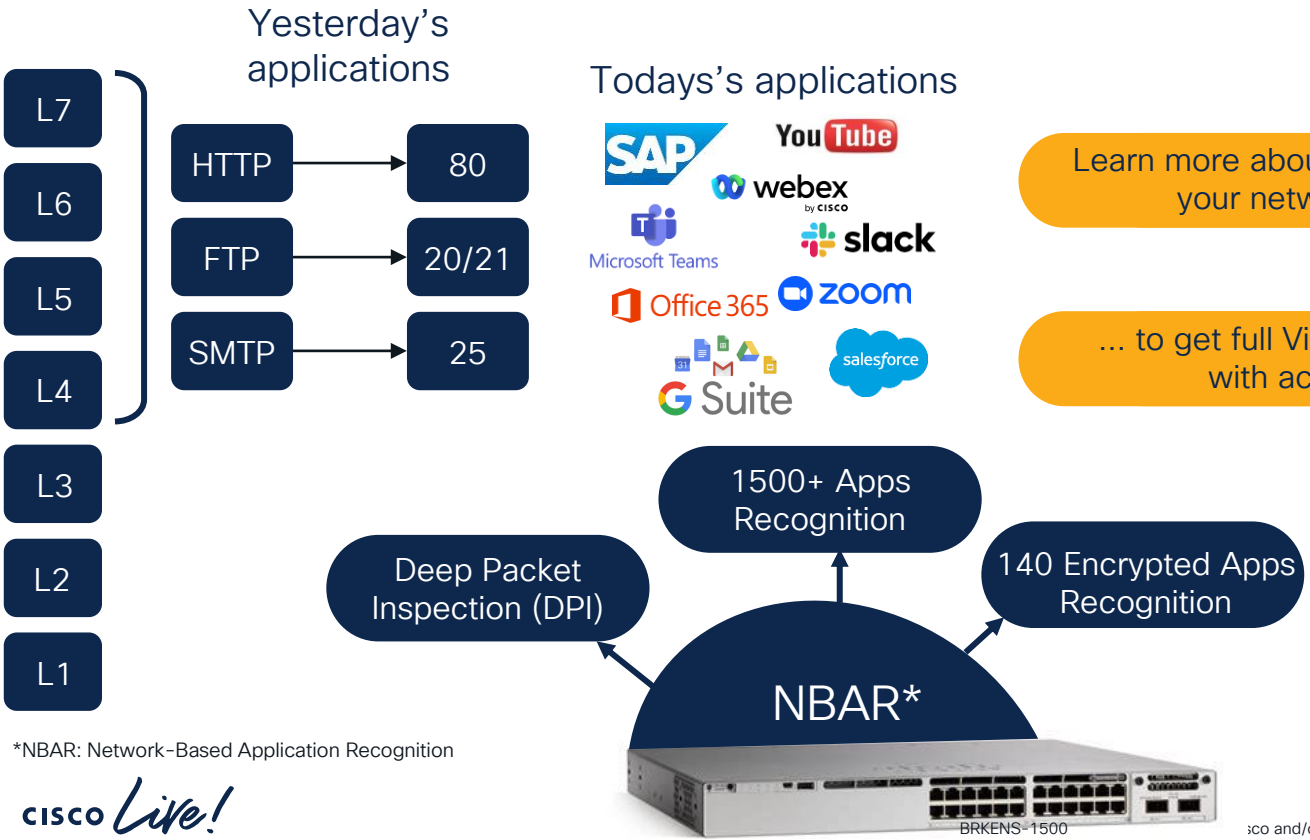
- AAA (Wired/Wireless)
- BYOD (Wireless)
- Gues Access (Wired/Wireless)
- Access Control (Wired/Wireless)
- Device Administration
- Context Exchange
- User defined network
- IoT Onboarding (Wired/Wireless)

Meraki Dashboard

- Group-based policy
- Adaptive Policy
- Meraki Dashboard policy scale and flexibility upgrade

ISE is a COMMON Policy Engine providing visibility and control across your network domains

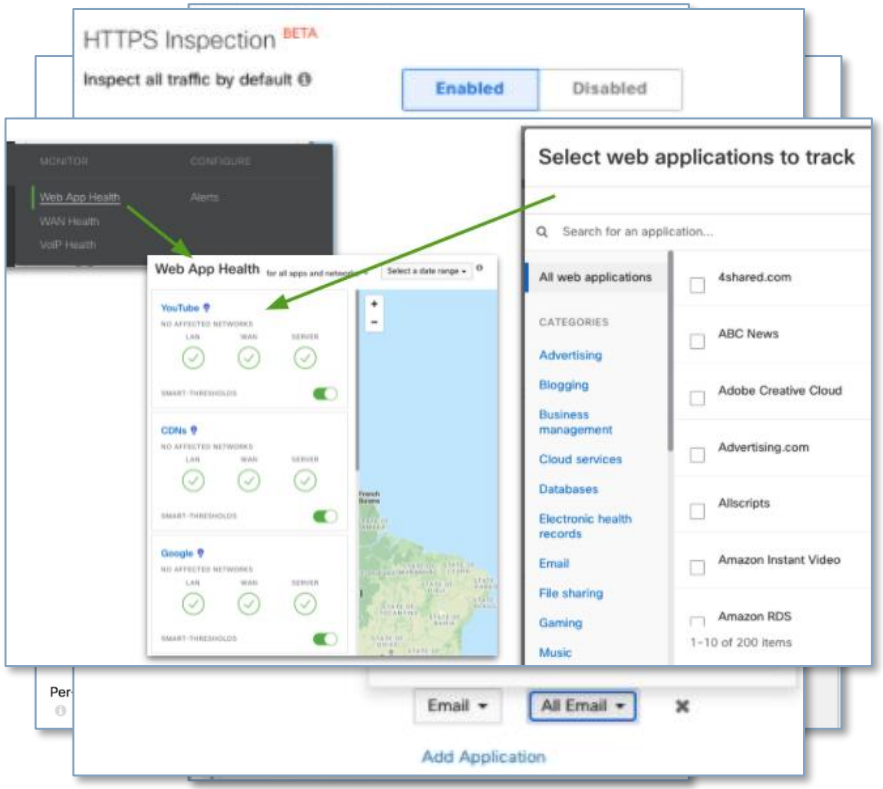
See more with Deep Packet Inspection (DPI)



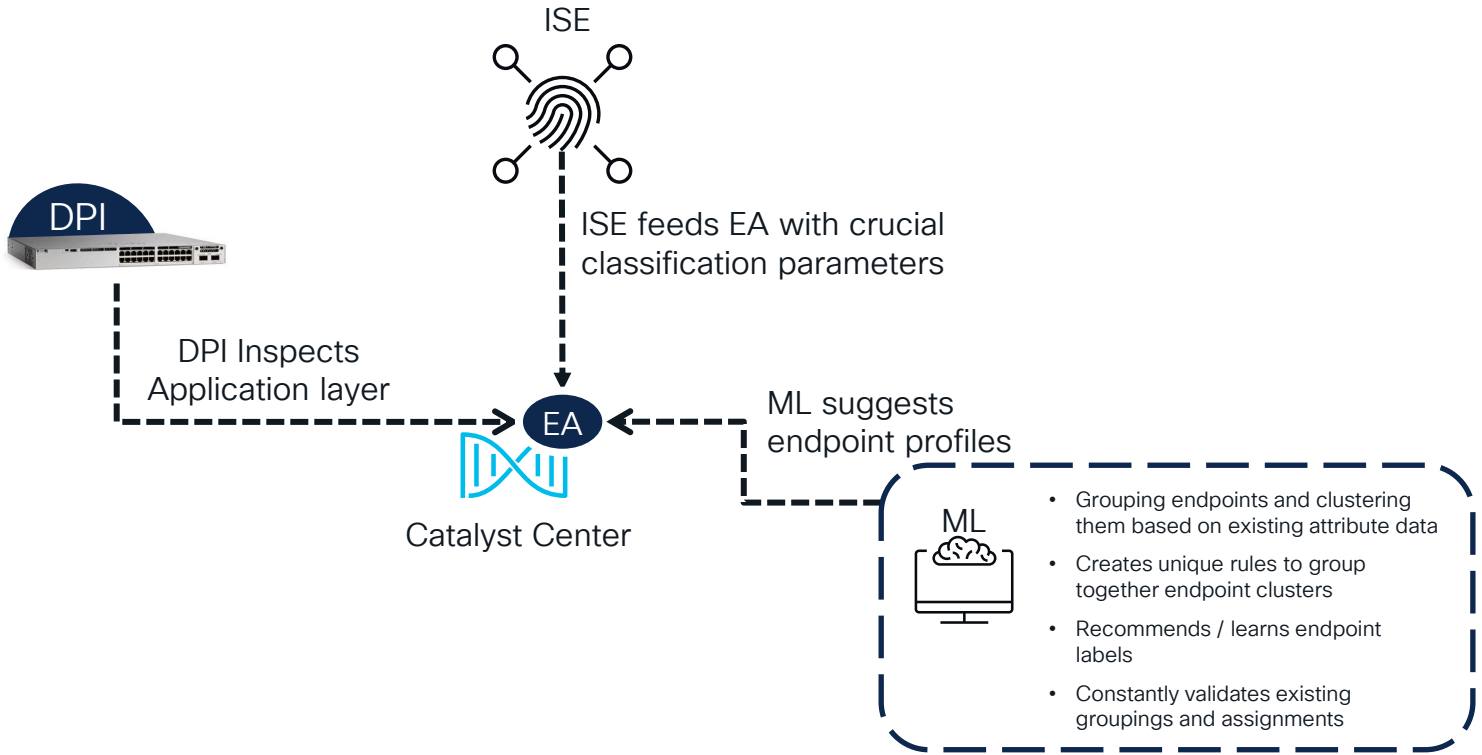
*NBAR: Network-Based Application Recognition

Leverage DPI in Meraki Dashboard

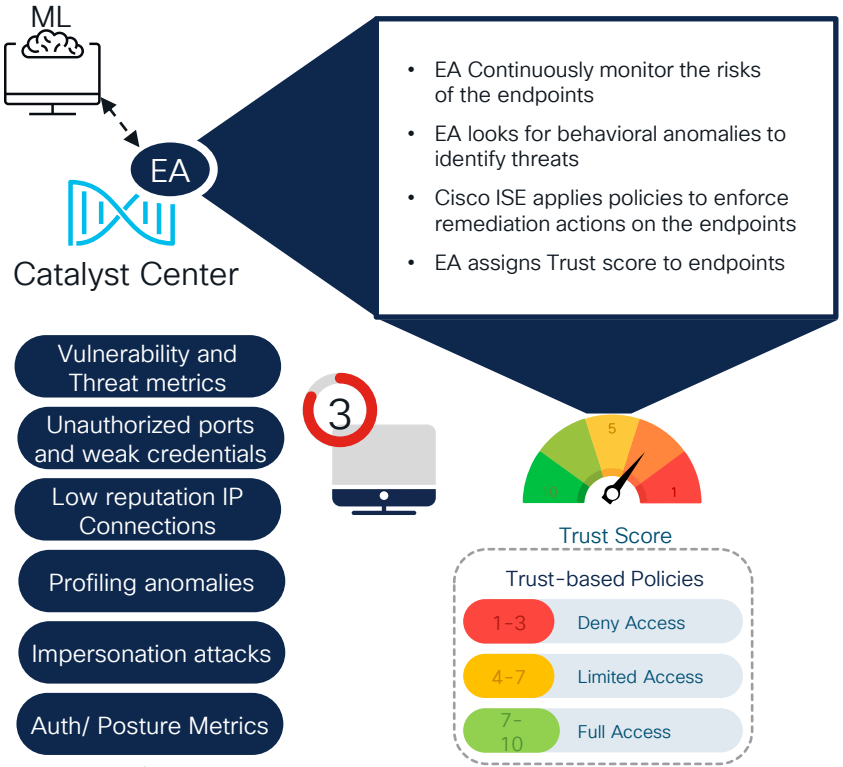
- More granular L7 firewall and traffic-shaping rules
- More flexibility into blocking and prioritizing desired application
- Application tracking
- HTTPS inspection
- Meraki Insight with ThousandEyes for specific applications.



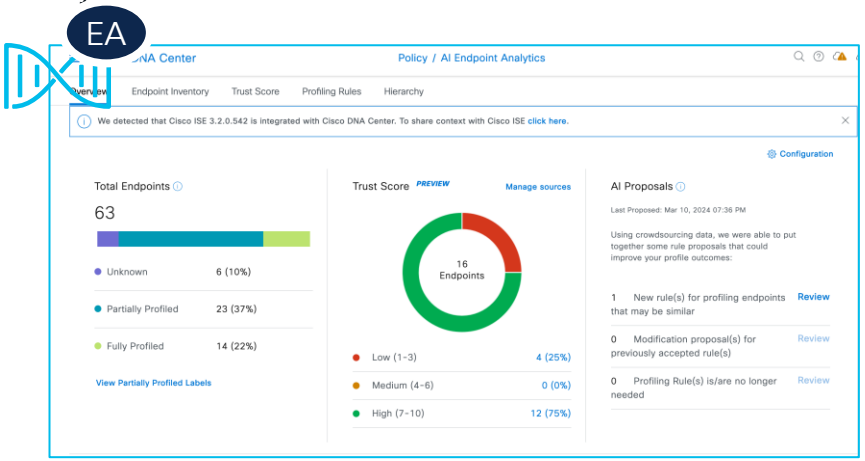
Gain ultimate Visibility with Endpoint Analytics



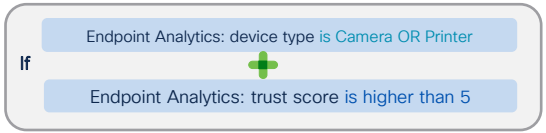
Gain ultimate Visibility with Endpoint Analytics



Catalyst Center



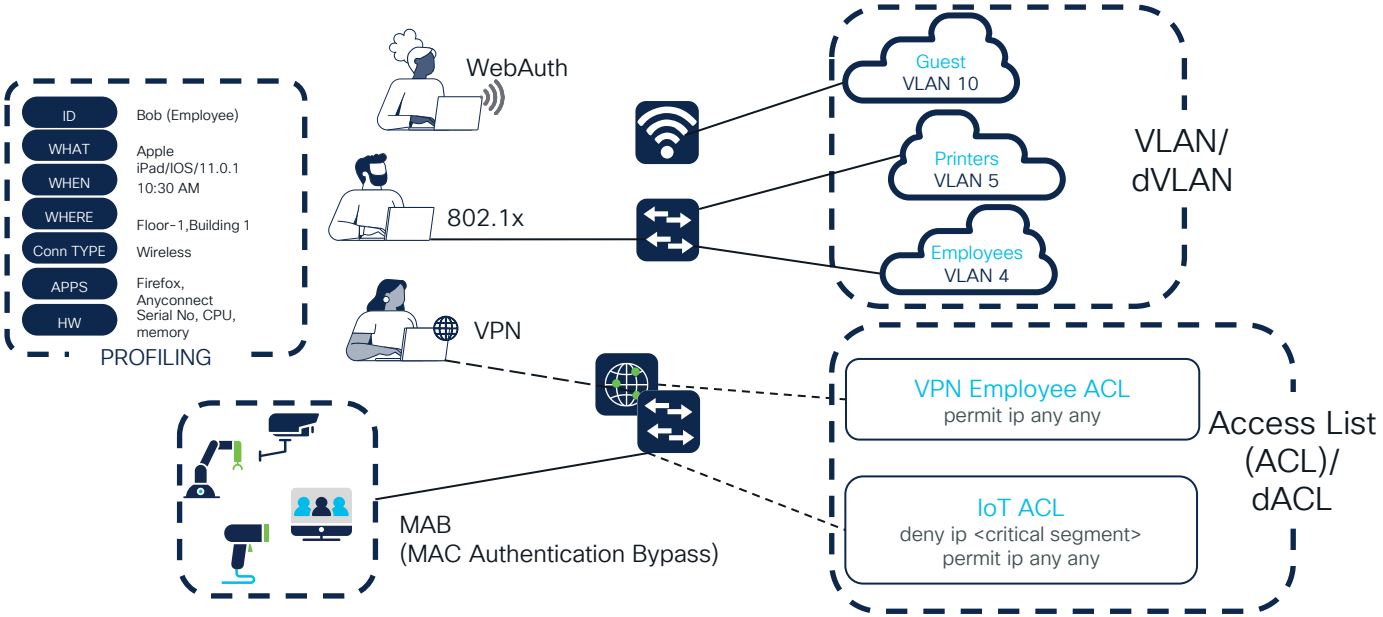
authorization policy for Low Trust - Printers:



You have Visibility...now what?

Endpoints Authenticated and Profiled

Basic segmentation options you have:



Limitations

Traditional segmentation depends on IP addressing

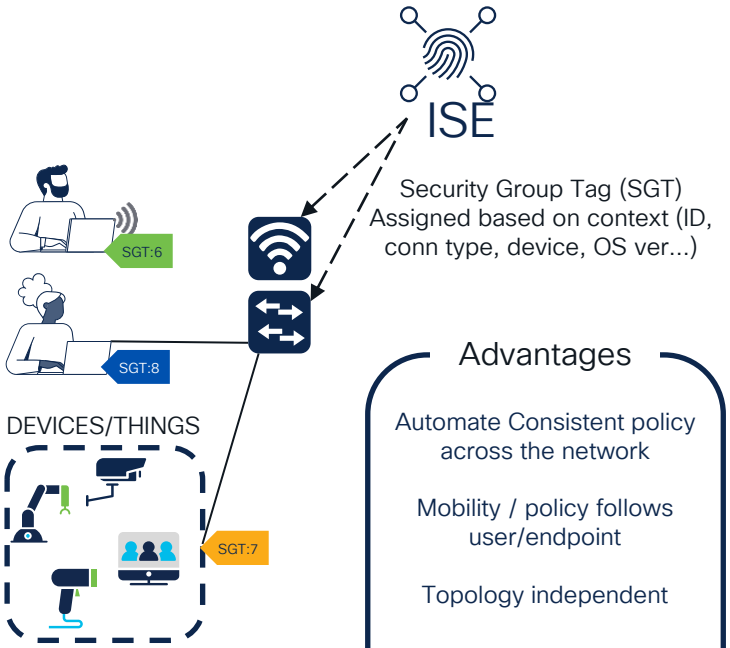
Security Policy based on Topology

Limited Flexibility

Complex maintenance

Design needs to be replicated for floors, buildings and across other facilities

Simpler, please... with Cisco TrustSec(CTS)



Advantages

Automate Consistent policy across the network

Mobility / policy follows user/endpoint

Topology independent

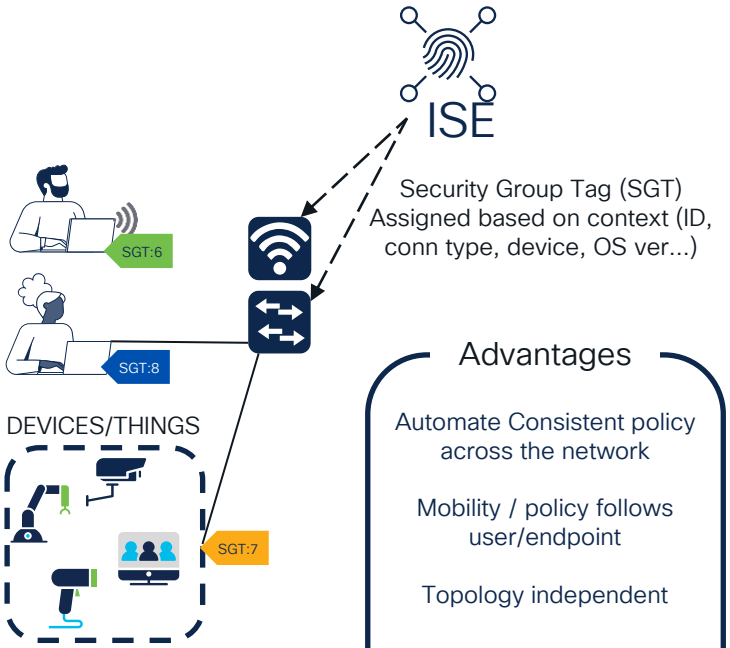
Central Policy Provisioning

REPLACE

Complex ACLs

```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
```

Cisco TrustSec(CTS)



Advantages

Automate Consistent policy across the network

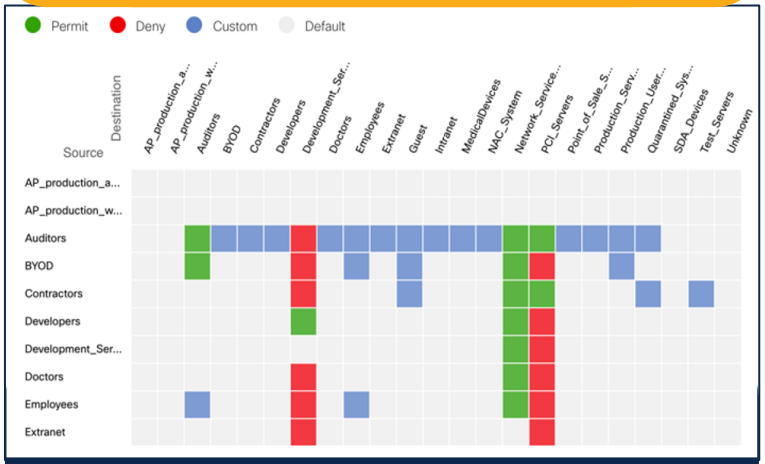
Mobility / policy follows user/endpoint

Topology independent

Central Policy Provisioning

WITH

CLEAN Matrix



DYNAMIC assignment of your INTENT
ADAPTIVE access based on IDENTITY and TRUST

SGT + Meraki = Adaptive Policy

ISE Integration enables Dynamic SGT assignment based on:

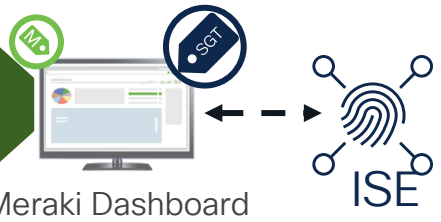
- Profile
- Posture
- Location
- Credentials
- Credential Type
- AD Group/s

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



Great option for Cloud-first Campus deployments

ISE + Catalyst Center

Great option for On-Prem and AirGap Campus deployments

Fabric Networks (LISP/EVPN)

SDA

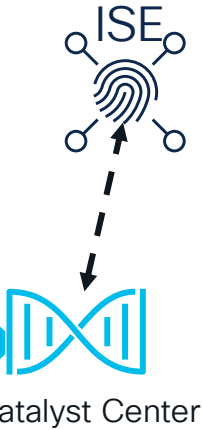
- Control-plane choice (LISP or EVPN)
- One Infrastructure
- Consistent zero-trust experience
- Full control of network within YOUR Intent
- Network AND Security Visibility
- Resilient Architecture
- Overlay and Underlay Automation
- Macro segmentation based on VRF
- Micro Segmentation based on SGT

Network-Wide intent-based policy

Utilizing Security Group Tags (SGTs)

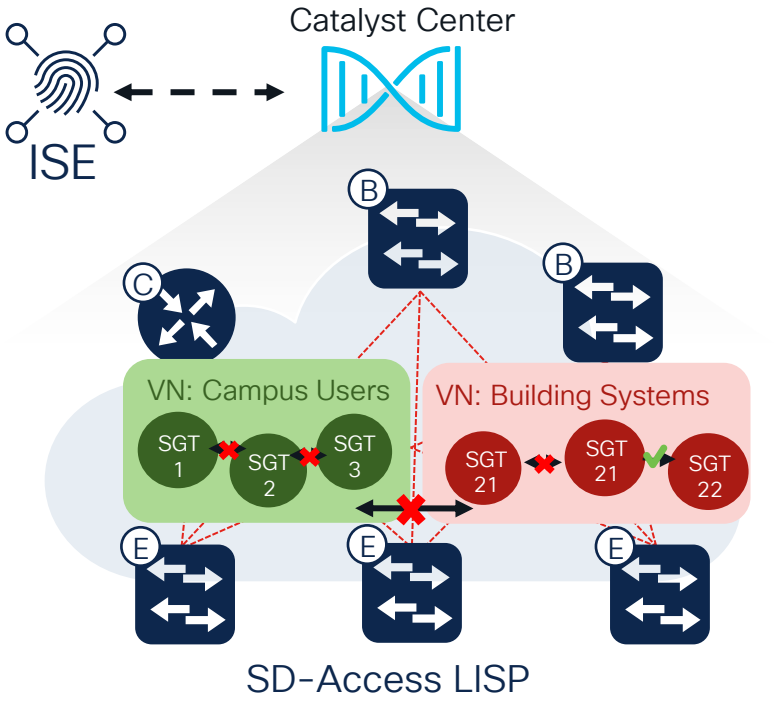
Automated Configuration/management of network

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



SD-Access LISP is Cisco's recommended Control Plane for Campus

Cisco SD-Access segmentation options



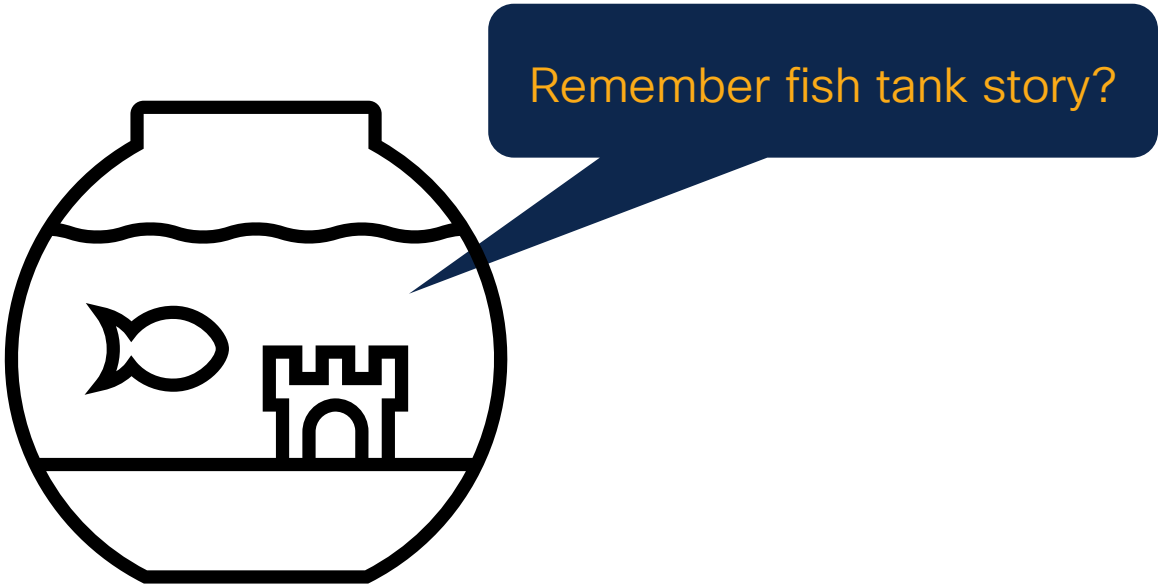
Macro Level: Virtual Network (VN)

First level Segmentation that ensures zero communication between specific groups.

Micro Level: Security Group (SGT)

Role based access control between two groups within a Virtual Network. i.e. line of businesses or functional blocks.

Segmentation is here to help you!

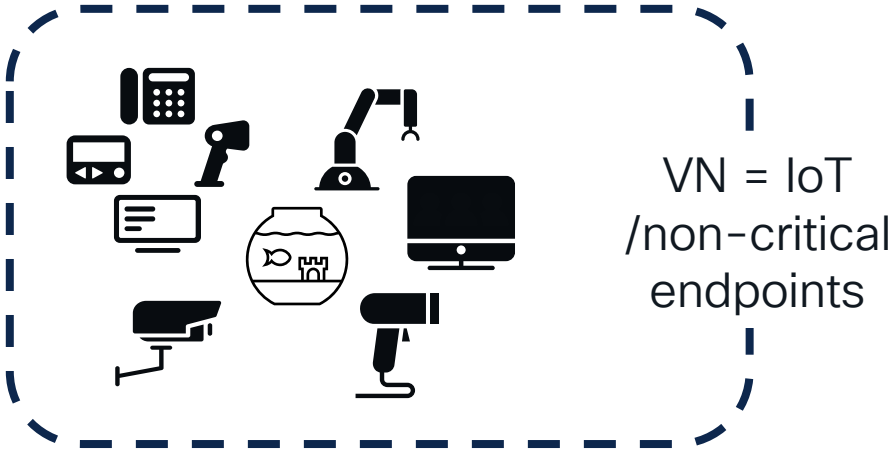


Segmentation is here to help you!

Proper Visibility would help notifying abnormal behaviour quickly

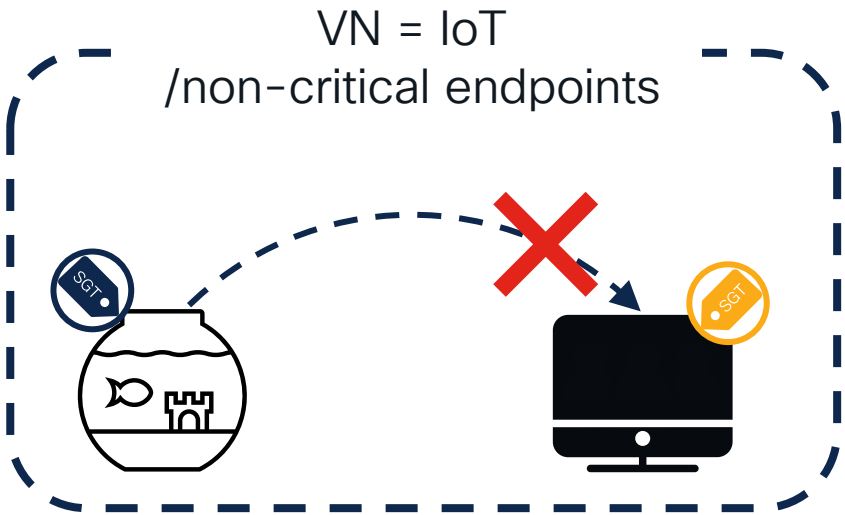
Segmentation is here to help you!

...but placing device into the right network segment (VN) would limit the range of damages



Segmentation is here to help you!

...while assigning proper SGT and enforcing the policy would NOT allow communication to happen at all



XDR - Extended Detection And Response

Detect, Act, Elevate and Build Resilience

Integrations (Native and APIs)

Microsoft Defender For Endpoint
ExtraHop
proofpoint.
Amazon GuardDuty
cisco

Devices and Users

Events

Intelligence

TALOS

Investigation

Threat Intel

aws
Azure
Google Cloud

Public Cloud

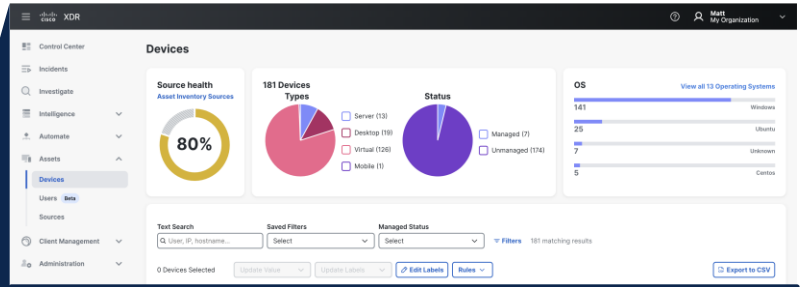
Flow Logs

Campus/Branch

Meraki and Catalyst

Flow logs
NetFlow
Syslog
Mirror/SAN
ISE

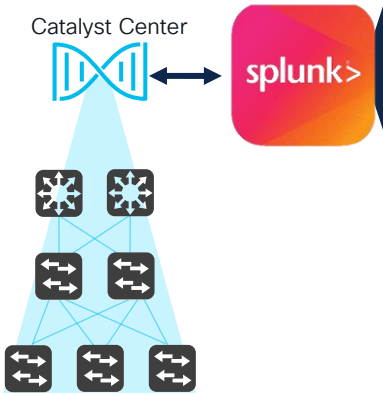
Cisco XDR

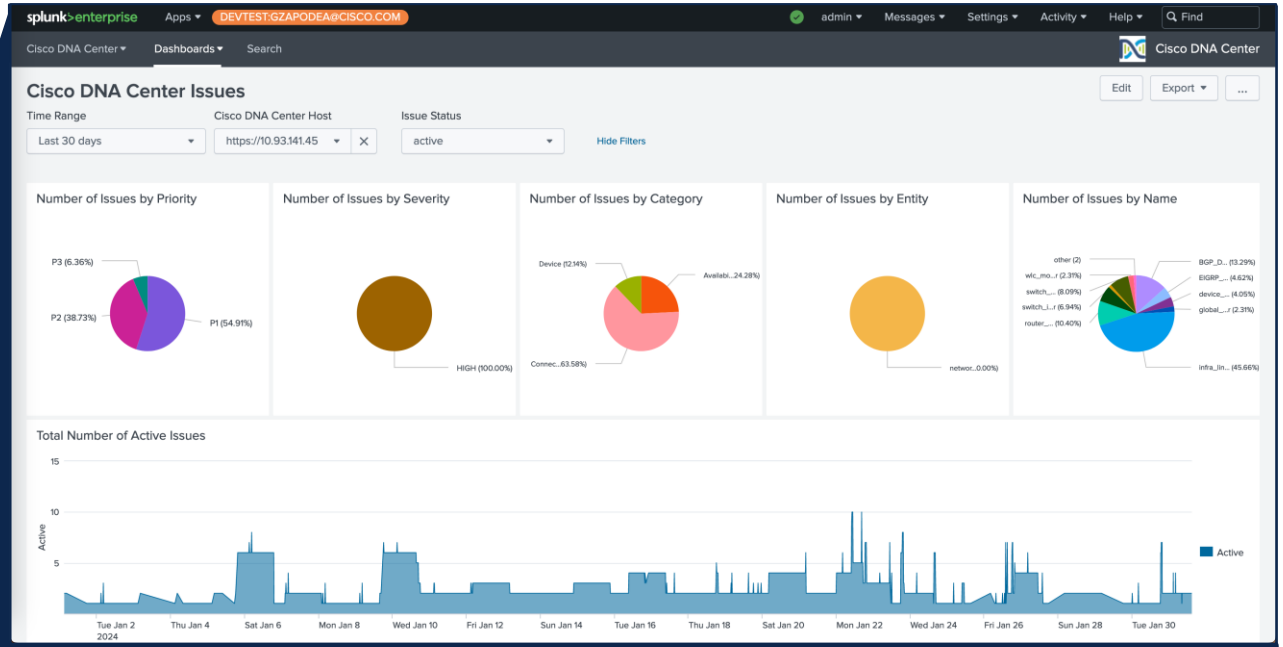


- Collects telemetry from multiple resources
- Provides full visibility into assets
- Analyzes gathered data using advanced analytics and maching learning algorithms
- Improves threat detection, response and remediation of maliciousness

XDR Overview
XDR 5-min Demo Video

Splunk Integration





Issues Dashboard, select the:

- Time range
- Catalyst Center host
- Issue status – active or resolved

Catalyst 9000 Switching Security

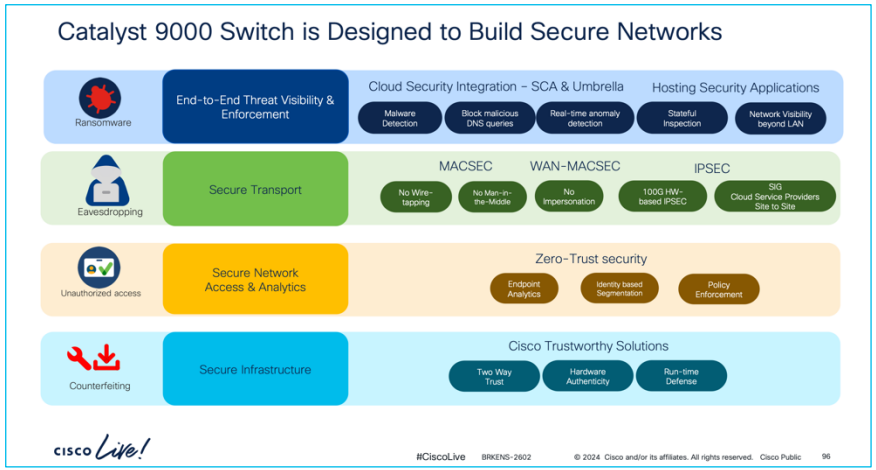
BRKENS-2602

End-to-End Security Strategy for Enterprise Campuses with Catalyst 9000 Series Switches

Ama Owusu-Hammond - Technical Marketing, Cisco

This session is focused primarily on the Cisco Catalyst 9000 Series Switches, which can provide end-to-end security from campus and branch to cloud.

The session also covers secure infrastructure with Cisco Trustworthy Solutions, secure transport with MACsec and IPsec (site-to-site, site-to-cloud), secure endpoints with native connectors, Cisco Secure Network Analytics (Stealthwatch), Cisco Umbrella, auto-profile and secure endpoints, and using endpoint analytics and trust analytics. After this session, you will be able to take away how Catalyst 9000 Series Switches are built with security in mind for fulfilling various use cases.



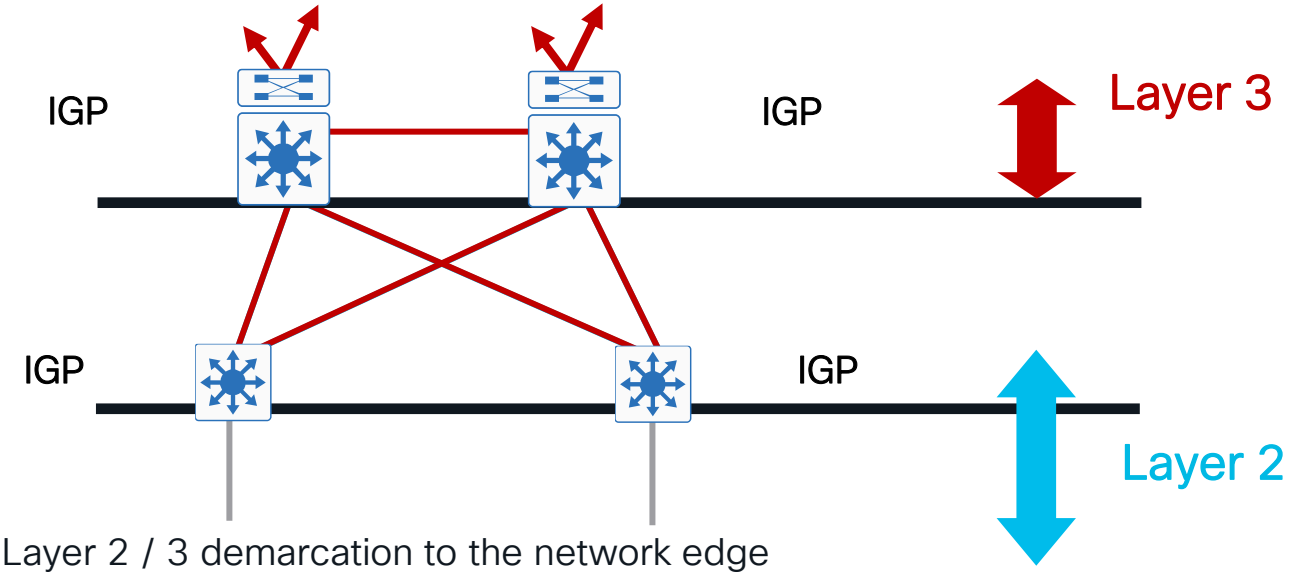
Design

Best Practices

- **LAN High Availability**
- **LAN Security**
- **Virtual Networking**
  - **Routed Access**
  - **Overlay**
  - **Virtual Networking Options**

Routed Access

Layer 3 distribution with Layer 3 access



- Move the Layer 2 / 3 demarcation to the network edge
- Leverages Layer 2 only on the access ports, but builds a Layer 2 loop-free network
- **Design Motivations** – Simplified control plane, ease of troubleshooting, highest availability

Routed Access

The **Routed Access PIN** (Tier 1) has the same purpose, but uses L3 IP routing to limit L2 scale

- Other names: IDF, Wiring Closet
- Semi-common in Campus & Branch networks

Main purpose is to connect users to network using L3 protocols to reduce L2 challenges.

- Mostly for network stability and simplicity of protocols
- Similar attributes & requirements as Distribution

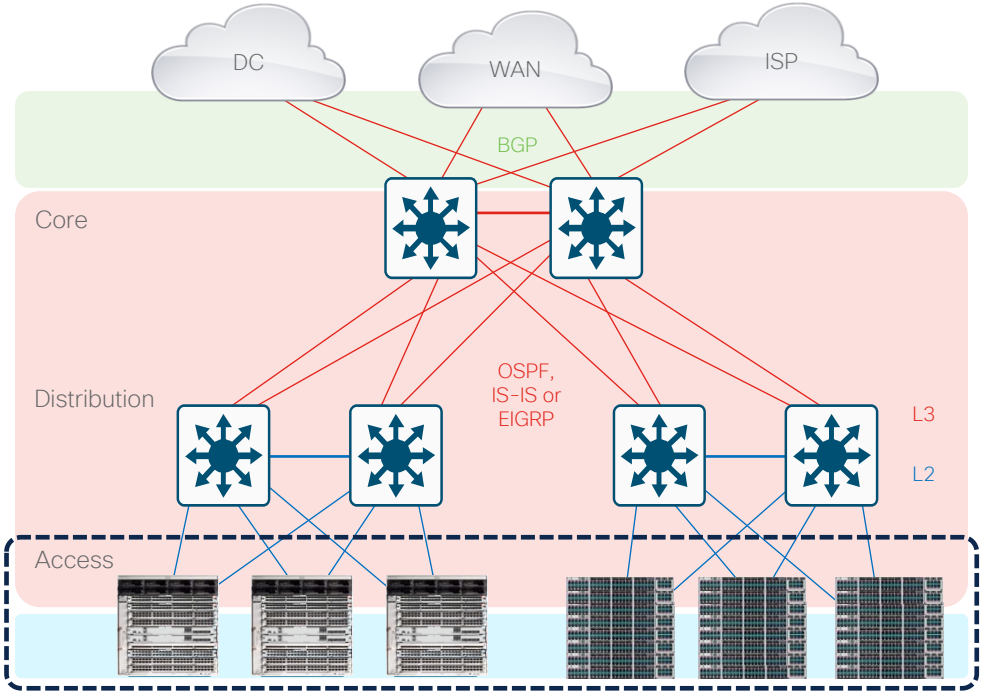
Tends to be both **L3 routed** (north) and **L2 switched** (south)

- North: SVI, HSRP/VRRP, ARP/ND, IGP, PIM
- South: VLAN, AAA, MAC, IGMP, STP Portfast

Tends to use multiple L2 & L3 features

- Access Security (e.g. IPDT/SISF, VACLs, PACLs, etc)
- Access QoS (e.g. NBAR, Classification & Marking)
- Access NetFlow (e.g. AVC, FNF, EPA & ETA)

Tends to require low-med L2 & L3 feature scale

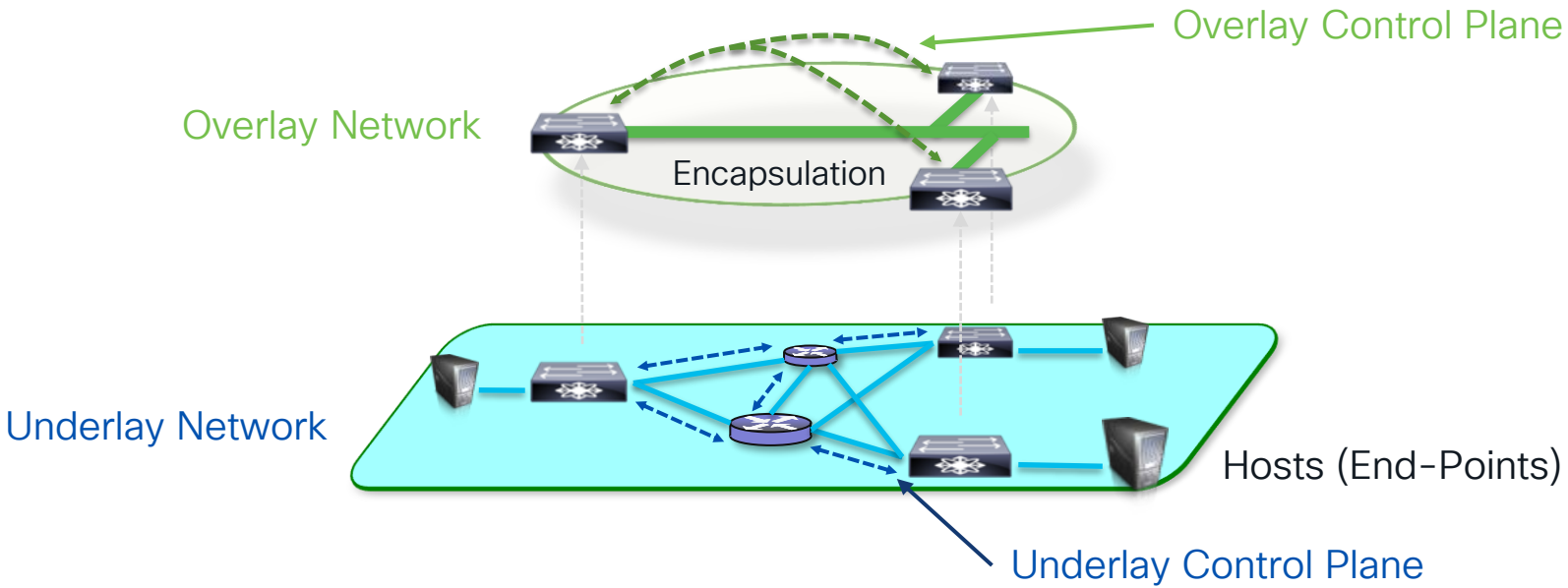


A Fabric is an Overlay

A logical mesh topology used to virtually connect devices

BRKENS-2501
BRKENS-2502

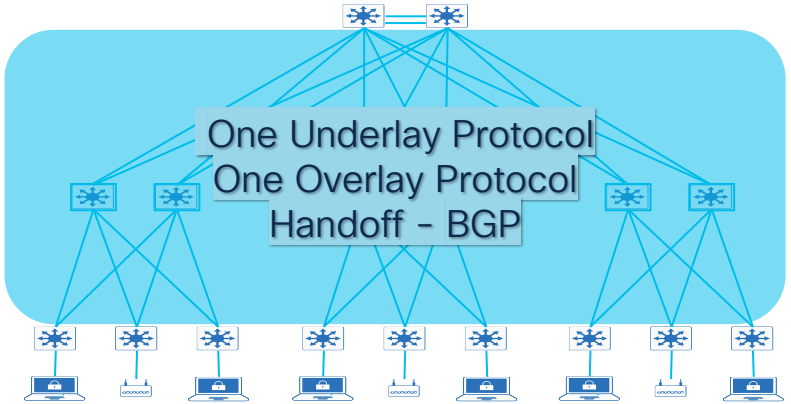
- Built on top of physical underlay topology – using encapsulation
- Provides additional L2/L3 services not provided by the underlay



Fabric Solves Network Problems

BRKENS-2501
BRKENS-2502

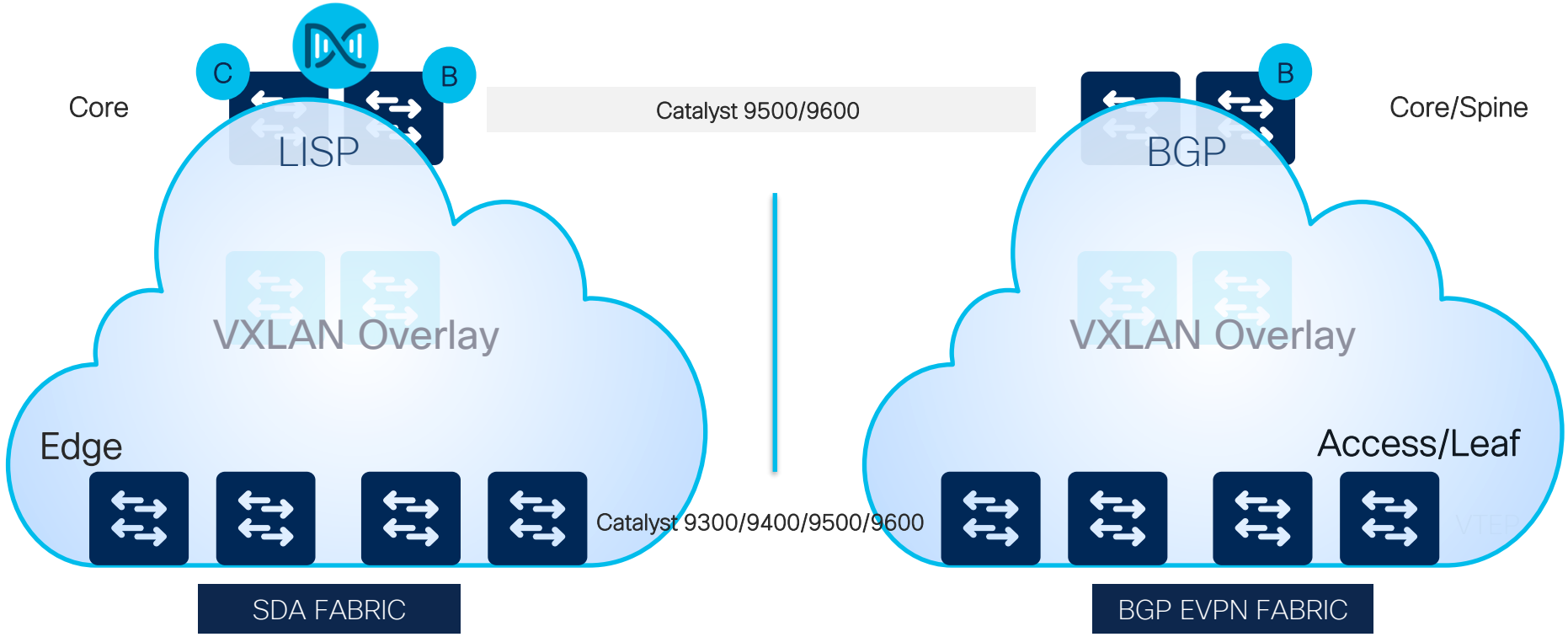
- ☑ Fabric to the Access removes L2 protocols (STP, DTP, VTP)
- ☑ Reliable Layer 2 extension – over simple Layer 3 network
- ☑ Simple, scalable, reliable *and* *automatable* network
- ☑ Consistent Access layer configurations
- ☑ Convergence of wired and wireless



Fabric Networks

Routed Access Evolution

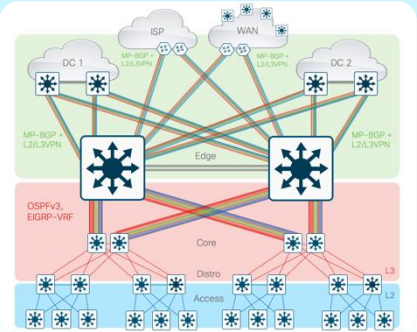
Live!
BRKENS-2050
BRKENS-2092
BRKENS-2830



Virtual Networking in Campus

Providing additional services (beyond basic PINs)

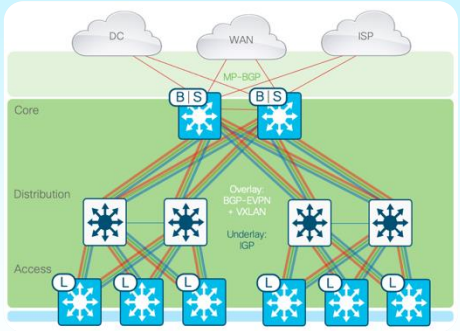
1 MPLS (L2/L3VPN)



- L3 Underlay + L2/L3 VPN Overlay
- Virtual Private Networks
- L3 VRF-based Segmentation
- WAN/Edge + VPN Services

MPLS/VPLS, **LDP**, SR, MP-BGP, PIC
MVPN, LSM, Extranet, MSR
SSO, NSF/NSR, ECMP, GIR
VPN-FNF, Uniform/Pipe QoS, PBR, IPACL

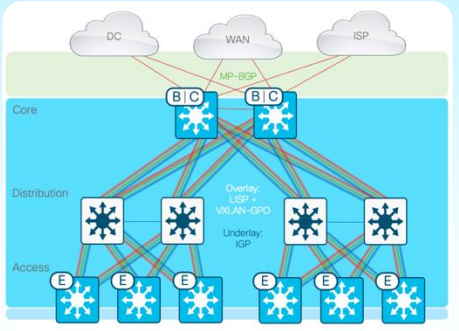
2 EVPN (L2/L3VNI)



- L3 Underlay + L2/L3 VNI Overlay
- Virtual Network Instances
- L2/L3 VNI-based Segments
- Common WAN/LAN Services

MP-BGP/EVPN, **VXLAN**, VRF-Lite
L2 TRM, L3 TRM, L2 BUM
SSO, NSF/NSR, ECMP, GIR
Fabric-FNF, Uniform QoS, IPACL/OGACL

3 LISP (L2/L3VNI + SGT)



- L3 Underlay + L2/L3 VNI Overlay
- VNIs + Scalable Group Tagging
- L2/L3 VNI + SGT Segments
- LAN Services + Group-Based Policy

LISP, **VXLAN-GPO**, MP-BGP, VRF-Lite
LISP HER, Native, L2 BUM
SSO, NSF/NSR, ECMP, GIR
Fabric-FNF, App QoS, SGACL

Catalyst 9000 Switching QoS

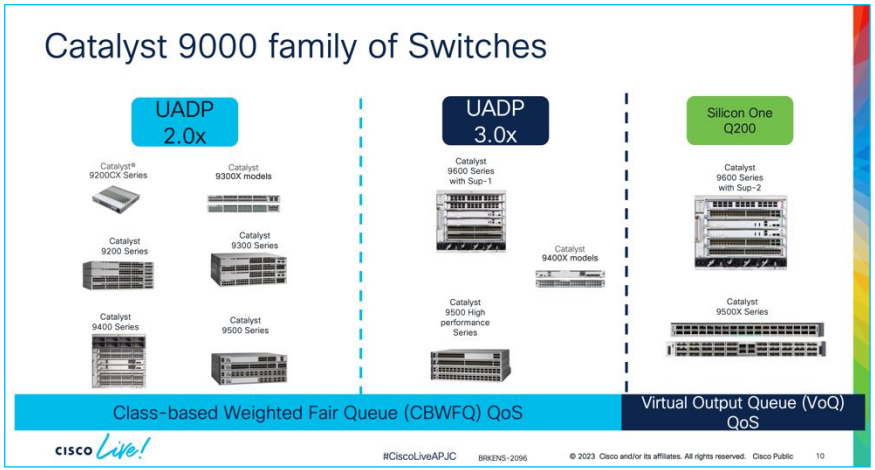
BRKENS-2096

Cisco Catalyst 9000 Switching QoS Deep Dive

Ninad Diwakar - Technical Marketing, Cisco

This session will deep dive into the QoS model used in the Cisco Catalyst 9000 Series of switches powered by the Cisco UADP and Cisco Silicon One Q200 ASICs.

The session will cover platform-specific designs for classification, policing, and ingress and egress queueing policies which are applicable to the Catalyst 9200, 9300, 9400, 9500 and the 9600 switches. To close things off, the session will cover thought processes to be followed for migration configurations from Catalyst 6500 Series switches over to the Catalyst 9500/9600 Series switches.

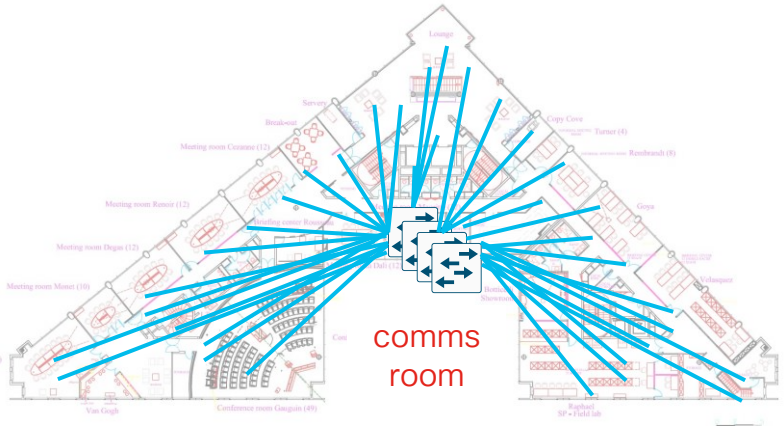


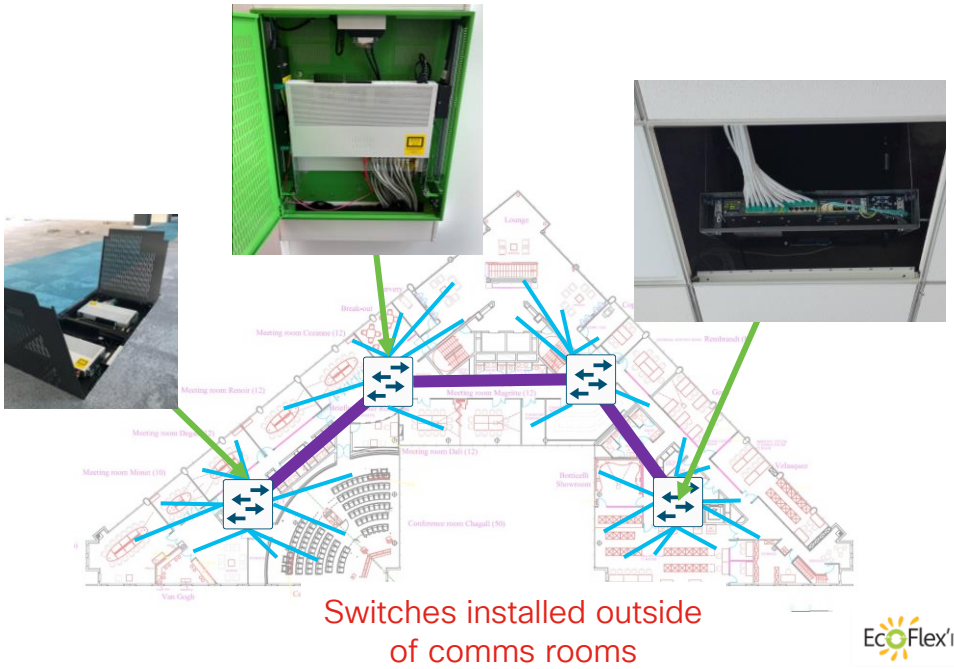
cisco Live!

Fiber To The Active Consolidation Point

EcoFlex'IT™

Upgrading Fiber/Ethernet cabling can be costly





Traditional deployment

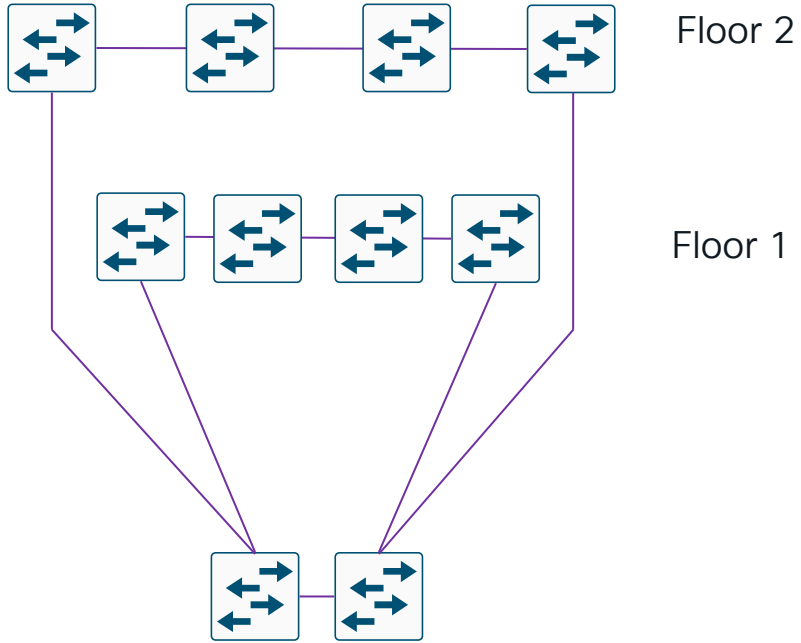
FTTACP-EcoFlex'IT™ deployment

https://osi.rosenberger.com/fileadmin/content/osi/EN/News/Whitepaper/Rosenberger_OSI_Whitepaper_FTT-ACP_EN.pdf

How Fabric Networks could help?

FTTACP example

- Rings
  ➔ Need to Avoid L2 loops
- More complex topology
  ➔ Need Abstraction
- More points of management
  ➔ Need Automation
- More devices in a path
  ➔ Need Assurance
- Connect building solutions to a converged network platform
  ➔ Need Security/Segmentation

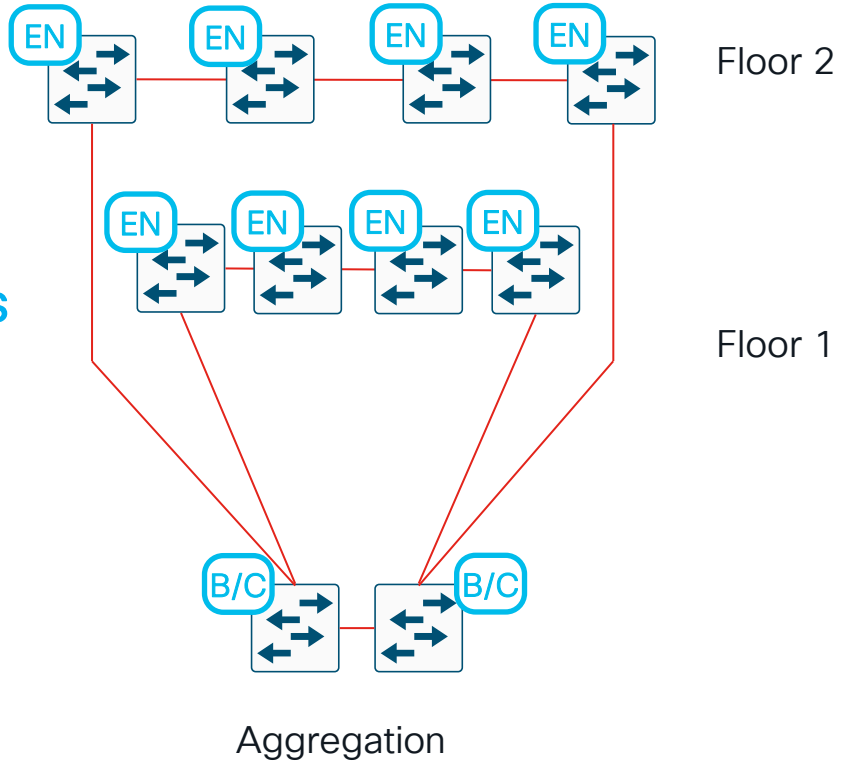


FTTACP deployment

Cisco SD-Access for FTTACP

- Remove L2 loops
- Abstraction
- Automation
- Assurance
- Security/Segmentation

Cisco SD-Access



MPLS-VPN Provider Edge

The **Provider-Edge PIN** (Tier 3-4) focuses on connecting multiple Campus areas to remote domains (SP/WAN) using MPLS-VPN.

Main goal is to connect EVPN fabric to other networks

Uses a **L3 Underlay + L3 Hand-off**

- North (outside): L3 MP-BGP + Inter-AS, PIM + MSDP
- South (inside): L3 IGP, PIM + MSDP

Uses a **Virtualized L2/L3 Overlay**

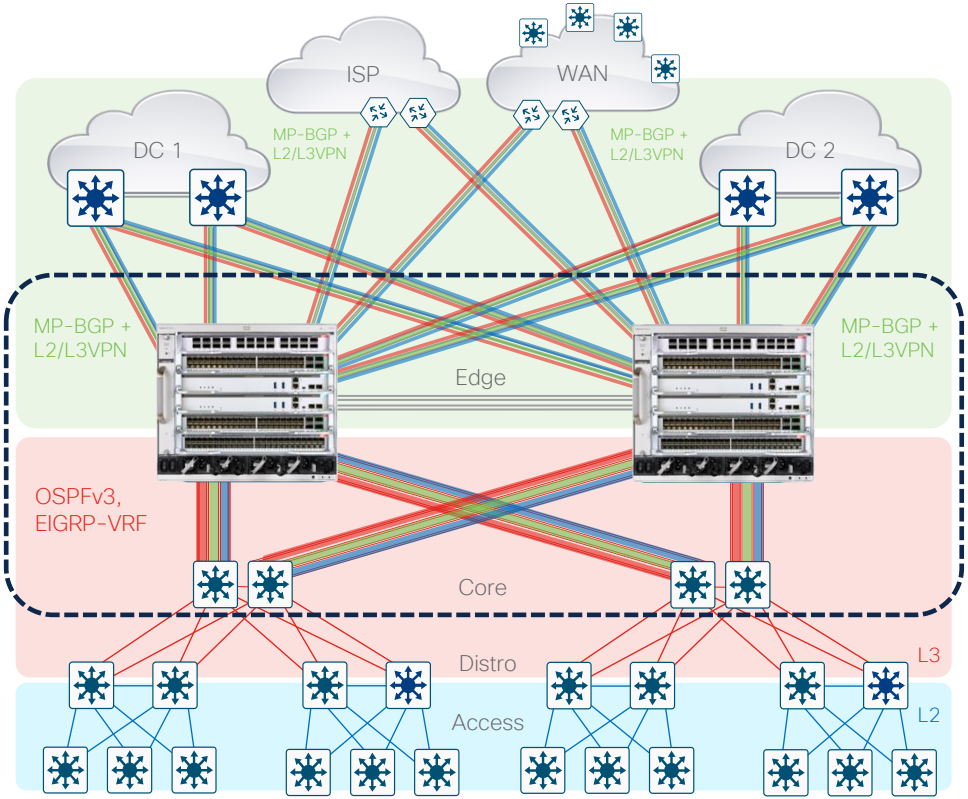
- Control-Plane: MPLS, EoMPLS/VPLS, MVPN
- Data-Plane: LDP, mLDP
- Policy-Plane: VPN ID

Tends to use Overlay-aware Features

- IP or OG ACLs (e.g. destined Outside)
- Uniform/Pipe QoS (e.g. separate Inner vs. Outer)
- Inter-VRF Routing (e.g. VRF-Lite, Leaking)
- MPLS-aware NetFlow (e.g. VPN ID in FNF)

May require multiple encapsulation(s)

Tends to require high L2/L3 & feature scale



EVPN Border & Spine

The **EVPN Border & Spine** PIN focuses on connecting an EVPN Fabric and/or other network domains.

- Typically, the same layer as Core or Edge (Tier 3-4)

Main goal is to connect EVPN fabric to other networks

Uses a **L3 Underlay + L3 Hand-off**

- North (outside): L3 MP-BGP + Inter-AS, PIM + MSDP
- South (inside): L3 IGP, PIM + MSDP

Uses a **Virtualized L2/L3 Overlay**

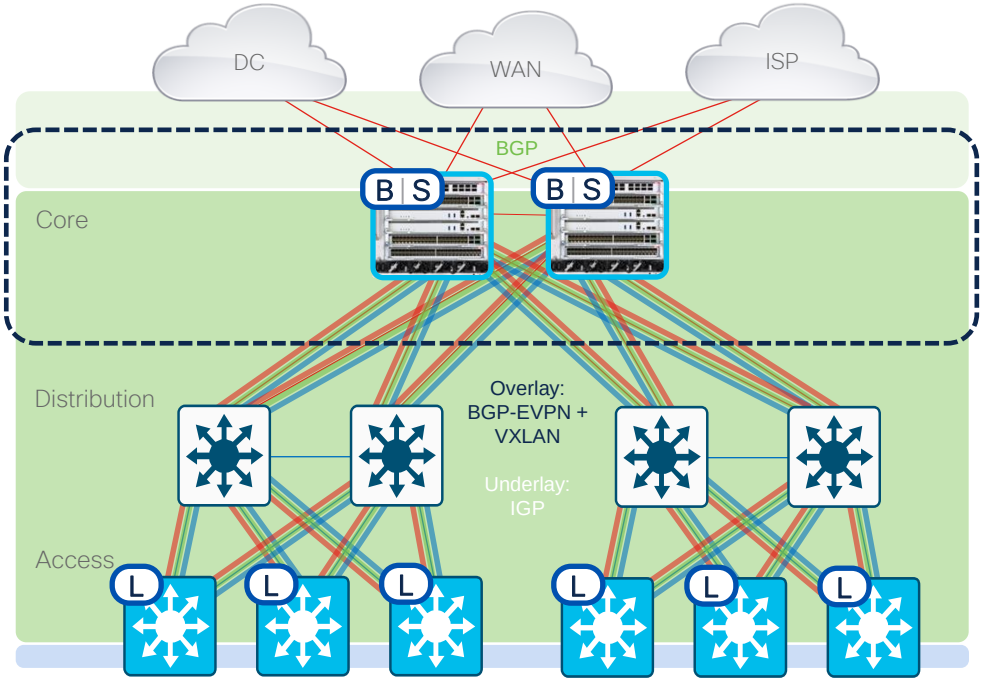
- Control-Plane: BGP-EVPN (RR), TRM
- Data-Plane: VXLAN
- Policy-Plane: L2/L3 VNID

Tends to use Overlay-aware Features

- IP/OG ACLs (e.g. destined Outside)
- Uniform QoS (e.g. copy Inner, queue Outer)
- Inter-VRF Routing (e.g. VRF-Lite, Leaking)
- Fabric NetFlow (e.g. VRF/VNID in FNF)

May require multiple encapsulation(s)

Tends to require high L2/L3 & feature scale



EVPN Leaf

The **EVPN Leaf** PIN focuses on connecting Wired endpoints to an EVPN Fabric domain.

- Typically, the same layer as Access or Extended (Tier 1)

Main goal is to connect Endpoints to EVPN network

Uses a **L3 Underlay + L2 Hand-off**

- North (inside): L3 IGP, PIM + MSDP
- South (outside): L2 VLAN (L3 SVI), STP, IGMP

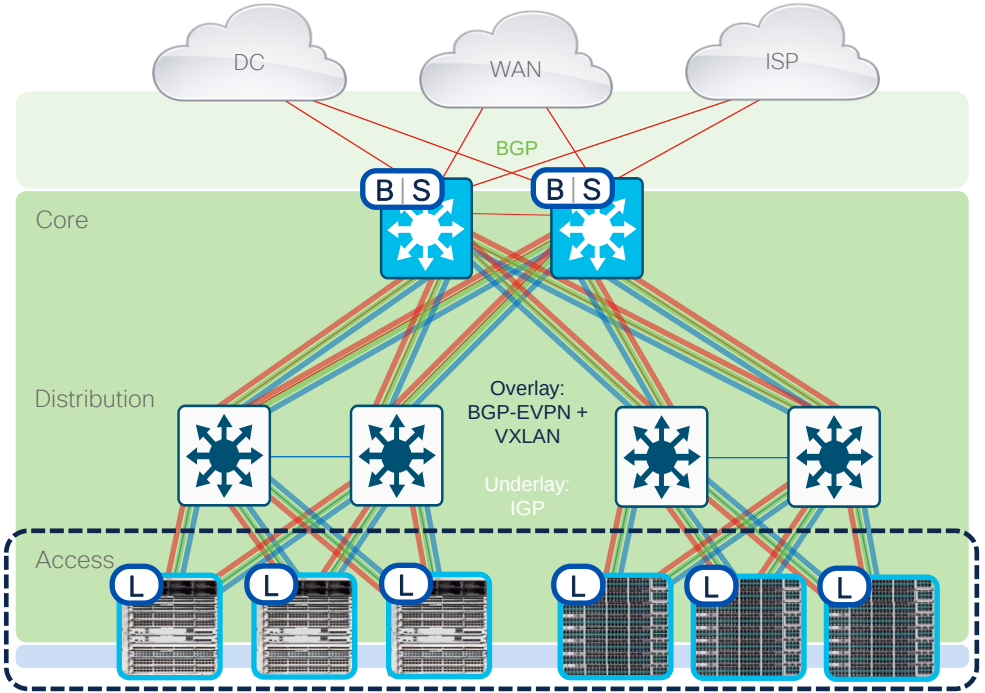
Uses a **Virtualized L2/L3 Overlay**

- Control-Plane: BGP-EVPN, TRM
- Data-Plane: VXLAN
- Policy-Plane: L2/L3 VNI

Tends to use Overlay-aware features

- IP/OG ACLs (e.g. destined outside)
- Uniform QoS (e.g. copy inner, queue outer)
- Inter-VRF Routing (e.g. VRF Leaking)
- Fabric NetFlow (e.g. FNF + VNID)

Tends to require med-high L2/L3 & feature scale



SD-Access Border & CP

The **SDA Border & CP** PIN focuses on connecting an SDA Fabric and/or other network domains.

- Typically, the same layer as Core or Core/Edge (Tier 3-4)

Main goal is to connect SDA fabric to other networks

Uses a **L3 Underlay + L3 Hand-off**

- North (outside): L3 MP-BGP + Inter-AS, PIM + MSDP
- South (inside): L3 IGP, PIM + MSDP

Uses a **Virtualized L2/L3 Overlay**

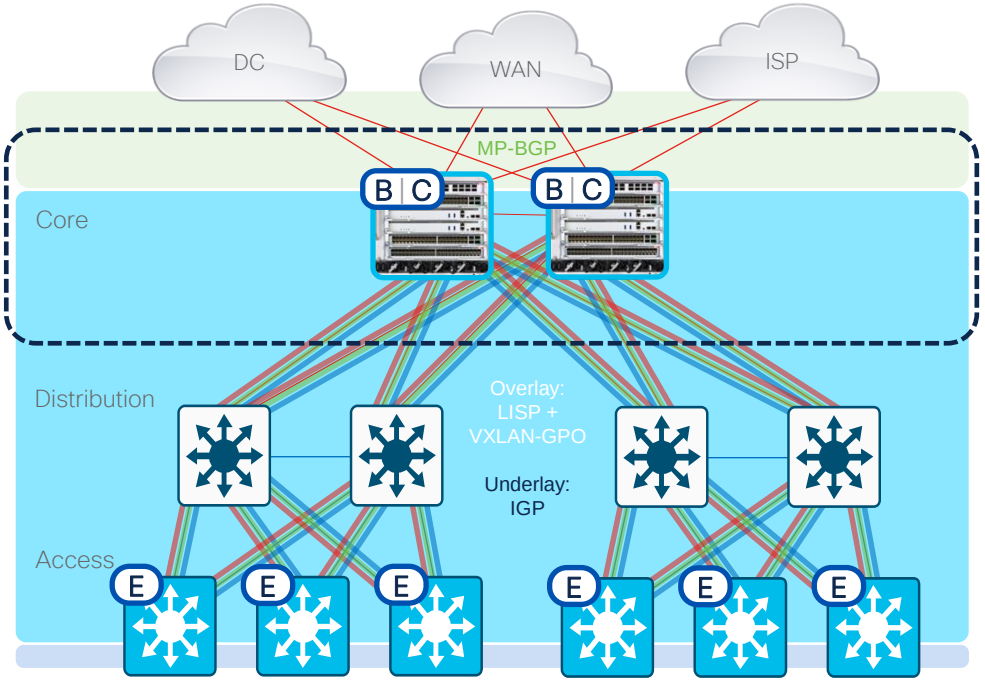
- Control-Plane: LISP (XTR, MS/MR), PIM
- Data-Plane: VXLAN-GPO
- Policy-Plane: L2/L3 VNI + SGT

Tends to use Overlay-aware features

- Security Group ACLs (e.g. destined outside)
- Uniform Pipe QoS (e.g. copy inner, queue outer)
- Inter-VRF Routing (e.g. VN Extranet, or VRF-Lite)
- Fabric NetFlow (e.g. VRF/VNID + SGT FNF, NaaS/ETA)

May require multiple encapsulation(s)

Tends to require higher L3 & feature scale



SD-Access Edge

The **SDA Edge** PIN focuses on connecting Wired/Wireless endpoints to an SDA Fabric domain.

- Typically, the same layer as Access or Extended (Tier 1)

Main goal is to connect Endpoints to SDA network

Uses a **L3 Underlay + L2 Hand-off**

- North (inside): L3 IGP, PIM + MSDP
- South (outside): L2 VLAN (L3 SVI), STP, IGMP

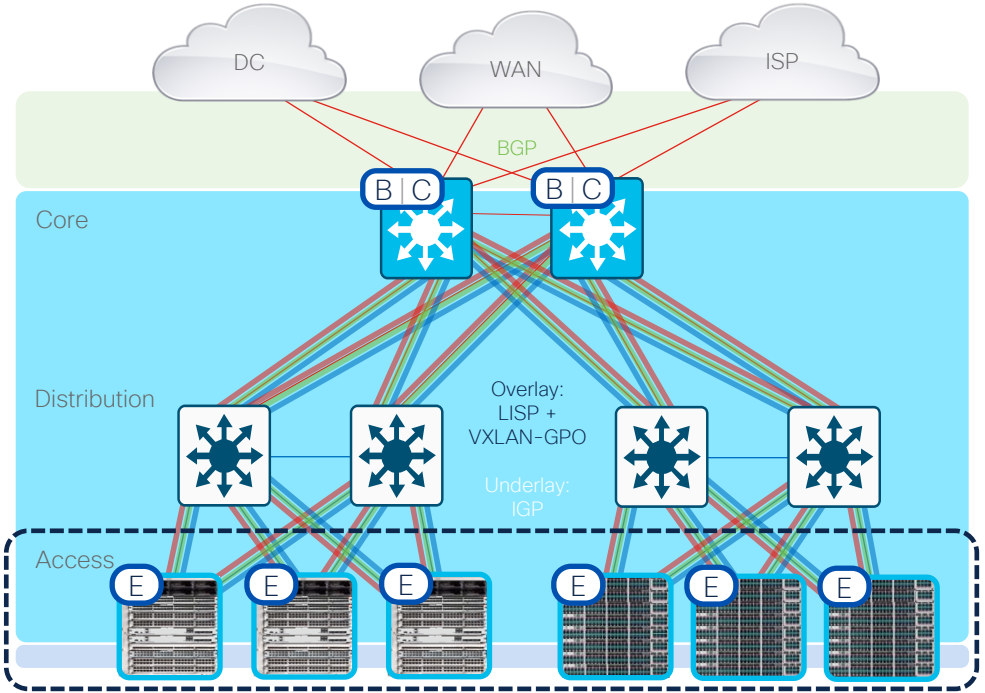
Uses a **Virtualized L2/L3 Overlay**

- Control-Plane: LISP (XTR), PIM
- Data-Plane: VXLAN-GPO
- Policy-Plane: VN + SGT

Tends to use Overlay-aware features

- Security Group ACLs (e.g. destined outside)
- Uniform Pipe QoS (e.g. copy inner, queue outer)
- Inter-VRF Routing (e.g. VN Extranet)
- Fabric NetFlow (e.g. FNF, NaaS)

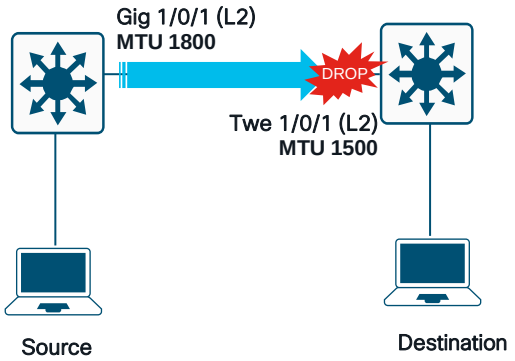
Tends to require higher L3 & feature scale



MTU Consideration

MTU is the Maximum Transmit Unit a device can forward.

- In general this "Unit" is the IP packet Length including the IP Header.
- L2 headers like, Dot1q tag, MacSec, SVL header etc, aren't accounted in this calculation
- System MTU vs Port MTU vs IP MTU
  - **System MTU** - System MTU is a global configuration, which sets the MTU of the whole device
  - **Per-port MTU** - Per-port MTU allows setting an MTU value on a per interface basis, and this takes precedence over the system MTU configuration. Once the per-port setting is removed, the interface will fall back to the system mtu.
  - **IP MTU** – is only applicable to IP packets. Other non-ip packet sizes will not be accounted for using this command.



Catalyst 9000 switches handle packet sizes from **64** bytes to **9238** bytes

Catalyst 9000 Overlay Fabrics

SD-Access with BGP EVPN
Catalyst Center

Beta Signup

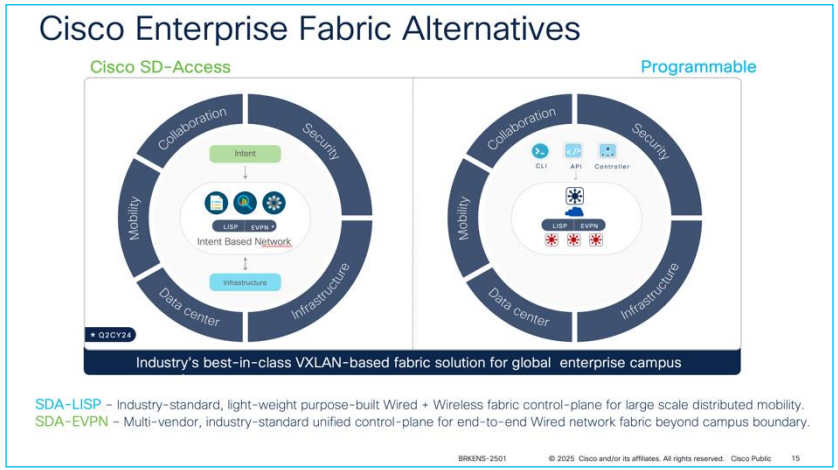
BRKENS-2501

Overlay Design Options for Campus Networks

Raj Kumar Goli – Technical Marketing, Cisco

This presentation will delve into the various overlay design options available with the state-of-the-art Catalyst 9000 Switching Platforms. We'll start by defining the concept of network overlay and its critical role in modern network architecture, especially in the era of cloud computing and virtualization.

The focus will then shift to the Catalyst 9000 series, exploring how these switches leverage advanced technologies to support multiple overlay design options. This includes discussion on technologies like Virtual Extensible LAN (VXLAN) and Software-Defined Access (SD-Access), which are integral for creating network overlays.



Catalyst 9000 SDA Design

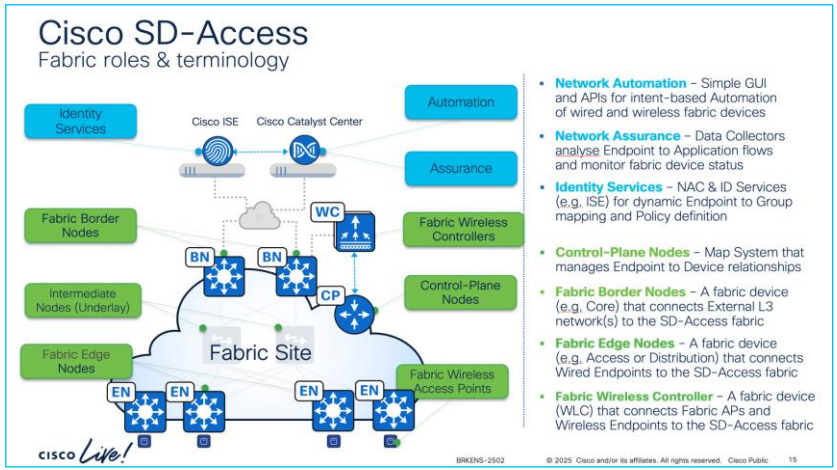
BRKENS-2502

Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment

Mahesh Nagireddy - Technical Marketing, Cisco

This session includes a brief introduction of Cisco SD-Access components, and dives into design and scale considerations and deployment options, for single-site designs covering greenfield and brownfield converged wired and wireless infrastructures.

Participants will gain insights into how Cisco SD-Access can provide a journey to digitalization and immediate benefits at every step of embracing the zero-trust architecture. This session will focus on multi-site design and deployment options, with the intent to provide end-to-end segmentation with consistent policy across the enterprise.



Cisco Live EMEA SD-Access Learning Map

Sunday–9th

- LABENS-2302 06:15 AM — SD-Access Troubleshooting
- LABENS-2410 07:00 AM — Explore the Art of Cross-Domain Automation with SD-Access and SD-WAN
- LABENS-2664 08:30 AM — Building the SD-Access Fabric with Ansible Playbooks: DIY SDA
- TECENS-3820a 01:30 PM — Software-Defined Access - Architecture Deep Dive - Part 1
- TECENS-2850 01:30 PM — Security in Enterprise - A cross-domain security primer across LAN, wLAN and WAN

Monday–10th

- TECENS-3688 08:30AM — Advanced Cisco SD-Access Troubleshooting
- TECENT-3688 08:30 AM — Advanced Cisco SD-Access Troubleshooting
- TECENS-3820b 08:45 AM — Software-Defined Access - Architecture Deep Dive - Part 2
- BRKENS-2810 02:15 PM — Cisco Software-Defined Access LISP Solution Fundamentals

Tuesday–11th

- CCP-1897 08:00AM — SD-Access and Zero Trust: Strategy, Impact, and Vision
- BRKENS-1852 08:00AM — TrustSec Refresh Reinforced with Common Policy Innovations
- LTRENS-2509 08:30 PM — Mastering Cisco SD-Access: LISP Pub/Sub and its Benefits Made Simple
- BRKENS-2811 02:30 PM — Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation
- BRKENS-2824 04:30 PM — Deploying Your First Cisco SD-Access Project

Wednesday–12th

- IBOENS-2820 09:00 AM — Deploying a Global SD-Access Zero-Trust Network
- BRKENS-1803 12:30 PM — Real-World Success Stories Powered by Cisco SD-Access!
- BRKENS-1851 01:00 PM — Zero Trust: Secure the Workplace with Cisco Software-Defined Access
- LTRENS-3751 02:00 PM — SD-Access as Code with Cisco Catalyst Center and ISE Automation
- BRKENS-2827 03:00 PM — Cisco SD-Access Migration Tools and Strategies
- BRKENS-2502 05:00 PM — Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment

Thursday–13th

- BRKENS-2820 08:45 AM — Demystifying IP Multicast in SD-Access
- BRKENS-3826 12:15 PM — Advanced LISP SD-Access Forwarding Architecture
- BRKTRS-3821 02:15 PM — Mastering Troubleshooting with Cisco Catalyst Center & SD-Access
- BRKENS-2819 03:00 PM — Cisco SD-Access and Multi-Domain Segmentation
- IBOENS-2820 03:00 PM — Deploying a Global SD-Access Zero-Trust Network
- BRKENS-3810 05:15 PM — How to Adopt Zero Trust using SD-Access and Default-Deny without Tears

Friday–14th

- BRKENS-3834 11:00:AM — 1 to 100: Master All Steps of Deployment, Seamless Integration, and Migration of Large SDA and SD-WAN Networks

Capture The Flag

@Hub All week long

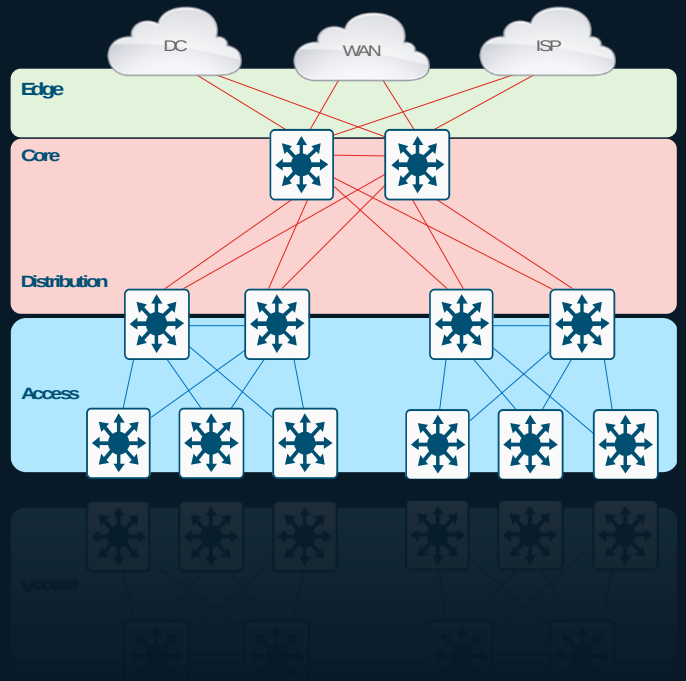
BU-led sessions

Catalyst Center

Cisco SD-Access LISP

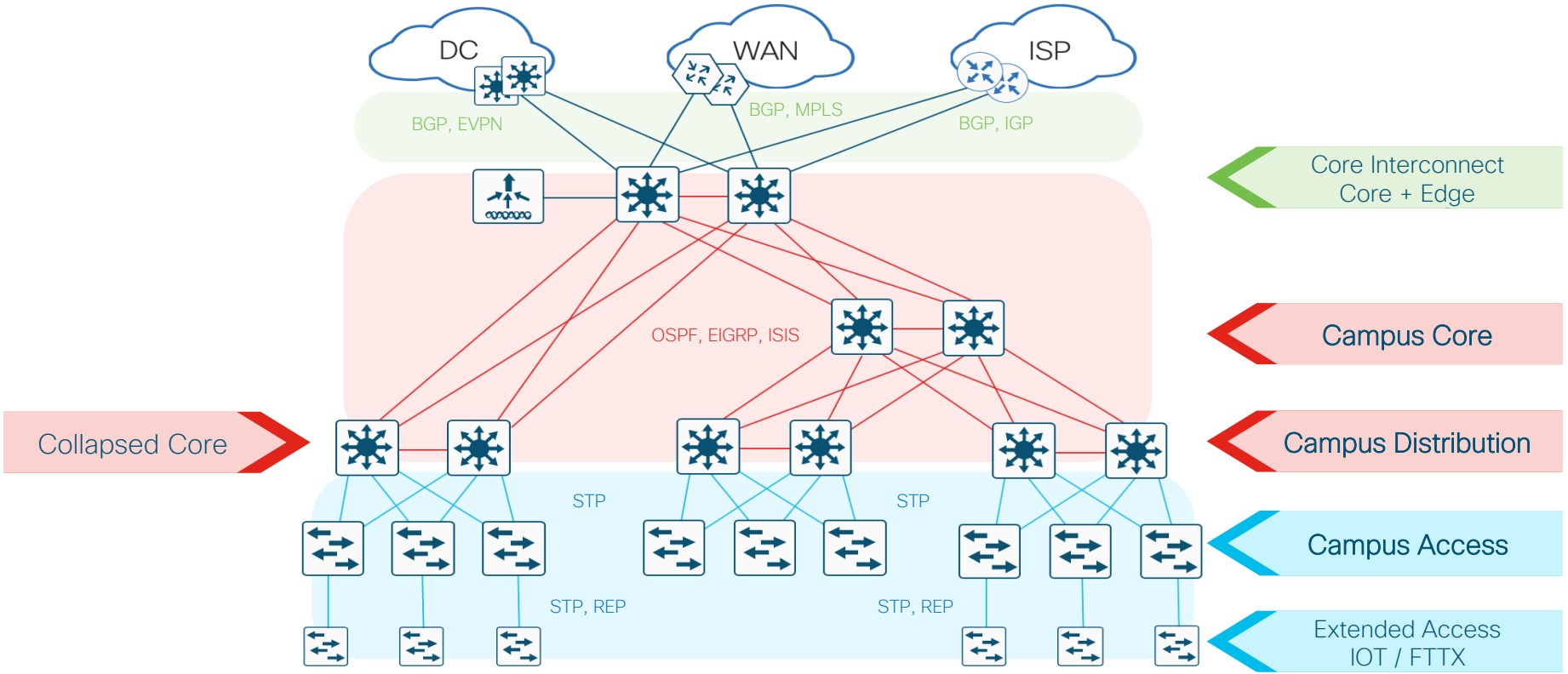
Wrap Up

- Know the Campus PINs
- Other References
- Keep Learning!! ☺



Remember: Campus PINs & Topology

RECAP



Hierarchical Campus – building blocks

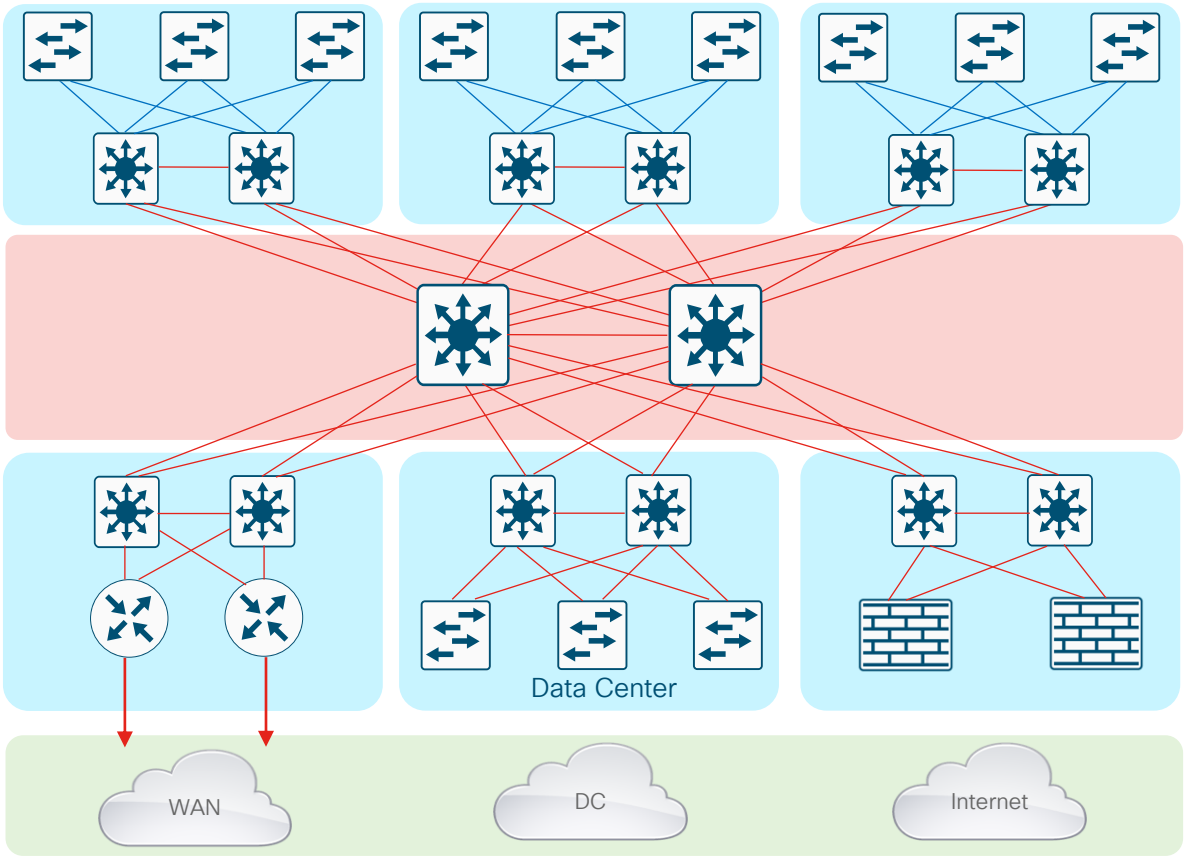
Access

Distribution

Core

Distribution

Access



Session Agenda - BRKENS-1500

Design Fundamentals

1 Campus Design Fundamentals

- What is “Campus”?
- Place in Network (PIN)

2 Campus Design Principles

- Multi-Layer Model
  - Hierarchical Design
- Access Layer
- Distribution Layer
- Core Layer

3 Campus Foundational Services

- Layer 1 physical layer & links
- Layer 2 switching protocols
- Layer 3 routing protocols

Design Considerations

4 Platform Design Considerations

- Chassis Considerations (Performance)
- Cabling Considerations (Speed)
- Feature Considerations (Scale)
  - L2 Features
  - L3 Features
  - Quality of Service (QoS)

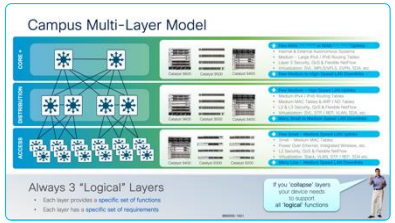
5 Campus Design Best Practices

- LAN High Availability
- LAN Security
- Virtual Networking

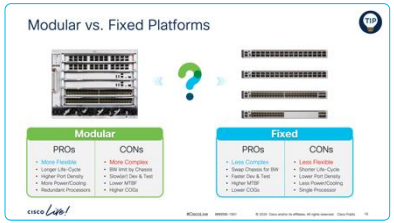
Remember: Campus Design Fundamentals

RECAP

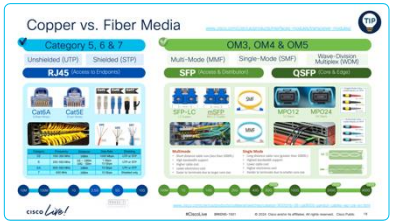
Collapse or Expand Layers?



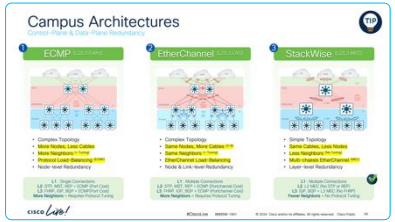
Modular or Fixed Platforms?



Fiber or Copper Links?

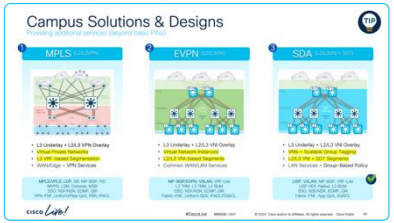


EtherChannel or Stacking?



What about Security?

L2/L3, LISP or EVPN?

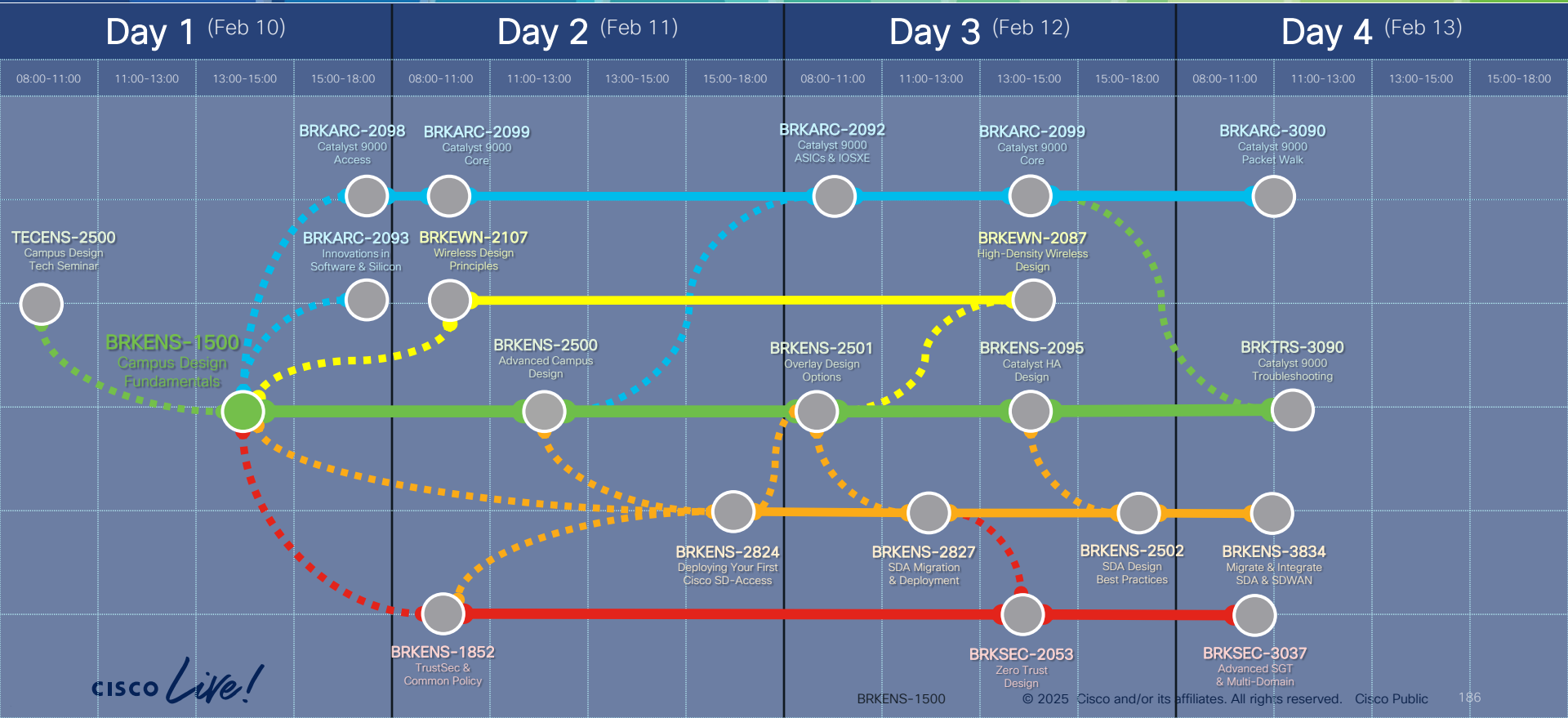


Cisco Campus Architecture

Cisco Live Amsterdam 2025 - Session Map

Sessions are available Online @ CiscoLive.com

You Are Here



Catalyst Leadership in Enterprise Networks

A Platform based Approach

New Feature
Enhanced

Catalyst Center and Meraki Dashboard

28M Network Devices Managed
50% Y/Y
19M APs | 6M Switches | 2.5M Routers | 830M Clients

13M
Devices on Catalyst Center

15.3M
Devices on Meraki Dashboard

Catalyst 9000 Family

100,000+ Customers, Millions of Switches

"Catalyst 9K continues to be the fastest ramping product in the company's history"

- Chuck Robbins, CEO Cisco Systems

Secure Networking

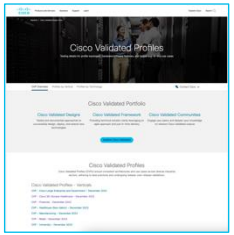
- Common Policy
- Secure Equipment Access
- SD-Access (LISP & EVPN)
- High-speed Encryption

Digital Experience

- Campus Automation
- AI Endpoint Analytics
- ThousandEyes Digital Experience
- AI Ops & Assurance

Operational Simplicity

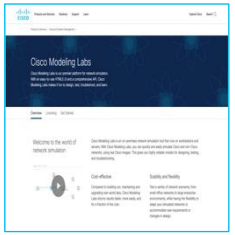
- Cloud Managed Catalyst
- Infrastructure as a Code
- S3 & CloudWatch Integration
- Visibility, Control & Rollback



Cisco Validated Profiles (CVP)

Industry Validated Reports

Industry Certifications

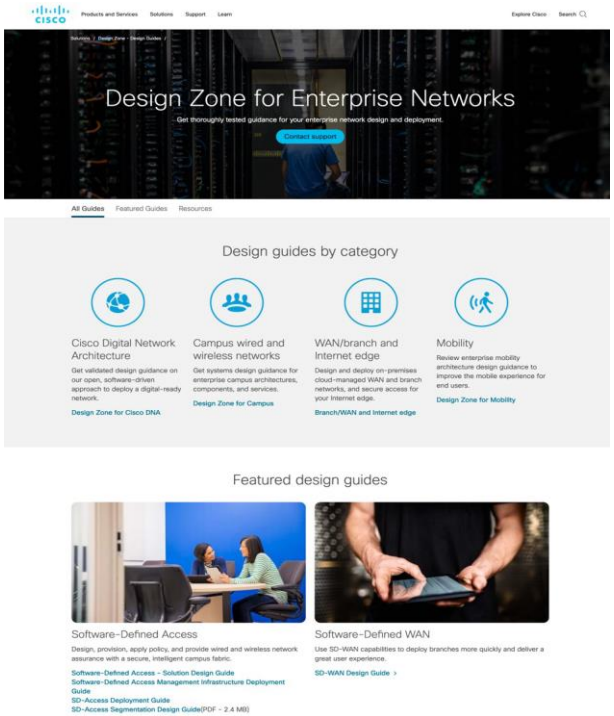


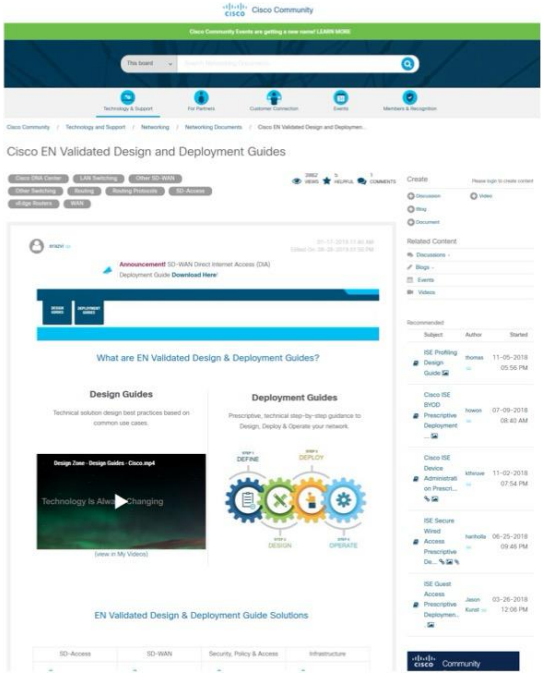
Cisco Modeling Labs

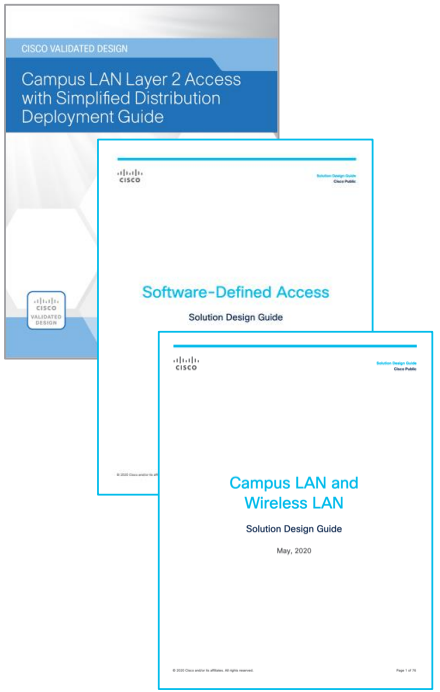
Keep Learning!

Cisco Validated Design (CVD)

cisco.com/go/cvd
cs.co/en-cvds







References – Multi-Layer Campus

Type	Sub-Type	References
General	Multi-Layer	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html www.ccexpert.us/network-design-2/designing-a-campus-network-design-topology.html networkdirection.net/articles/network-theory/hierarchicalnetworkmodel www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/
Core	Edge	www.atlantic.net/managed-services/network-edge/ www.ccexpert.us/network-design/enterprise-edge-modules.html what-when-how.com/ipv6-for-enterprise-networks/enterprise-edge-network-design-ipv6/
	Interconnect	www.geeksforgeeks.org/difference-between-lan-and-man www.ti.com/solution/intra-dc-interconnect-metro en.wikipedia.org/wiki/Backbone_network
	Baseline	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#Corelayer www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html#wp1107724 www.ccexpert.us/network-design/campus-core-design-considerations.html en.wikipedia.org/wiki/Hierarchical_internetworking_model#Core_layer
Distribution	Collapsed Core	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#Twotierdesign www.econfigs.com/ccna-1-5-compare-and-contrast-collapsed-core-and-three-tier-architectures interestingtraffic.nl/2018/06/08/collapsed_core_design oreilly.com/library/view/ccna-data-center/9780133860429/ch01lev3sec4.html
	Baseline	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#Distributionlayer www.ccexpert.us/network-design/building-distribution-layer-design-considerations.html en.wikipedia.org/wiki/Hierarchical_internetworking_model#Distribution_layer
Access	Baseline	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#Accesslayer www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html#wp1107746 www.ccexpert.us/network-design/building-access-layer-design-considerations.html en.wikipedia.org/wiki/Hierarchical_internetworking_model#Access_layer
	Routed Access	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#Layer3routedaccesscampusdesign www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html#wp1108952
	Extended/IOT	www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg/cci-dg.html#99480 www.geeksforgeeks.org/5-layer-architecture-of-internet-of-things/

References – ECMP & StackWise(Virtual)

Type	Sub-Type	References
General	Redundancy	www.cisco.com/c/en/us/solutions/hybrid-work/what-is-high-availability.html#~infrastructure-elements www.ccexpert.us/network-design/designing-link-redundancy.html www.geeksforgeeks.org/redundant-link-problems-in-computer-network/
Core	ECMP	www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5212-46.html www.ccexpert.us/routing-protocols/equalcost-load-balancing.html en.wikipedia.org/wiki/Equal-cost_multi-path_routing
	EtherChannel	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#EtherChannel en.wikipedia.org/wiki/Link_aggregation#Network_backbone en.wikipedia.org/wiki/Multi-chassis_link_aggregation_group
	SVL	www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2650.pdf www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#StackWiseVirtualTechnology
Distribution	ECMP	www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5212-46.html www.ccexpert.us/routing-protocols/equalcost-load-balancing.html en.wikipedia.org/wiki/Equal-cost_multi-path_routing
	EtherChannel	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#EtherChannel en.wikipedia.org/wiki/Link_aggregation en.wikipedia.org/wiki/Multi-chassis_link_aggregation_group
	SVL	www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2650.pdf www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#StackWiseVirtualTechnology
Access	ECMP	www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10555-15.html en.wikipedia.org/wiki/Spanning_Tree_Protocol#Path_to_the_root_bridge en.wikipedia.org/wiki/Flex_links
	EtherChannel	www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#EtherChannel en.wikipedia.org/wiki/EtherChannel
	Stacking	www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2650.pdf www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/white-paper-c11-741468.html www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-stackwise-architecture-cte-en.html www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#SwitchStacksandCiscoStackWiseTechnology

References – SD-Access, EVPN & MPLS

Type	Sub-Type	References
General	SDN/IBN	www.cisco.com/c/en/us/solutions/intent-based-networking.html www.networkworld.com/article/3281447/a-new-era-of-campus-network-design.html www.geeksforgeeks.org/difference-between-software-defined-network-and-traditional-network/
Core	SDA	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKCRS-2810.pdf#page=27 www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#BorderNode www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#ControlPlaneNode
	EVPN	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2021/pdf/BRKENS-2003.pdf#page=12 www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-7/configuration_guide/vxlan/b_177_bgp_evpn_vxlan_9500_cg/bgp_evpn_vxlan_overview.html#id_126799 www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#AlternativevirtualizationdesignforcampusBGPEVPNVXLAN
	MPLS	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKMPL-1100.pdf#page=48 www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKMPL-2112.pdf#page=42 www.geeksforgeeks.org/multi-protocol-label-switching-mpls/
Distribution	SDA	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKCRS-2810.pdf#page=19 www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#IntermediateNode
	EVPN	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2021/pdf/BRKENS-2003.pdf#page=12 www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-7/configuration_guide/vxlan/b_177_bgp_evpn_vxlan_9500_cg/bgp_evpn_vxlan_overview.html#id_126799
	MPLS	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKMPL-1100.pdf#page=48 www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKMPL-2112.pdf#page=42 www.geeksforgeeks.org/multi-protocol-label-switching-mpls/
Access	SDA	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKCRS-2810.pdf#page=24 www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#EdgeNode www.cisco.com/c/dam/en/us/solutions/collateral/internet-of-things/nb-09-intent-based-iot-wp-cte-en.pdf www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#CiscoSoftwareDefinedAccesscampusdesign
	EVPN	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2021/pdf/BRKENS-2003.pdf#page=12 www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-7/configuration_guide/vxlan/b_177_bgp_evpn_vxlan_9500_cg/bgp_evpn_vxlan_overview.html#id_126799
	MPLS	www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKMPL-1100.pdf#page=48 www.geeksforgeeks.org/multi-protocol-label-switching-mpls/

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install 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 February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

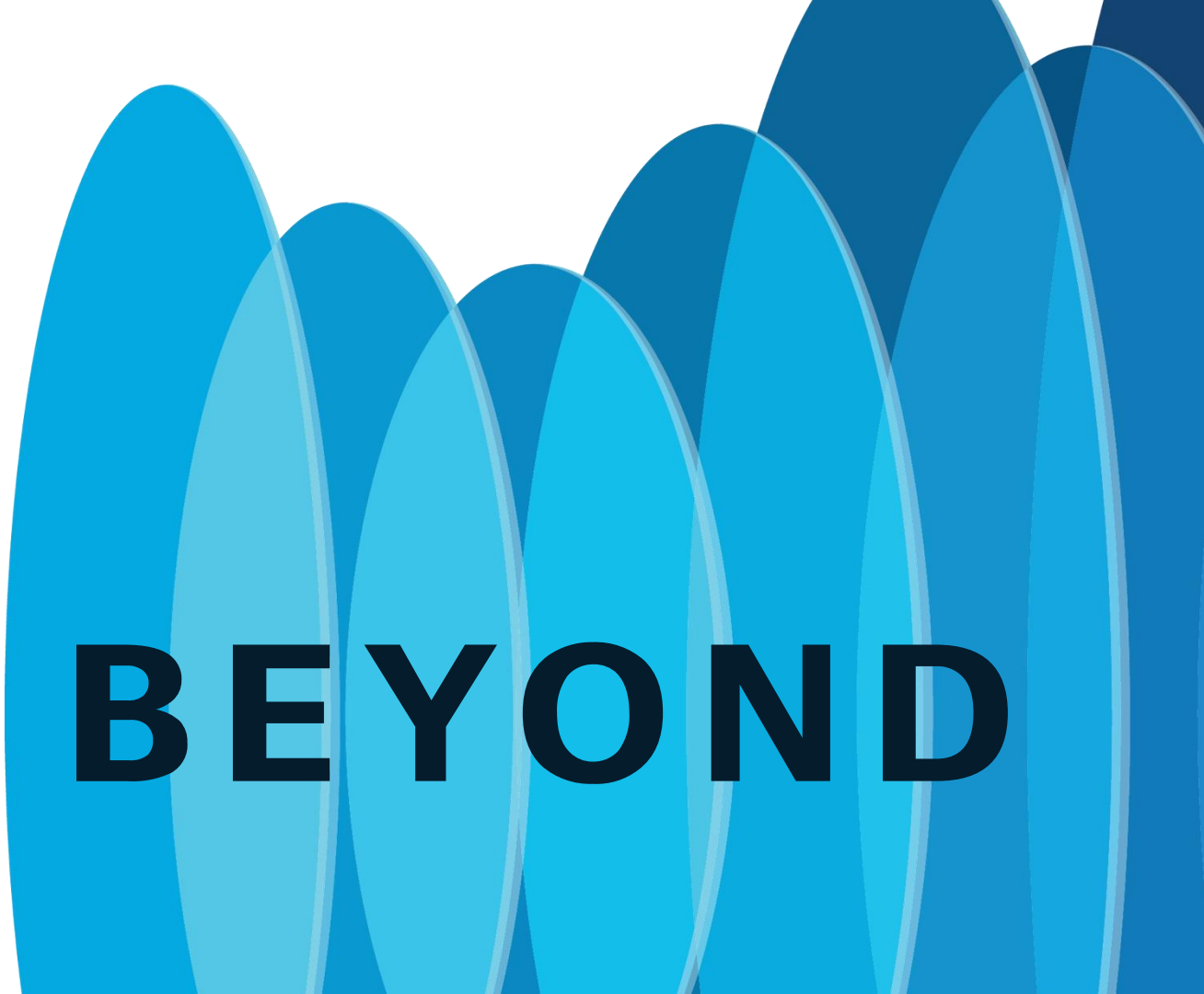
Continue your education

- 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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: jamatela@cisco.com


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND