

The Cisco Live! logo features the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy lines and geometric shapes, transitioning from dark blue on the left to bright yellow and white on the right, with a sunburst effect on the right side.

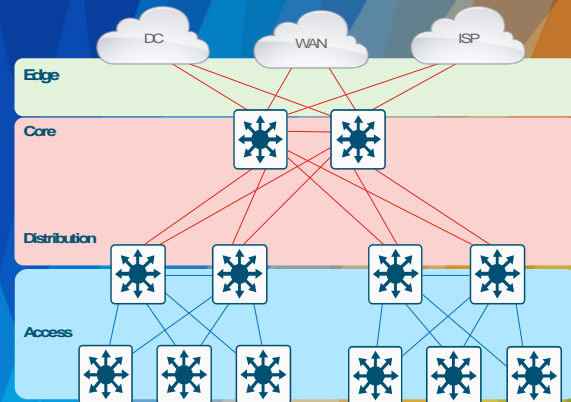
CISCO *Live!*

Let's go

123 - Enterprise Campus Wired Design Fundamentals

Back to Basics

Shawn Wargo, Principal TME
@Shawn_Wargo



Agenda

1 What is a Campus Network?

2 1-2-3 or 4+ Tier Design

3 ECMP ^{vs.} StackWise

4 MPLS ^{vs.} EVPN ^{vs.} SD-Access

5 Wireless & Security Notes

6 Summary & References

Campus Networks

- What is “Campus”?
- Place in Network (PIN)
- Multi-Layer Model
- Chassis Types
- Campus Cabling
- PIN Features

1

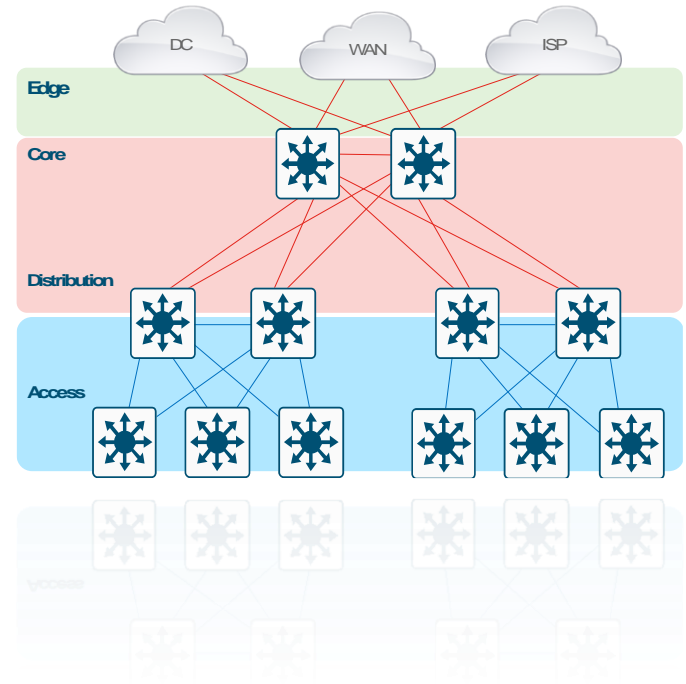
2

3

4

5

6





What is a “Campus”?

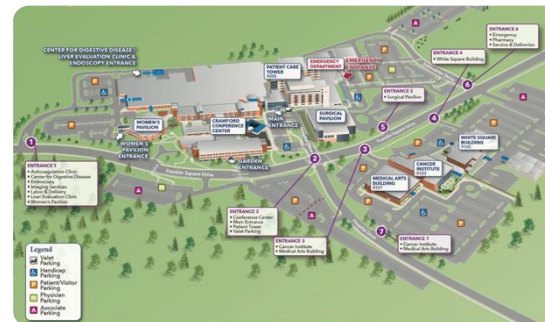
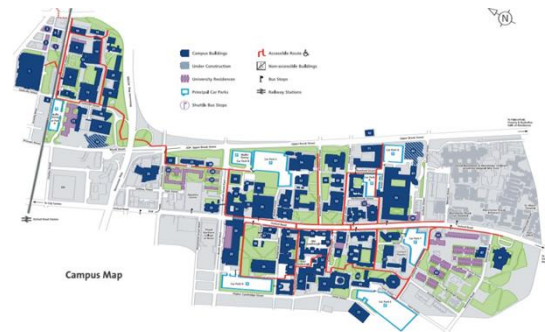
The basic Merriam-Webster definition of a [Campus](#) is: *A group of **one or more buildings**, and surrounding grounds, where **people and their belongings** work together.*

Common examples are Hospitals & Research Centers, Schools & Universities and Corporations & Offices.

Using this – it’s clear a [Campus Network](#) is focused on:

- **People** (Users, Vendors, etc.)
- **People's devices** (PCs, Phones, Printers, etc.)
- **Similar geographic area** (LAN, WLAN or MAN, etc.)
- **Access to 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

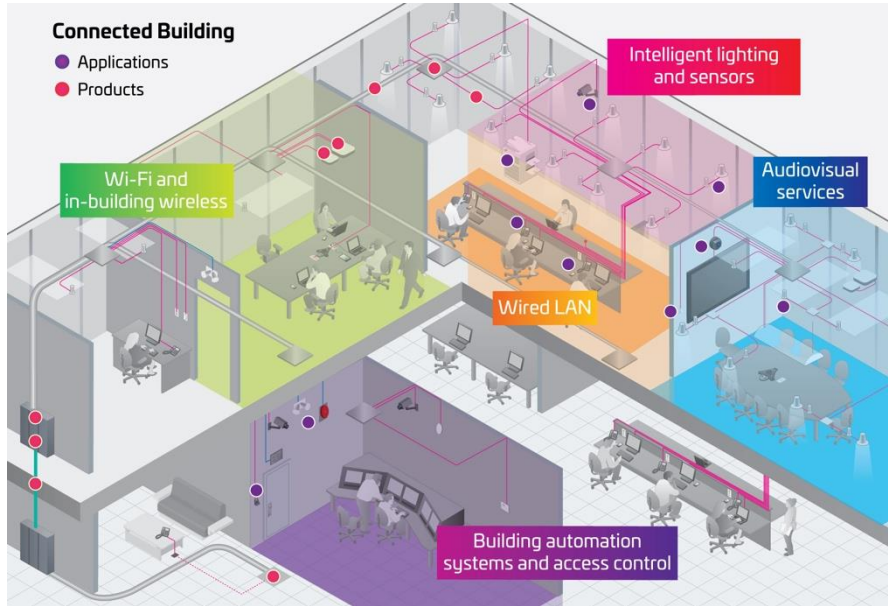


www.cisco.com/c/en/us/solutions/cisco-on-cisco/enterprise-networks.html

CISCO *Live!*

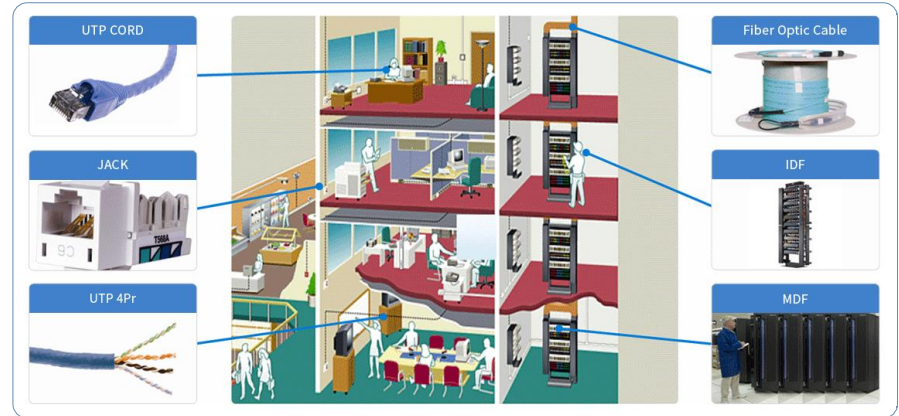
Campus Networks

Building MDF/IDF & Wiring Closets



MDF = Main Distribution Framework (Core)

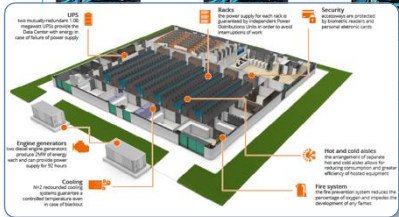
IDF = Intermediate Distribution Framework (Distro/Access)



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

Campus ≠ Data-Center

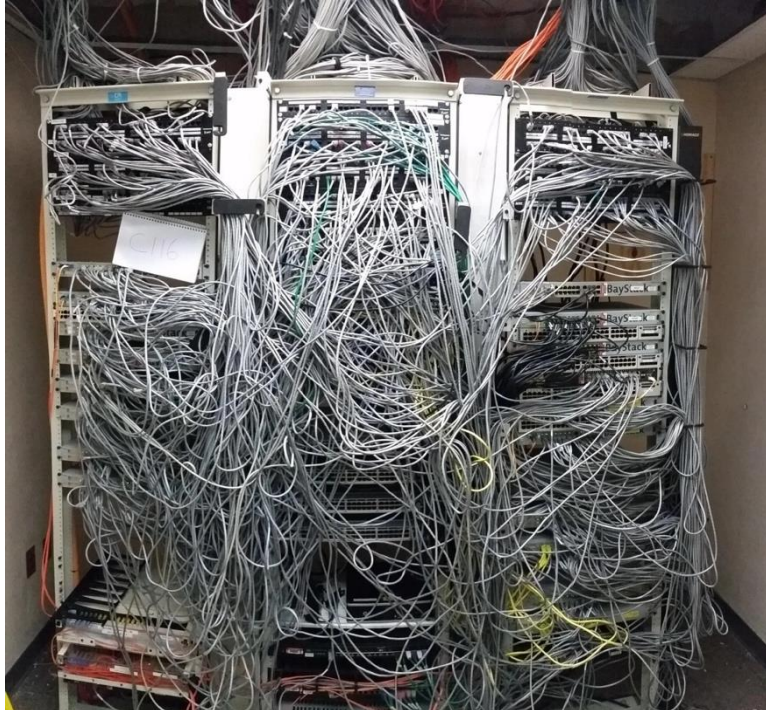
One or few large buildings nearby. Usually a single floor.



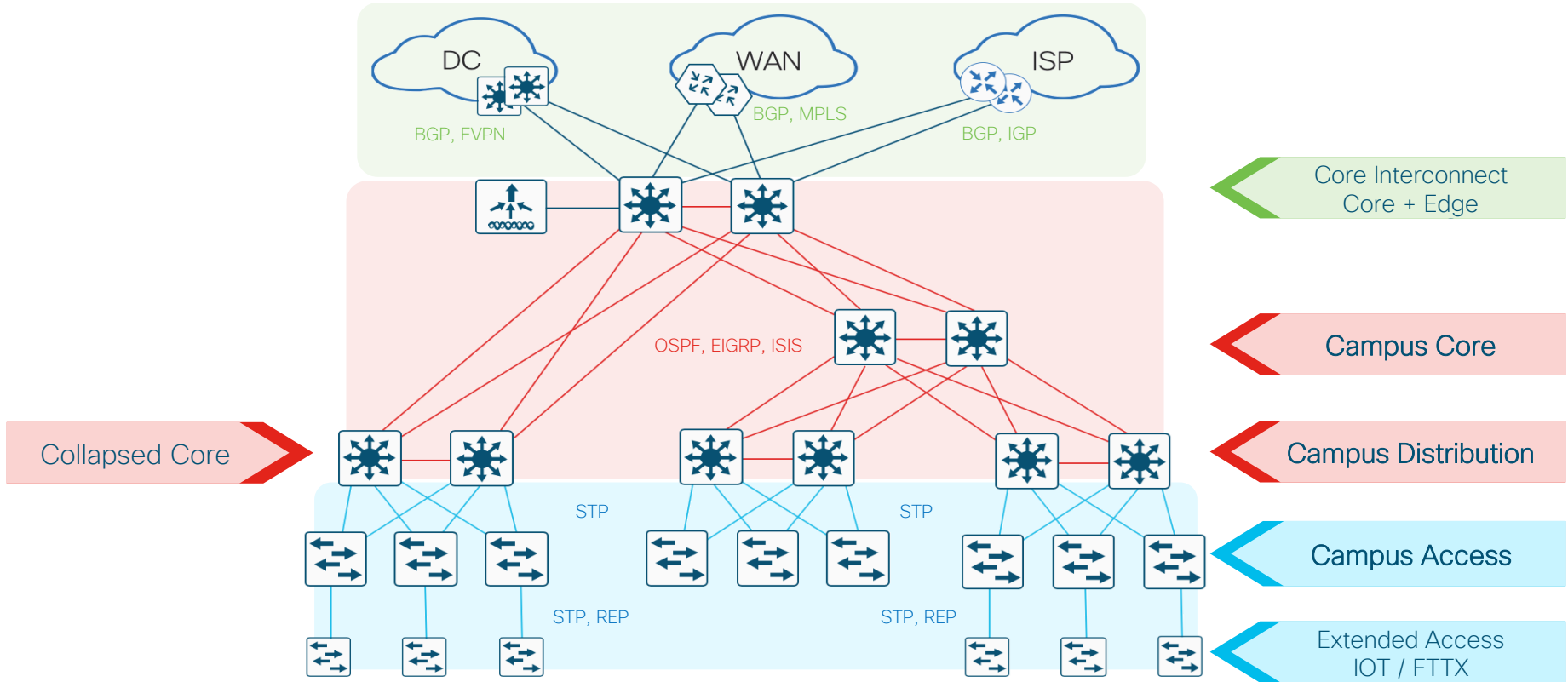
www.cisco.com/c/en/us/solutions/cisco-on-cisco/enterprise-networks.html



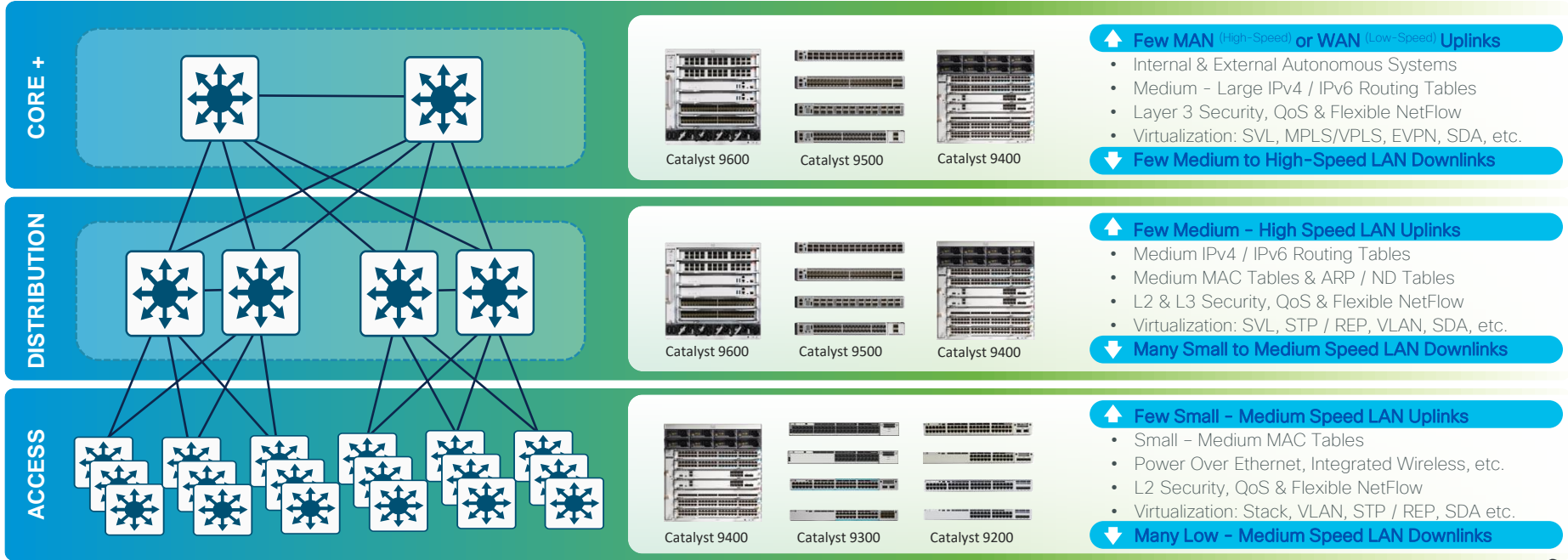
Campus Networks - Real Life



Campus PINs & Topology



Campus Multi-Layer Model



Always 3 “Logical” Layers

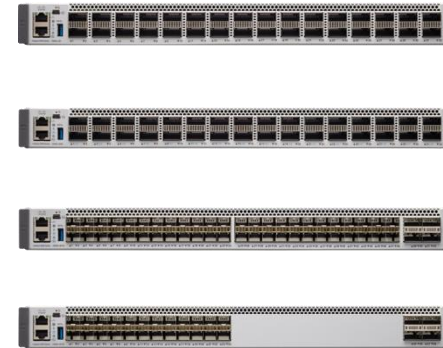
- Each layer serves a specific set of functions
- Each layer has a specific set of requirements

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





Modular vs. Fixed Platforms



Modular

PROs

- **More Flexible**
- Longer Life-Cycle
- Higher Port Density
- More Power/Cooling
- Redundant Processors

CONs

- **More Complex**
- BW limit by Chassis
- Slow(er) Dev & Test
- Lower MTBF
- Higher COGs

Fixed

PROs

- **Less Complex**
- Swap Chassis for BW
- Faster Dev & Test
- Higher MTBF
- Lower COGs

CONs

- **Less Flexible**
- Shorter Life-Cycle
- Lower Port Density
- Less Power/Cooling
- Single Processor

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

OM3, OM4 & OM5

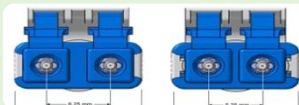
Multi-Mode (MMF)

Single-Mode (SMF)

Wave-Division Multiplex (WDM)

SFP (Access & Distribution)

QSFP (Core & Edge)



SFP-LC
LC Duplex

mSFP
Mini LC Duplex



SMF



MMF



MPO12
12 Fibers

MPO24
24 Fibers



Single-Mode Color Coded Boots on MTP
Red - 24 Fiber
Black - 12 Fiber
Gray - 8 Fiber



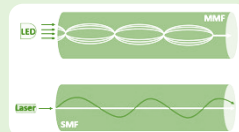
Multimode Color Coded Boots on MTP
Red - 24 Fiber
Blue - 12 Fiber
Gray - 8 Fiber

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



CISCO *Live!*

NBASE-T
ALLIANCE



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

Campus Networks

L2/L3 Unicast Technologies

IPv4 Unicast

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

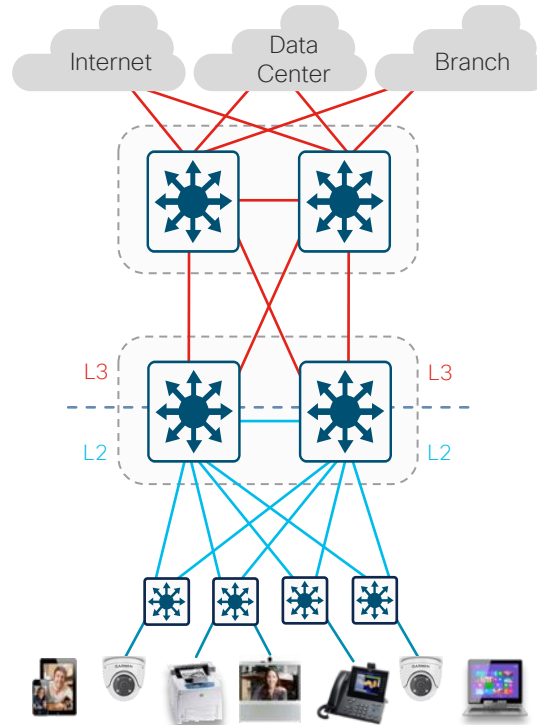
Core

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

Distribution

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

Access



IPv6 Unicast

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

Core

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

Distribution

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

Access

Campus Networks

L2/L3 Multicast Technologies

IPv4 Multicast

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

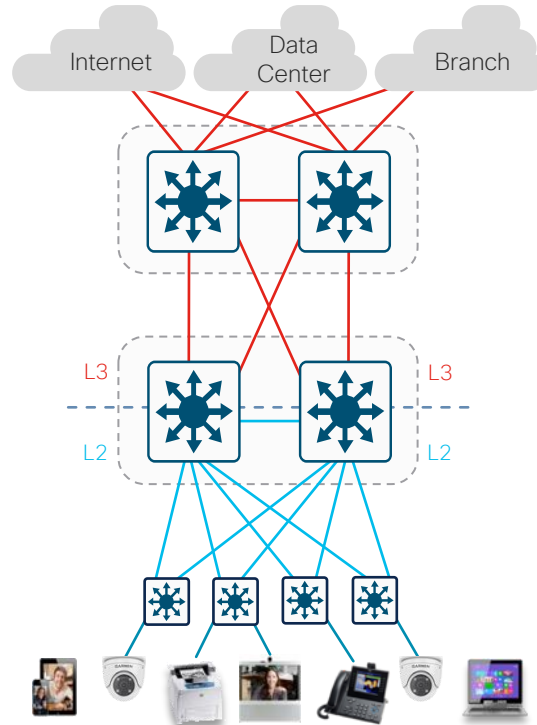
Core

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

Distribution

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

Access



IPv6 Multicast

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

Core

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

Distribution

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

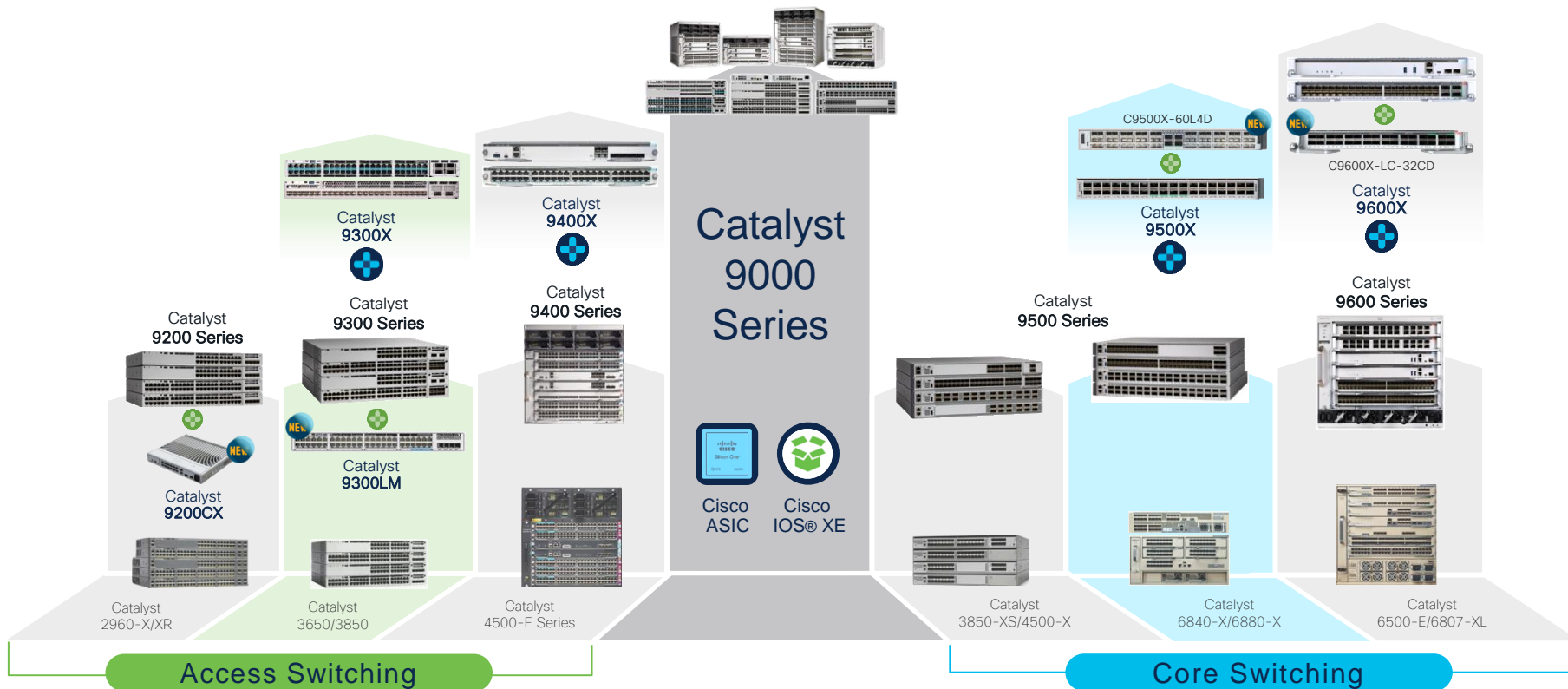
Access

Cisco Catalyst 9000 Switching Portfolio

One Family from Access to Core – Common Hardware & Software

2023

NEW

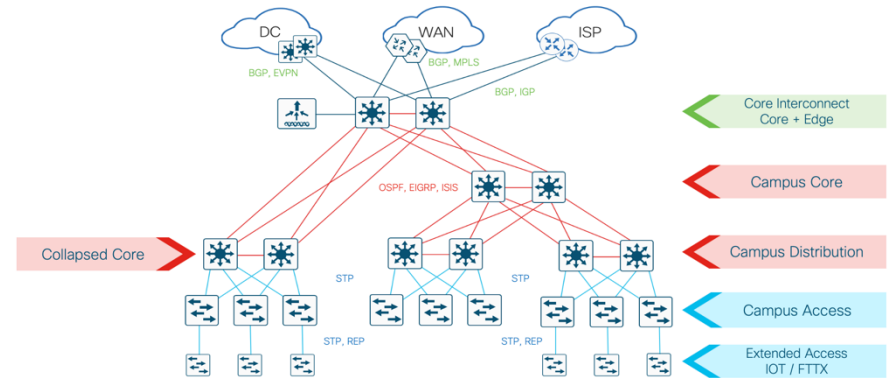


Core & Edge

- Campus Core (Baseline)
- Campus Core Interconnect
- Campus Core + WAN Edge



Campus PIN & Topology



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

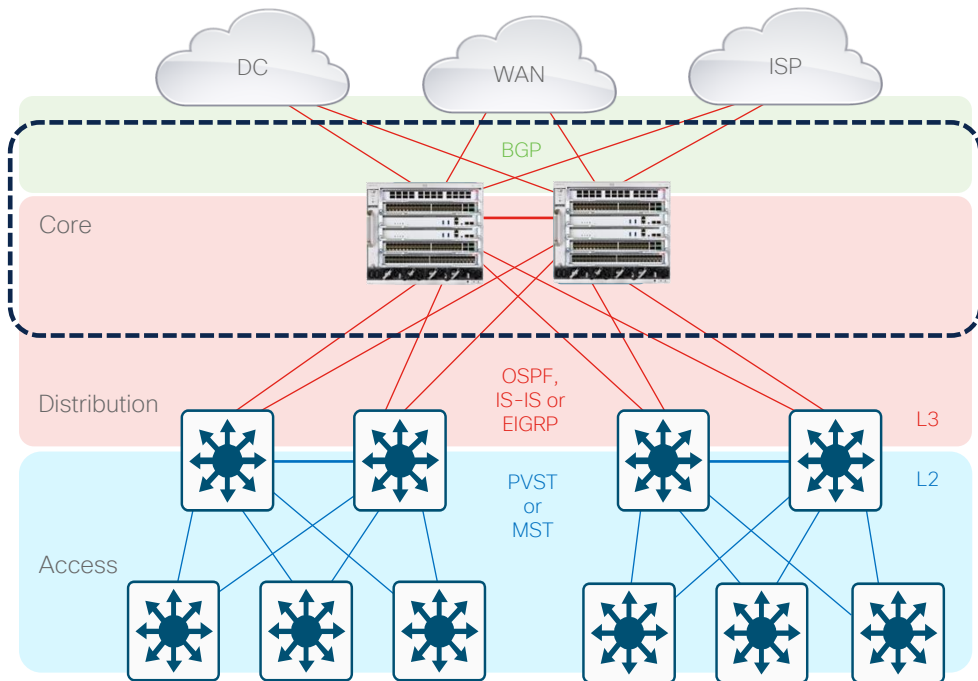
Tends to be **L3 routed** (north & south)

- 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)

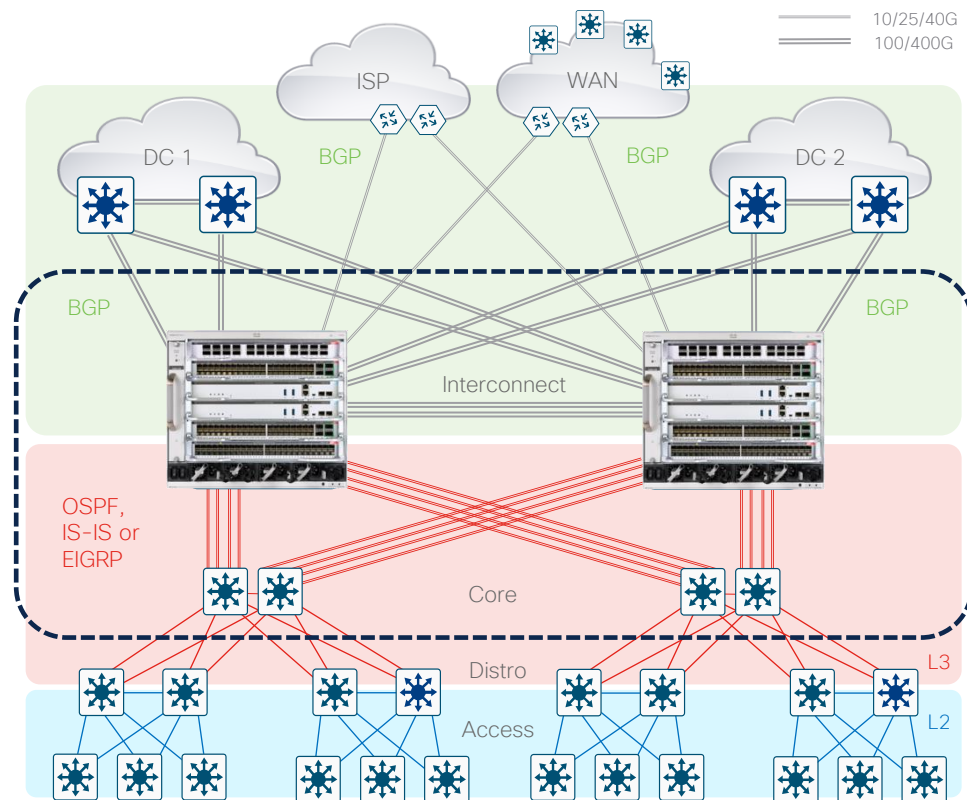
Tends to require high L3 forwarding scale



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



Campus Core + (SP/WAN) Edge

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

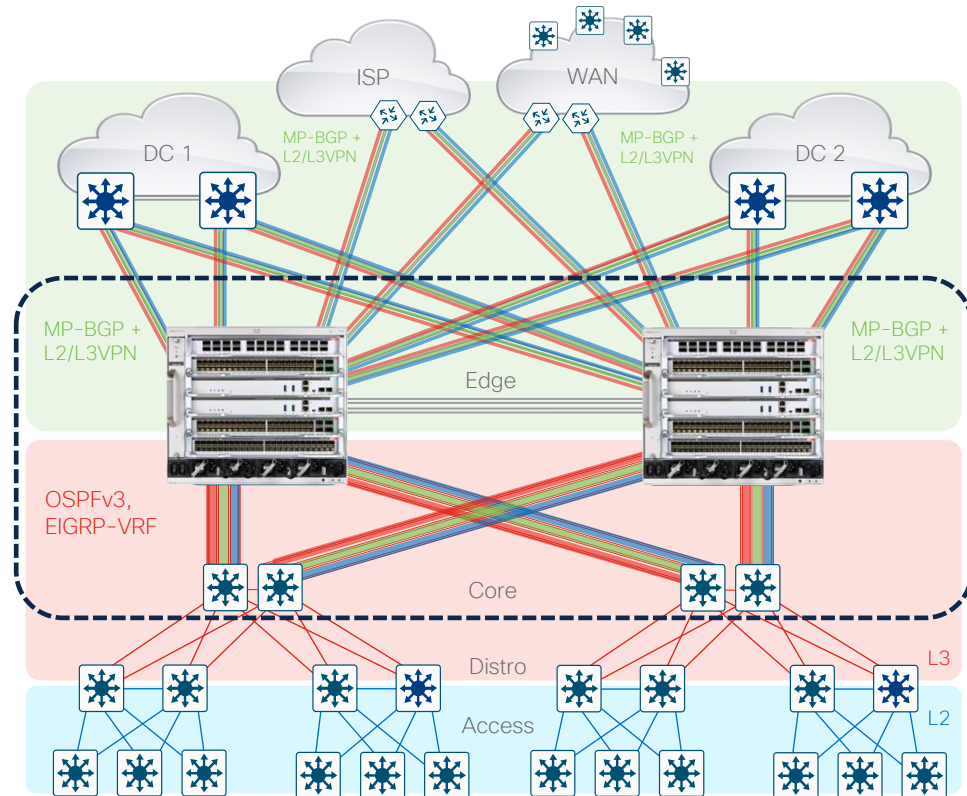
Tends to use **Virtualization & Tunnels**

- 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**

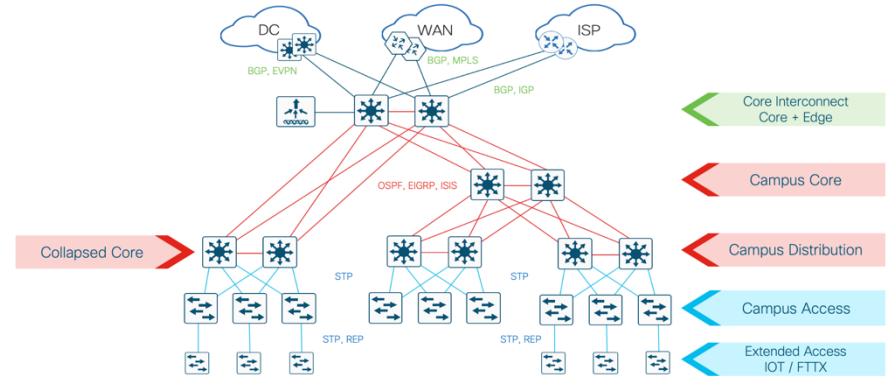


Distribution

- Campus Distribution (Baseline)
- Collapsed Core + Distro
- Campus Distro + Ext. Access



Campus PIN & 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](#)

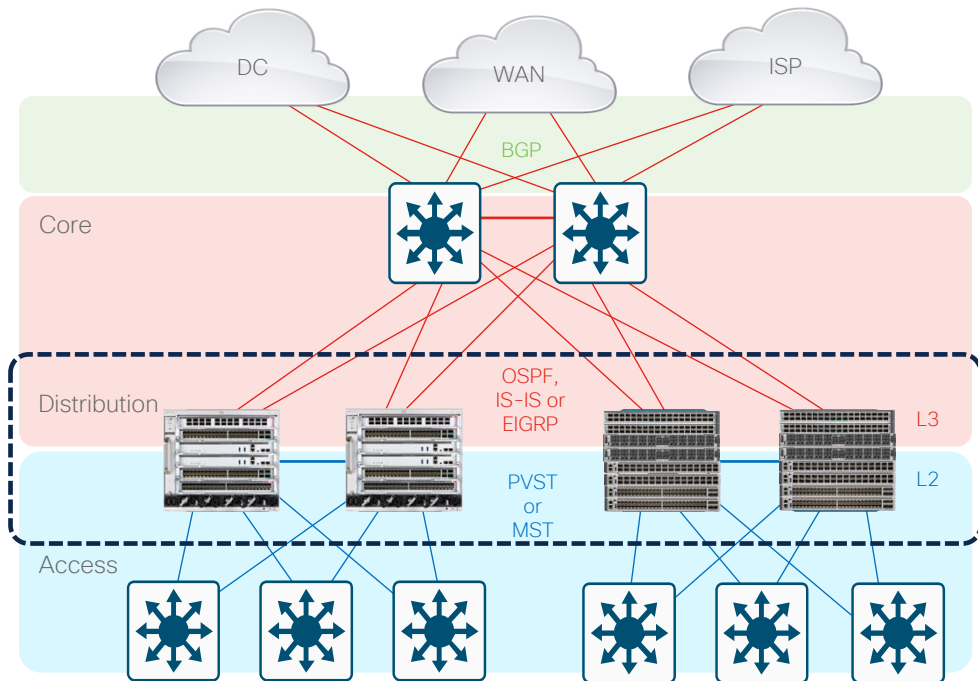
Tends to be both **L3 routed** (north) and **L2 switched** (south)

- 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 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](#)

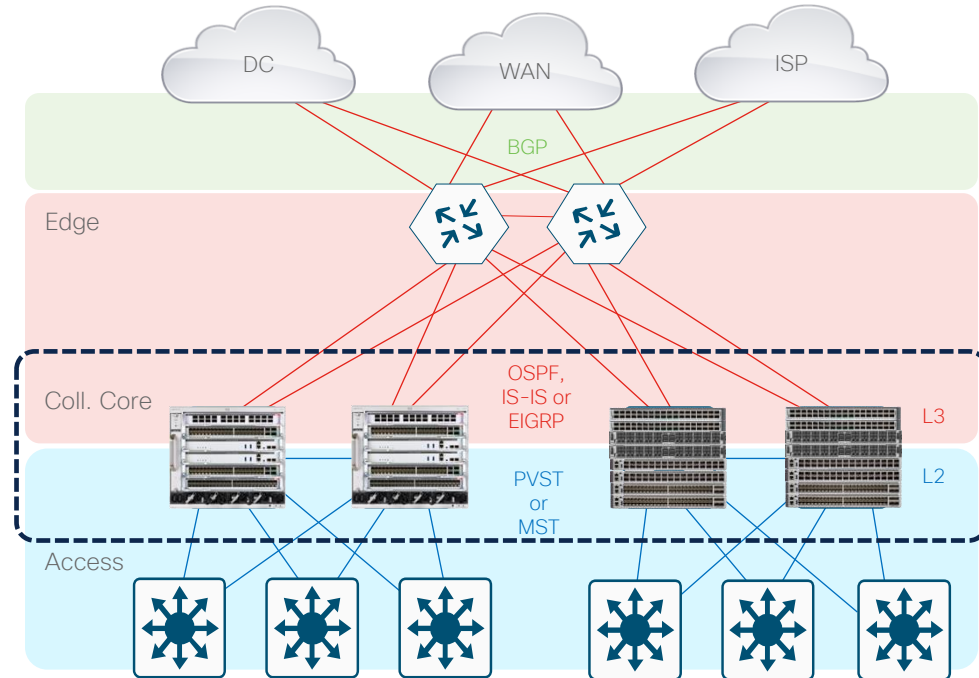
Tends to be both **L3 routed** (north) and **L2 switched** (south)

- 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**

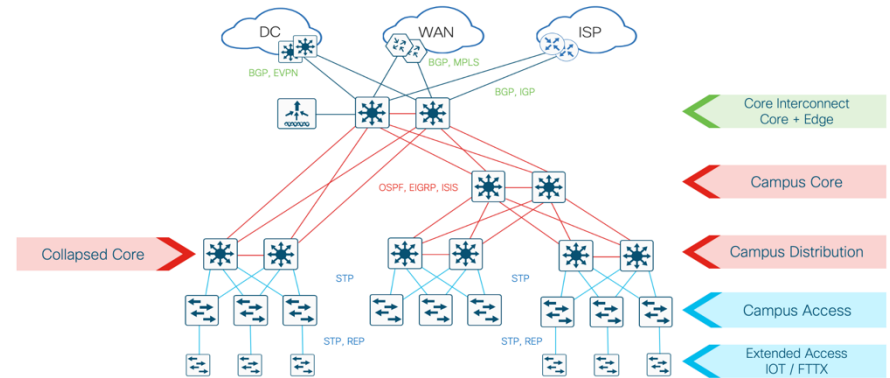


Campus Baseline Access

- Campus Access (Baseline)
- Routed Access
- Extended Access (IOT & FTTX)



Campus PIN & Topology



Campus Access (Baseline)

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

- Other names: [IDE](#), [Wiring Closet](#)
- Common in all Campus & Branch networks

Main purpose is to connect users to network

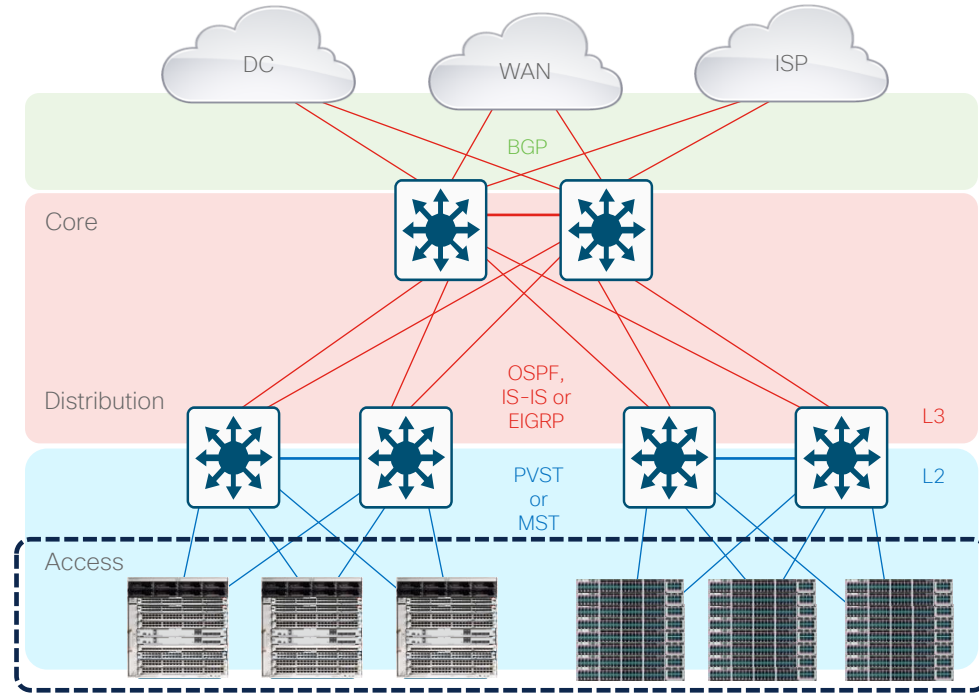
Tends to be **L2 switched** (north & south)

- 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

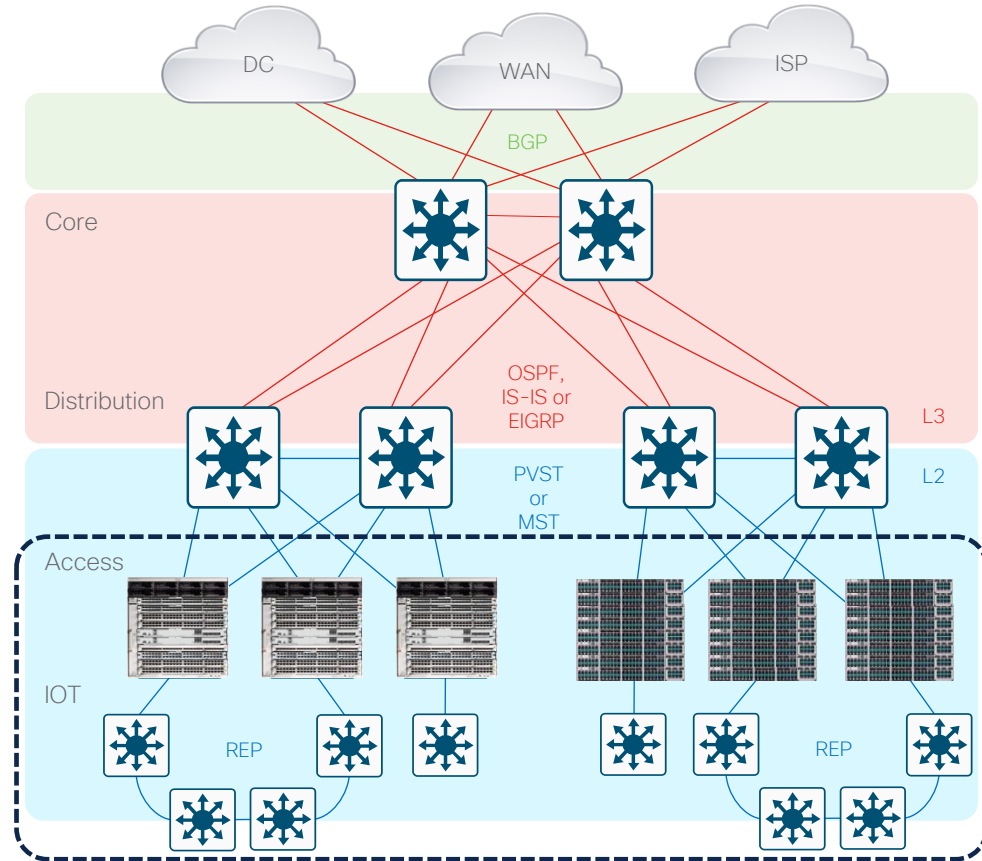
Tends to be **L2 switched** (north & south)

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

Tends to use **multiple L2** features & services

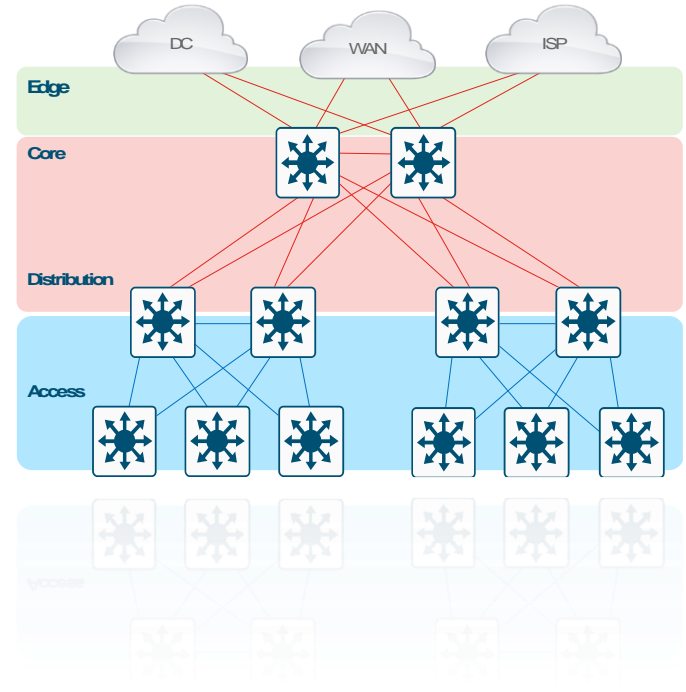
- **Access Security** (e.g. 802.1x, VACLs, PACLs, etc)
- **Access QoS** (e.g. L2 CoS, Classification & Marking)
- **Access NetFlow** (e.g. AVC, FNF, EPA & ETA)

Tends to require **med-high L2 & feature scale**



Campus Architecture

- Equal Cost Multi-Path
- Virtual Switches (StackWise)



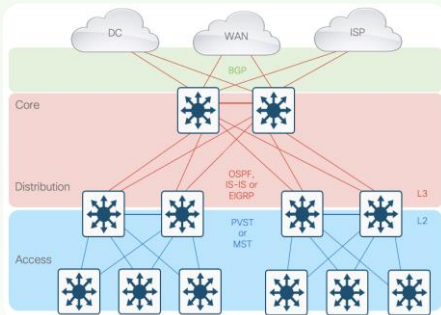
Campus Architectures

Control-Plane & Data-Plane Redundancy



1

ECMP (L2/L3 Paths)

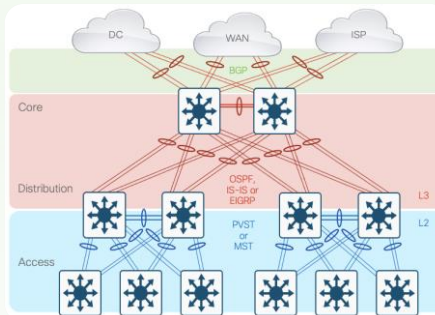


- Complex Topology
- More Nodes, Less Cables
- More Neighbors (+ Tuning)
- Protocol Load-Balancing (ECMP)
- Node-level Redundancy

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)

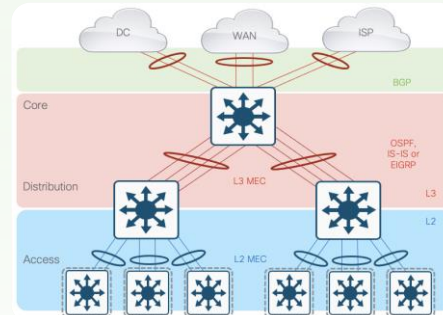


- Complex Topology
- Same Nodes, More Cables (2-8)
- Same Neighbors (+ Tuning)
- EtherChannel Load-Balancing
- Node & Link-level Redundancy

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

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)

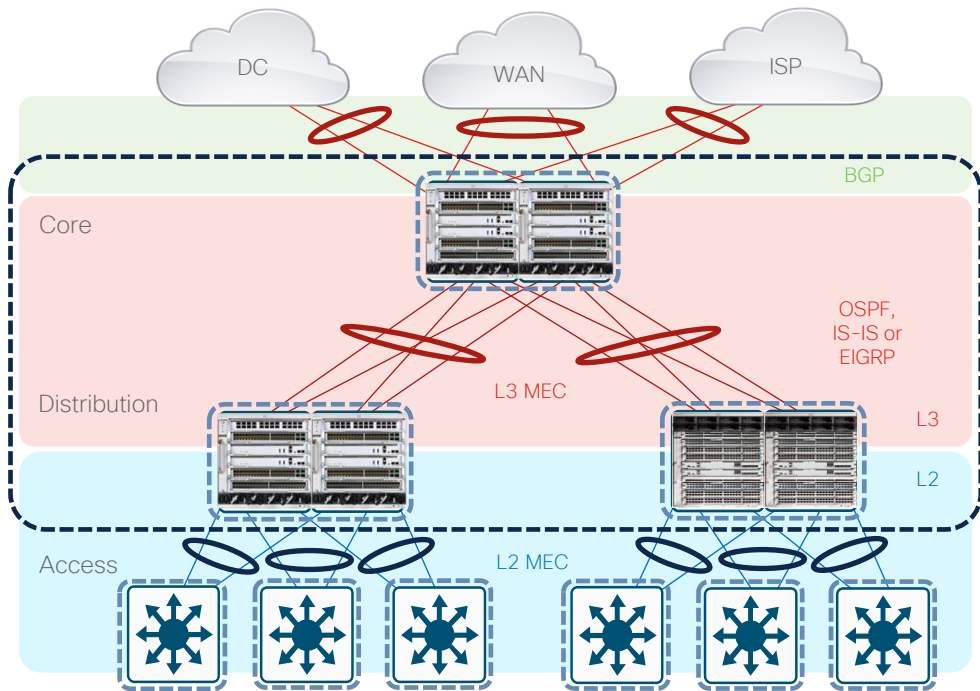
Leverages **Stateful Switchover (SSO)**

- 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



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

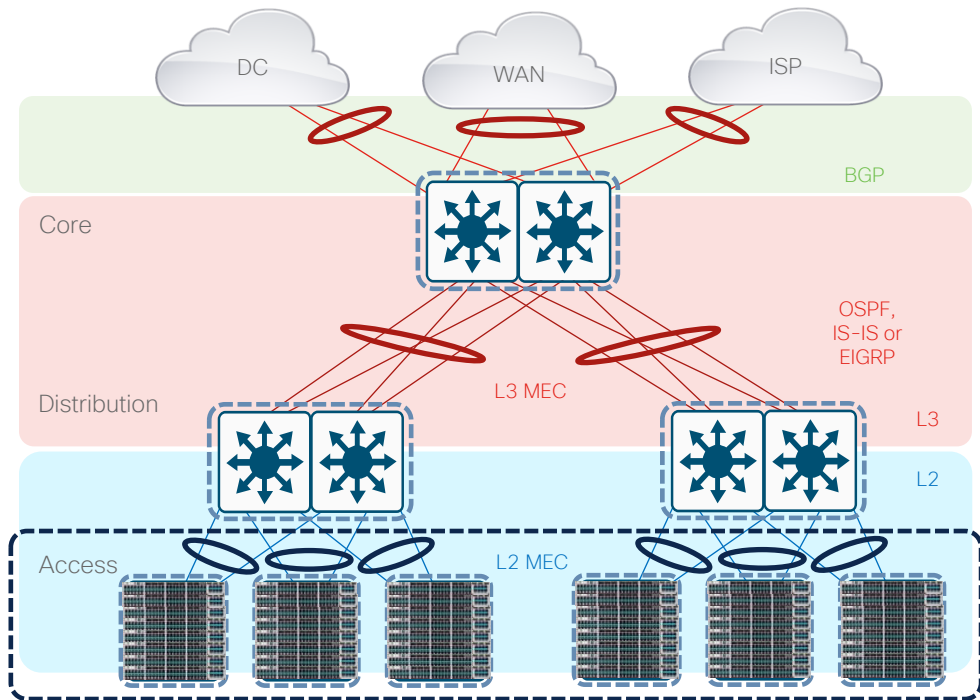
Leverages **Stateful Switchover (SSO)**

- 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



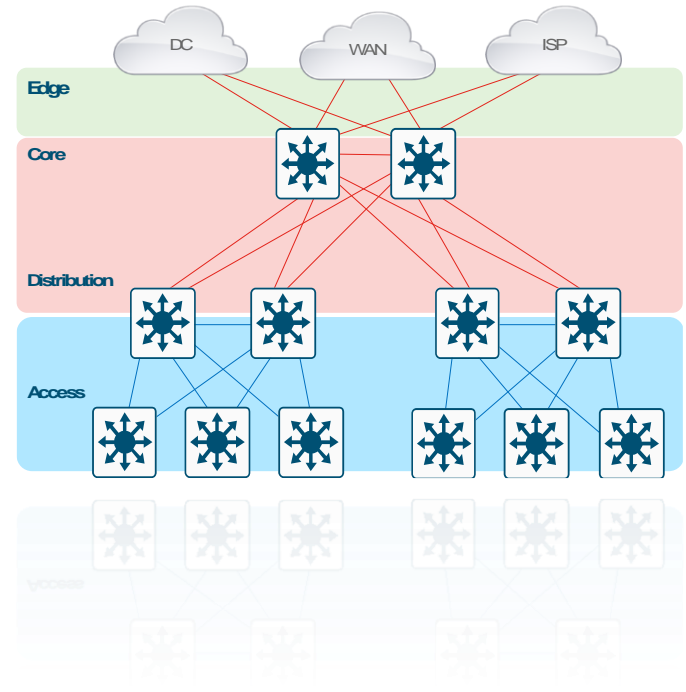
Campus Baseline

Campus Solutions

- **MPLS/VPLS** (L2/L3VPN)
- **BGP-EVPN** (L2/L3VNI)
- **SD-Access** (L2/L3VNI + SGT)



CISCO *Live!*



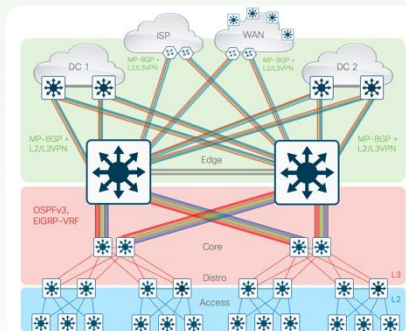
Campus Solutions & Designs

Providing additional services (beyond basic PINs)



1

MPLS (L2/L3VPN)

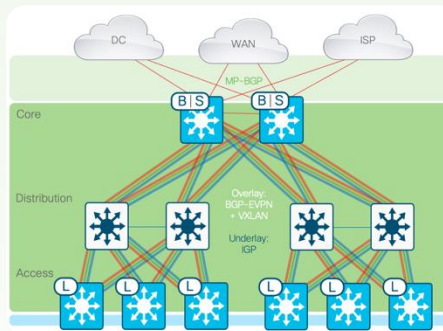


- L3 Underlay + L2/L3 VPN Overlay
- Virtual Private Networks
- L3 VRF-based Segmentation
- WAN/Edge + VPN Services

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)

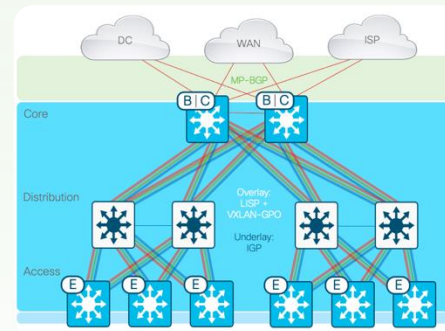


- L3 Underlay + L2/L3 VNI Overlay
- Virtual Network Instances
- L2/L3 VNI-based Segments
- Common WAN/LAN Services

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

3

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

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**

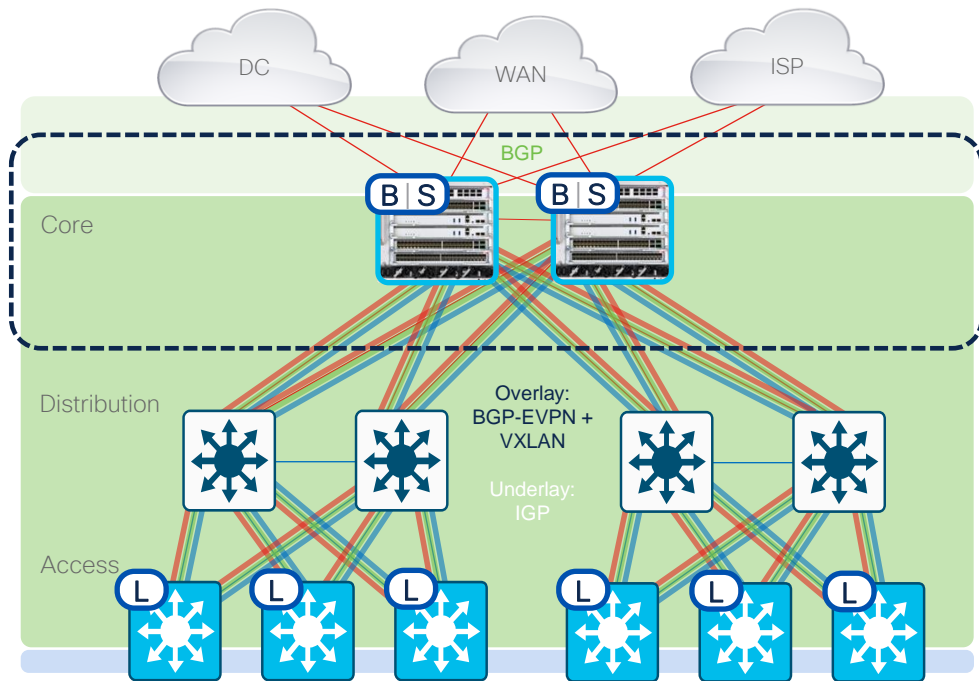
- Control-Plane: **BGP-EVPN (RR), TRM**
- Data-Plane: **VXLAN**
- Policy-Plane: **L2/L3 VNID**

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

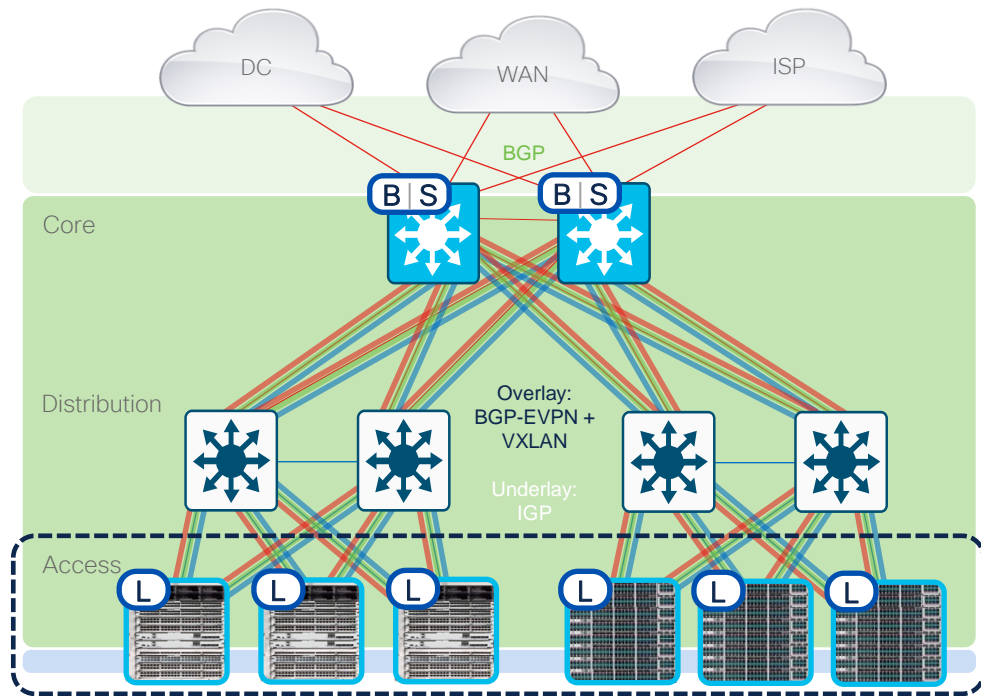
Uses a **Virtualized L2/L3 Overlay**

- 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**

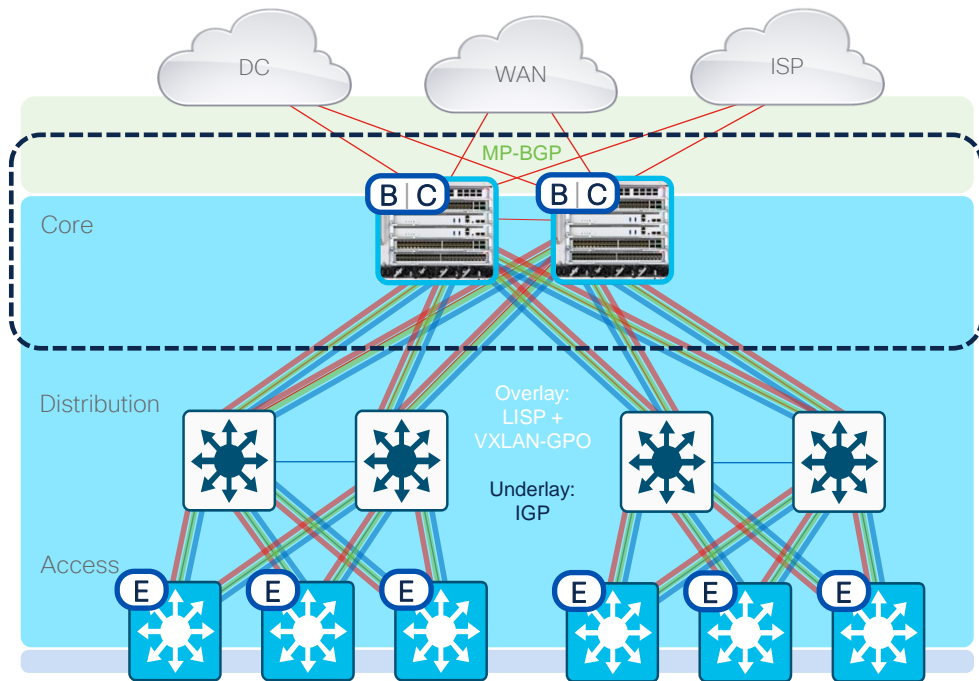
- Control-Plane: **LISP (XTR, MS/MR), PIM**
- Data-Plane: **VXLAN-GPO**
- Policy-Plane: **L2/L3 VNI + SGT**

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

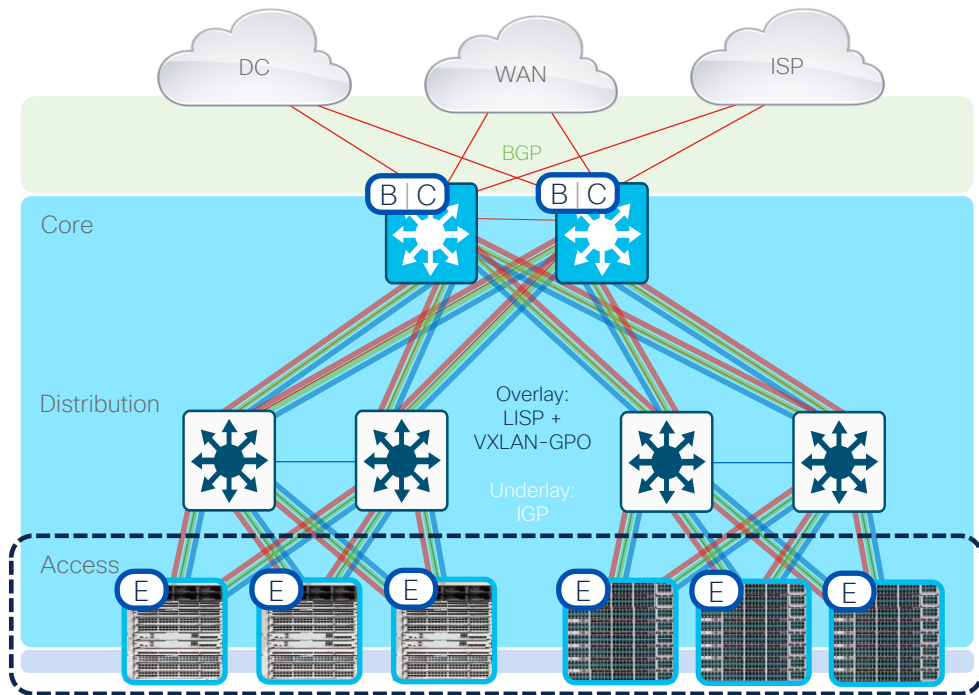
Uses a **Virtualized L2/L3 Overlay**

- 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



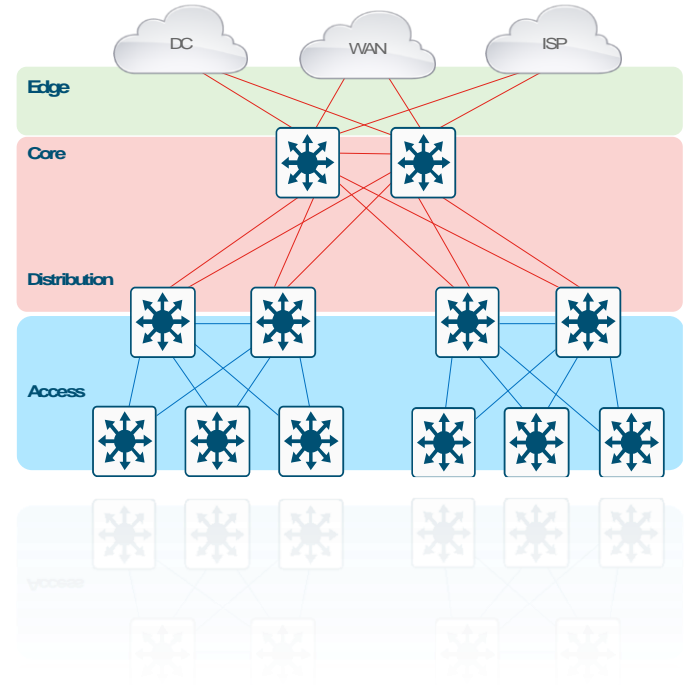
Campus Baseline

Wireless & Security

- Central Wireless
- Firewalls & ACLs



CISCO *Live!*



Wireless LAN

The **Central Wireless PIN** focuses on connecting Wireless APs centrally to one or multiple WLCs.

- WLC is typically connected to Core, Edge or DC (Tier 3+)
- APs are typically connected to Access (Tier 1)

Main goal is to connect Wireless Endpoints (via APs) to a Wireless LAN (WLAN) - centrally in the network

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

- North (to WLC): L2 VLAN + 802.1Q, L3 SVI, IGP
- South (to AP): L2 VLAN + 802.1Q, STP, IGMP

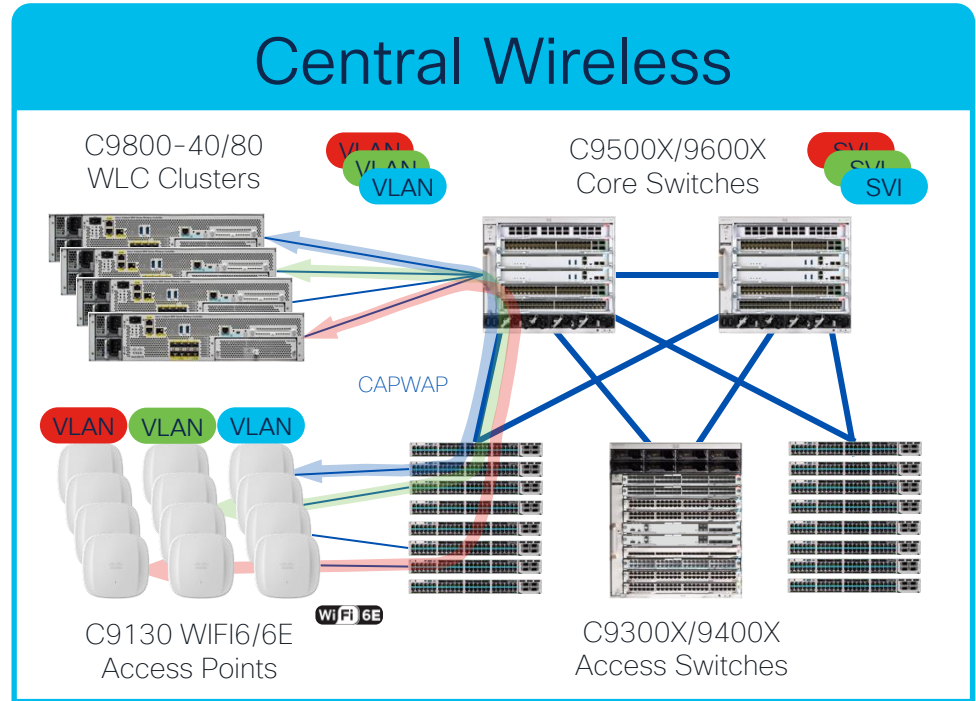
Uses a **Tunneled L2 Overlay**

- Control-Plane: **CAPWAP, DTLS, LWAPP**
- Data-Plane: **CAPWAP, DTLS**

Tends to require **L2 (WLAN) features**

- **L2 ACLs** (e.g. VACL, MAC ACL)
- **L2 QoS** (e.g. VLAN QoS)
- **L2 NetFlow** (e.g. FNF, AVC, EPA & ETA)

Tends to require **higher L2/L3 + feature scale**



Firewalls & ACLs

The **Firewall (DMZ) PIN** focuses on controlling access into or out of different network areas.

- Typically connected to Core, Edge or DC (Tier 3+)
- Complex designs may use Distro or Access (Tier 1-2)

Main goal is to prevent unauthorized access to different network domains (segments).

- Evolved from “Edge” Access-Control Lists (ACLs)
- Can be either L2, L3 or VRF-aware
- Tends to focus on L4-L7 flows (with or w/o DPI)

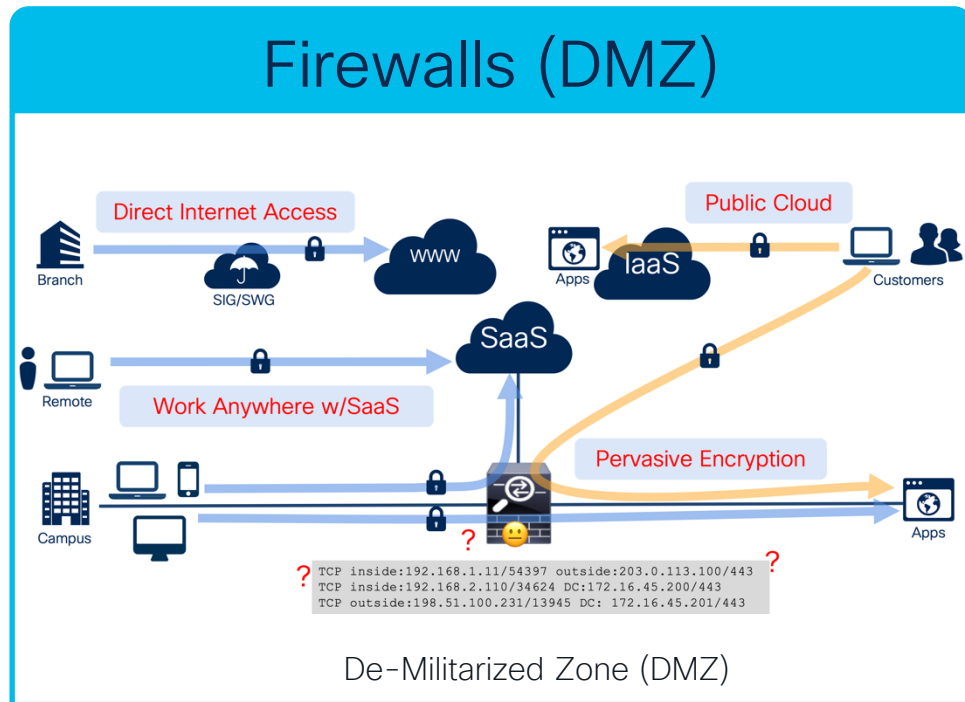
Uses a **L2 or L3/VRF + ACLs**

- North (outside): L2 802.1Q, L3 (SVI, Sub-Ints), IGP, BGP
- South (inside): L2 802.1Q, L3 (SVI, Sub-Ints), IGP, BGP

Tends to use **L2 & L3/VRF + DPI & ACL** features

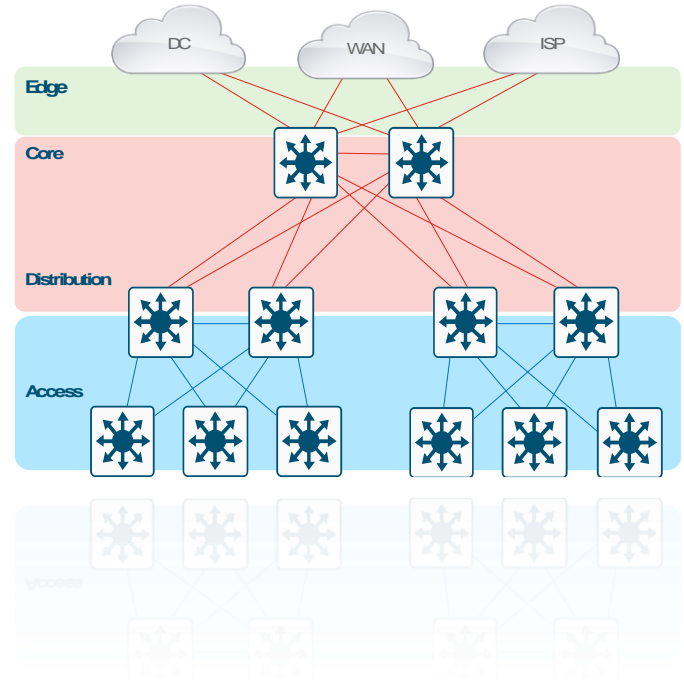
- **L4/App ACLs** (e.g. VACL, MAC ACL)
- **L4/App QoS** (e.g. VLAN QoS)
- **L4/App NetFlow** (e.g. FNF, AVC, EPA & ETA)

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

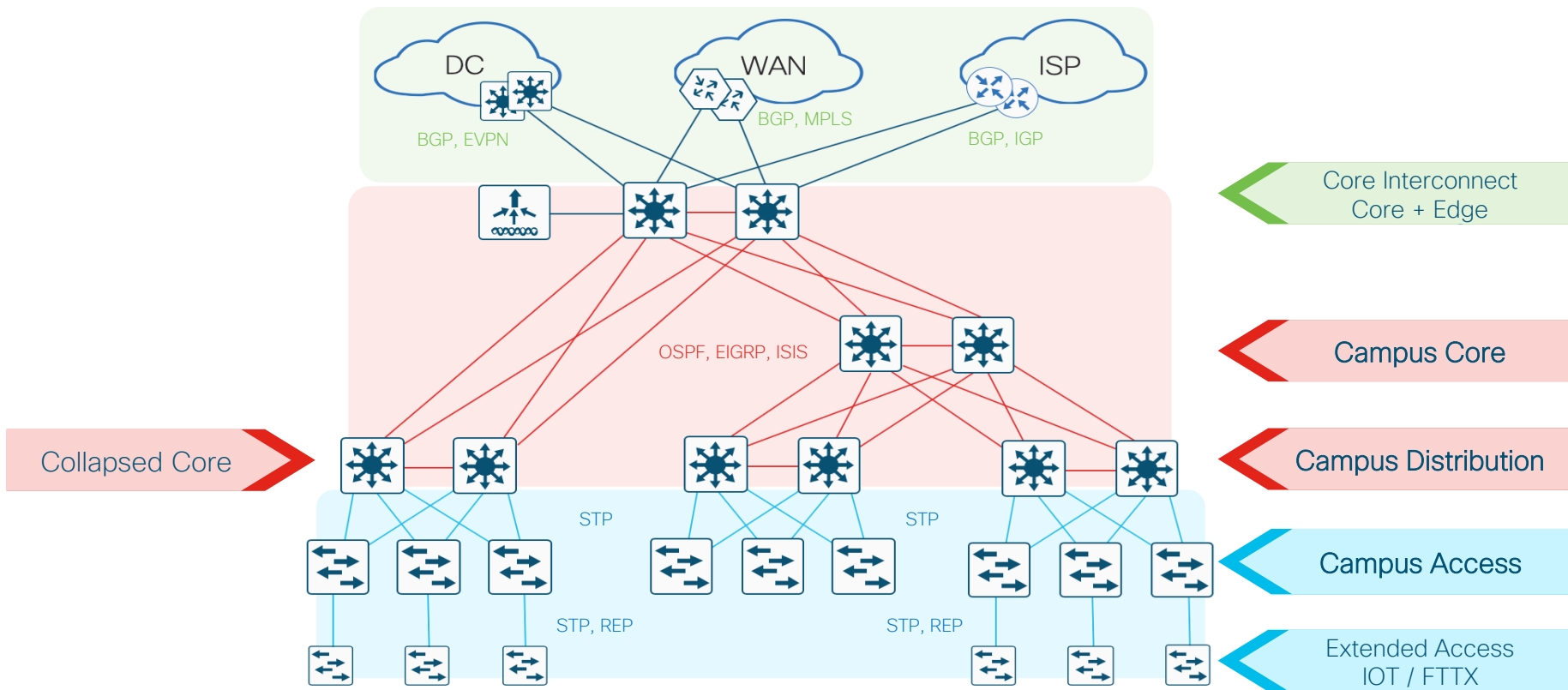


Conclusion

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



Campus PINs & Topology



Keep Learning!

Cisco Validated Design (CVD)

cisco.com/go/cvd

cs.co/en-cvds



What is a Cisco Validated Design Guide (CVD)?

Cisco Validated Designs (CVDs) provide the foundation for systems design. They are based on common use cases or engineering system priorities. Each guide incorporates a broad set of technologies, features, and applications to address your needs. Most important, it has been comprehensively tested by Cisco engineers to help ensure a faster, more reliable, and fully predictable deployment.

What a Validated Design Guide provides



Reliability

CVDs are extensively tested. You can confidently set performance expectations when you deploy your solution.



Less risk

Using a CVD reduces both the risk that products won't work together and the risk that they won't perform as promised.



Comprehensiveness

CVDs provide everything from system designs to configuration instructions to a bill of materials (BOM).



24-hour support

Because CVD solutions are guaranteed to work as specified, we offer 24-hour support options for any issues that might arise.

Featured design guides



SD-Access Design

Design, provision, apply policy, and provide wired and wireless network assurance with a security...



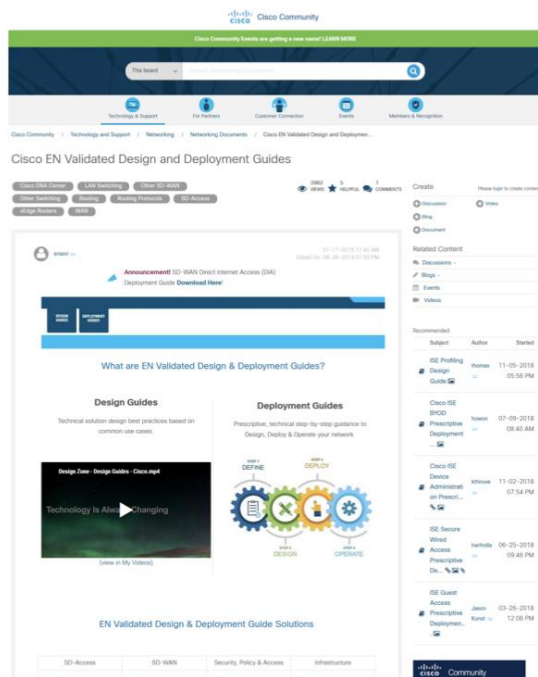
SD-Access Deployment

Automate the deployment of a secure software-defined wired and wireless campus network.



Data Center Design Playbook

A comprehensive summary of Cisco UCS Solution CVDs, in one place.



Webex App

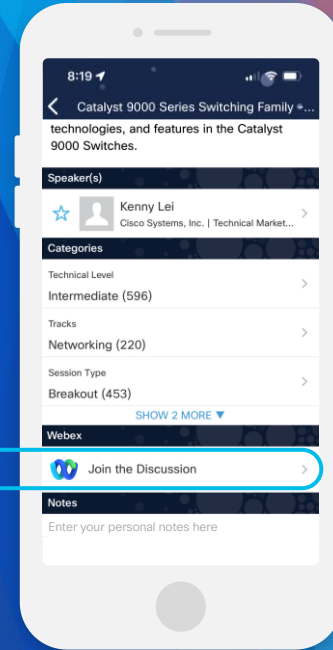
Questions?

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 23, 2024.



<https://cislive.ciscoevents.com/cislivebot/#BRKENS-1501>

Fill out your session surveys!



Participants who fill out a minimum of **four session surveys and the overall event survey** will get a 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 into the Session Catalog and clicking the 'Participant Resource Center' link at

<https://www.ciscolive.com/emea/learn/session-catalog.html>.



Continue your education

CISCO *Live!*

- 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 February 23.



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, creating a sense of motion and energy.

CISCO *Live!*

Let's go