
Networking Infrastructure: The Backbone of the Digital World



ATGsys[®]

Kyaw Pyae Sone Win

CCIE#61458

Solutions Manager

Agenda

- What is a “Smart Campus”?
- Campus Place in Network & Topology
- Campus Networks Architecture
- Evolution of Wi-Fi
- Network Access Control
- Advanced Technology

What is a “Smart 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** (Uses, Wndos, e.)
- **People's devices** (PCs, Phones, Pribt, e.)
- **Similar geographic area** (LAN, WLAN or MAN, e.)
- **Access to other domains** (WAN, ISPDC & Cloud, e.)

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

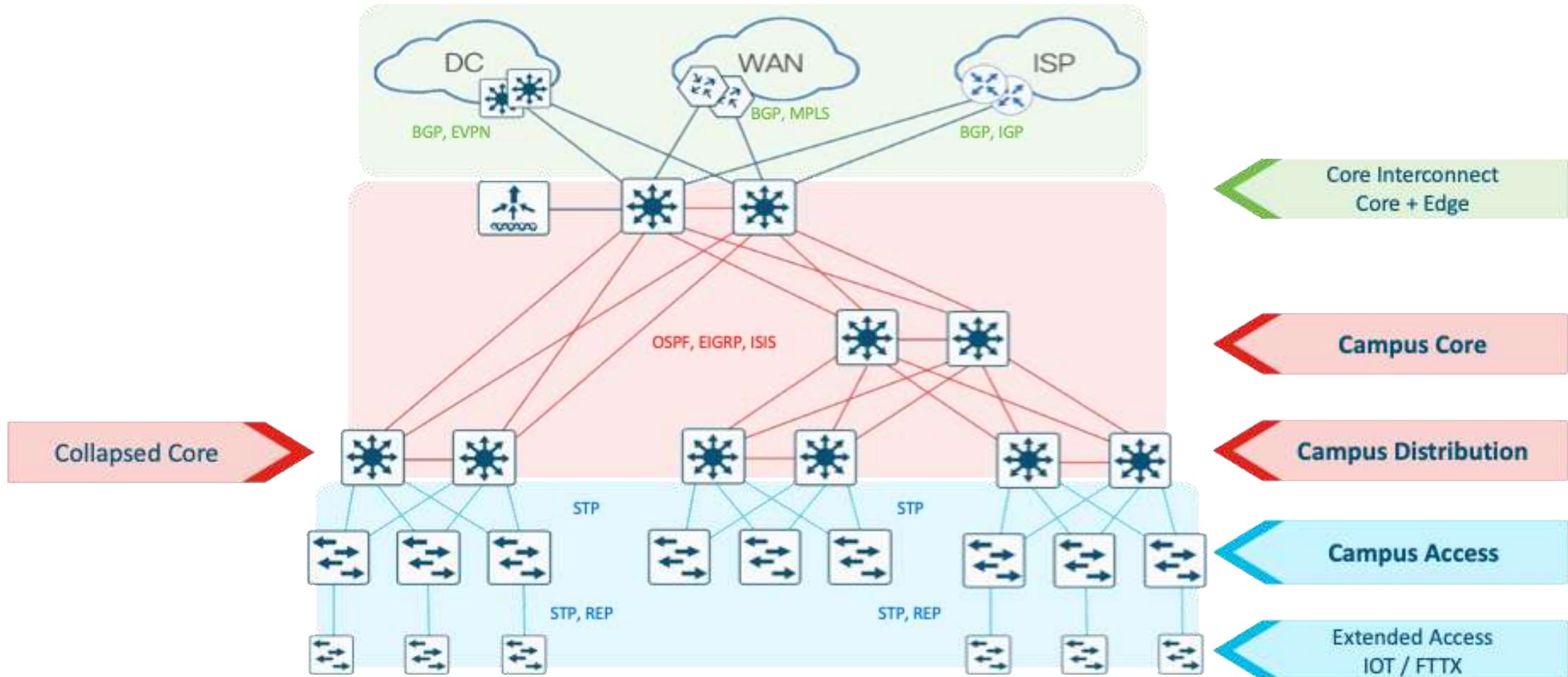


Campus is focused on User Access

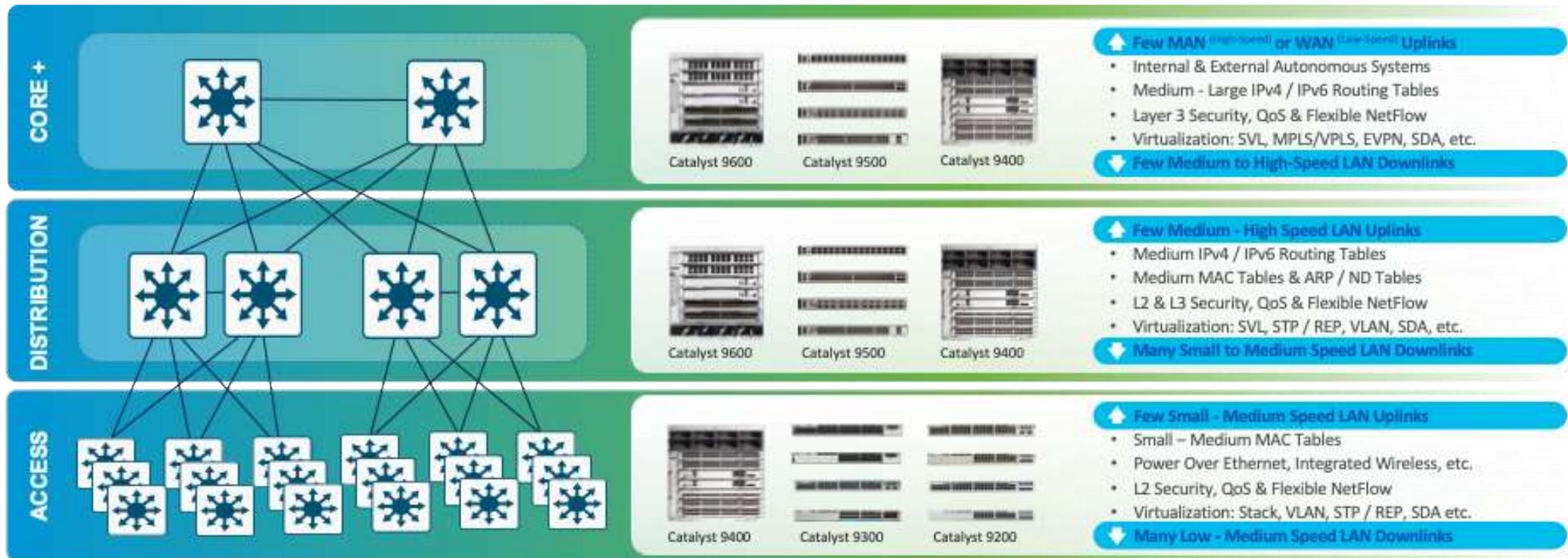
Campus Networks - Real Life



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

Design Fundamentals



Modular	
PROs	CONs
<ul style="list-style-type: none"> • More Flexible • Longer Life-Cycle • Higher Port Density • More Power/Cooling • Redundant Processors 	<ul style="list-style-type: none"> • More Complex • BW limit by Chassis • Slow(er) Dev & Test • Lower MTBF • Higher COGs

Fixed	
PROs	CONs
<ul style="list-style-type: none"> • Less Complex • Swap Chassis for BW • Faster Dev & Test • Higher MTBF • Lower COGs 	<ul style="list-style-type: none"> • Less Flexible • Shorter Life-Cycle • Lower Port Density • Less Power/Cooling • Single Processor

Campus Networks

L2/L3 Unicast Technologies

IPv4 Unicast

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

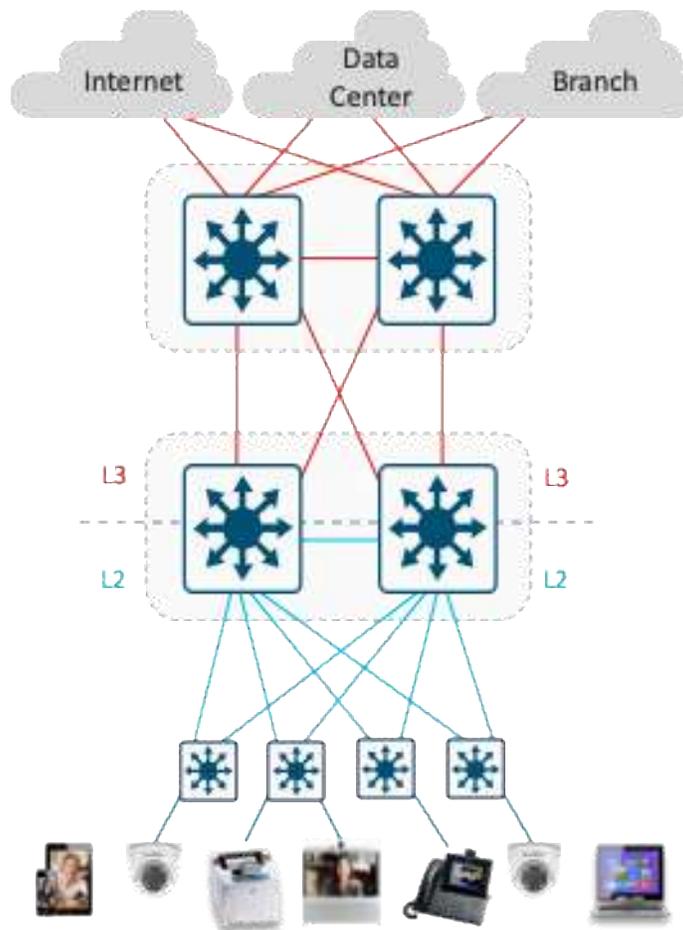
Core

- 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 Learning
- 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 Learning
- 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

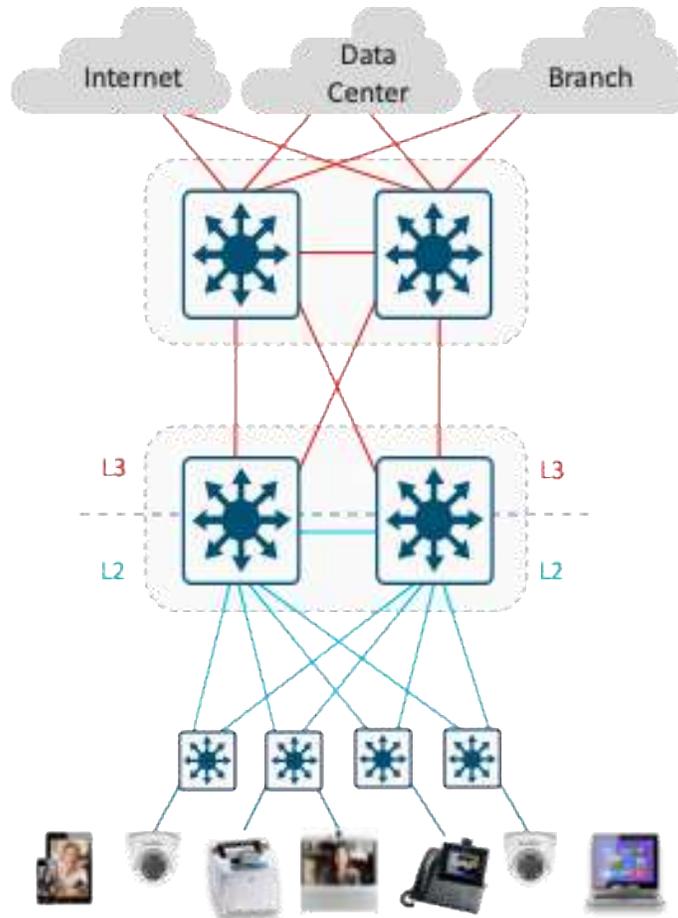
Core

- 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

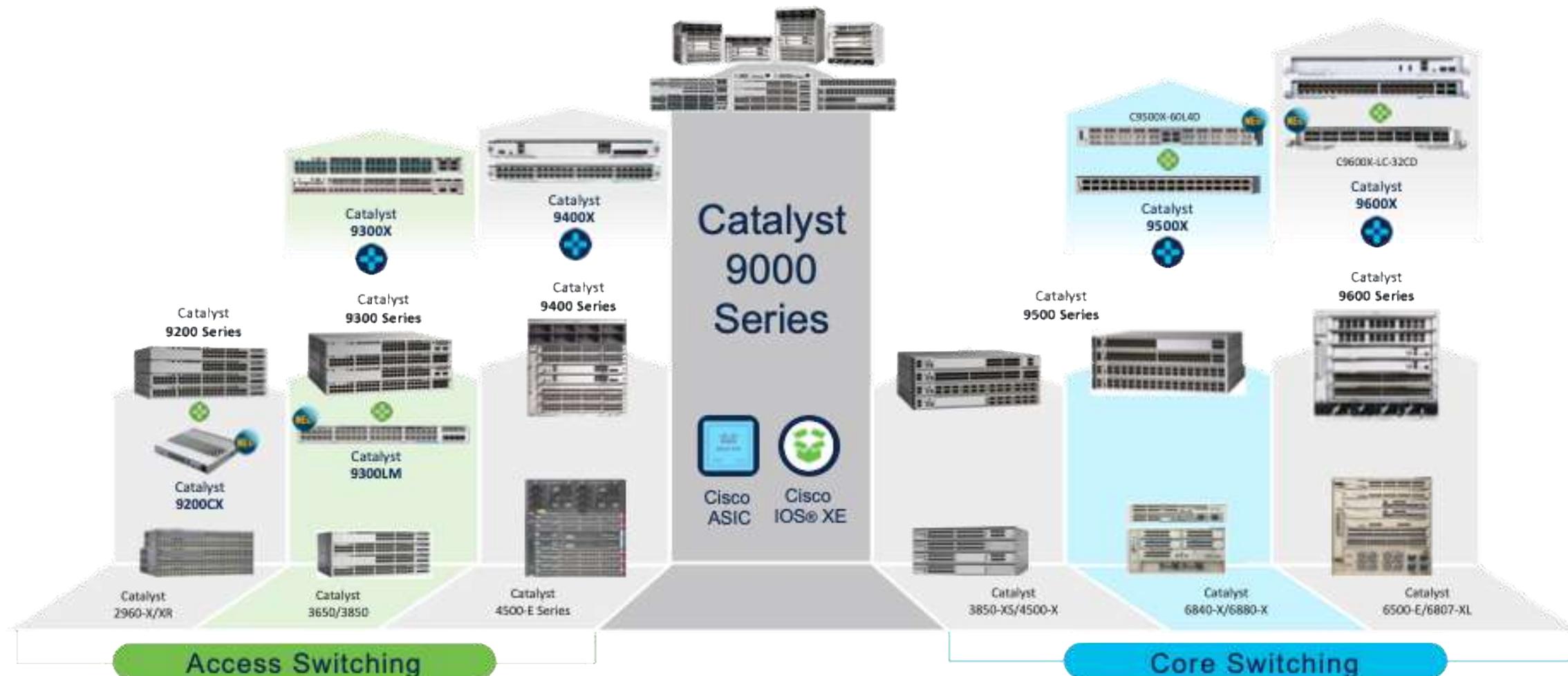
Distribution

- 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



Campus Core

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

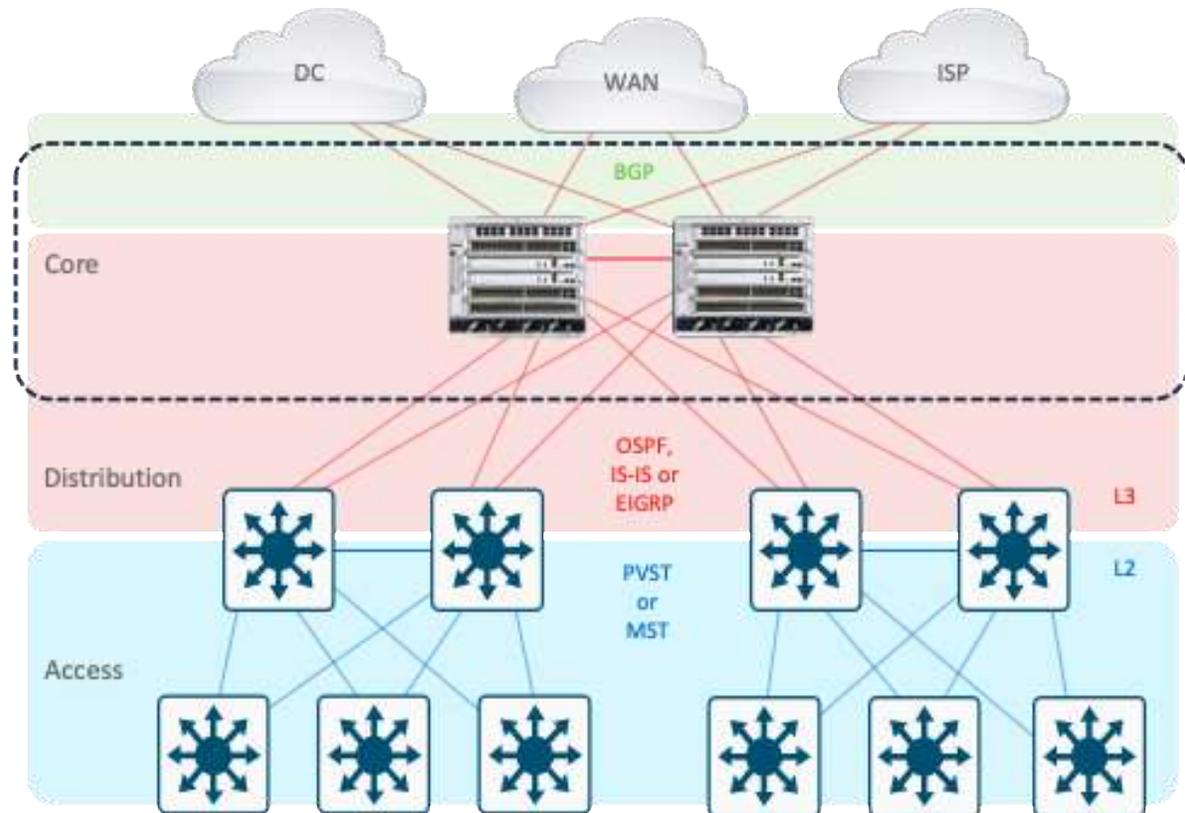
Tends to be **L3 routed (north & south)**

- 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)

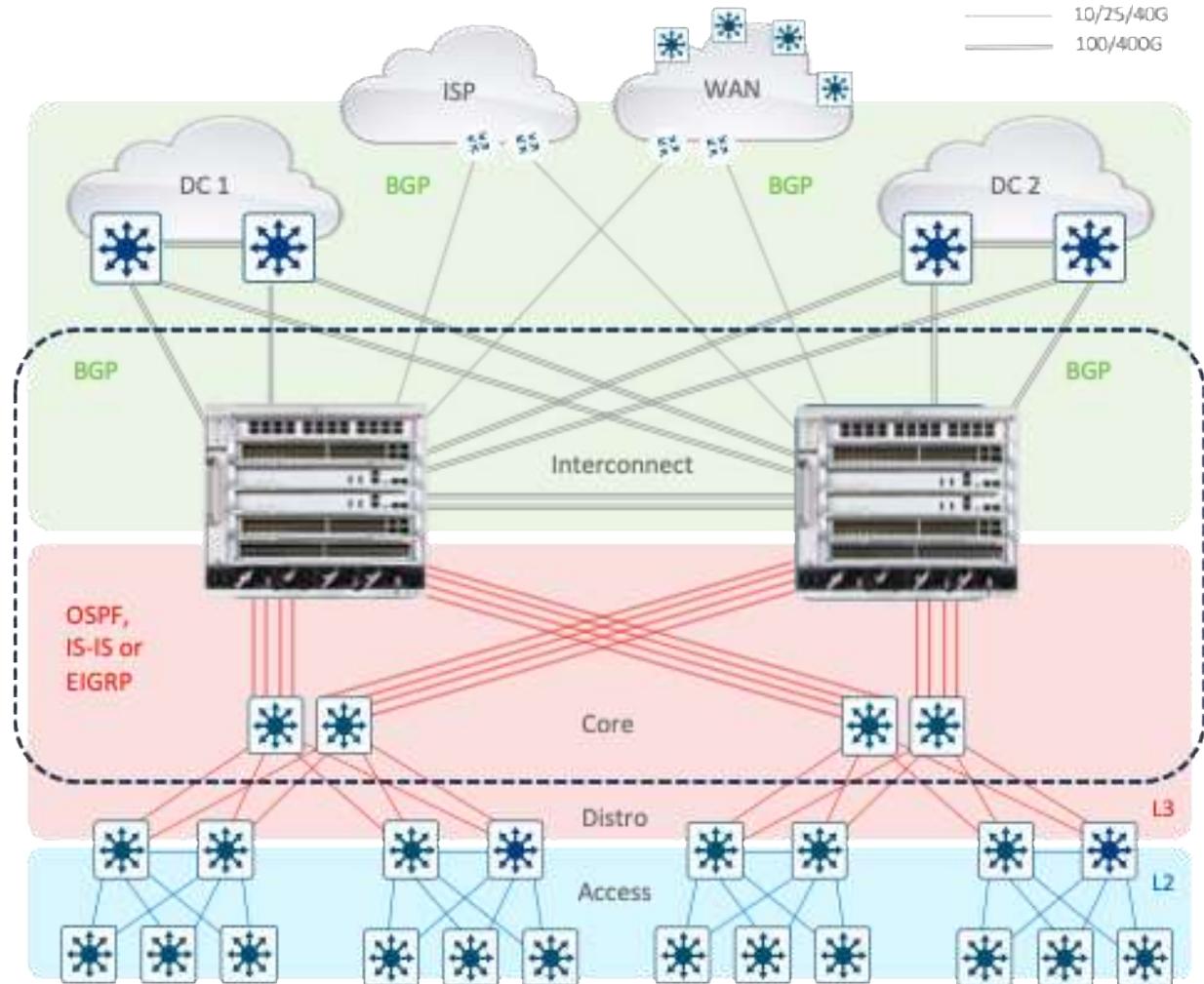
Tends to require **high L3 forwarding scale**



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**

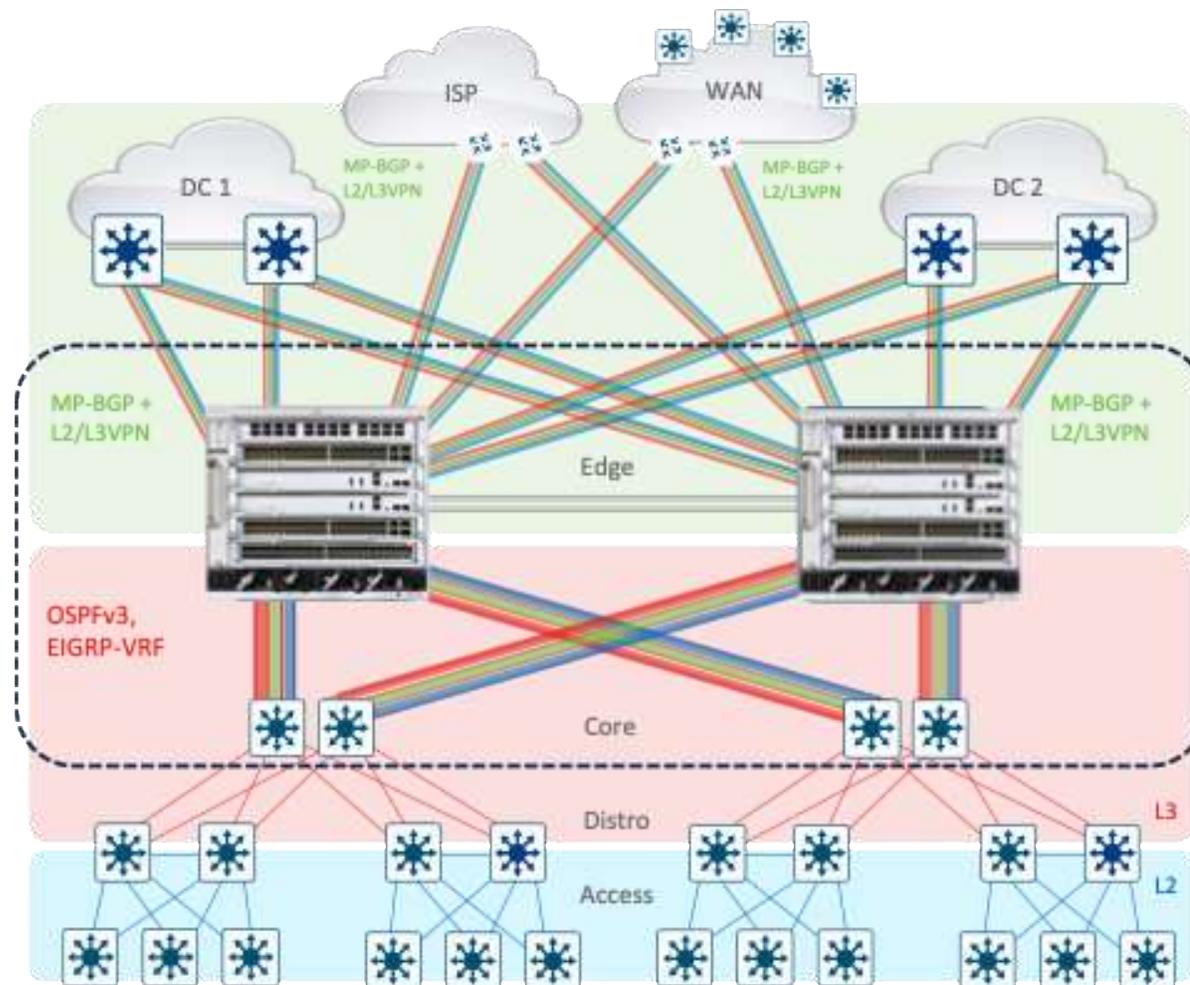
Tends to use **Virtualization & Tunnels**

- 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. RAACL, CBAC, ZBFW)
- **Hierarchical QoS** (e.g. Class-based Queuing, Shaping)
- **Policy Based Routing** (e.g. WAAS & WCCP)
- **WAN NetFlow** (e.g. L3/VRF NF, WAN ETA)

Tends to require **highest L3/VRF & feature scale**



Campus Distribution

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](#)

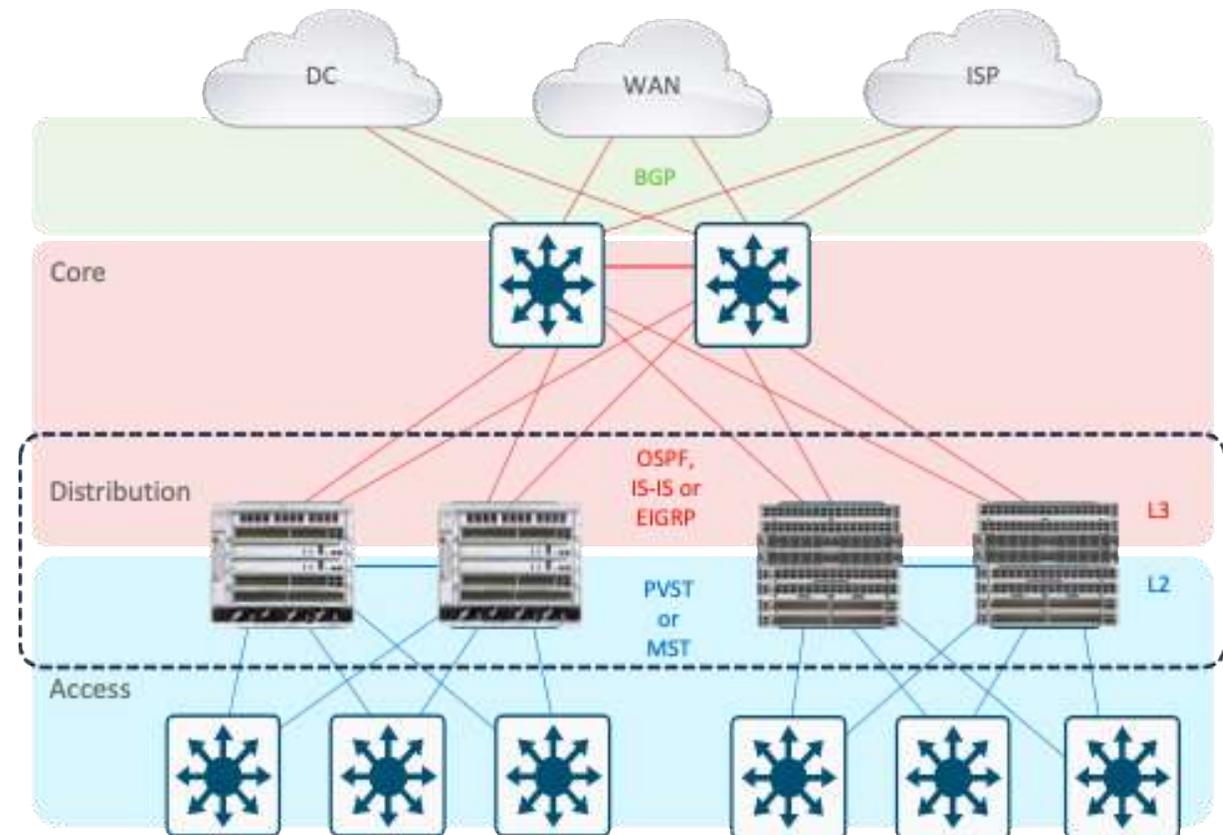
Tends to be **both L3 routed (north)**
and L2 switched (south)

- 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/SISE](#), [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](#)

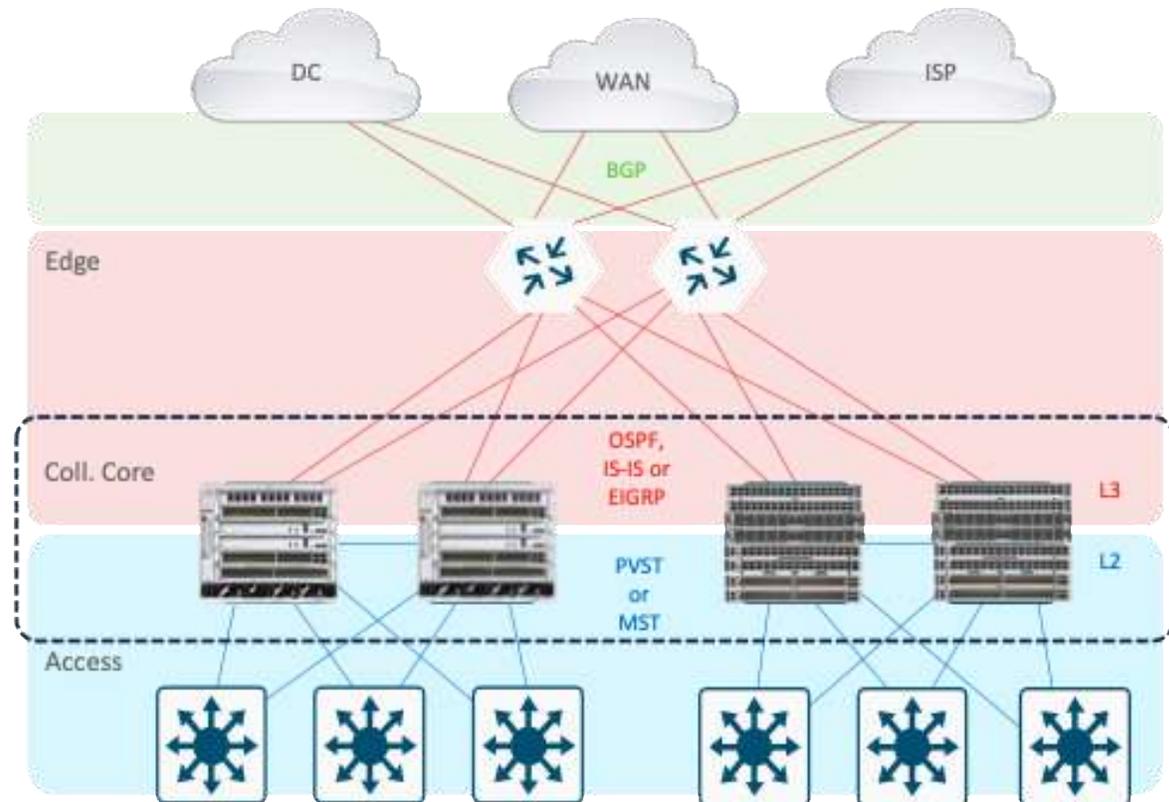
Tends to be **both L3 routed (north) and L2 switched (south)**

- 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/SISE](#), [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 Access

The **Access PIN (Tier 1)** focuses on connecting Users & Devices, and 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

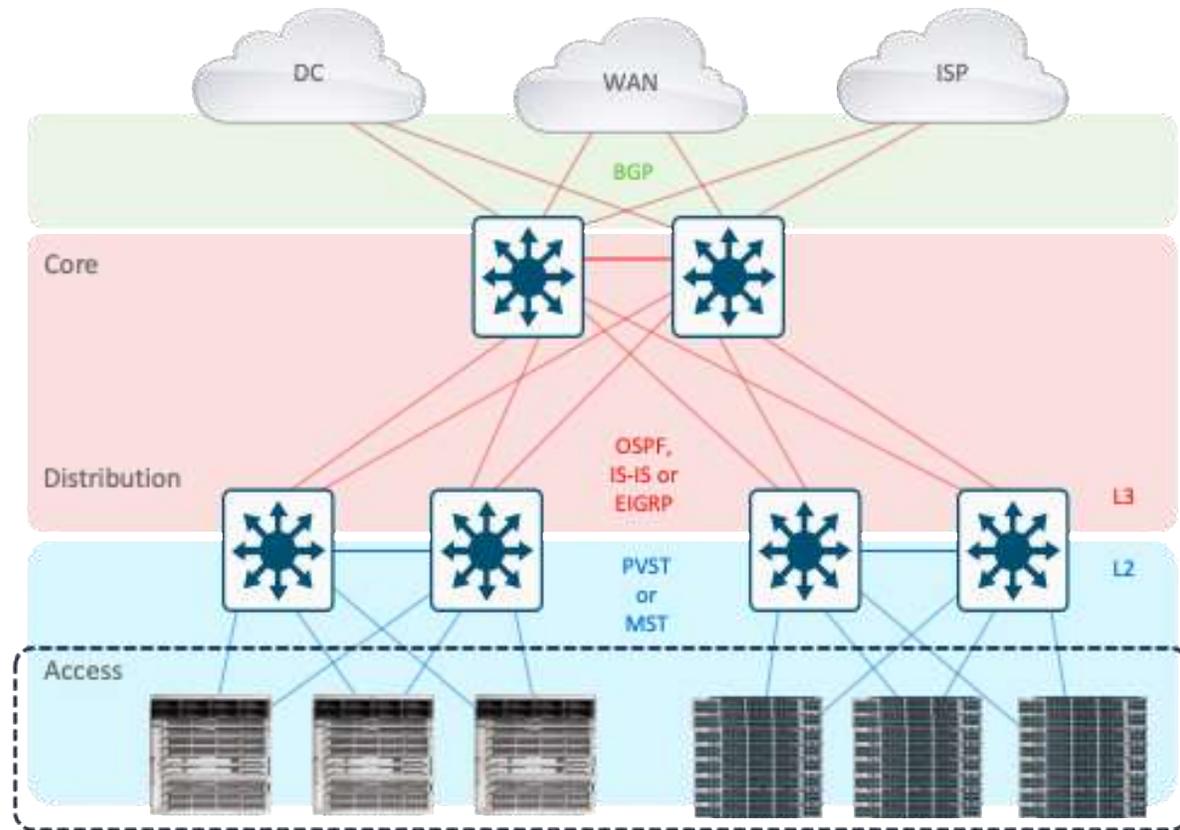
Tends to be **L2 switched (north & south)**

- 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, FNE, EPA & ETA)

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



Extended Access

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

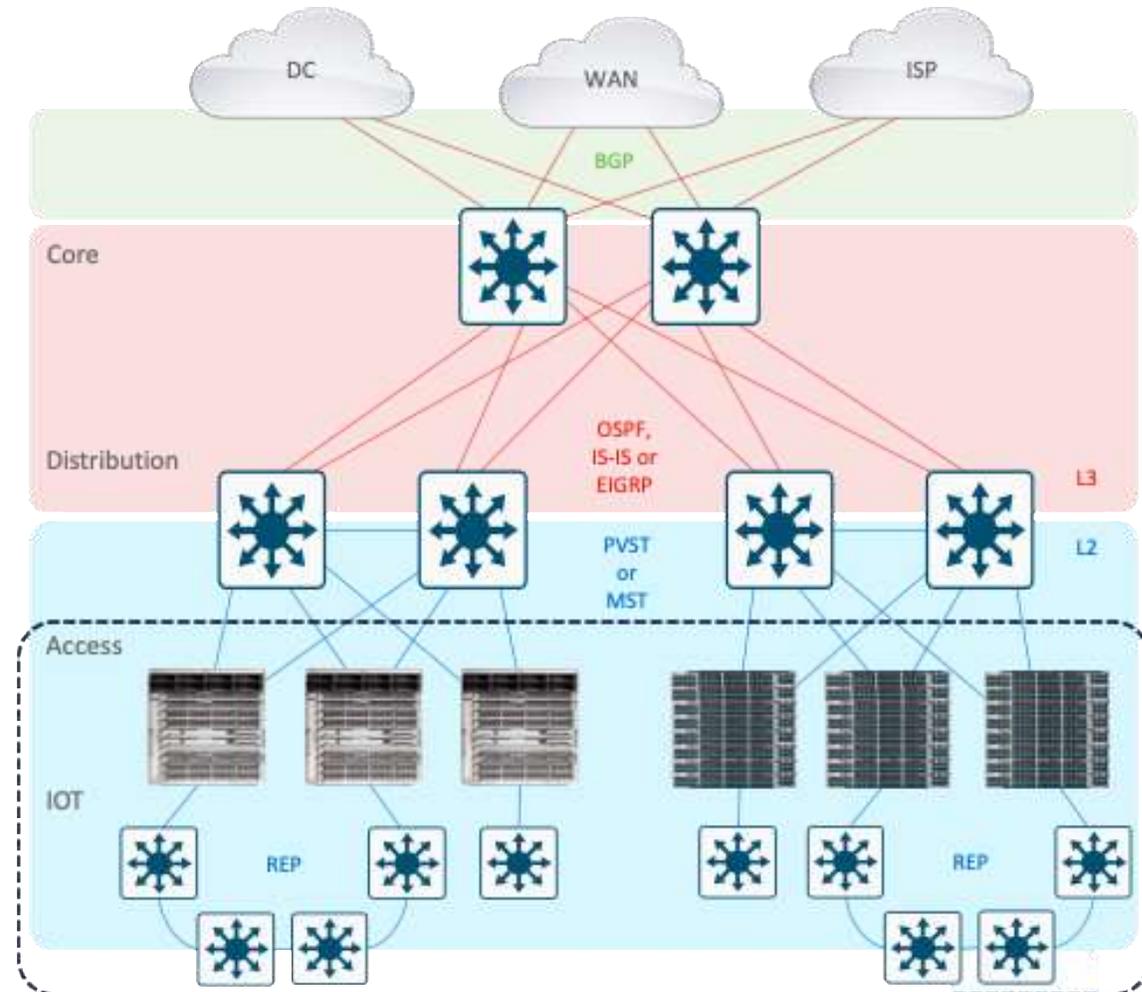
Tends to be **L2 switched (north & south)**

- 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, PAACLs, etc)
- **Access QoS** (e.g. L2 CoS, Classification & Marking)
- **Access NetFlow** (e.g. AVC, FINE, EPA & ETA)

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



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

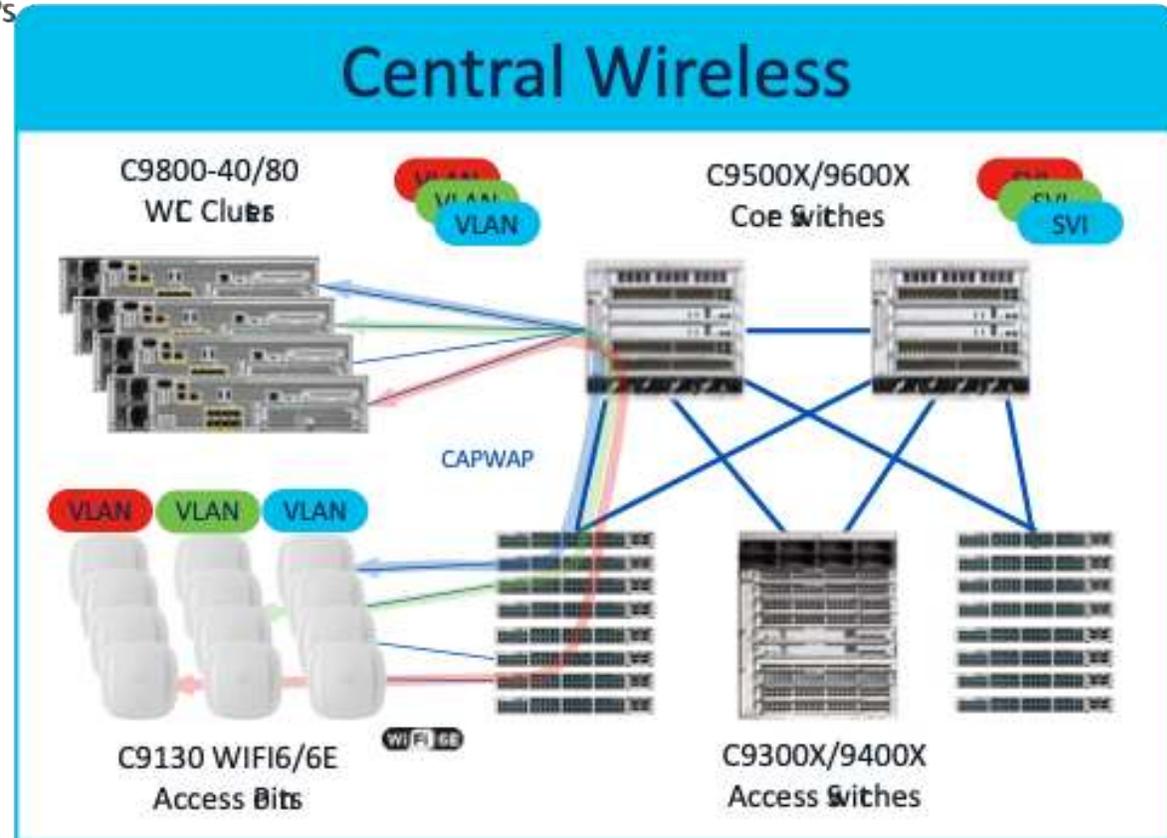
Uses a **Tunneled L2 Overlay**

- 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)

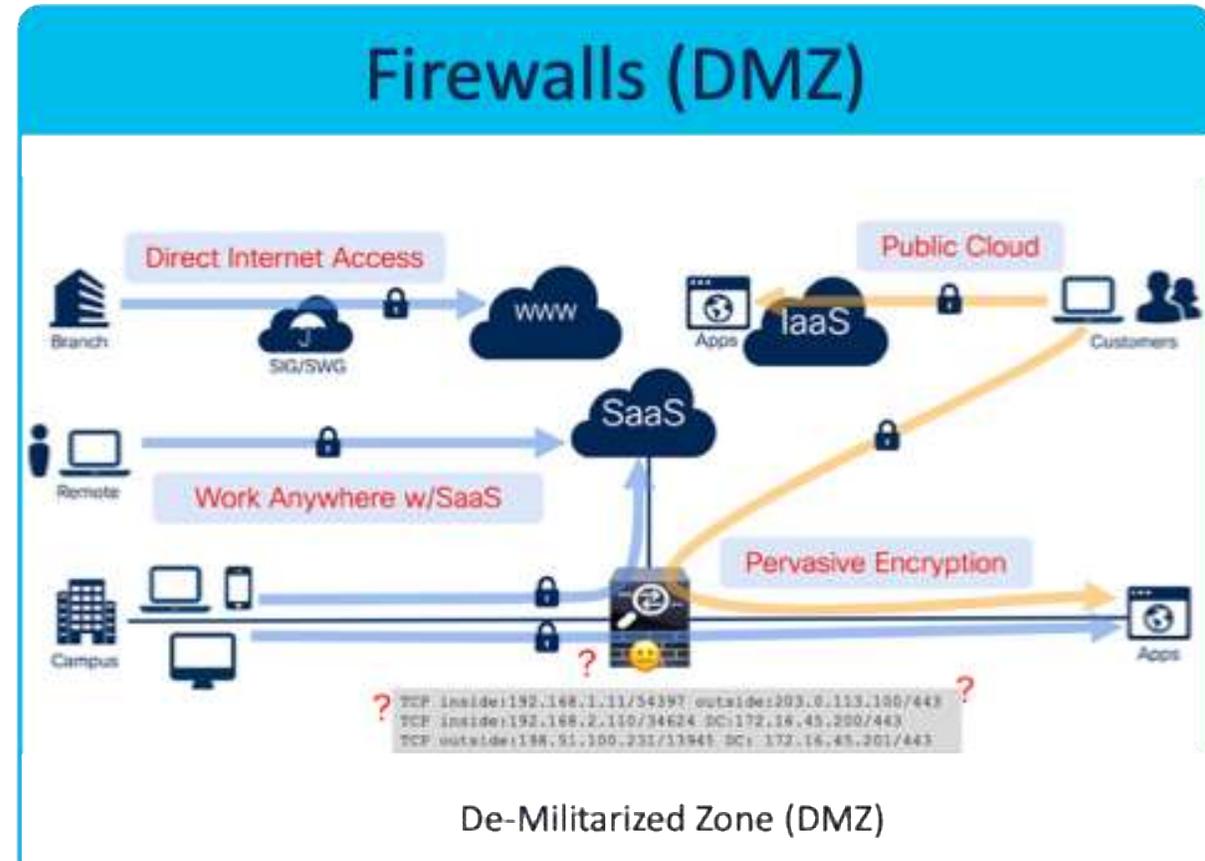
Uses a **L2 or L3/VRF + ACLs**

- 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**

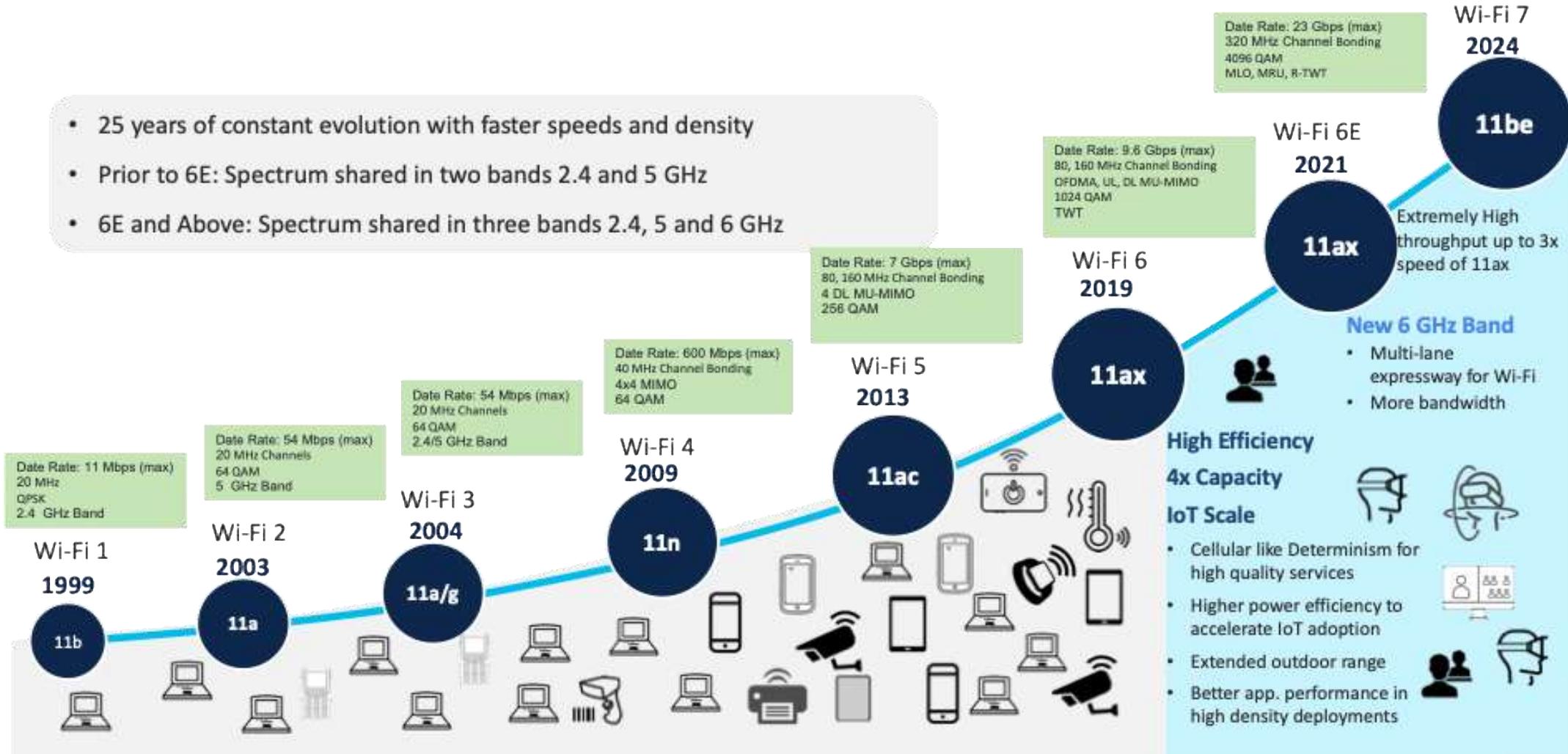
- **L4/App ACLs** (e.g. VACL, MAC ACL)
- **L4/App QoS** (e.g. VLAN QoS)
- **L4/App NetFlow** (e.g. FNF, AVC, EPA & ETA)

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



Wi-Fi Evolution

- 25 years of constant evolution with faster speeds and density
- Prior to 6E: Spectrum shared in two bands 2.4 and 5 GHz
- 6E and Above: Spectrum shared in three bands 2.4, 5 and 6 GHz



Agenda Enhanced Catalyst Wi-Fi 6/6E Product Line

Purpose-built for Immersive Experiences

Enhanced Catalyst Wi-Fi 6/6E Product Line



The Wi-Fi 7 portfolio



CW9176I

12 Spatial Streams
4x4: 4 MU-MIMO
across 3 radios, 3 bands
(2.4/5GHz (XOR), 5 GHz, 6GHz)

BLE/IoT radio

Single 10Gbps multigigabit

Ultra Wide Band (UWB)

USB 2.0 – 9W

Accelerometer

Built-in GPS/GNSS, w/ support for
ext. antenna

Integrated Omnidirectional Antenna



CW9176D1

12 Spatial Streams
4x4: 4 MU-MIMO
across 3 radios, 3 bands
(2.4/5GHz (XOR), 5 GHz, 6GHz)

BLE/IoT radio

Single 10Gbps multigigabit

Ultra Wide Band (UWB)

USB 2.0 – 9W

Accelerometer

Built-in GPS/GNSS, w/ support for
ext. antenna

Integrated Directional Antenna
(70x70)



CW9178I

16 Spatial Streams
4x4: 4 MU-MIMO
across 4 radios, 3 bands
(2.4 GHz, dual 5GHz, 6GHz)

BLE/IoT radio & accelerometer

Dual 10Gbps multigigabit

Ultra Wide Band (UWB)

USB 2.0 – 9W

Accelerometer

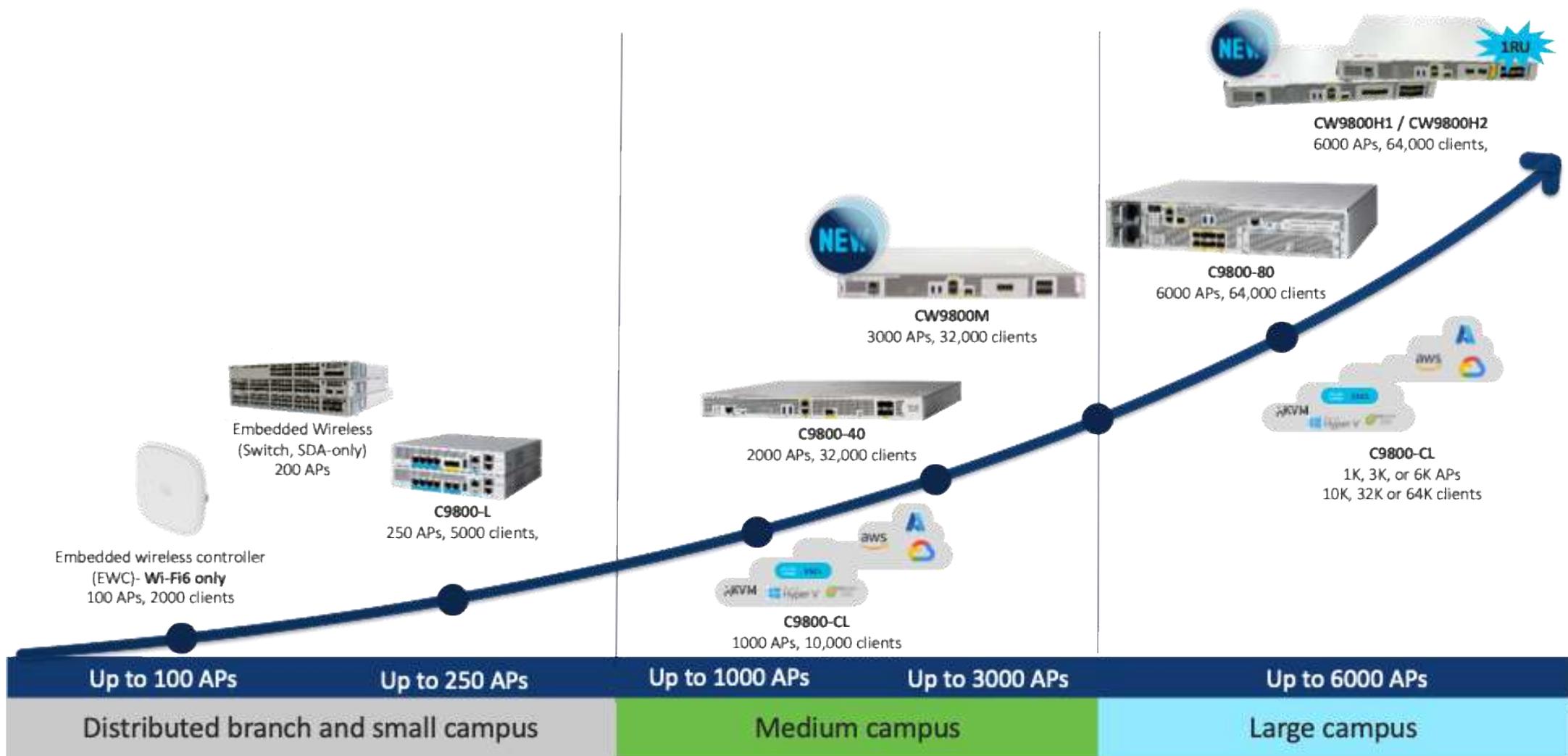
Built-in GPS/GNSS, w/ support for
ext. antenna

Integrated Omnidirectional Antenna

Same brackets as always

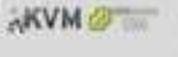
Already Wi-Fi 7 certified!

Cisco Catalyst WLC Portfolio



New addition to existing fleet

With High Performance and Efficiency

<p>Up to 200 APs**</p>  <p>Branch</p>	 <p>EWC on Cisco® Catalyst® 9100</p>	 <p>9800-L On-premises</p>	 <p>9800-CL for public cloud*</p>	 <p>9800-CL for private cloud</p>
<p>200 to 3000 APs**</p>  <p>Campus</p>	 <p>CW9800M On-premises</p>	 <p>9800-40 On-premises</p>	 <p>9800-CL for public cloud*</p>	 <p>9800-CL for private cloud</p>
<p>3000 to 6000 APs**</p>  <p>Large campus</p>	 <p>CW9800H1/H2 On-premises</p>	 <p>9800-80 On-premises</p>	 <p>9800-CL for private cloud^</p>	

*SD-Access only.

**Refer to data sheet for more information.

^Only with Cisco FlexConnect® and Fabric mode for 6000 AP support.

*Cisco Catalyst 9800 for public cloud: Cisco FlexConnect only.

Why Customers Buy ISE



	Device Administration	TACACS+ Allows for secure, identity-based access to the network devices	https://cs.co/ise-tacacs
	Secure Access	Secure wired, wireless, or VPN access using industry standard protocols RADIUS and 802.1X	https://cs.co/ise-wired
	Guest Access	Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options	https://cs.co/ise-guest
	Asset Visibility	Use the probes in ISE and Cisco devices to classify endpoints and authorize them	https://cs.co/ise-profiling
	Compliance & Posture	Use agentless posture , Cisco Secure Client , MDM , or EMM to check endpoints' posture	https://cs.co/ise-posture
	Context Exchange	Integrate applications and vendors with ISE for endpoint identity, context, and automated Enforcement	https://cs.co/ise-pxgrid
	Segmentation	Group-based Policy with Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACLs	https://cs.co/segmentation-resources
	Cisco Catalyst Center	ISE integrates with Catalyst Center to automate the network fabric and policies using SDA	https://cs.co/ise-ccc
	EMM/MDM	Endpoint Management is required for provisioning endpoints with certificates and controls for secure network access	https://cs.co/ise-mdm
	Threat Containment	Use Threat Analysis tools to grade an endpoint's threat score and automatically quarantine it if	https://cs.co/ise-tnac

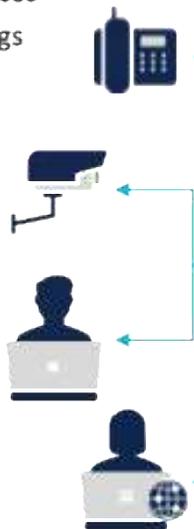
ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things



Network Devices

- Switches
- WLCs / APs
- VPN



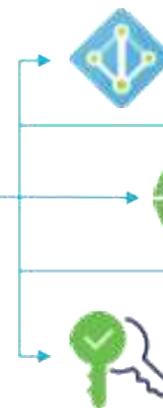
Cisco ISE

- Shared or Distributed
- VM/Appliance/Cloud
- Up to 2M Endpoints
- RADIUS and TACACS



Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA



Security Services

- Cloud Analytics
- Secure Firewall
- Partners



See It

Secure It

Share It

What is Cisco ACI?

An application centric model- networking framework

Software-defined network that takes a systems approach to deliver best-in-class automation through integration of hardware, software, physical and virtual elements



The unified point of automation and management for the Cisco ACI fabric, policy enforcement and health monitoring for physical, virtual and cloud infrastructures

ACI: One Network, any location



So, what is SD-WAN?



Transport Independence

- IPsec overlay
- Scalable
- Traffic distribution over multiple pathways (Internet, cellular, MPLS)
- Cost efficient



Application Control

- App visibility & control (GUI dashboard, group-based policies, traffic analytics)
- Application QoS & bandwidth optimization



Secure Connectivity

- Intuitive, automatic, scalable VPN solution to connect remote branch sites
- Next generation firewall at the edge to protect DIA (Direct Internet Access)

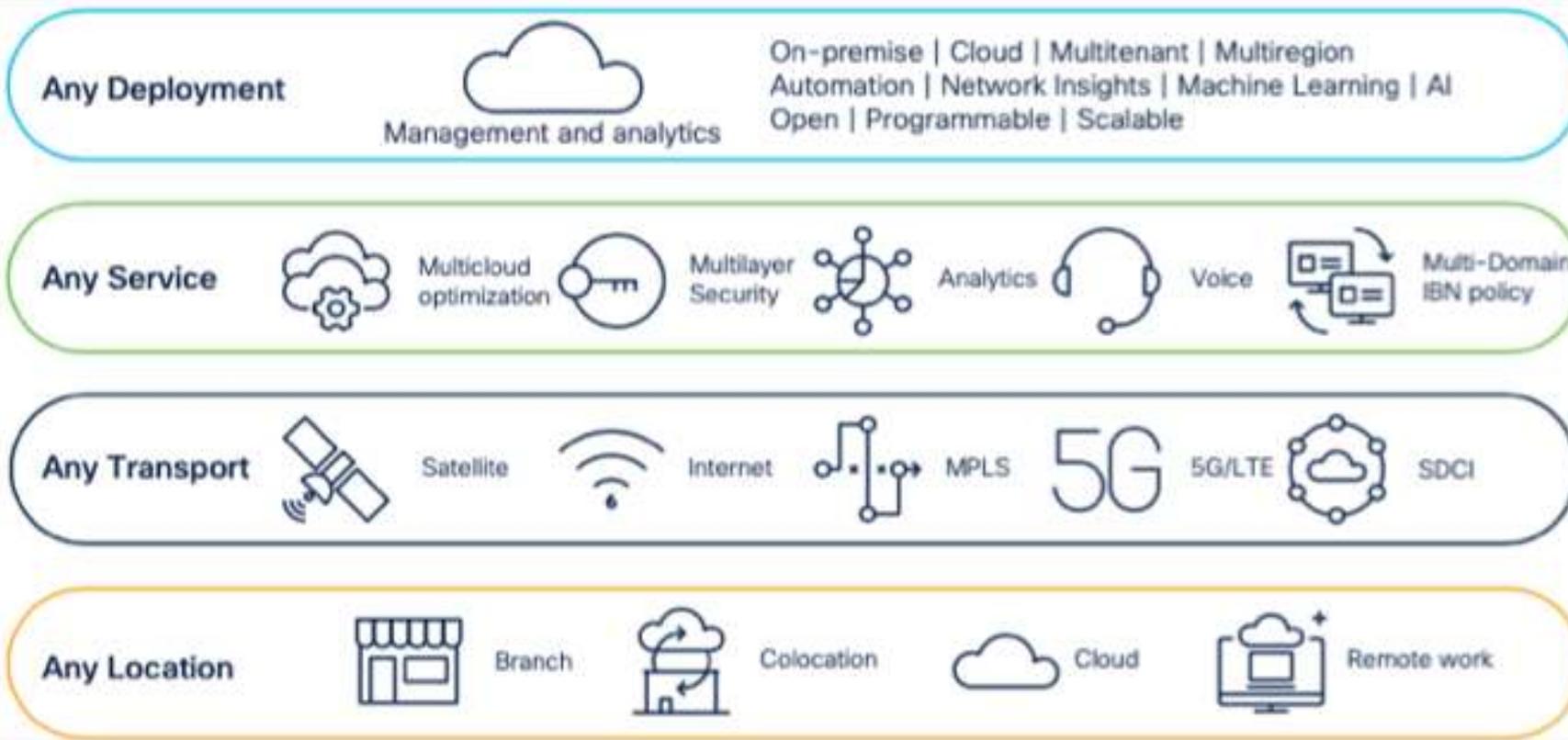


Intelligent Path Control

- Dynamic path selection based on SLA (latency, jitter and loss)
- Uplink assigned by traffic protocol, subnet, source, destination, etc. (Policy-based routing and Application-based routing)

Cisco Catalyst SD-WAN

Flexible and scalable architecture for network transformation



* Software Defined Cloud Interconnect



Questions & Answer

ATG Systems



ATGsys®

Your Reliable Partner in Myanmar.



Thank You



ATGsys®