Общие принципы проектирования классической ЛВС (I)

Network Design

Hierarchical design

- Main design options

L2/L3 access options

- + L3 access – why?

Access layer attributes

Distribution layer attributes

- + simplified design

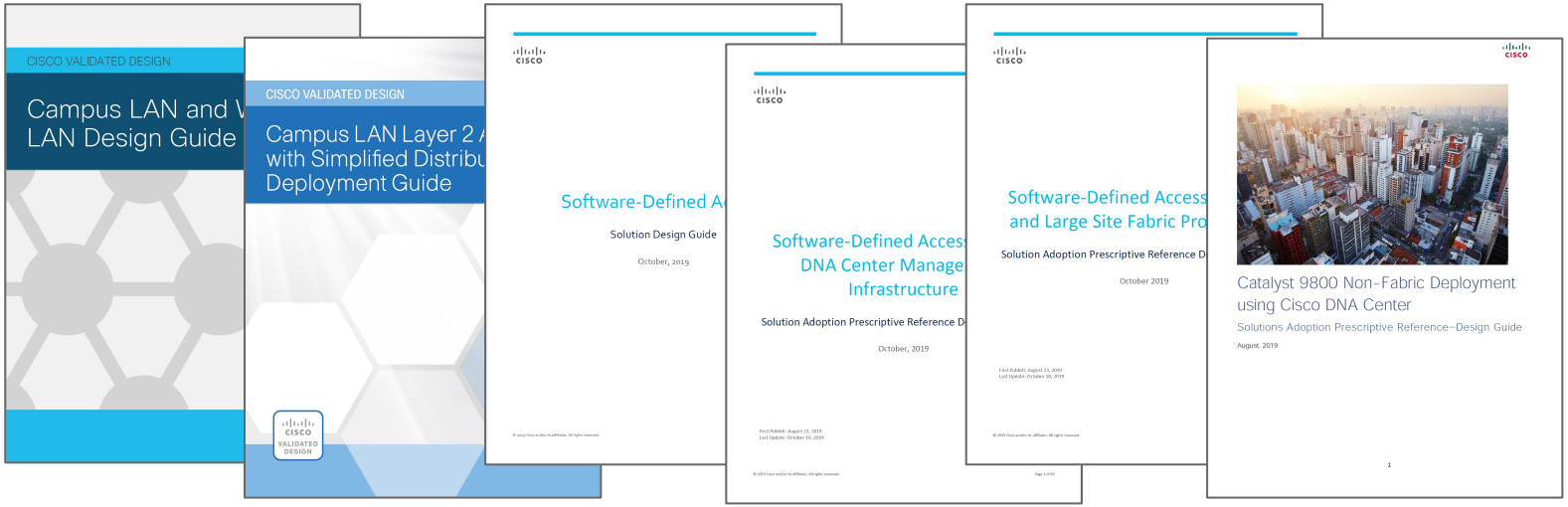
Core layer attributes

Summary

Cisco Validated Designs

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

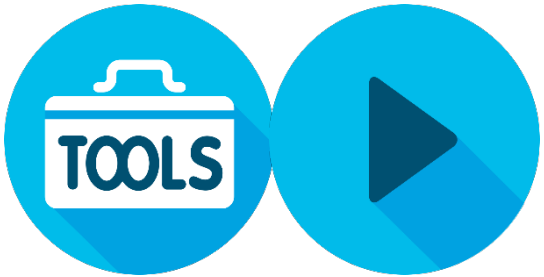
Solution Design Guides + Prescriptive Deployment Guides



[Design Zone: cisco.com/go/cvd/campus](cisco.com/go/cvd/campus)

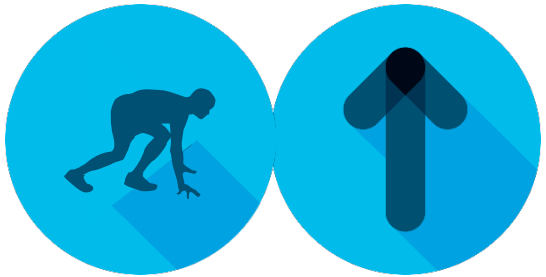
[Cisco Community: https://cs.co/en-cvds](https://cs.co/en-cvds)

LAN design principles

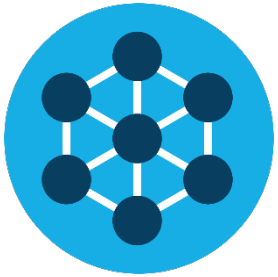


Ease of deployment

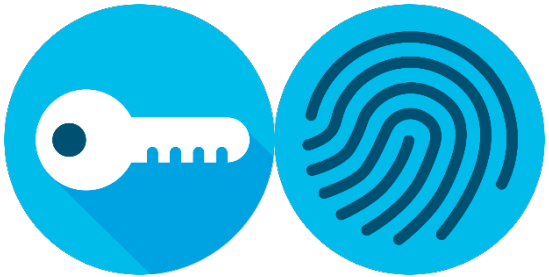
Easy to manage



Flexibility and scalability



Resiliency

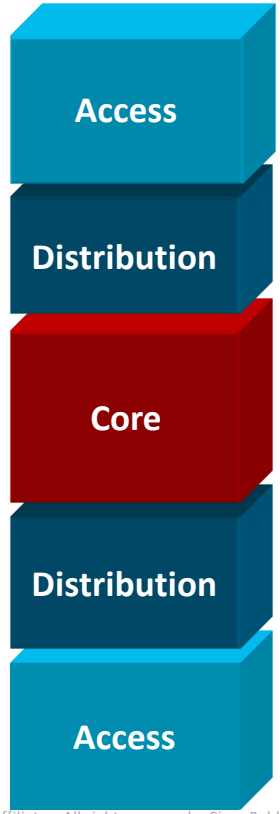


Security

Advanced technology ready

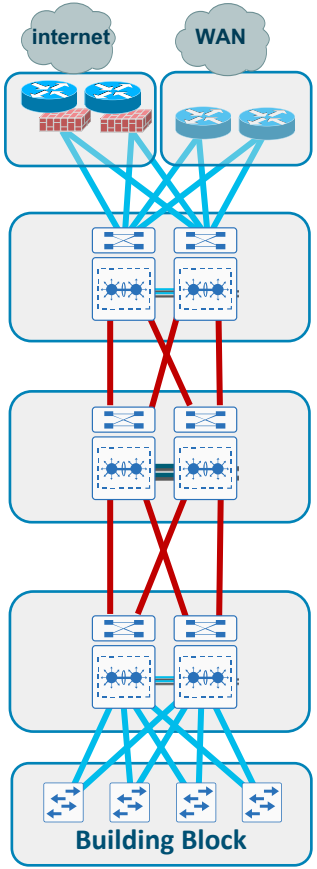
Hierarchical network design

High availability using modularity, hierarchy, and structure



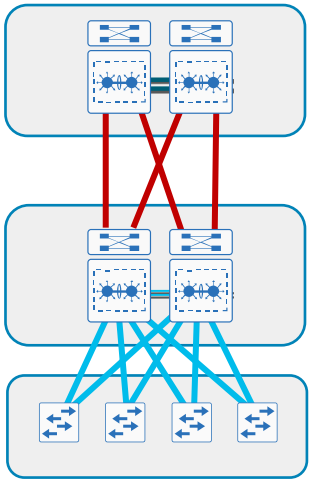
- Each layer in **hierarchy** has a specific role
- **Modular** topology—building blocks
- **Modularity** makes it easy to grow, understand, and troubleshoot
- **Structure** creates small fault domains and predictable network behavior—clear demarcations and isolation

- Promotes load balancing and resilience
- 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



Hierarchical network design: Campus wired LAN

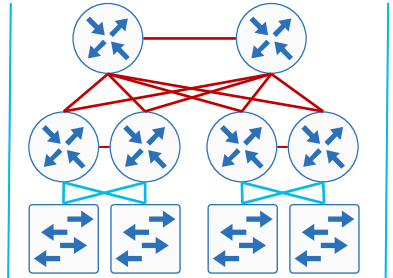
- Core
  - Connectivity, availability and scalability
- Distribution
  - Aggregation for wiring and traffic flows
  - Policy and network control point (FHRP, L3 summarization)
- Access
  - **Physical** – Ethernet wired 10/100/1000(802.3z)/mGig(802.3bz); 802.3af(PoE), 802.3at(PoE+), and Cisco Universal POE (UPOE)
  - **Policy enforcement** – security: 802.1x, port security, DAI, IPSG, DHCP snooping; identification: CDP/LLDP; QoS: policing, marking, queuing
  - **Traffic control** – IGMP snooping, broadcast control



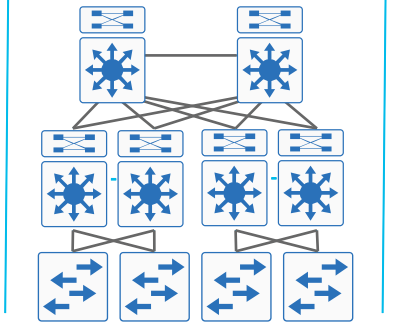
Campus wired LAN design

Option 1: Traditional multilayer campus (BRKCRS-2031)

Logical topology—
L3: core/dist.
L2: dist./acc.



Physical topology:
2 core
2 dist./acc.

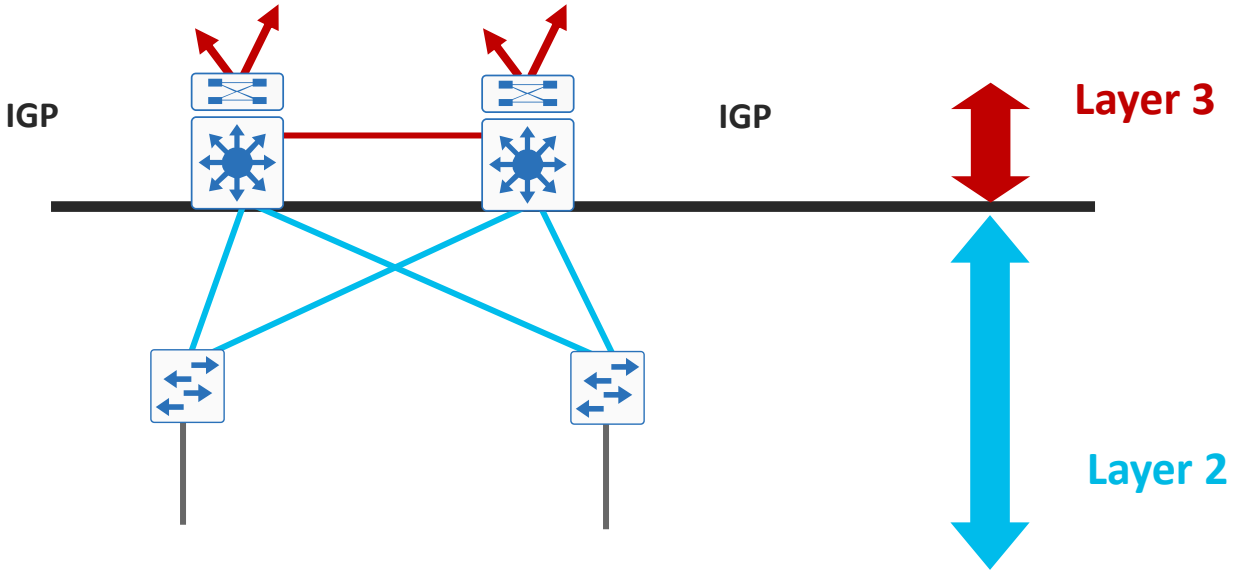


- Common design since the 1990's
- Complex configurations (prone to human error) related to spanning-tree, load balancing, unicast and multicast routing
- Requires heavy performance tuning resulting from reliance on FHRPs (HSRP, VRRP, GLBP)

Survives device and link failures	✔
Easy mitigation of Layer 2 looping concerns	
Rapid detection/recovery from failures	
Layer 2 across all access blocks within distribution	✔
Device-level CLI configuration simplicity	
Automated network and policy provisioning included	

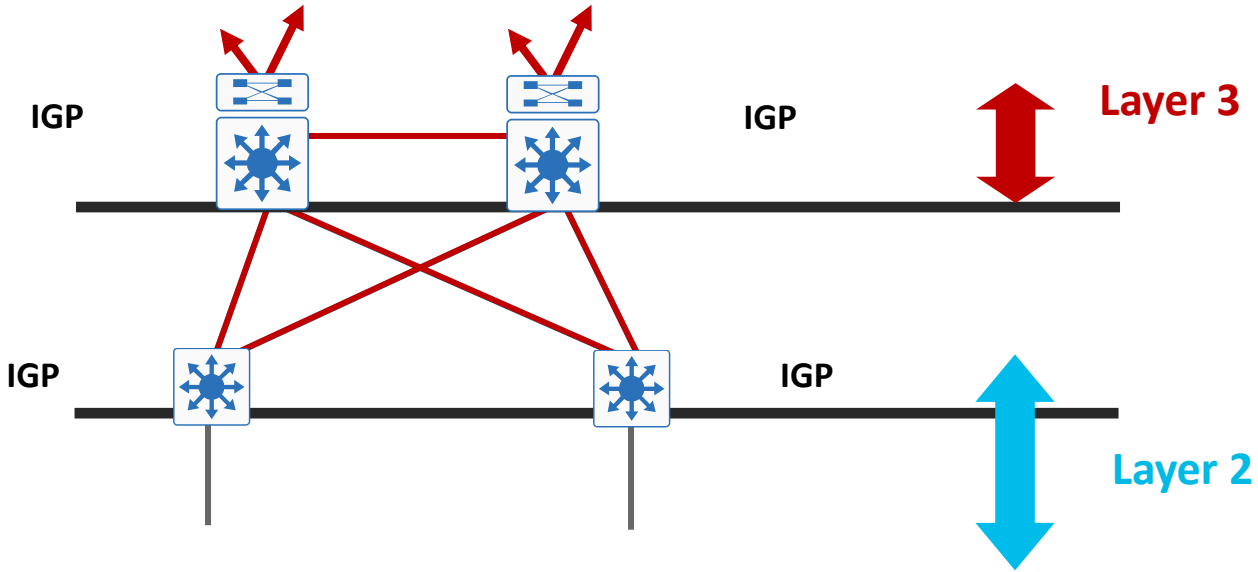
Transforming multilayer campus

Before: Layer 3 distribution with Layer 2 access



Simplification with routed access design

After: Layer 3 distribution with Layer 3 access



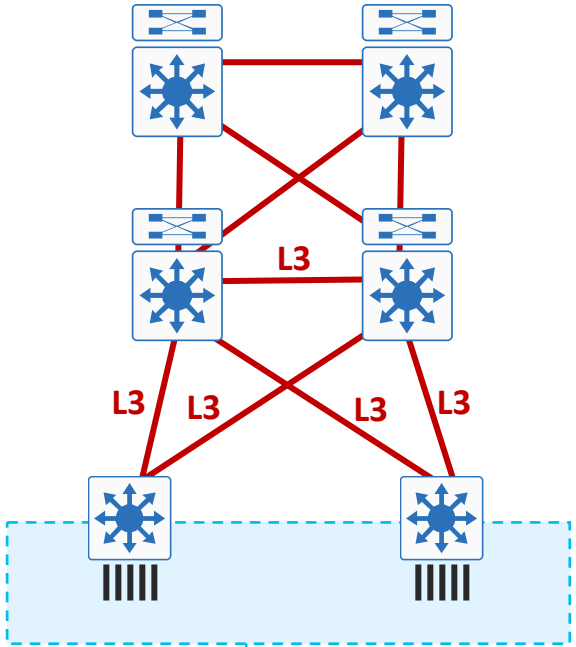
- Move the Layer 2 / 3 demarcation to the network edge
- Leverages Layer 2 only on the access ports, but builds a Layer 2 loop-free network
- **Design Motivations** – Simplified control plane, ease of troubleshooting, highest availability

Routed access advantages

Simplified control plane

- Simplified Control Plane
  - **No STP** feature placement (root bridge, loopguard, …)
  - **No default gateway** redundancy setup/tuning (HSRP, VRRP, GLBP ...)
  - **No matching of STP/HSRP priority**
  - **No asymmetric flooding**
  - **No** L2/L3 **multicast** topology **inconsistencies**
  - **No Trunking** Configuration Required

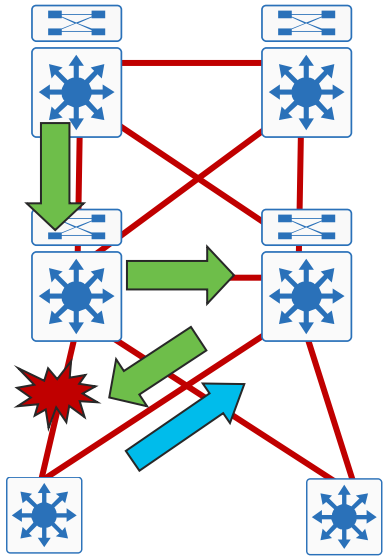
- L2 Port Edge features still apply:
  - Spanning Tree Portfast
  - Spanning Tree BPDU Guard
  - Port Security, DHCP Snooping, DAI, IPSG
  - Storm Control



Routed access advantages

Simplified network recovery

- Routed access network recovery is dependent on L3 re-route
- **Upstream** traffic restoration: ECMP re-route
  - Detect link failure
  - Process SW RIB update
  - Update HW FIB
- **Downstream** traffic restoration: routing protocol re-route
  - Detect link failure
  - Determine new route
  - Process SW RIB update
  - Update HW FIB



Upstream Recovery: ECMP
Downstream Recovery: Routing Protocol

Compare to…

- RPVST+ convergence times dependent on FHRP tuning
- Proper FHRP design and tuning can achieve sub-second times
- EIGRP converges <200 msec
- OSPF converges <200 msec with LSA and SPF tuning

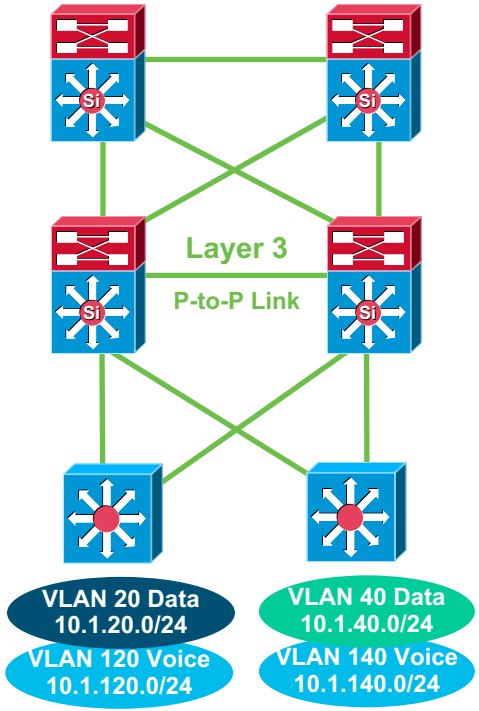
Routing to the Edge
Advantages, Yes in the Right Environment

Advantages:

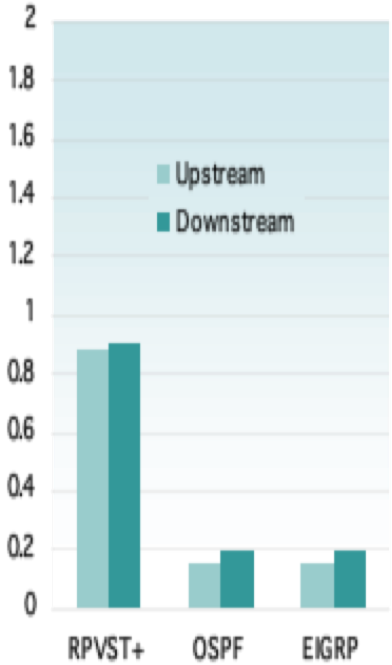
- Ease of implementation, less to get right
  - No matching of STP/HSRP/GLBP priority
  - No L2/L3 Multicast topology inconsistencies
- Single Control Plane and well known tool set
  - traceroute, show ip route, show ip eigrp neighbor, etc.…
- Most Catalysts support L3 Switching today
- EIGRP converges in <200 msec
- OSPF with sub-second tuning converges in <200 msec
- RPVST+ convergence times dependent on GLBP / HSRP tuning

Considerations:

- Do you have any Layer 2 VLAN adjacency requirements between access switches?
- IP addressing—Do you have enough address space and the allocation plan to support a routed access design?



Both L2 and L3 Can Provide Sub-Second Convergence



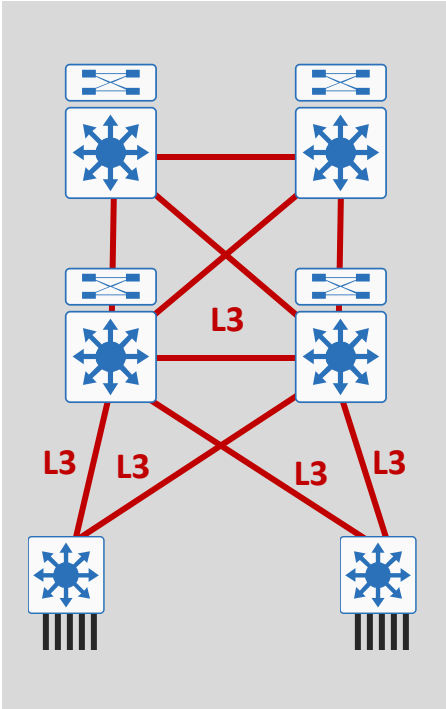
Why isn’t routed access deployed everywhere?

Routed access design constraints

- VLANs don’t span across multiple wiring closet switches/switch stacks

  Does this impact your requirements?

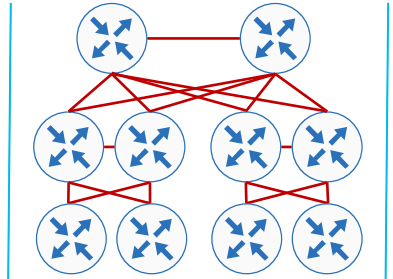
- IP addressing changes: more DHCP scopes and subnets of smaller sizes increase management and operational complexity
- Deployed access platforms must be able to support routing features



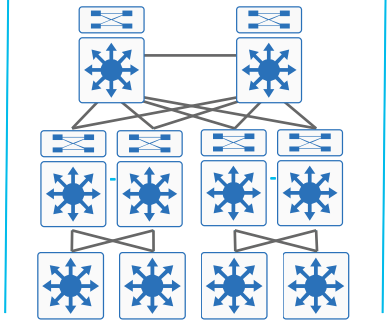
Campus wired LAN design

Option 2: Layer 3 routed access (BRKCRS-3036)

Logical topology—
L3: everywhere
L2: edge only



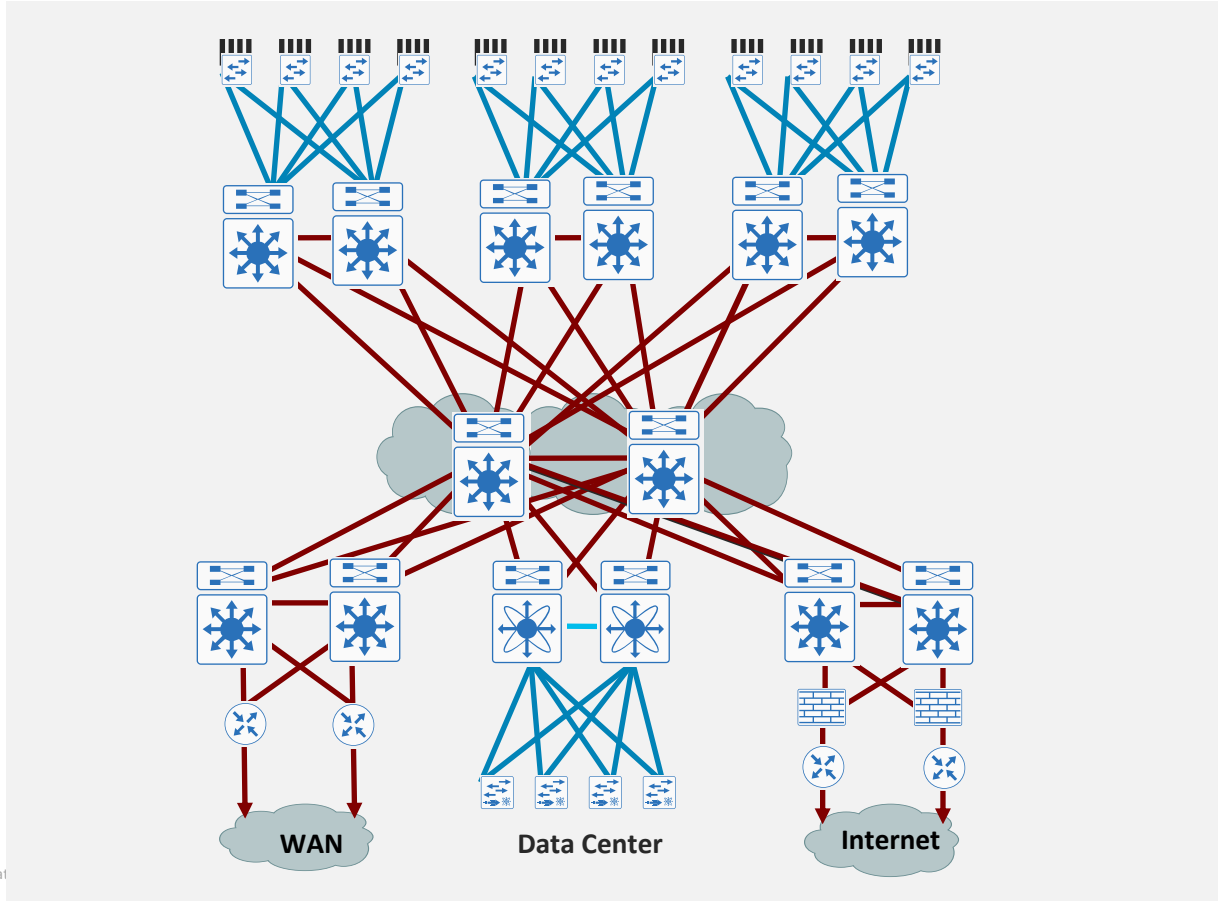
Physical topology:
2 core
2 dist./acc.



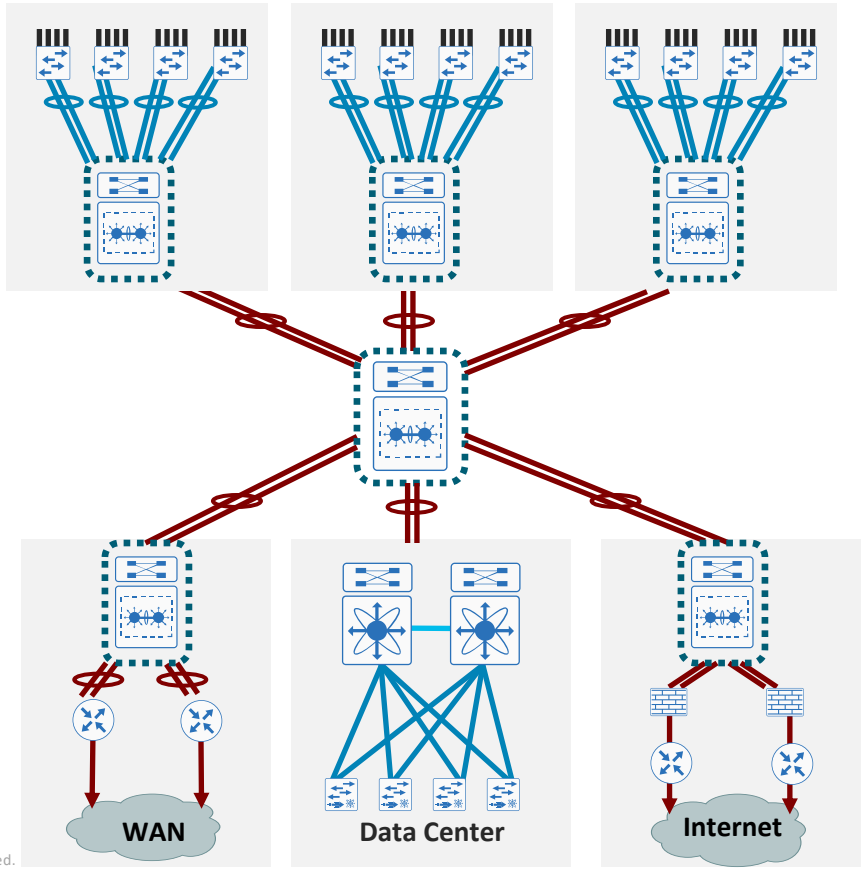
- Complexity reduced for Layer 2 (STP, trunks, etc.)
- Elimination of FHRP and associated timer tuning
- Requires more Layer 3 subnet planning; might not support Layer 2 adjacency requirements

Survives device and link failures	✔
Easy mitigation of Layer 2 looping concerns	✔
Rapid detection/recovery from failures	✔
Layer 2 across all access blocks within distribution	
Device-level CLI configuration simplicity	✔
Automated network and policy provisioning included	

Traditional multilayer campus design



What if we could do a simplified design?



Standalone (multilayer) versus simplified

~~STP Loop~~

~~FHRP~~

~~FHRP Tunings~~

~~PIM DR Priority~~

~~PIM Tunings~~

~~Protocol Dependent Scale~~

~~Unicast Flooding~~

~~Asymmetric Forwarding~~

L2 Hardening

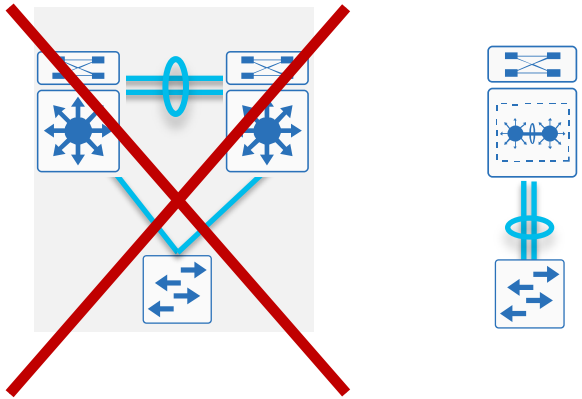
~~Network/System Redundancy Tradeoff~~

~~Protocol Dependent Recovery~~

~~CAM/ARP Tunings~~

~~OSPF LSA/SPF Tuning~~

~~Control/Management/Forwarding Complexity~~



Scale-independent Recovery

Network/System Level Redundancy

Hardware Driven Recovery

Increase Unicast Capacity

Increase Multicast Capacity

Simplified Network Topologies

Control-plane Simplicity

Operational Simplicity

L2-L4 Load Sharing

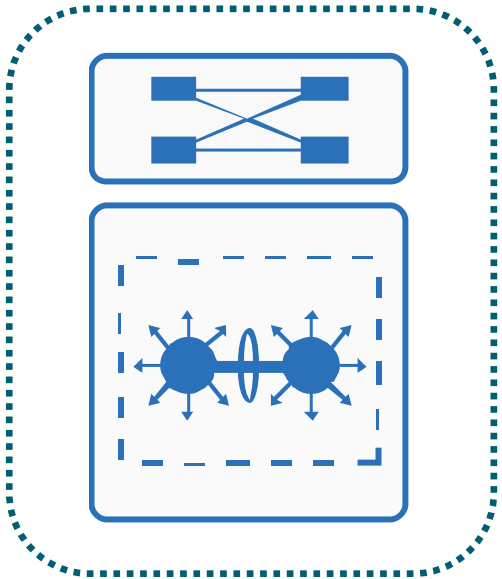
Flat L2 Network

Unified system architecture

StackWise Virtual (SWV) and Virtual Switching System (VSS)

Simplified Control-Plane

- Single control-plane to manage two physical systems
- Consistent IOS software feature parity as Standalone
- Centralized programming for distributed forwarding



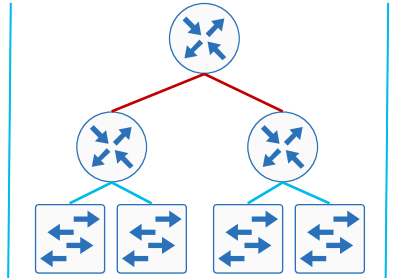
Common Management

- Single virtual system for OOB/in-band management of two physical systems
- Common SNMP MIBs, traps with advanced MIBS
- Single troubleshooting point

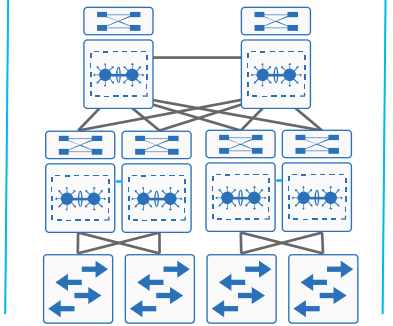
Campus wired LAN design

Option 3: Layer 2 access with “simplified” distribution (BRKCRS-1500)

Logical topology—
L3: core/dist.
L2: dist./acc.



Physical topology:
2 core
2 dist./acc.



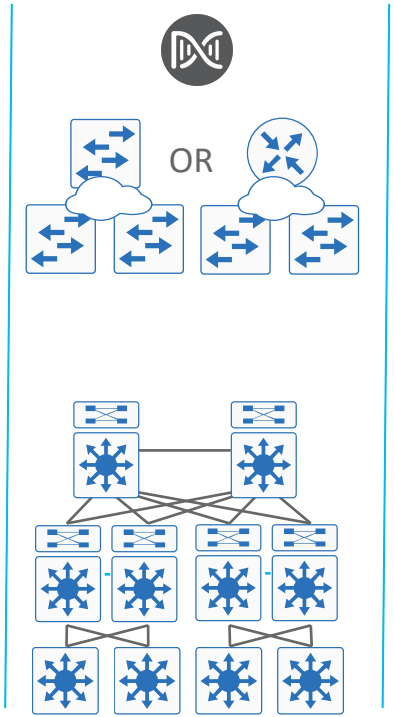
- Leading campus design for easy configuration and operation when using stacking or similar technology (VSS, StackWise Virtual)
- Flexibility to support Layer 2 services within distribution blocks, without FHRPs.
- Easy to scale and manage

Survives device and link failures	✔
Easy mitigation of Layer 2 looping concerns	✔
Rapid detection/recovery from failures	✔
Layer 2 across all access blocks within distribution	✔
Device-level CLI configuration simplicity	✔
Automated network and policy provisioning included	

Campus wired LAN design

Option 4: Cisco Software-Defined Access (BRKCRS-1501, many others)

Logical topology—
L2/L3: flexible overlays

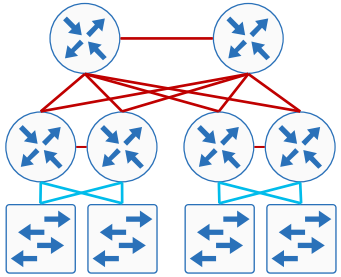
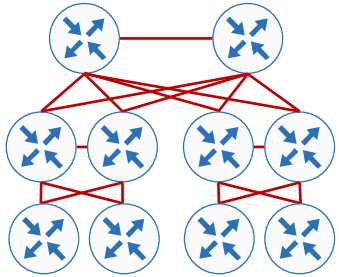
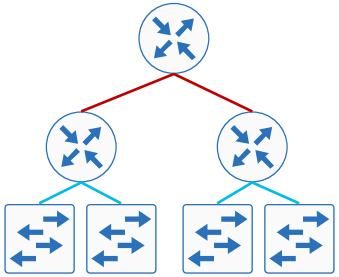
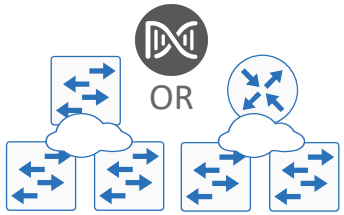
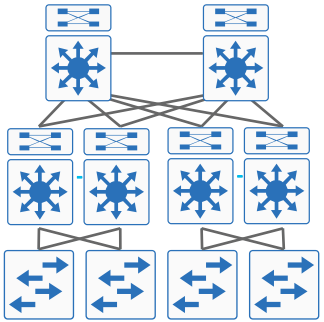
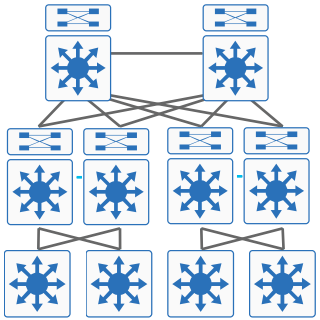
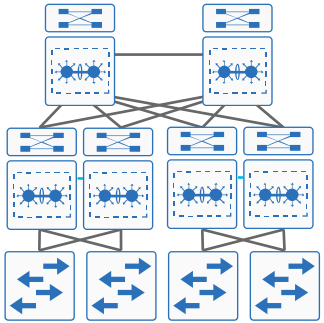
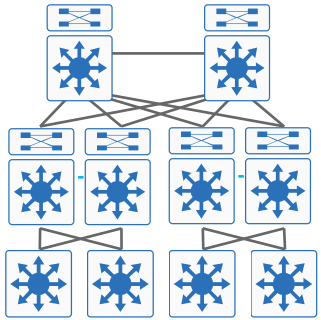


Physical topology:
2 core
2 dist./acc.

- Uses advantages of a routed access physical design, with Layer 2 capable logical overlay design
- Provisioning and policy automation
- Integrates wireless into the same policy
- Requires automation to simplify configuration

Survives device and link failures	✔
Easy mitigation of Layer 2 looping concerns	✔
Rapid detection/recovery from failures	✔
Layer 2 across all access blocks within distribution	✔
Device-level CLI configuration simplicity	
Automated network and policy provisioning included	✔

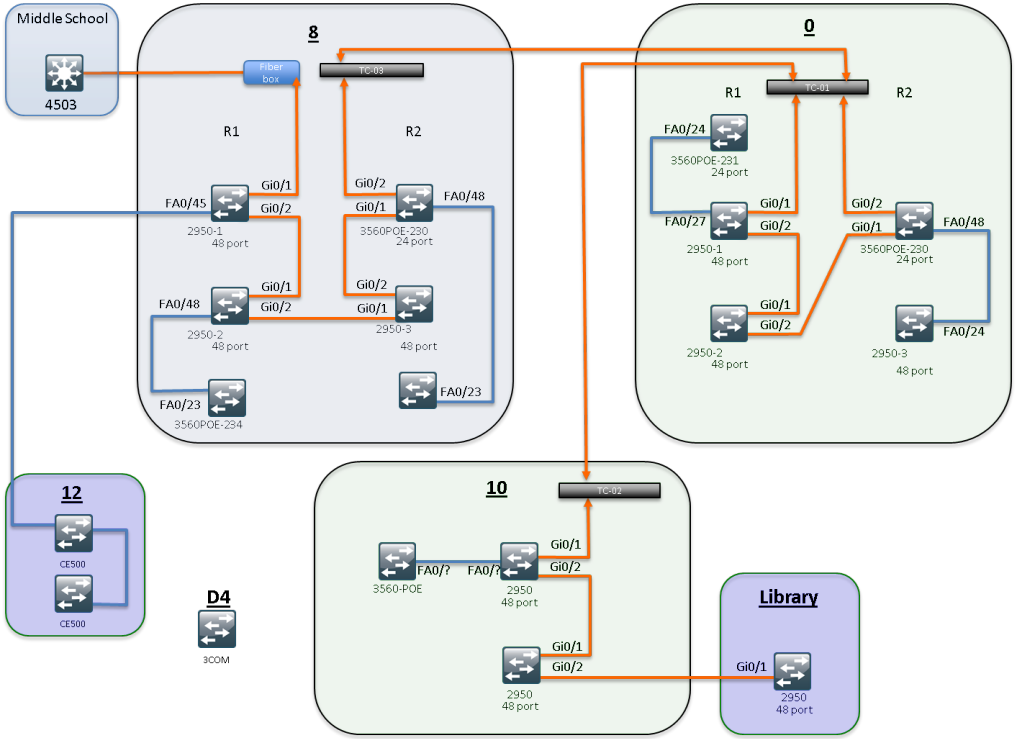
Campus wired LAN design options—summary

	Traditional Multilayer Campus BRKCRS-2031	Layer 3 Routed Access BRKCRS-3036	L2 Access / Simplified Distribution BRKCRS-1500	SD-Access / Fabric for Campus BRKCRS-1501 (and many others)
Logical topology				
Design notes	Protocols / Tuning	L3 Planning Limited L2	Flexible, Easy, Scalable	Flexible, Tools to Simplify
Physical topology: 2 core 2 dist./acc.				

What we are trying to avoid!

No hierarchy

Multiple
single points of failure

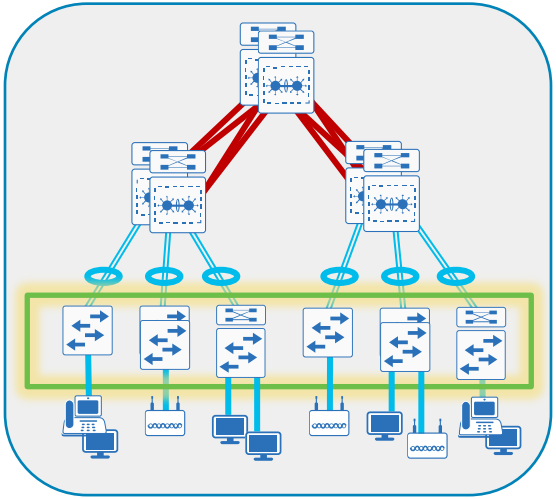


Hard to troubleshoot

Poor performance

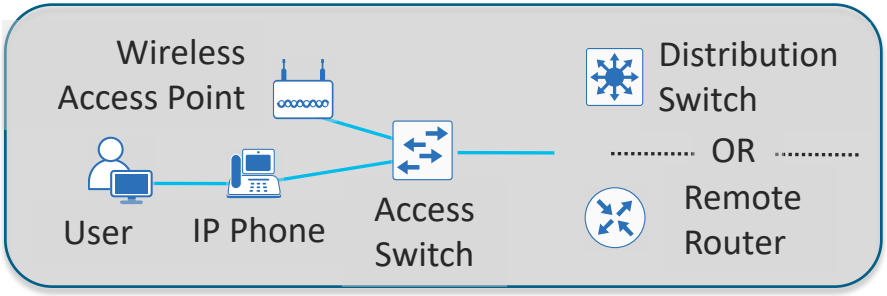
Access layer attributes

- Ethernet network access
  - Wired 10/100/1000(802.3z)/mGig(802.3bz)
  - Supports Wireless LAN 802.11a/b/g/n/ac/ax access APs
- Simplified and flexible design
  - Layer 2 edge for applications that require spanned vlans
  - Avoid Spanning Tree loops for resiliency
- Policy enforcement point
  - Secure network and applications from malicious attacks
  - Packet marking for QoS
- Advanced Technologies support
  - Deliver PoE services: 802.3af(PoE), 802.3at(PoE+), and Cisco Universal POE (UPOE) – 60 watts per port
  - QoS enforcement to protect multimedia applications



Access layer design

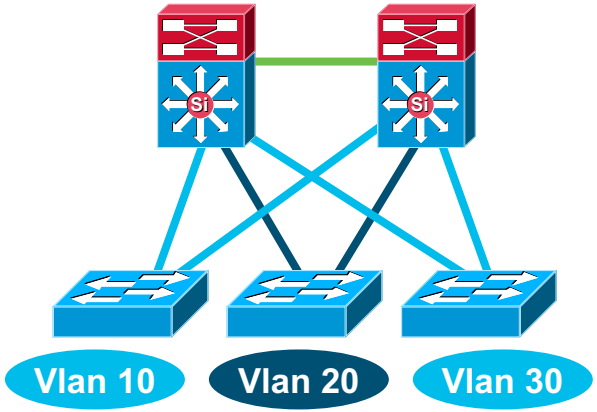
Uniform deployment in the network



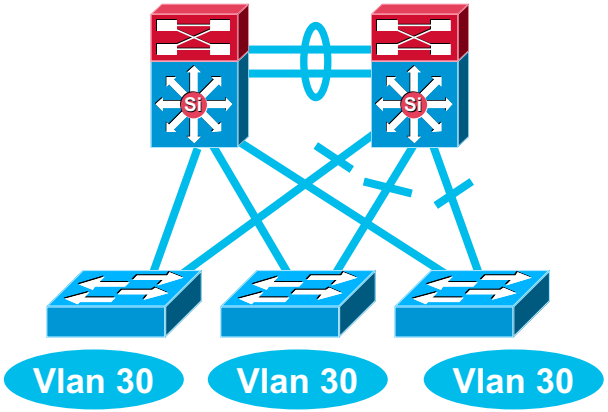
- A common deployment method is used for all access layer devices in the design
  - Whether they are located in the headquarters or at a remote site.
- A single interface configuration is used for a standalone computer, an IP phone, or an IP phone with an attached computer.
- The LAN access layer is configured as a Layer 2
  - All Layer 3 services provided by directly connected distribution layer switch or router.

Multilayer Network Design

Layer 2 Access with Layer 3 Distribution

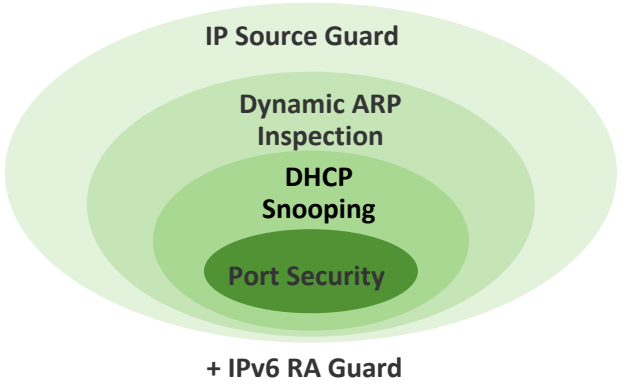


- Each access switch has unique VLANs
- No Layer 2 loops
- Layer 3 link between distribution
- No blocked links

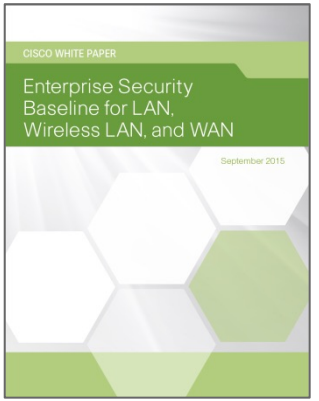


- At least some VLANs span multiple access switches
- Layer 2 loops
- Layer 2 and 3 running over link between distribution
- Blocked links

Access layer – hardening the edge



The Cisco Validated Design uses Catalyst Integrated Security Features to protect your network from intentional and unintentional attacks

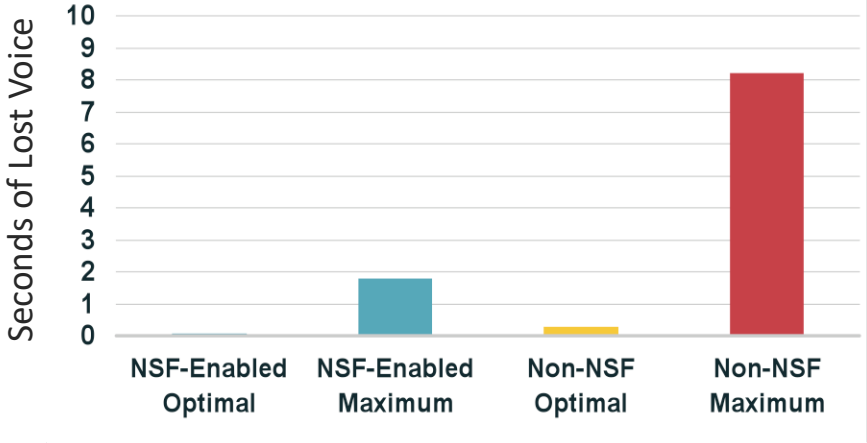


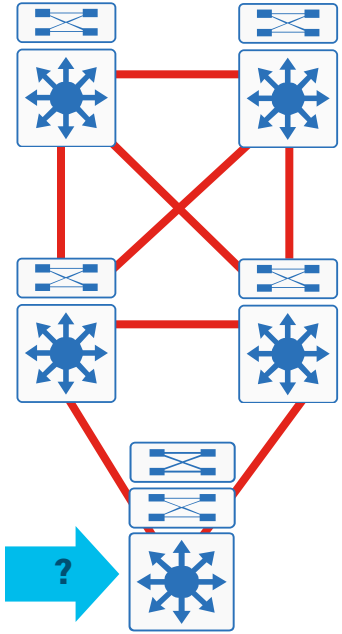
- Port security prevents CAM attacks and DHCP Starvation attacks
- DHCP Snooping prevents Rogue DHCP Server attacks
- Dynamic ARP Inspection prevents current ARP attacks
- IP source guard prevents IP/MAC Spoofing
- IPv6 router advertisement guard prevents IPv6 Man-in-the-Middle attacks

Chassis Redundancy at the Access

Recommended for highest availability

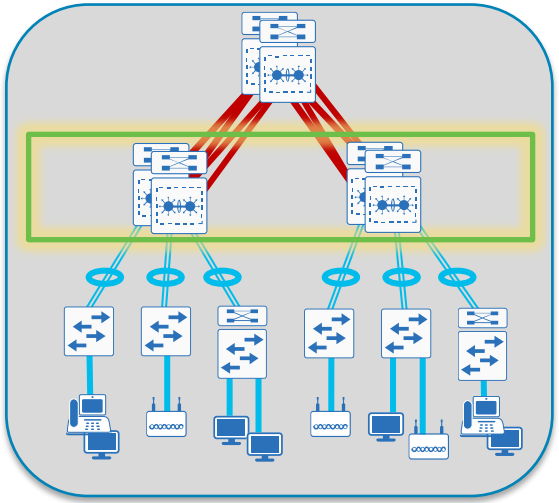
- Access switch is the single point of failure in best practices HA design
- Supervisor failure is most common cause of access switch service outages





Campus LAN distribution layer attributes

- Primary function is access layer aggregation for a building or geographic area.
- Resilient design to reduce failure impact
- Layer 2 boundary for access layer
  - Spanning tree protocol boundary
  - Broadcast packet boundary
  - Provides load balancing to access layer
- Layer 3 features and functions
  - Default IP gateway for L2 access layer
  - IP routing summarization to rest of network
  - Efficient IP multicast
  - Provides load balancing to core layer
- QoS to manage congestion caused by many to few links

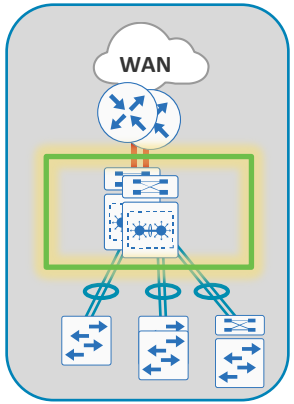


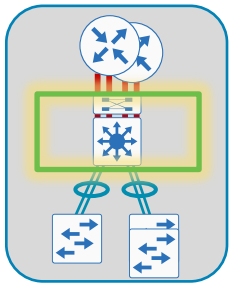
Alternative distribution layer attributes

LAN distribution layer

Collapsed core:
Two tier main campus LAN and WAN core

- LAN access layer aggregation
- Central connect point for all services



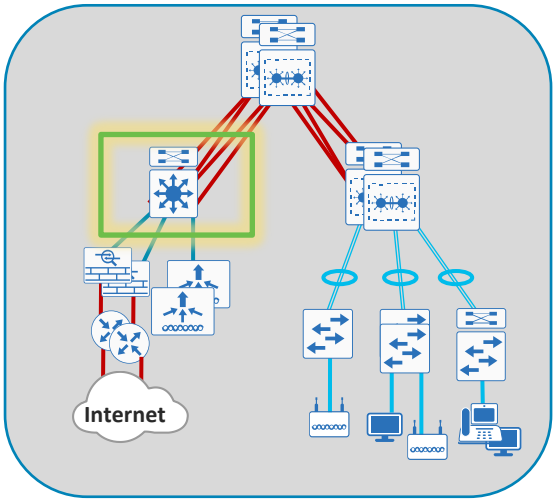


Two tier remote site:

- Aggregates LAN access layer and connects to WAN routers

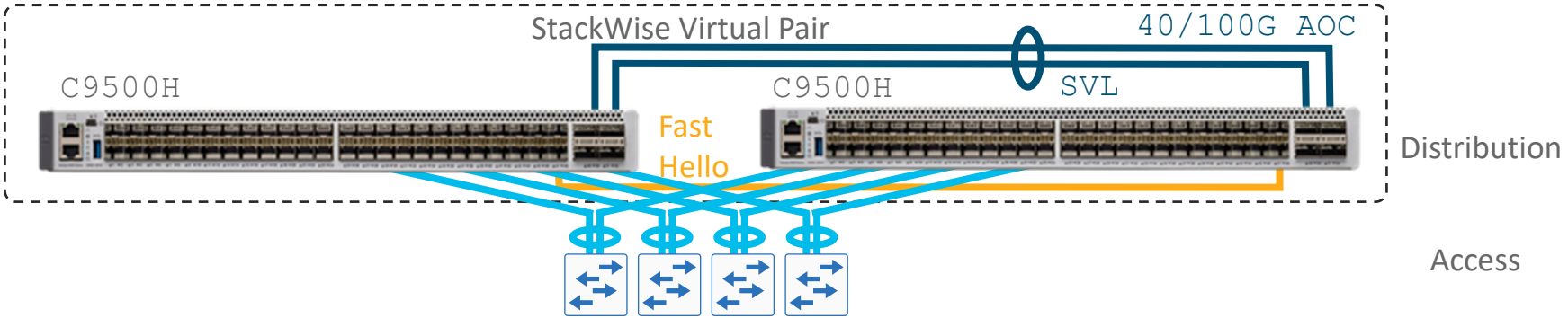
Large LAN services block

- Connection point for services
- Drives modular building block design



“How can I simplify my distribution?”

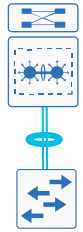
Cisco StackWise Virtual



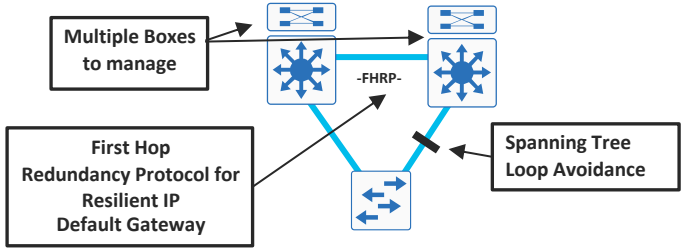
Simplified distribution layer design

LAN distribution layer

- Traditional two box distribution layer has many points to manage
- Preferred distribution layer uses a “single box design”
  - Two switches acting as a single logical switch (StackWise Virtual or Virtual Switching System)
  - A multiple member switch stack acting as a single logical switch
- Simplified design benefits
  - Fewer boxes to manage
  - Simplified configuration
  - Logical hub-and-spoke topology

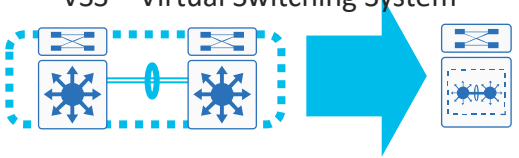


Traditional two box design

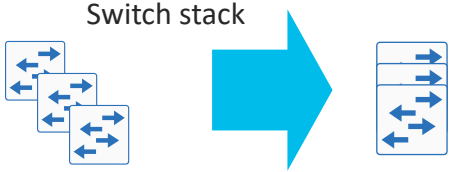


SWV – StackWise Virtual

VSS – Virtual Switching System



Switch stack

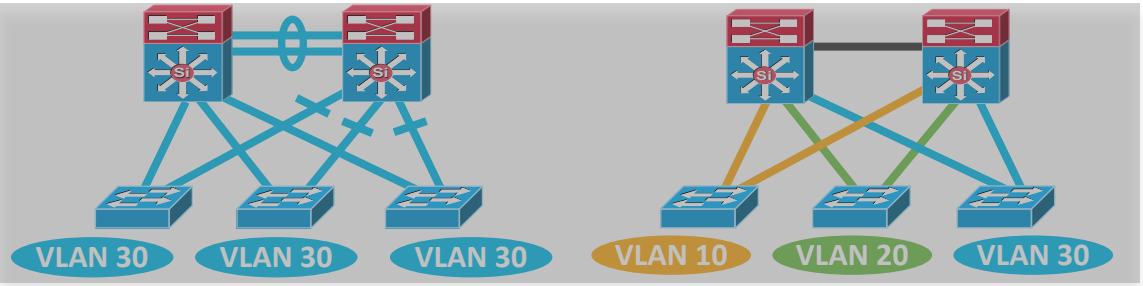


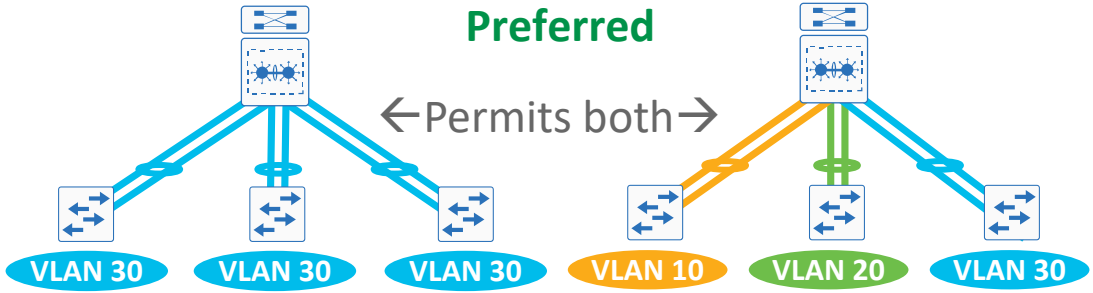
Traditional design compared to simplified design

LAN distribution layer

Traditional designs:

- Looped design with spanned VLANs
  - Relies on STP to block loops
  - Reduces available bandwidth
- Loop free design
  - Can increase bandwidth
  - Still relies on FHRP
  - Multiple distribution layer boxes to configure



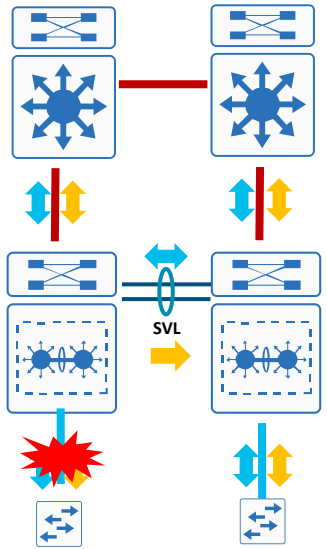


Preferred—simplified design:

- EtherChannel - resilient links, all links forwarding
- No FHRP - single default IP gateway
- Works with VLAN per closet or few VLANs spanned designs
- Logical hub-and-spoke topology
- Reduced dependence on spanning tree - keep RPVST+ for edge protection

StackWise Virtual – single-homed connections

- Regardless of system modes (SWV, VSS, or standalone), single-homed connections are not recommended
- Cannot leverage distributed architecture benefits.
- Non-congruent Layer 2 or Layer 3 network design with –
  - Centralized network control-plane processing over VSL
  - Asymmetric forwarding plane. Ingress data may traverse over VSL interface and oversubscribe the ports
- Single-point of failure in various faults – Link/SFP/module failure, SSO switchover, ISSU etc..
- Cannot be trusted switch for dual active detection purposes

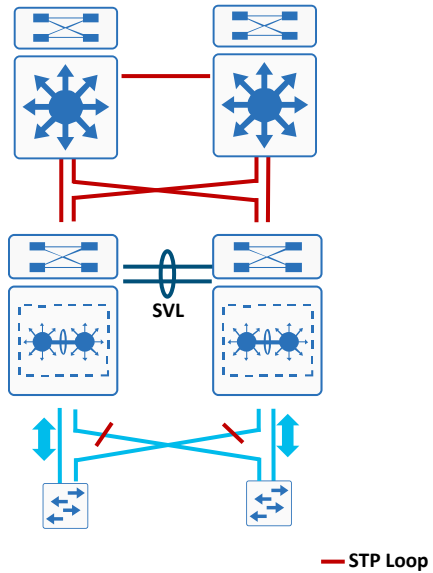


StackWise Virtual– multi-homed physical connections

- Redundant network paths per system delivers best architectural approach

However, without MultiChassis Etherchannel on Access Layer uplinks:

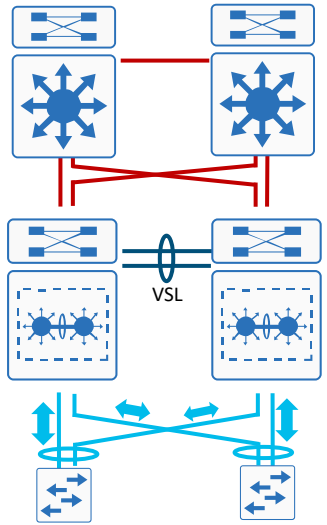
- Parallel Layer 2 paths between bridges builds sub-optimal topology :
  - Creates STP loop. Except for root port, all other ports are in blocking mode
  - Slow network convergence
- Parallel Layer 3 doubles control-plane processing load :
  - ACTIVE switch needs to handle control plane load of local and remote-chassis interfaces
  - Multiple unicast and multicast neighbor adjacencies
  - Redundant routing and forwarding topologies



StackWise Virtual– Multichassis EtherChannel

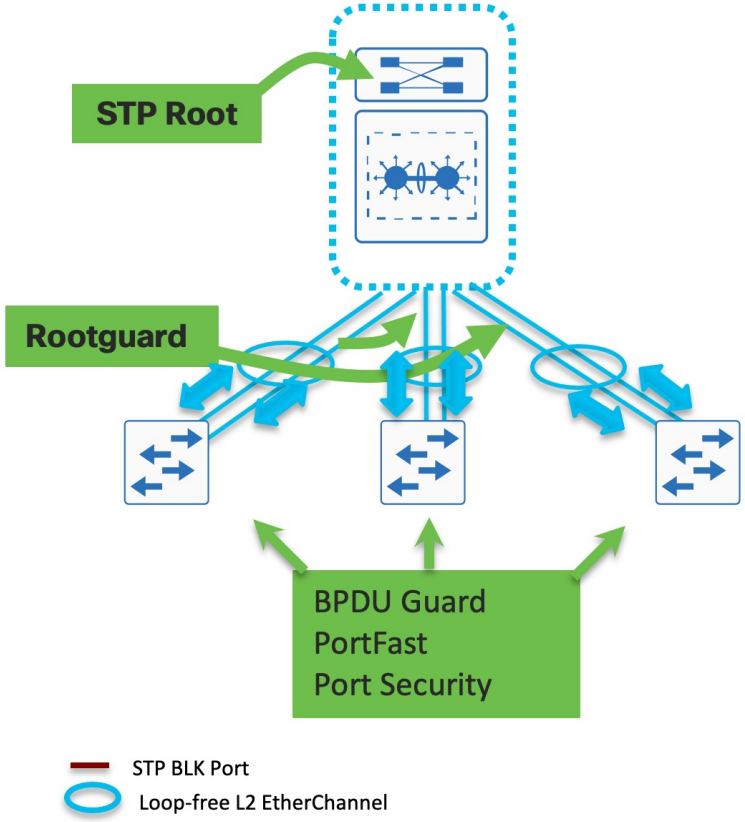
Multichassis EtherChannel (MEC) enables
Distributed link bundling into single logical L2/L3 Interface

- MEC enables:
  - Simplified STP loop-free network topology
  - Consistent L3 control-plane and network design as traditional standalone system
  - Deterministic sub-second network recovery
- MECs can be deployed in two modes
  – Layer 2 or Layer 3



StackWise Virtual – simplified STP topology

- StackWise Virtual simplifies STP
  – it does not eliminate STP. Never disable STP.
- Multiple parallel Layer 2 network path
  builds STP loop network
- StackWise Virtual with MEC
  builds single loop-free network to utilize
  all available links.
- Distributed EtherChannel minimizes STP
  complexities compared to standalone distribution
  design
- STP toolkit should be deployed
  to safe-guard multilayer network



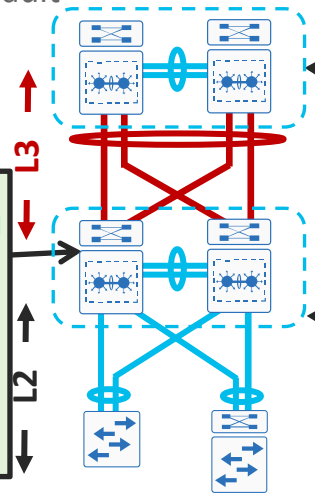
Distribution layer IP unicast routing – EIGRP

LAN distribution layer

EIGRP was chosen for…
simplicity, scalability, and flexibility

- Named mode configuration
- Tie EIGRP router-id to loopback 0 for max stability
- Enable all routed links to be passive by default
- Enable EIGRP for address space
- Each distribution is a stub network

```
router eigrp [NAME]
  address-family ipv4 unicast autonomous-system [AS]
    af-interface default
       passive-interface
    exit-af-interface
    network [network] [inverse mask]
    eigrp router-id [ip address of loopback 0]
    eigrp stub summary
    nsf
  exit-address-family
```



Single logical distribution layer design

- Uses stateful switchover (SSO) and non-stop forwarding (NSF)
- SSO provides sub-second failover to redundant supervisor
- NSF maintains packet forwarding while control plane recovers

NSF aware
- Nothing to enable.
- Only need IOS version that supports NSF for EIGRP

NSF capable
- Works on dual supervisor system
- Signals peer of SSO and to delay adjacency timeout
- Once control plane recovers, re-establishes peering

Distribution layer IP unicast routing – OSPF

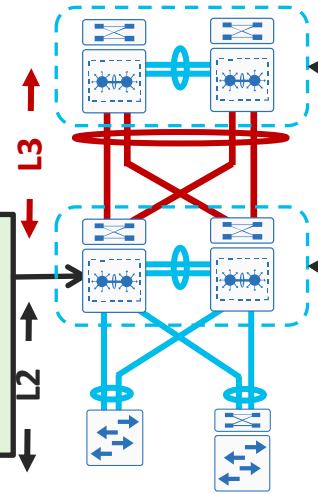
LAN distribution layer

OSPF is available for…

compatibility

- Tie OSPF router-id to loopback 0 for max stability
- Enable all routed links to be passive by default
- Enable OSPF for address space
- Each distribution is a stub area and ABR

```
router ospf [process]
 router-id [ip address of loopback 0]
 nsf
 area [area number] stub no-summary
 passive-interface default
 network [network] [inv. mask] area [area #]
 network [network] [inverse mask] area 0
```



Single logical distribution layer design

- Uses stateful switchover (SSO) and non-stop forwarding (NSF)
- SSO provides sub-second failover to redundant supervisor
- NSF maintains packet forwarding while control plane recovers

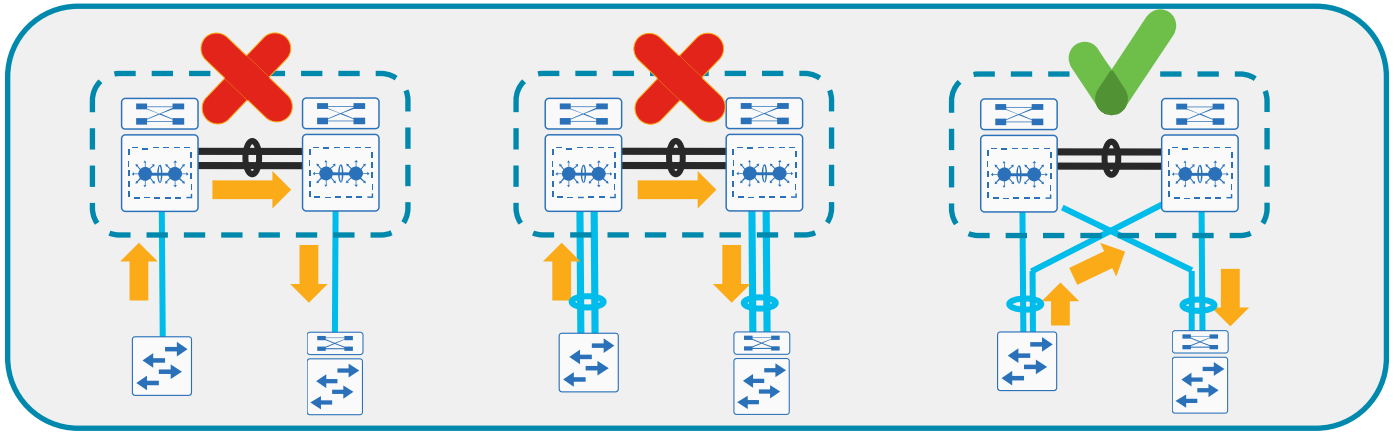
NSF aware
- Nothing to enable.
- Only need IOS version that supports NSF for OSPF

NSF capable
- Works on dual supervisor system
- Signals peer of SSO and to delay adjacency timeout
- Once control plane recovers, re-establishes peering

SWV/VSS: connecting distribution to access layer

Resilient connectivity

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

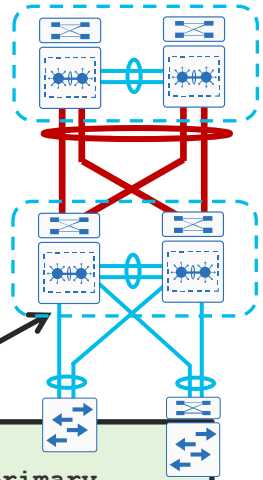


- Alternatively…
  With StackWise distribution layer, home EtherChannel uplinks to multiple switches in stack

Layer 2 connectivity to access layer

LAN distribution layer

- Configure Layer 2
  - With hub-and-spoke design, no STP loops, still enable RPVST+
  - Configure VLANs servicing access layer
  - Set distribution layer to be STP root for access layer VLANs
- Configure EtherChannel member interfaces
  - Uses LACP for EtherChannel protocol
  - For Layer 2 EtherChannel, configure physical interfaces prior to logical interface
  - Apply egress QoS macro (if not using Application Policy or EasyQoS)
- Configure 802.1Q trunk on EtherChannel logical port (port-channel) interface

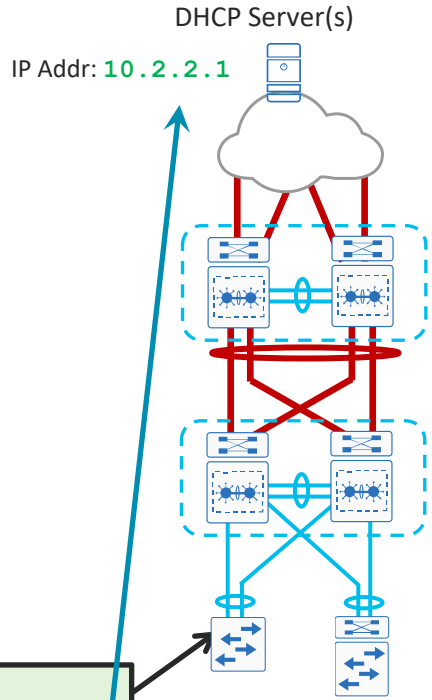


```
vlan 10,20,30
spanning-tree vlan 1-4094 root primary
!
Interface range gigabit 1/1/1, gigabit 2/1/1
  macro apply EgressQoS
  channel-protocol lacp
  channel-group 10 mode active
!
interface port-channel 10
  switchport trunk encapsulation dot1q
  switchport trunk allowed 10,20,30
  switchport trunk native vlan 999
  switchport mode trunk
```

Layer 3 connectivity for access layer

LAN distribution layer

- Configure Layer 3 for access layer VLANs
  - Configure a VLAN interface(SVI) for every access layer VLAN
  - SVI is the IP default gateway for the access layer hosts in the VLAN
- Configure ip-helper address on each SVI
  - IP helper forwards DHCP requests from hosts in the VLAN to the DHCP server
  - IP helper-address points to the DHCP server for the VLAN
  - If more than one DHCP server, you can list multiple ip-helper commands
- Configure ip pim sparse-mode
  - Enables IP multicast packets to flow to hosts on the VLAN




```
interface vlan [number]
  ip address [ip address] [mask]
  ip helper-address  10.2.2.1
  ip pim sparse-mode
```

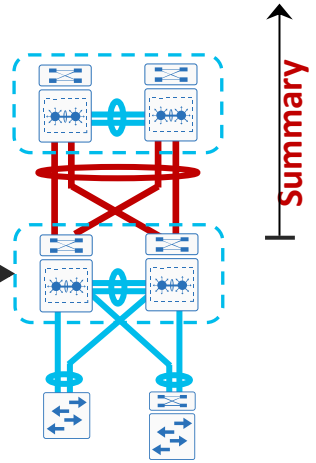
Layer 3 connectivity to core layer – EIGRP routing configuration

LAN distribution layer

- Enable authentication of neighbor routing protocol communication on interface to the core

```
key chain EIGRP-KEY
 key 1
  key-string [KEY STRING]
!
router eigrp [NAME]
  address-family ipv4 unicast autonomous-
system [AS]
    af-interface port-channel 20
      authentication mode md5
      authentication key-chain EIGRP-KEY
      no passive-interface
      summary-address [network] [mask]
    exit-af-interface
  exit-address-family
```

- Enable EIGRP for the core-facing interface (disable passive-interface)



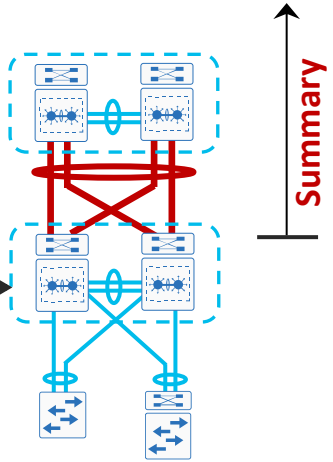
- As networks grow, IP address summarization is used
  - To reduce bandwidth required for routing updates
  - To reduce convergence time around a link failure
  - Summarize all subnets in the distribution layer to the rest of the network

Layer 3 connectivity to core layer – OSPF routing configuration

LAN distribution layer

- Enable authentication of neighbor routing protocol communication on interface to the core

```
interface Port-channel 20
 ip ospf message-digest-key [key id] md5 [key]
!
router ospf 100
 area 0 authentication message-digest
 area [area number] range [address range] [mask]
 no passive-interface Port-channel 20
```

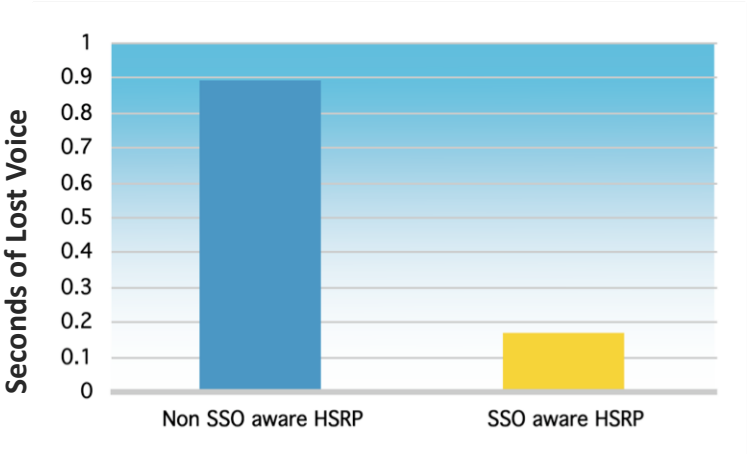


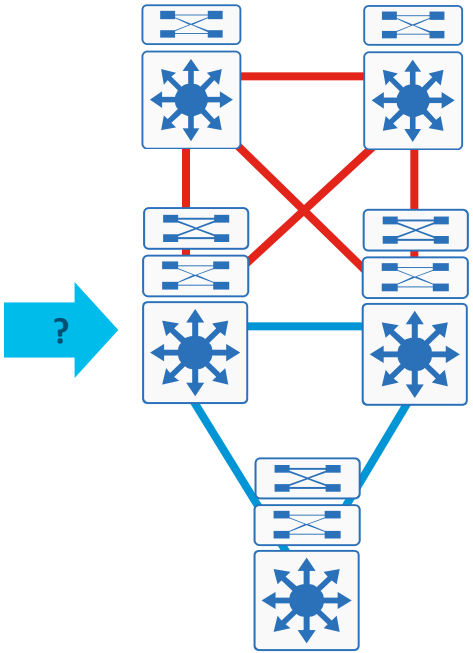
- Enable OSPF for the core-facing interface (disable passive-interface)
- As networks grow, IP address summarization is used
  - To reduce bandwidth required for routing updates
  - To reduce convergence time around a link failure
  - The OSPF area range command allows you to summarize all subnets in the distribution layer to the rest of the network

Chassis Redundancy at the Distribution

Recommended

- HSRP doesn't flap on Supervisor SSO switchover
- Reduces the need for sub-second HSRP timers



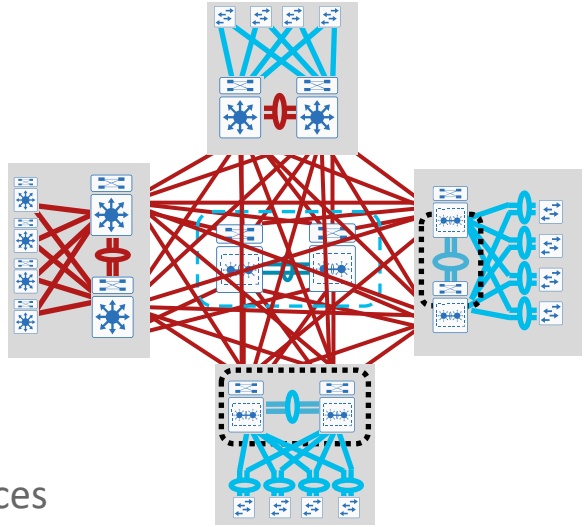


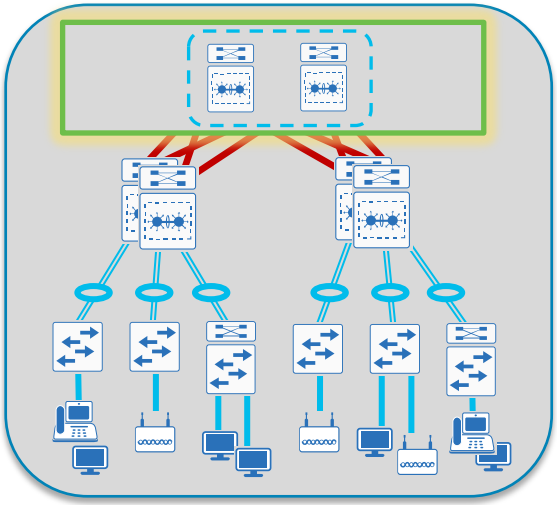
Core layer attributes

LAN core layer

- Primary function is distribution layer aggregation for large or geographically dispersed LAN deployment
- Lowers the complexity and cost of a fully meshed distribution layer

Do I need a core layer?



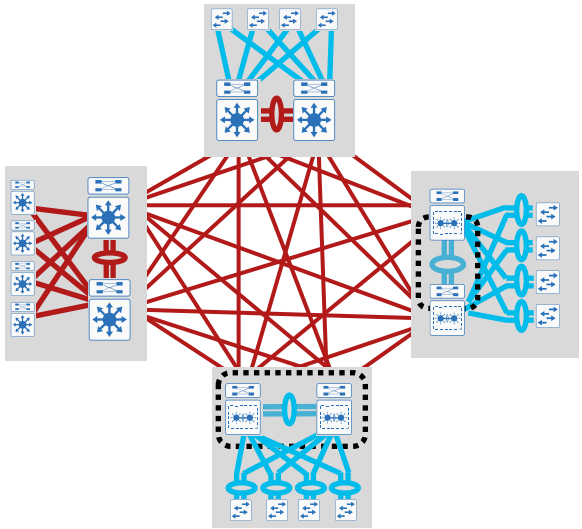


- Must be highly resilient
  – no single points of failure in design
- No high touch/high complexity services
  - Avoid constant tuning or configuration changes
- Layer 3 transport
  - No spanning tree convergence or blocking

Hierarchical network design: Campus wired LAN

Do I really need a core layer?

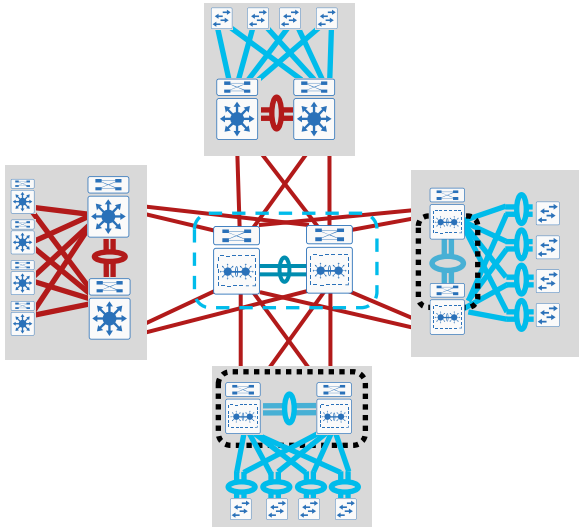
- It is a question of operational complexity and a question of scale
  - n x (n-1) scaling for redundant distribution layer
  - Routing peers
  - Fiber, line cards, and port counts ($,€,£)



Hierarchical network design: Campus wired LAN

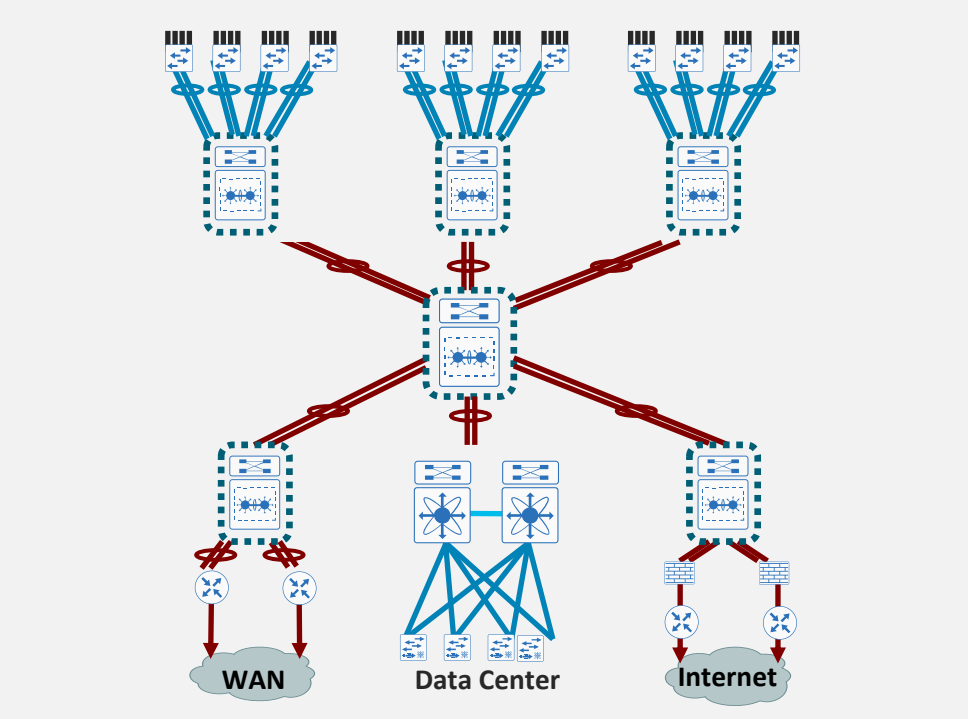
Do I really need a core layer?

- It is a question of operational complexity and a question of scale
  - n x (n-1) scaling
  - Routing peers
  - Fiber, line cards, and port counts ($,€,£)
- Capacity planning considerations
  - Easier to track traffic flows from a block to the common core than to ‘n’ other blocks
- Geographic factors may also influence the design
  - Multi-building interconnections may have fiber limitations



StackWise Virtual-enabled campus core design

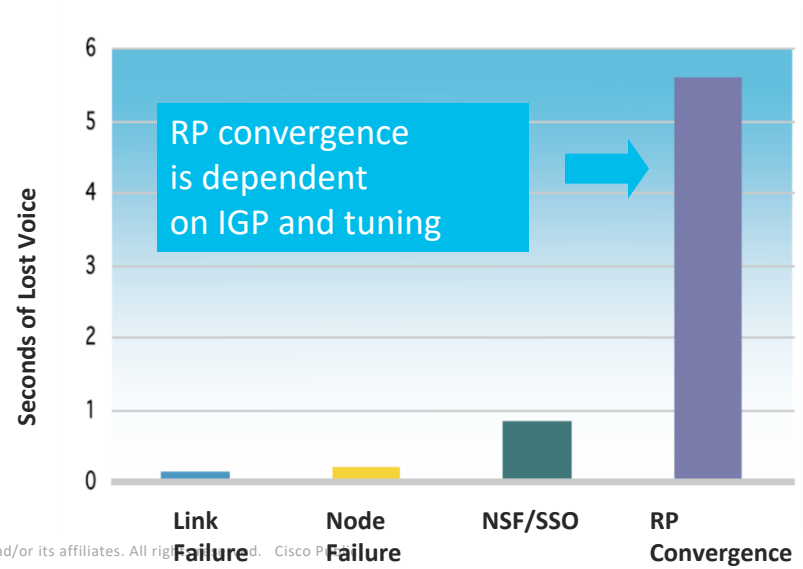
- Extend StackWise Virtual architectural benefits to campus core layer network
- SWV-enabled core increases capacity, optimizes network topologies and simplifies system operations
- Key SWV-enabled core best practices :
  - Protect network availability and capacity with NSF/SSO
  - Simplify network topology and routing database with single MEC
  - Leverage self-engineer SWV and MEC capabilities for deterministic network fault detection and recovery

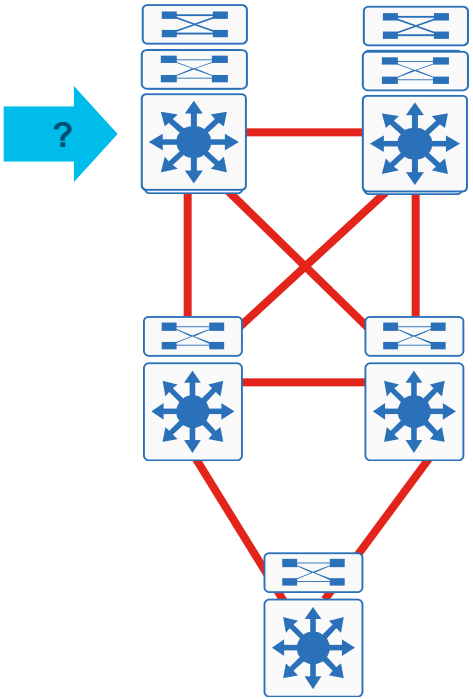


Chassis Redundancy at the Core

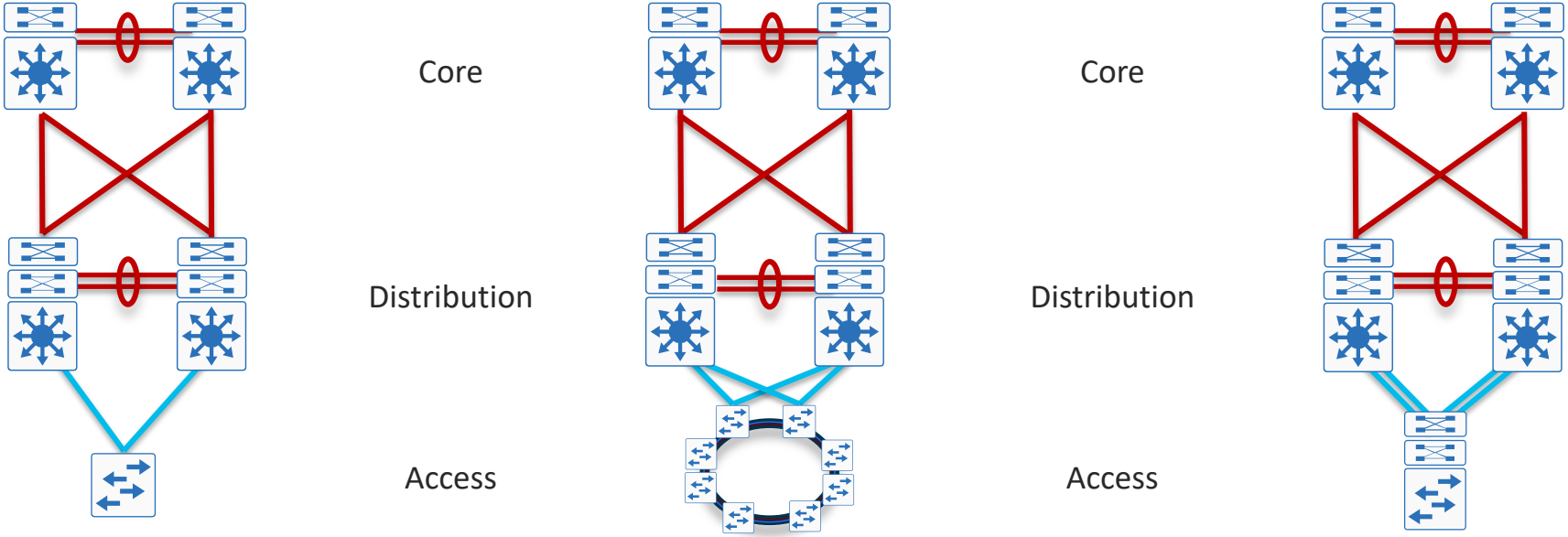
Depends on topology

- Redundant topologies with equal cost multi-paths (ECMP) provide sub-second convergence
- NSF/SSO provides superior availability in environments with non-redundant paths





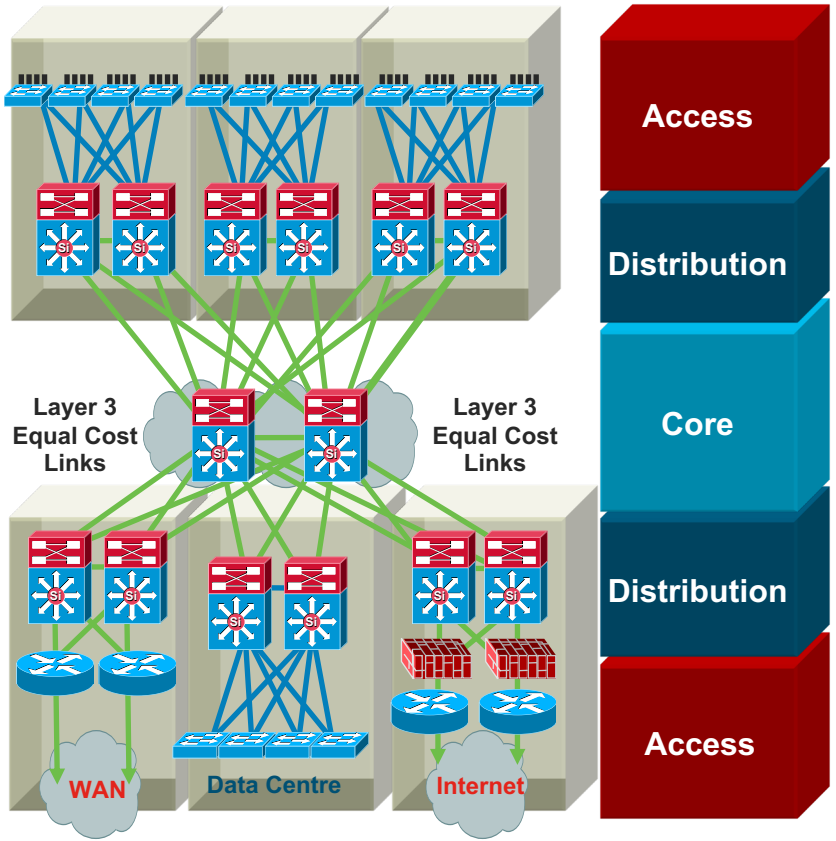
Structured campus network design



- Optimize data load-sharing, redundancy design for best application performance
  - Diversify uplink network paths with cross-stack and dual-sup access-layer switches
  - Build distributed and full-mesh network paths between Distribution and Access-layer switches

Summary

- 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

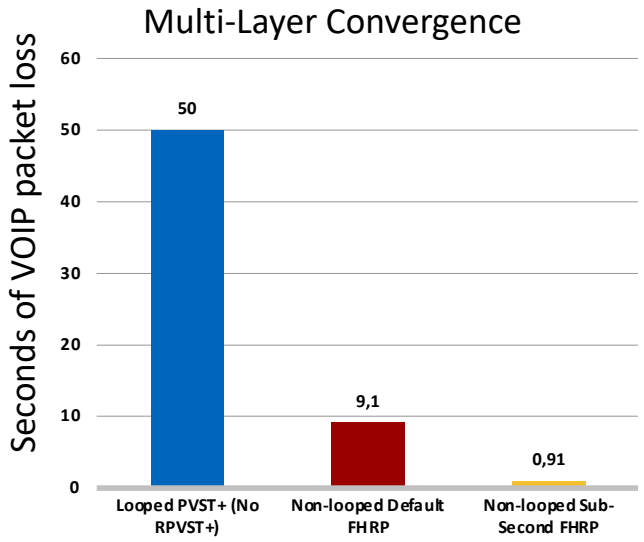


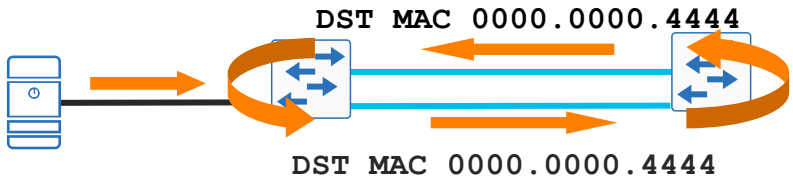
References

- Design Zone https://cisco.com/go/cvd/campus
- Cisco Community https://cs.co/en-cvds
- CiscoLive materials
  - Introduction to Campus Wired LAN Deployment Using Cisco Validated Designs https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-1500.pdf
  - Enterprise Campus Design: Multilayer Architectures and Design Principles https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2031.pdf
  - Designing for High Availability Switching and Wireless in Your Campus LAN – techtorial (460+ slides) https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/TECCRS-2001.pdf

Multilayer campus network design— It is a good solid design, but…

- Utilizes multiple control protocols
  - Spanning tree (802.1w), HSRP / GLBP, EIGRP, OSPF
- Convergence is dependent on multiple factors –
  - FHRP – 900msec to 9 seconds
  - Spanning tree – Up to 50 seconds
- Load balancing –
  - Asymmetric forwarding
  - HSRP / VRRP – per subnet
  - GLBP – per host
- Unicast flooding in looped design
- STP, if it breaks badly, has no inherent mechanism to stop the loop





Thank you

www.cisco.com/go/cvd