LET'S
BUILD
TOMORROW
TODAY

Wired LAN Deployment Using the Cisco Validated Design for Campus

Dana Daum, CCIE 5060, Communications Architect, EISG

BRKCRS-1500

Cisco live!

Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

Abstract

Wired LAN Deployment Using the Cisco Validated Design for Campus

This session discusses LAN design and deployment best practices covered in the Campus Wired LAN Technology Design Guide - a Cisco Validated Design (CVD). LAN deployments from single switch remote sites to large multi-building campuses are detailed. Cisco Validated Design offers a framework for design guidance based on common use cases, along with technology design guides focusing on deployment details, including products and best practices, accelerating the adoption of technology. The session discusses the consistent enablement of capabilities such as high availability, quality of service, multicast, and security across a range of Cisco LAN platforms. Also included are the decision criteria that can help an organization choose between platforms. The cornerstones of the approach and techniques discussed in this session are real-world use cases, prescriptive design guidance, and modular architectural components. Although not required to register for this session, attendees for this session will benefit from an understanding of LAN switching and routing fundamentals equivalent to a CCNA level.

Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

The Challenge

I want to design and deploy a network….

How can I anticipate what the network might need to do in the future so I don't have to revisit my design and deployment?

How can I do it quickly?

How do I manage it?

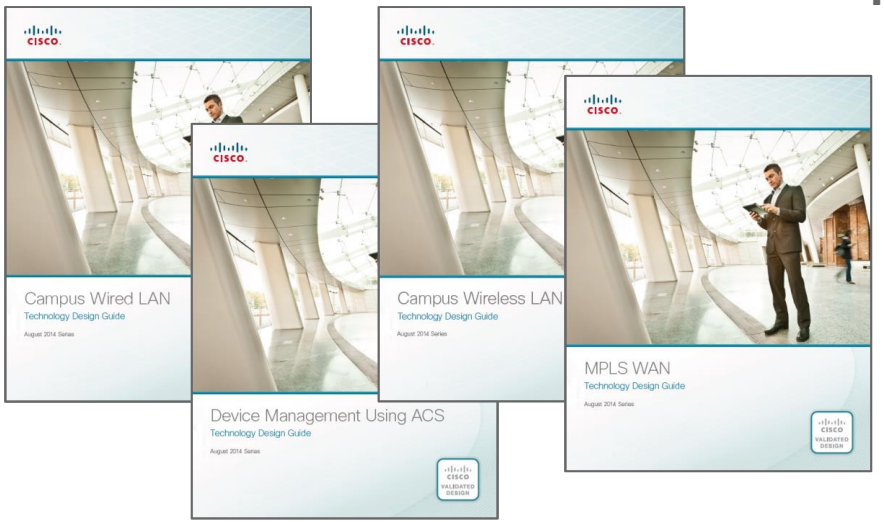
How do I put it all together?

Which platform should I choose?

Many to choose from at each place in the network

What are the best practices?

The Cisco Validated Design – provides a framework for design and deployment guidance based on common use cases.



Inside the Technology Design Guides

- CVD Navigator
- Use Cases
- Design Overview
- Deployment Details
- Product and Software Versions
- Configuration Files Appendix

The Cisco Design Zone

Technology/Solution Design Guides

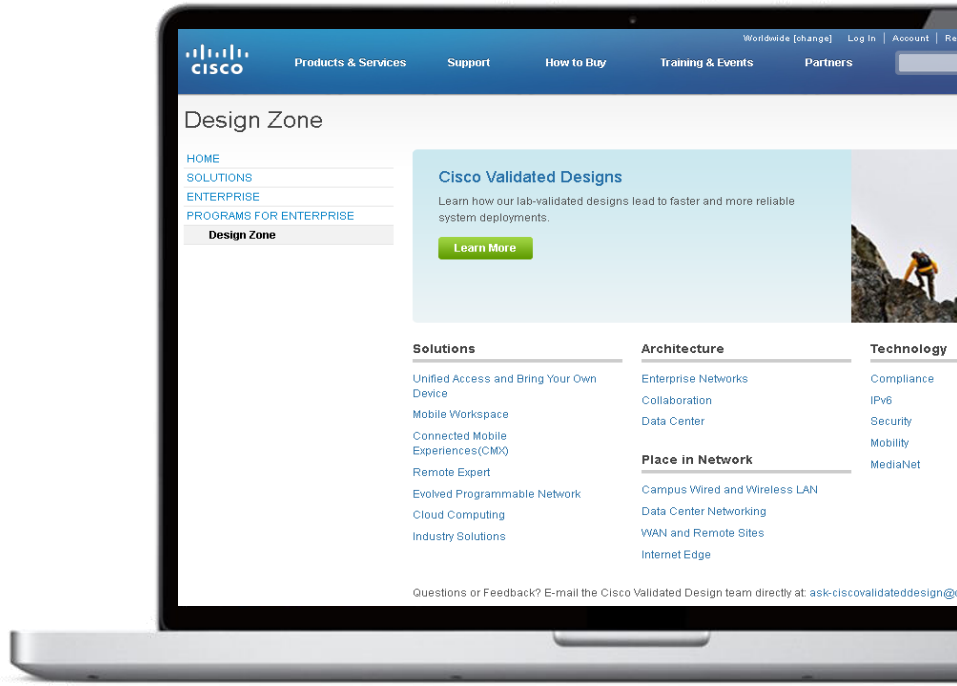
Overview Documents

At-a-Glance Documents

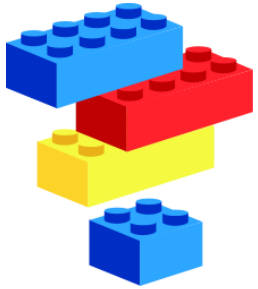
Business Presentations

www.cisco.com/go/cvd

www.cisco.com/go/cvd/campus



LAN Deployment Principles



Ease of Deployment

Flexibility and Scalability

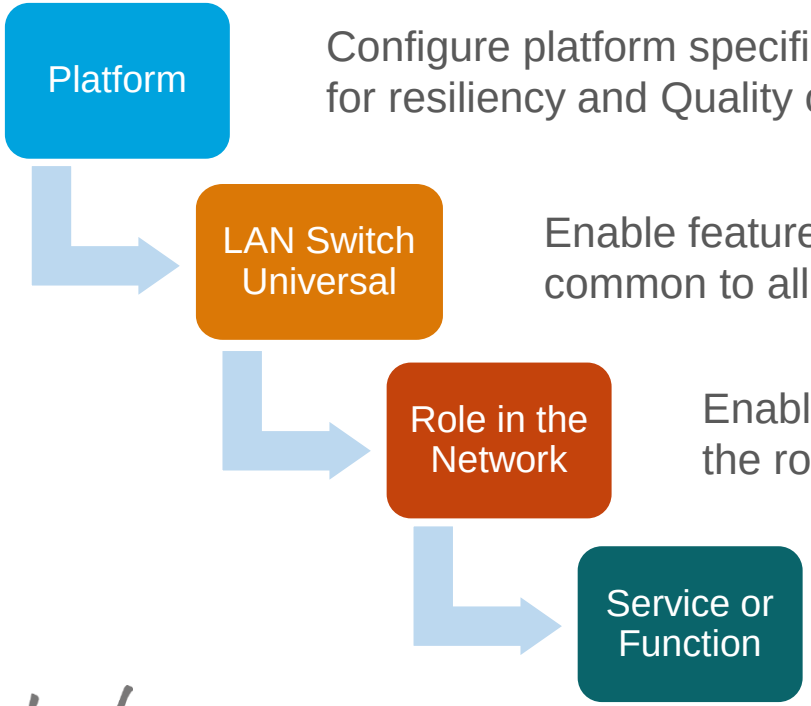
Easy to Manage

Resiliency and Security

Advanced Technology Ready

Deployment Process Flow Chart

- Each layer follows the same process

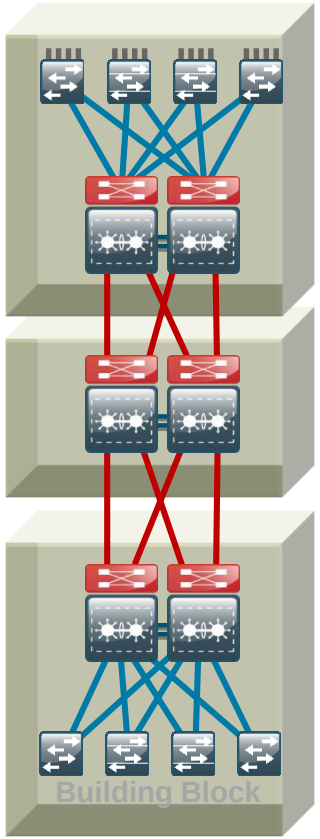


Hierarchical Network Design

- 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 resilience

.....

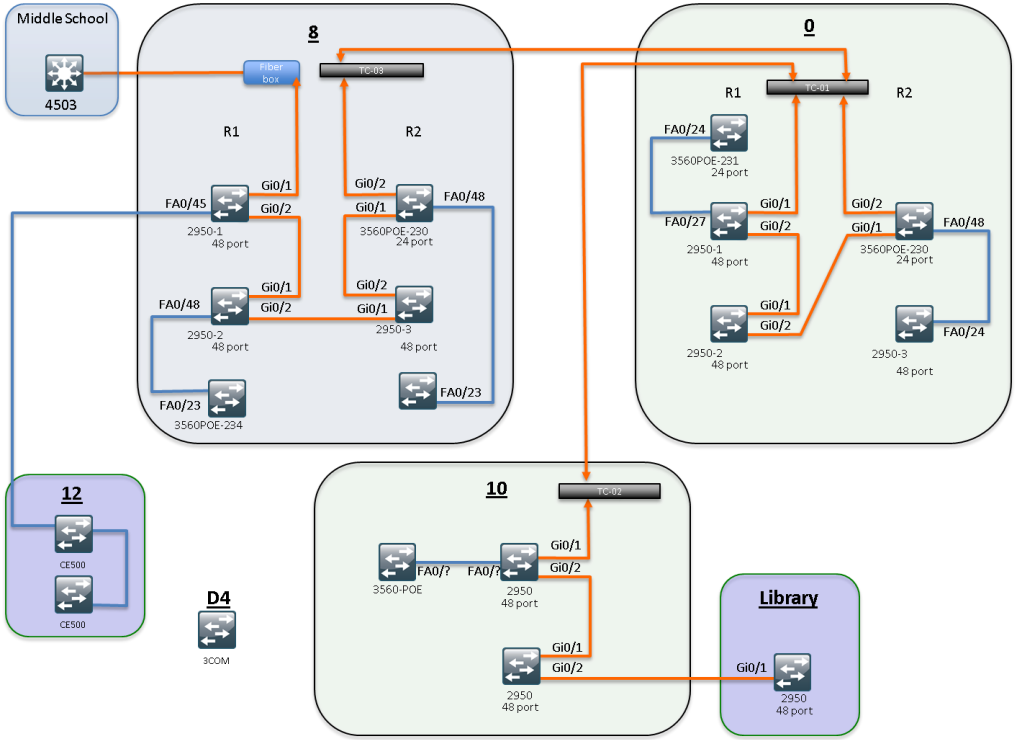
Also maps well to our session agenda!



What We are Trying to Avoid!

No hierarchy

Multiple single points of failure



Hard to troubleshoot

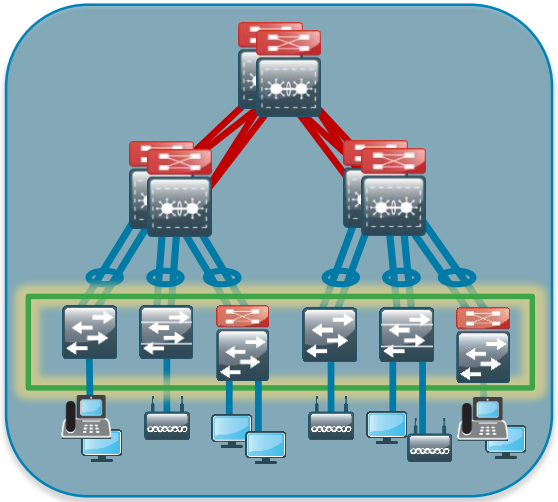
Poor performance

Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Client facing interfaces
  - Uplinks to Distribution Layer
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

Access Layer Attributes

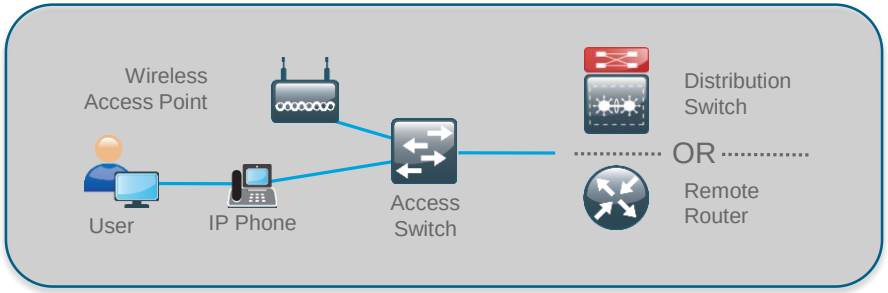
New Access Options Coming with mGig!



- Ethernet network access
  - Wired 10/100/1000
  - Wireless 802.11a/b/g/n/ac
- 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) – 60watts 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.

Access Layer Platform Options

Catalyst 4500-E with Supervisor 8-E / 7L-E

- Modular switch with 1:1 redundancy for all critical systems (supervisors, power supplies, fans)
- Stateful switchover provides subsecond supervisor recovery
- Multiple Ethernet Connectivity options (fiber or copper with various densities)
- In-Service Software Upgrades
- PoE, PoE+, and UPOE
- Energy Efficient Ethernet
- Sup8-E - Future WLAN

Catalyst 3850 and Catalyst 3650

- Fixed configuration stackable switch with central config and control
- Stateful switchover provides subsecond recovery
- Modular Uplinks (3850), power supplies, and fans
- StackWise480 and StackPower (3850), StackWise160 (3650)
- Up to 9 switches in a stack
- PoE, PoE+, UPOE
- UADP – Wireless Capable

Catalyst 2960-X

- Fixed configuration stackable switch with central config and control
- Up to 8 switches in a stack
- FlexStack+ 80G stacking (Stack Module Required)
- Stack or stack member failure recovery max 1 -2 seconds
- PoE and PoE+

Option available - see BRKCRS-3502
Advanced Enterprise Campus Design: Instant Access

Agenda

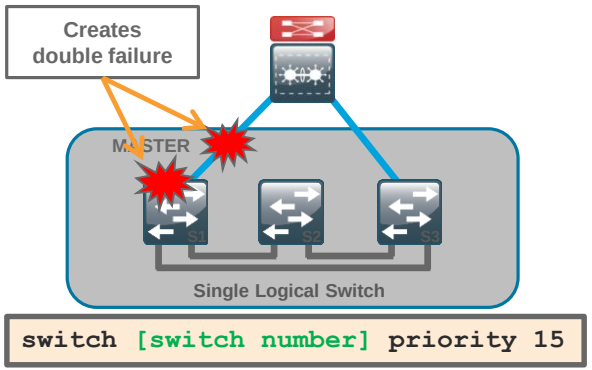
- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Client facing interfaces
  - Uplinks to Distribution Layer
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

Catalyst 2960-X Resiliency

Platform Specific Configuration

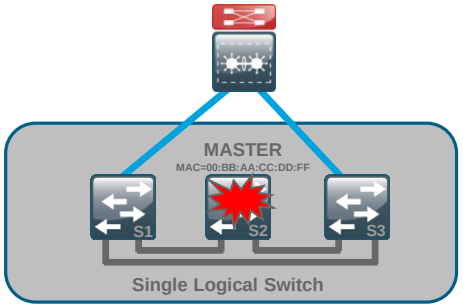
- Stack Master provides central control over multiple Catalyst 3750 or 2960 Series switches configured in a stack
- To increase resiliency in a 2960 stack of three or more switches:

Configure the Stack Master on a switch that does not have uplinks configured




```
switch [switch number] priority 15
```

Ensure that the original Stack Master MAC address remains the stack MAC address after a failure to prevent protocol restart




```
stack-mac persistent timer 0
```

Catalyst 4500 and 3850/3650 Resiliency
– Stateful Switchover

Platform Specific Configuration

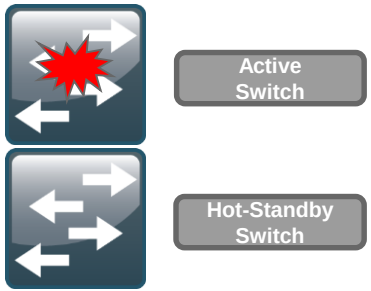
When a 4500 has two supervisors installed for resiliency, Stateful Switchover (SSO) should be configured – minimizes traffic loss when the primary supervisors has a failure.

SSO is the default configuration for Catalyst 3850 and Catalyst 3650 with at least two members in a stack.

Stateful Switchover

Catalyst 4500

Catalyst 3850/3650



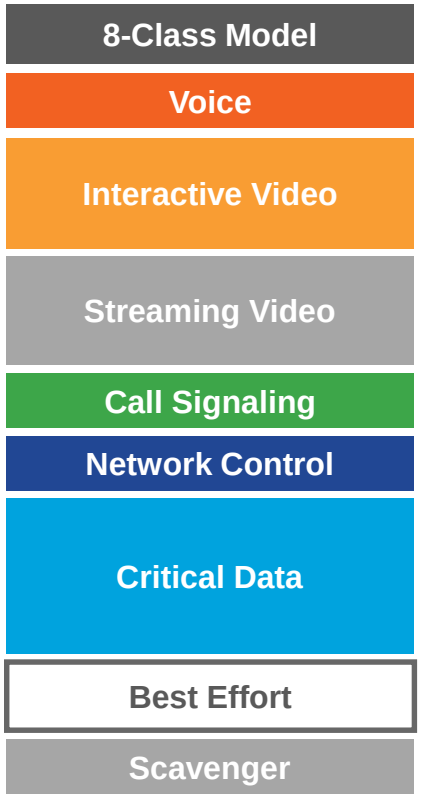

```
A4507R(config)#redundancy
A4507R(config-red)# mode sso
^C
A4507R#show redundancy state
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 3

Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured)  = Stateful Switchover
Redundancy State              = Stateful Switchover
    Manual Swact = enabled
 Communications = Up
```

Note: Catalyst 4500 SSO operation requires ipbase or enterprise services license level

Cisco live!

Quality of Service Overview



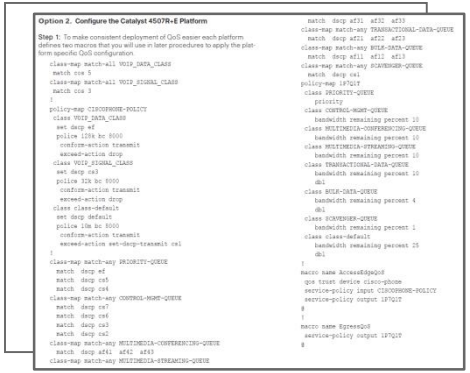
- 8-Class Model is used as the standard in the LAN
- Conditional-Trust model used as the standard model of QoS deployment
- Platform specific QoS configurations to achieve the 8-class model are mapped to common macro names for easy deployment
- AutoQoS is used where possible in the platform configuration process

QoS SRND 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1100873

Quality of Service Deployment

Macros Ease the Deployment Process

Platform Specific Quality of Service Commands



Option 2. Configure the Catalyst 4507R-E Platform

Step 1: To make consistent deployment of QoS easier each platform defines two macros that you will use in later procedures to apply the platform specific QoS configuration.

```
class-map match-all VOIP_DATA_CLASS
 match cos 5
class-map match-all VOIP_SIGNAL_CLASS
 match cos 3
!
policy-map CISCOPHONE-POLICY
 class VOIP_DATA_CLASS
  set dscp ef
  police 128k bc 8000
   conform-action transmit
   exceed-action drop
 class VOIP_SIGNAL_CLASS
  set dscp cs3
  police 32k bc 8000
   conform-action transmit
   exceed-action drop
 class class-default
  set dscp default
  police 10m bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit cs1
!
class-map match-any PRIORITY-QUEUE
 match  dscp ef
 match  dscp cs5
 match  dscp cs4
class-map match-any CONTROL-MGMT-QUEUE
 match  dscp cs7
 match  dscp cs6
 match  dscp cs3
 match  dscp cs2
class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
 match  dscp af41  af42  af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
 match  dscp af31  af32  af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
 match  dscp af21  af22  af23
class-map match-any BULK-DATA-QUEUE
 match  dscp af11  af12  af13
class-map match-any SCAVENGER-QUEUE
 match  dscp cs1
policy-map 1P7Q1T
 class PRIORITY-QUEUE
  priority
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 10
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  dbl
 class BULK-DATA-QUEUE
  bandwidth remaining percent 4
  dbl
 class SCAVENGER-QUEUE
  bandwidth remaining percent 1
 class class-default
  bandwidth remaining percent 25
  dbl
!
macro name AccessEdgeQoS
 qos trust device cisco-phone
 service-policy input CISCOPHONE-POLICY
 service-policy output 1P7Q1T
@
!
macro name EgressQoS
 service-policy output 1P7Q1T
@
```

Macros Used Later in the Deployment Process

1. AccessEdgeQoS Macro
   Applied on all client facing interfaces
2. EgressQoS Macro
   Applied on all other interfaces

Complex → Simplified

Using Macros to Deploy Quality of Service…

- Removes the platform specific QoS configuration from the day to day repetitive configuration tasks
- Eases the deployment process and allows for easier creation of deployment templates

Initial Configuration Defines Macros and Platform-specific Global Settings

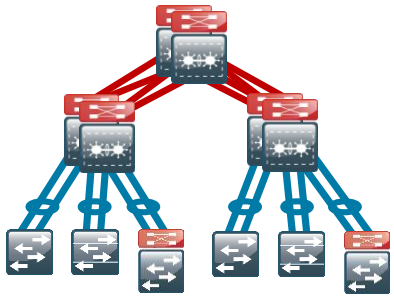
Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Client facing interfaces
  - Uplinks to Distribution Layer
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

Resiliency Features for LAN Switches

Global LAN Switch Configuration

- Rapid PVST+ – improved topology change detection over classic STP Layer 2 loop detection
- BPDUguard default – detect spanning tree BPDUs on portfast-enabled ports for L2 loop prevention
- UDLD – detect and protect against unidirectional links caused by incorrect physical interconnects that can cause spanning tree loops
- Error disable recovery – allows recovery without intervention of automatically disabled ports, post-event
- VTP transparent – ignore VTP updates to avoid accidental outages from unplanned VLAN changes
- Load-Interval – reduce time to compute interface load for better visibility to traffic bursts



Protection across the LAN

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
udld enable
errdisable recovery cause all
vtp mode transparent
load-interval 30
```


Enabling Device Management

Global LAN Switch Configuration

Enable secure management of ALL LAN devices

- Enabled through encrypted protocols SSH, HTTPS, and SCP
- Less secure protocols, Telnet and HTTP, should be turned off

```
ip domain-name cisco.local
no ip http server
ip http secure-server
ip ssh version 2
ip scp server enable
line vty 0 15
  transport input ssh
  transport preferred none
```

SSH requires domain-name
Disables HTTP
Enables HTTPS and creates default modulus Crypto Key
Enables Secure Copy for file management
Enables SSH ONLY on IP access to console
Eliminate annoying long wait for mistyped commands

Use SNMP to manage network devices by a Network Management System.

– SNMP(v2c) should be configured for both a read-only and a read-write community string.

```
snmp-server community [SNMP RO] RO
snmp-server community [SNMP RW] RW
```

Optionally, secure vty and SNMP access

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community [SNMP RO] RO 55
snmp-server community [SNMP RW] RW 55
```

Device Management Authentication

Global LAN Switch Configuration

- Management access to the network infrastructure devices (SSH and HTTPS) should be controlled with AAA.
  - Centralized and easy control of password expiration; Ability to rapidly revoke access for employee departure
- TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server.
- A local AAA user database defined on each network infrastructure device to provide a fallback authentication source

New Method

```
enable secret [enable password]
service password-encryption
!
username admin secret [admin password]
aaa new-model
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key [tacacs key]
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Local username and password for fallback

Define tacacs+ server and secret key

Use tacacs+ first, fallback to local

Traditional Method

```
enable secret [enable password]
service password-encryption
!
username admin password [admin password]
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization console
ip http authentication aaa
tacacs-server host 10.4.48.15 key [tacacs key]
```

Synchronize the Clock on All Devices

Global LAN Switch Configuration

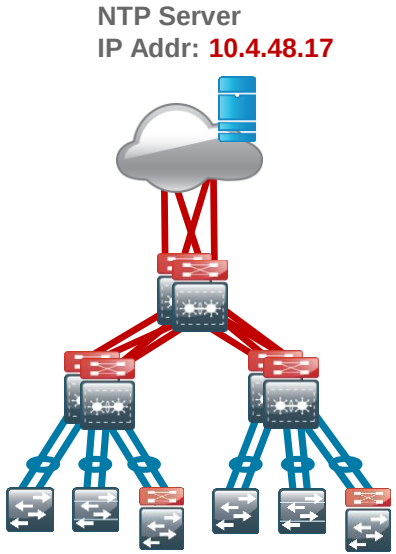
- Troubleshooting a network event requires correlation across multiple devices (switches and routers)
- Network devices should be programmed to synchronize time to a local NTP server in the network.
  - allows event log timestamps from multiple devices to be correlated
- Configure console messages, logs, and debug output to provide time stamps

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Update hardware clock on Catalyst 6500 and 4500

Set local timezone, offset from UTC

Timestamp output with local NTP synchronized time



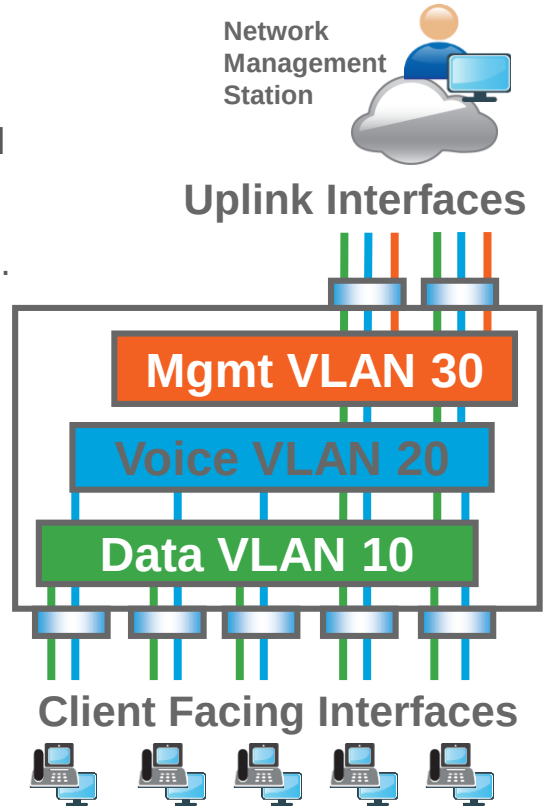
Access Layer Virtual LANs

Access Switch Configuration

- The **Data VLAN** provides access to the network for all attached devices other than IP Phones.
- The **Voice VLAN** provides access to the network for IP Phones.
- The **Management VLAN** provides in-band access to the network for the switches management interface.

```
vlan 10
  name Data
vlan 20
  name Voice
vlan 30
  name Management
```

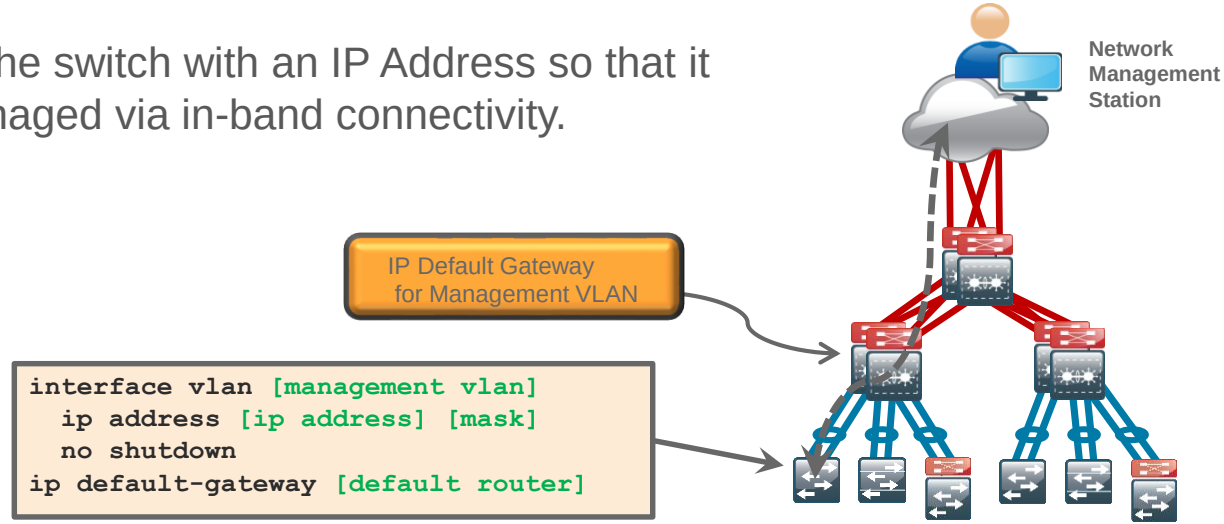
Note: The management VLAN is never configured on user facing interfaces



In-Band Management

Access Switch Configuration

Configure the switch with an IP Address so that it can be managed via in-band connectivity.



Note: Do not use the **ip default-gateway** command on the Catalyst 4500 since it has ip routing enabled by default and the “ip default-gateway” command will not have any effect.

Instead use the following command on the Catalyst 4500.

```
ip route 0.0.0.0 0.0.0.0 [default router]
```

Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Client facing interfaces
  - Uplinks to Distribution Layer
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

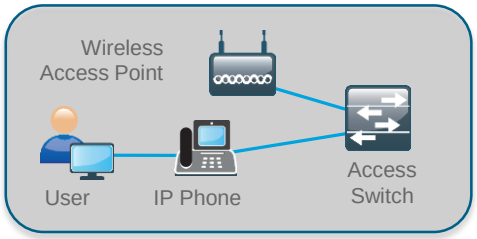
Client Facing Interfaces

Access Switch Configuration

The host interface configuration supports PCs, phones, or wireless access points.

- Use a single port profile for all access ports

```
interface range [interface type] [port number]-[port number]
  switchport access vlan [data vlan]
  switchport mode access
  switchport voice vlan [voice vlan]
```



- Apply configuration supporting end-user devices

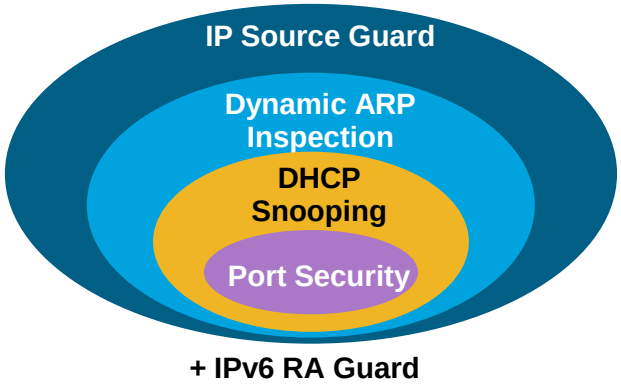
```
switchport host
```

This single command does the following:
- removes any channel-group configuration (incompatible with access mode)
- enables switchport access mode (disables trunk negotiation, enables VLAN participation)
- enables PortFast (moves interface directly into spanning-tree forwarding mode for faster connect time)

- To enable QoS, use the configured Macro:

```
macro apply AccessEdgeQoS
```

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

Port Security

Client Facing Interface Configuration

Protect your switch from CAM table overflow attacks.

Client

Advertises MAC

00:10:10:10:10:10
00:10:10:10:10:11
00:10:10:10:10:12
00:10:10:10:10:13
00:10:10:10:10:14
00:10:10:10:10:15
00:10:10:10:10:16
00:10:10:10:10:17
00:10:10:10:10:18
00:10:10:10:10:19
00:10:10:10:10:1A
00:10:10:10:10:1B

Configure on the client interface:

```
switchport port-security
switchport port-security maximum 11
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security violation restrict
```

Exceeds Maximum

DHCP Snooping

Client Facing Interface Configuration

Example DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Configure in the global configuration:

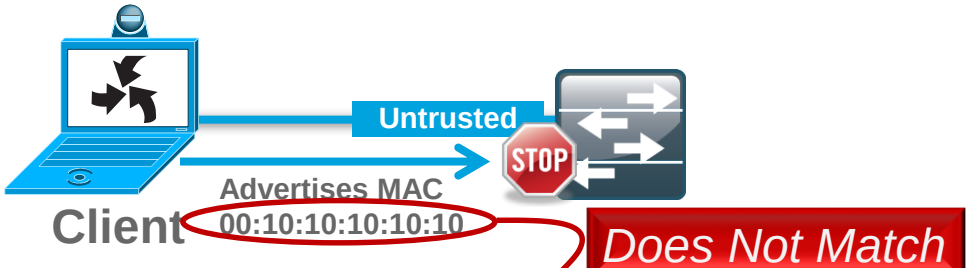
```
ip dhcp snooping vlan [data vlan], [voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

Configure on the client interface:

```
ip dhcp snooping limit rate 100
```

ARP Inspection

Client Facing Interface Configuration



Example DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Configure in the global configuration:

```
ip arp inspection vlan [data vlan], [voice vlan]
```

Configure on the client interface:

```
ip arp inspection limit rate 100
```

IP Source Guard

Client Facing Interface Configuration

Example DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Configure on the client interface:

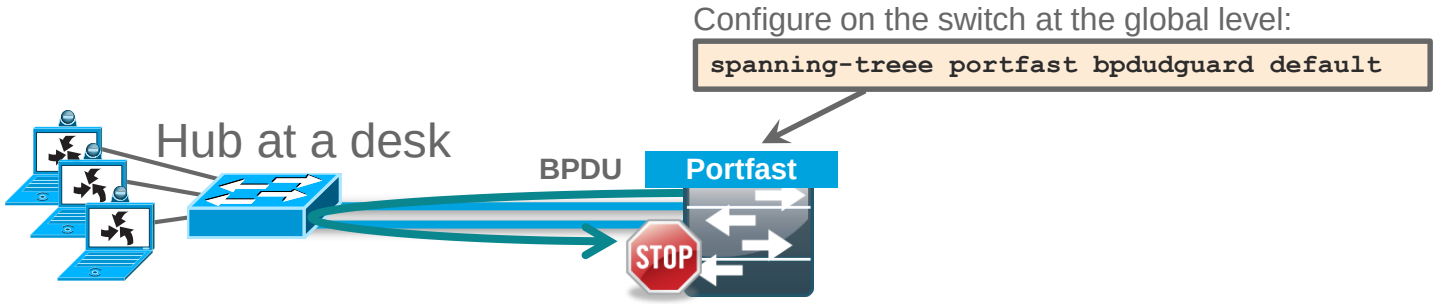
```
ip verify source
```

On the Catalyst 4500 configure on the interface:

```
ip verify source vlan dhcp-snooping
```

BPDU Guard

Client Facing Interface Configuration



- If a portfast configured interface receives a BPDU, an invalid configuration exists, such as the connection of an unauthorized device.
- BPDU guard prevents loops by moving a nontrunking interface into an errdisable state when a BPDU is received on an interface when portfast is enabled.

IPv6 Router Advertisement Guard

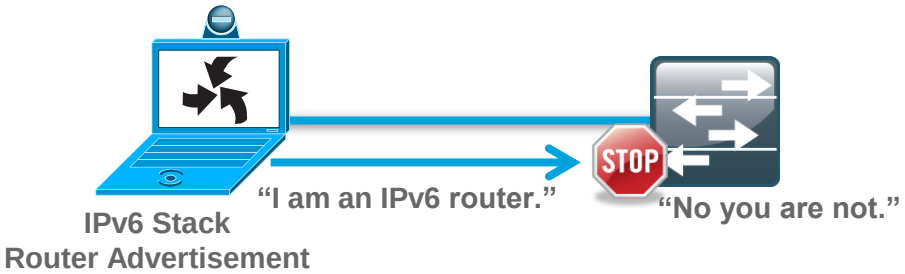
Client Facing Interface Configuration

Define policy in the global configuration:

```
ipv6 nd raguard policy HOST_POLICY
  device-role host
```

Attach policy configuration to the client interface:

```
ipv6 nd raguard attach-policy HOST_POLICY
```



- If a port device role is configured as host, IPv6 First Hop Security (FHS) RA Guard drops all IPv6 Router Advertisement messages
- Useful even for IPv4-only networks
- Other port device role options include: monitor, router, and switch

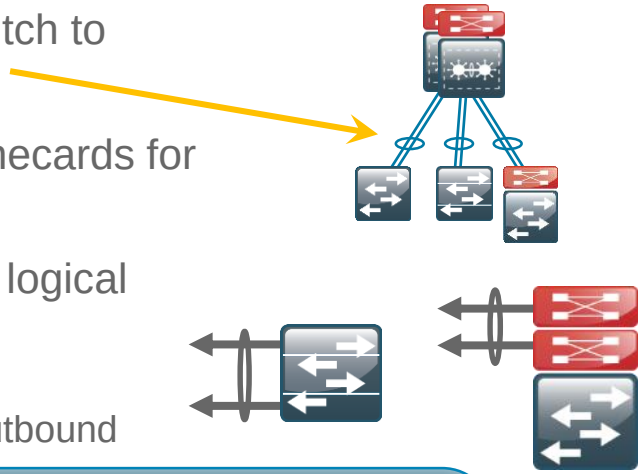
Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Client facing interfaces
  - Uplinks to Distribution Layer
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

EtherChannel Member Interfaces

Uplink Interface Configuration

- Layer 2 EtherChannels are used to interconnect the switch to upstream devices.
- Member interfaces should be on different switches or linecards for resiliency.
- Configure the physical interfaces before configuring the logical portchannel interface.
  - Uses LACP for EtherChannel protocol
  - Add Egress QoS macro for trust inbound traffic and queue outbound



```
interface range [type] [port], [type] [port]
  switchport
  channel-protocol lacp
  channel-group 10 mode active
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Note: ISR routers do not support LACP. Therefore, when connecting a remote site access switch to an ISR router with an EtherChannel you must configure the switch with mode forced on.

```
interface range [type] [port], [type] [port]
  switchport
  channel-group 10 mode on
  macro apply EgressQoS
```

Trunk Configuration

Uplink Interface Configuration

- When using EtherChannel the interface type will be port-channel and the number must match channel-group configured on the previous slide.

```
interface port-channel 10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [data],[voice],[mgmt]
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
 logging event link-status
 no shutdown
```

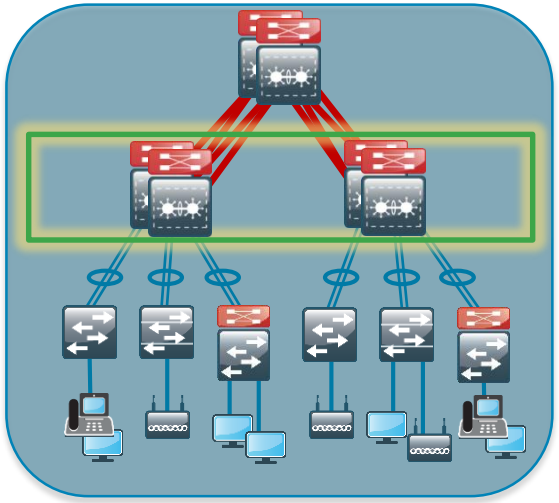
- An 802.1Q trunk is used for the connection to the upstream device
  - Allows upstream device to provide the Layer 3 services to all the VLANs defined on the access layer switch.
  - VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch.
  - DHCP Snooping and ARP Inspection are set to trust.

Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Connectivity to Access and Core Layers
- Core Layer Deployment
- Conclusion

Campus LAN Distribution Layer Attributes

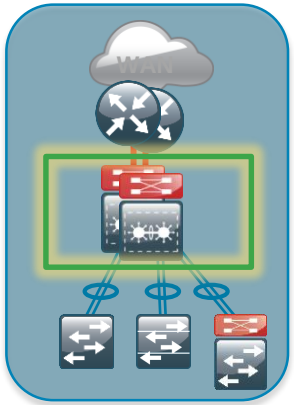
- Primary function is access layer aggregation for a building or geographic area.
- Resilient design to reduce failure impact
- Layer 2 boundary for access layer
  - Spanning Tree Protocol boundary
  - Broadcast packet boundary
  - Provides load balancing to access layer
- Layer 3 features and functions
  - 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



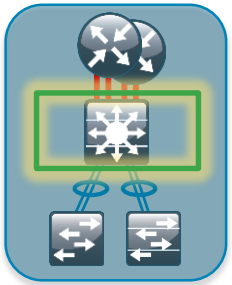
Alternative Distribution Layer Attributes

LAN Distribution Layer

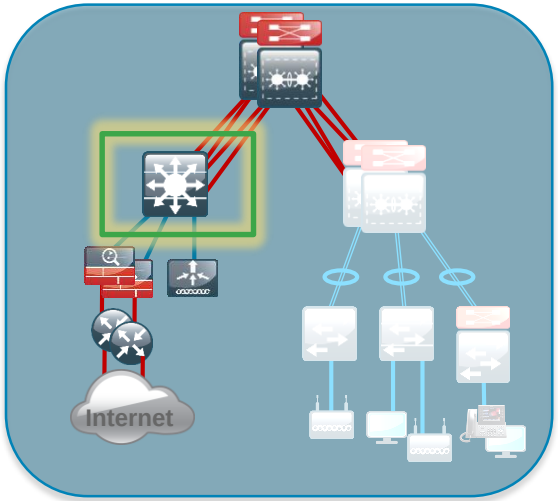
- Collapsed Core: Two tier main campus LAN and WAN Core
  - LAN Access Layer aggregation
  - Central connect point for all services



- Two tier remote site:
  - Aggregates LAN Access Layer and connects to WAN routers



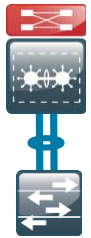
- Large LAN Services Block
  - Connection point for services
  - Drives modular building block design

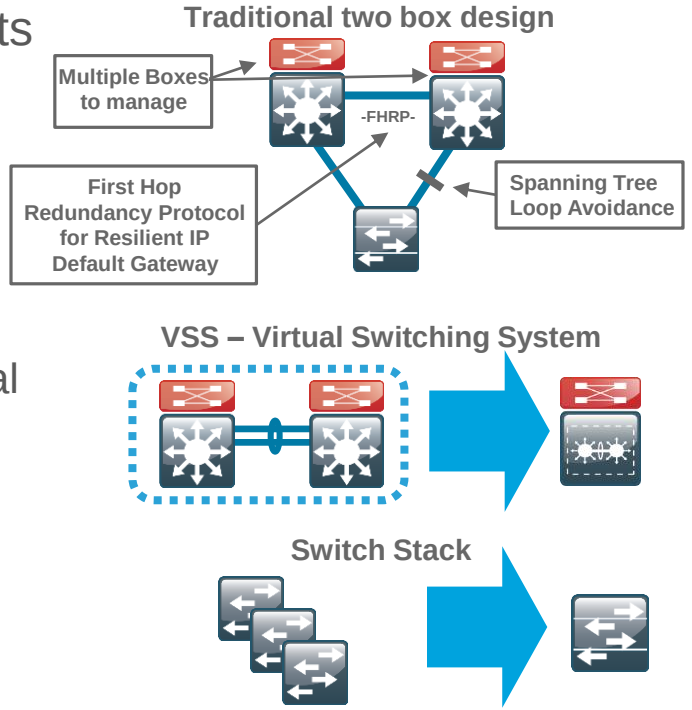


Simplified Distribution Layer Design

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 (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



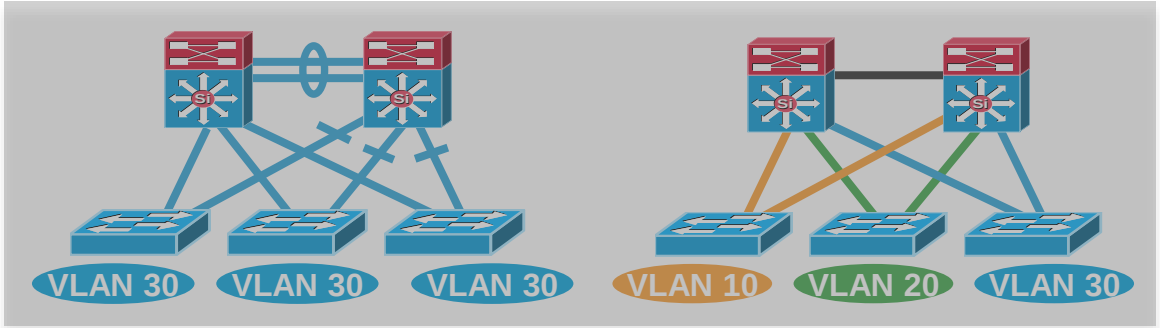


Traditional Design Compared to Simplified Design

LAN Distribution Layer

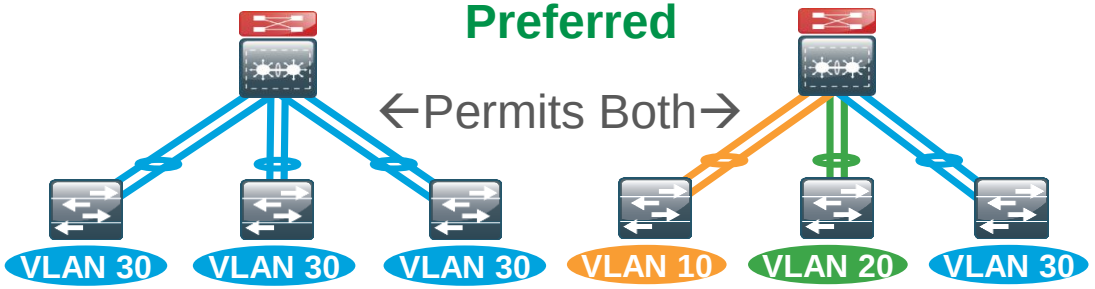
Traditional designs:

- 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:

- Uses EtherChannel for resilient links with all links forwarding
- No need for FHRP, acts as a 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 enabled for edge protection (RPVST+)



Cisco live!

Distribution Layer Platform Options

Guide with Sup8-E Distribution in Planning

Density, Resilience, Throughput, Scalability, Reduced failover times

Catalyst 6500/6807 Supervisor 2T (VSS)

- Physically separate and resilient supervisors, line cards, and power supplies
- Clusters two physical chassis into a single logical entity
- Highest density Gigabit and 10 Gigabit Ethernet
- 40 Gigabit Ethernet
- Stateful Switchover (SSO) + Quad-Supervisor SSO (VS4O) available option
- VSS and Multi-Chassis EtherChannel for highly resilient connectivity

Catalyst 6880-X (VSS)

- Extensible fixed base chassis, with resilient line card expansion and power supplies
- Clusters two physical chassis into a single logical entity
- Used to aggregate a smaller number of Gigabit or 10 Gigabit access layer switches
- Stateful Switchover between chassis
- Enhanced Fast Software Upgrade (eFSU) capable

Catalyst 4500-E Supervisor 7-E (VSS) Catalyst 4500-X (VSS)

- Physically separate chassis, line cards, and power supplies, with fixed/modular options
- Clusters two physical chassis into a single logical entity
- Used to aggregate a smaller number of Gigabit or 10 Gigabit access layer switches
- Stateful Switchover between chassis
- In Service Software Upgrades (ISSU)

Catalyst 3850-12S (Stack)

- Centralized stack configuration, control, and management plane
- Used to aggregate a smaller number of Gigabit access layer switches
- Distributed, per switch, Layer 2/Layer 3 forwarding, CAM tables, and BPDU processing
- UADP – Wireless Capable

One common approach to configuring and operating the Distribution Layer

Agenda

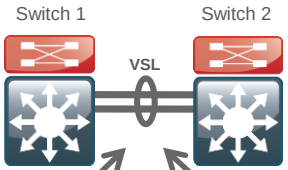
- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Connectivity to Access and Core Layers
- Core Layer Deployment
- Conclusion

Catalyst VSS Setup

LAN Distribution Layer

1) Prepare standalone switches for VSS

```
Router#conf t
Router(config)# hostname VSS-Sw1
VSS-Sw1(config)#switch virtual domain 100
VSS-Sw1(config-vs-domain)# switch 1
```



1) Prepare standalone switches for VSS

```
Router#conf t
Router#config)# hostname VSS-Sw2
VSS-Sw2(config)#switch virtual domain 100
VSS-Sw2(config-vs-domain)# switch 2
```

2) Configure Virtual Switch Link

```
VSS-Sw1(config)#interface port-channel 63
VSS-Sw1(config-if)#switch virtual link 1
VSS-Sw1(config)#interface range tengigabit 5/4-5
VSS-Sw1(config-if)#channel-group 63 mode on
VSS-Sw1(config-if)#no shutdown
```

2) Configure Virtual Switch Link

```
VSS-Sw2(config)#interface port-channel 64
VSS-Sw2(config-if)#switch virtual link 2
VSS-Sw2(config)#interface range tengigabit 5/4-5
VSS-Sw2(config-if)#channel-group 64 mode on
VSS-Sw2(config-if)#no shutdown
```

3) Validate Virtual Switch Link Operation

```
VSS-Sw1# show etherchannel 63 ports
            AND
VSS-Sw2# show etherchannel 64 ports
            Ports in the group:
            -------------------
Port: Te5/4   Port state    = Up Mstr In-Bndl
Port: Te5/5   Port state    = Up Mstr In-Bndl
```

Cisco live!

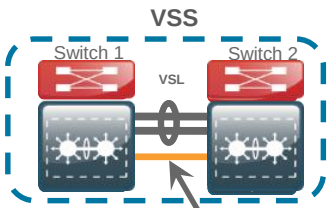
Catalyst VSS Setup

LAN Distribution Layer

4) Enable Virtual Mode Operation

VSS-Sw1# switch convert mode virtual
Do you want to proceed? (yes/no) yes

• The switch now renumbers from y/z to x/y/z
• When process is complete, save configuration when prompted, switch reloads and forms VSS.



4) Enable Virtual Mode Operation

VSS-Sw2# switch convert mode virtual
Do you want to proceed? (yes/no) yes

• The switch now renumbers from y/z to x/y/z
• When process is complete, save configuration when prompted, switch reloads and forms VSS.

5) Verify Operation and Rename Switch

VSS-Sw1# show switch virtual redundancy

• Check for both switches visible, Supervisors in SSO mode, second Supervisor in Standby-hot status

VSS-Sw1(config)# hostname VSS
VSS(config)#

6) Configure Dual-Active Detection

• Connect a Gigabit Link between the VSS switches
VSS(config)# switch virtual domain 100
VSS(config-vs-domain)# dual-active detection fast-hello
VSS(config)# interface range gigabit1/1/24, gigabit2/1/24
VSS(config-if-range)# dual-active fast-hello
VSS(config-if-range)# no shut

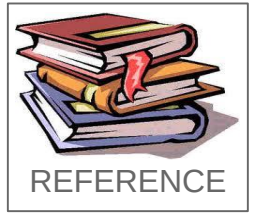
7) Configure the System Virtual MAC Address

VSS(config)# switch virtual domain 100
VSS(config-vs-domain)# mac-address use-virtual

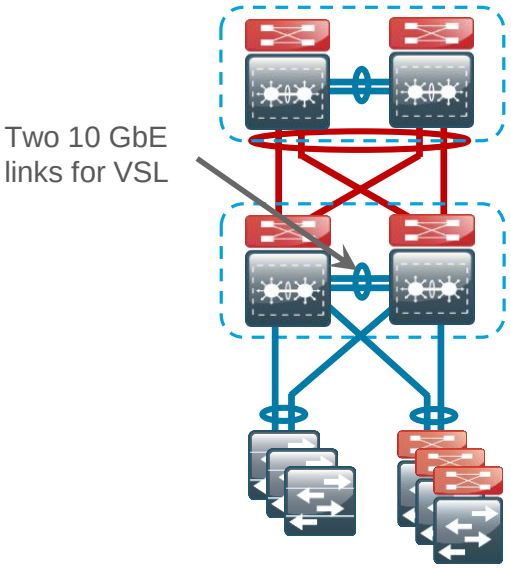
Configured Router mac address is different from operational value. Change will take effect after config is saved and the entire Virtual Switching System (Active and Standby) is reloaded.

Catalyst 6500 VSS – VSL Considerations

LAN Distribution Layer

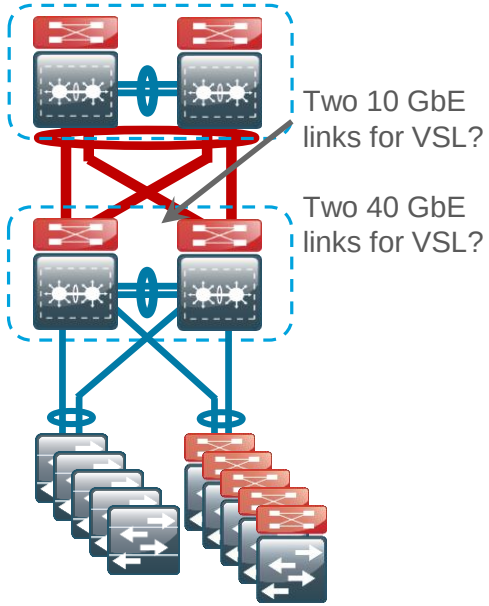


Dual 10 GbE links to core from each VSS Node



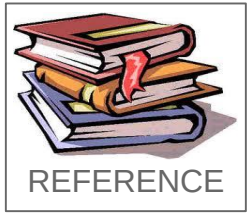
- Bandwidth requirements and service module placement affect VSL sizing
- VSL connection must carry traffic during link failure
- A VSL connection on the Supervisor allows the VSL to come up sooner
- VSL capable linecard prioritizes VSLP and BPDU traffic over all other traffic
- Make sure Network Routing protocols are marked for priority over VSL

Dual 40 GbE links to core from each VSS Node



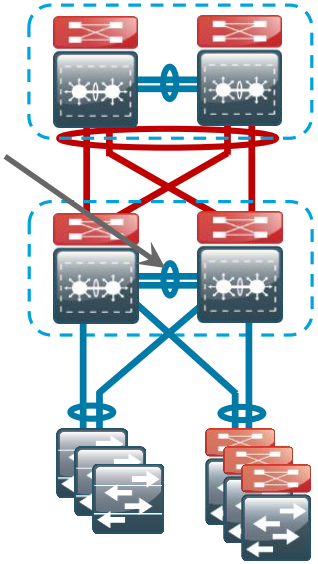
Catalyst 6500 VSS – Physical Connections

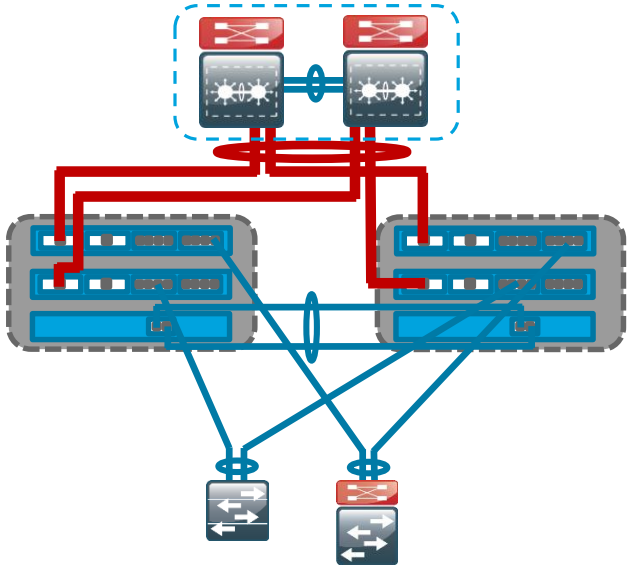
LAN Distribution Layer



Dual 10 GbE links to core from each VSS Node

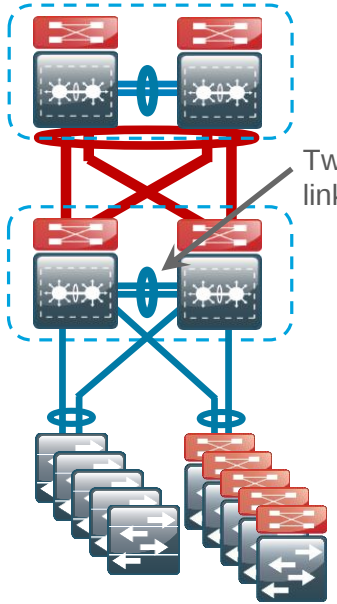
Two 10 GbE links for VSL





Dual 40 GbE links to core from each VSS Node

Two 10 GbE links for VSL



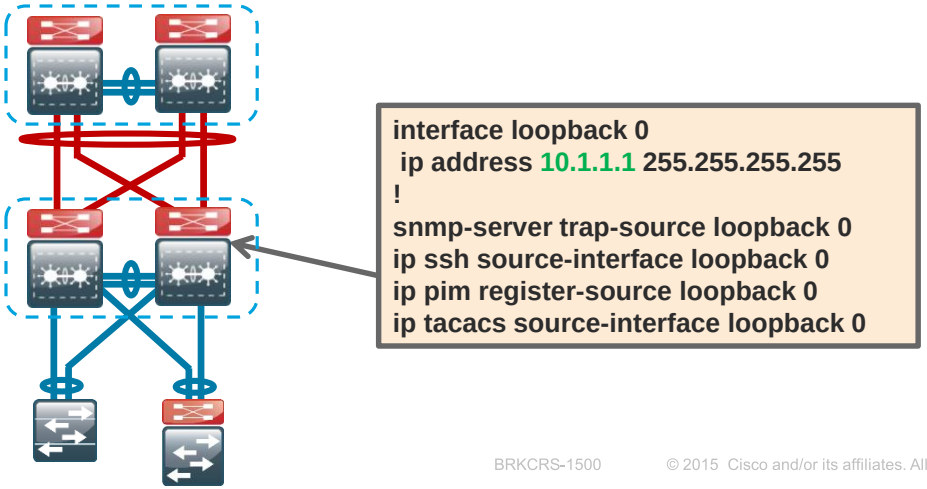
Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Connectivity to Access and Core Layers
- Core Layer Deployment
- Conclusion

In-Band Management Interface

LAN Distribution Layer

- The loopback interface is the preferred way to manage when using in-band access
  - Logical interface
  - Always available as long as device is operational
  - Commonly a host address (32-bit address mask)
- Bind SNMP, SSH, TACACS and PIM processes to Loopback interface address for optimal resiliency



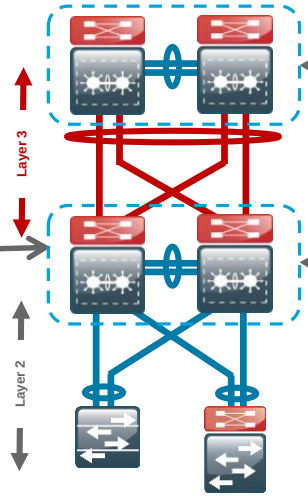
Distribution Layer IP Unicast Routing – EIGRP

LAN Distribution Layer

EIGRP was chosen for…
simplicity, scalability, and flexibility

- Named Mode configuration
- Tie eigrp router-id to loopback 0 for maximum resiliency
- 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

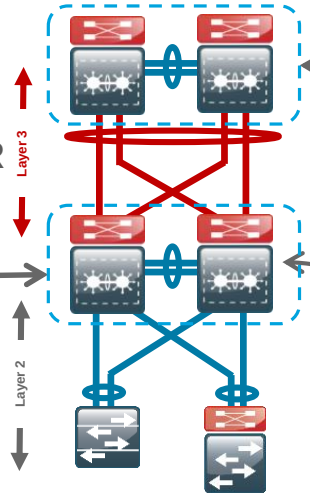
Distribution Layer IP Unicast Routing – OSPF

LAN Distribution Layer

OSPF is available for…
compatibility

- Tie ospf router-id to loopback 0 for maximum resiliency
- 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] [inverse mask] area [area number]
 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

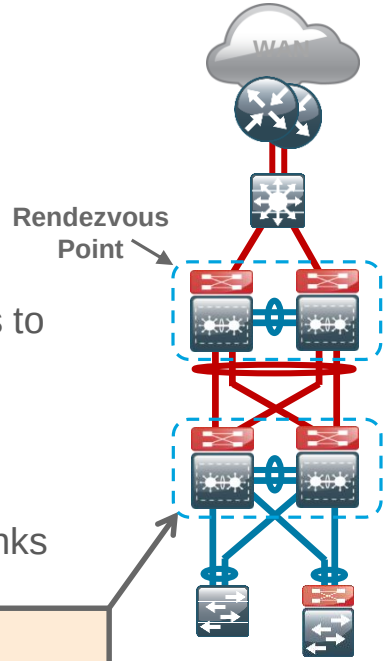
NSF Aware
- Nothing to enable.
- Only need IOS version that supports NSF for EIGRP

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 Multicast Routing

LAN Distribution Layer

- IP Multicast allows a single IP data stream to be replicated by the infrastructure (Routers and Switches)
  - More efficient than multiple IP Unicast streams
  - Beneficial for IPT Music on Hold and IP Broadcast video streams
- IP PIM Sparse-Mode
  - Sparse-mode uses a Rendezvous Point(RP) to allow IP Multicast receivers to find IP Multicast Sources
  - Place IP Multicast RP in the center or Core of the network
- On every Layer 3 switch and router
  - Configure ip pim autorp listener to enable discovery across sparse mode links
  - Enable pim sparse-mode on all Layer 3 interfaces




```
ip multicast-routing
ip pim autorp listener
!
interface GigabitEthernet 1/0/1
ip pim sparse-mode
```

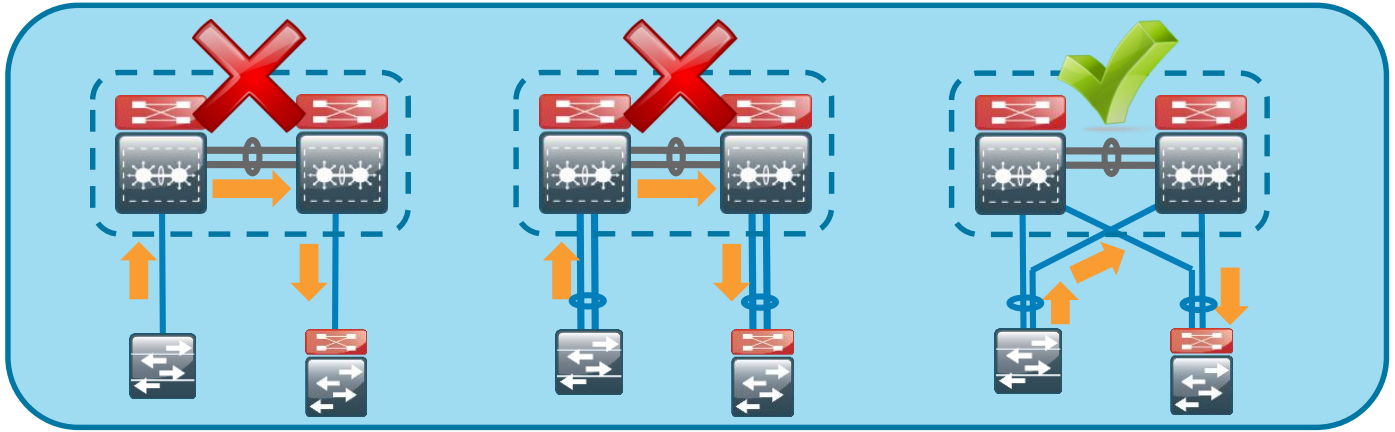
Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
  - Attributes and platform choices
  - Platform Specific
  - Global Options
  - Connectivity to Access and Core Layers
- Core Layer Deployment
- Conclusion

VSS Distribution Connectivity to Access Layer

Resilient Connectivity

- Use EtherChannel for link resiliency and load sharing
- With VSS use Multi-Chassis EtherChannel, home to each switch

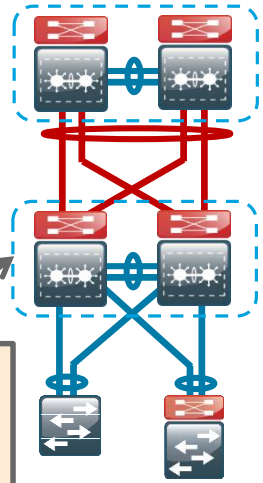


- Alternatively…
  - With switch stack distribution layer, home EtherChannel uplinks to multiple switches in stack

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
- Configure 802.1Q Trunk on EtherChannel logical port (port-channel) interface

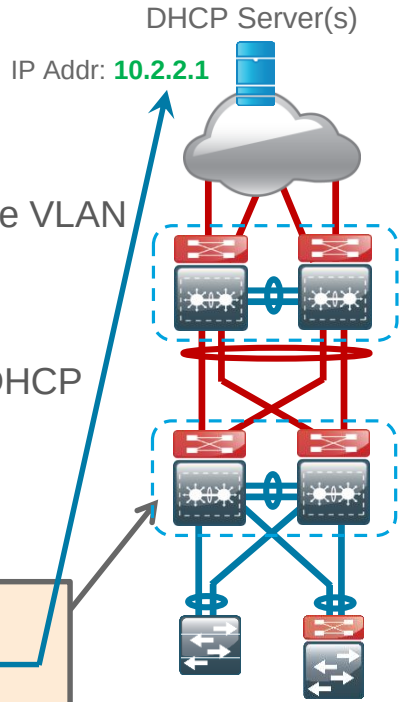


```
vlan 10,20,30
spanning-tree vlan 1-4094 root primary
!
Interface range gigabit 1/1/1, gigabit 2/1/1
  macro apply EgressQoS
  channel-protocol lacp
  channel-group 10 mode active
!
interface port-channel 10
  switchport trunk encapsulation dot1q
  switchport trunk allowed 10,20,30
  switchport trunk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

Layer 3 Connectivity for Access Layer

LAN Distribution Layer

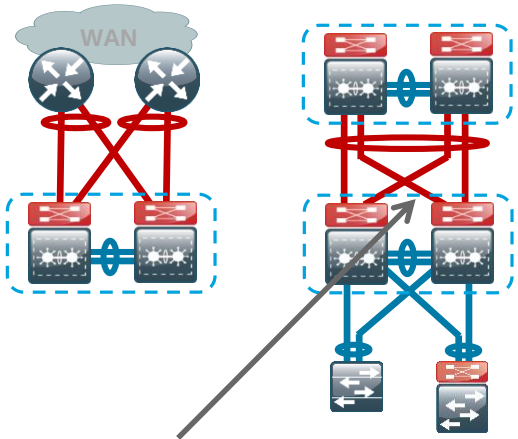
- Configure Layer 3 for Access Layer VLANs
  - Configure a VLAN interface(SVI) for every Access Layer VLAN
  - This SVI is the IP Default Gateway for the Access Layer hosts in the VLAN
- Configure ip-helper address on each SVI
  - IP helper forwards DHCP requests from hosts in the VLAN to the DHCP Server
  - 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



Layer 3 Connectivity to Core Layer
– Interface Configuration

LAN Distribution Layer

- If no Core Layer, links to WAN routers are Layer 3 links



- Links from Distribution Layer to Core are Layer 3 links
- Configure Layer 3 EtherChannel interface
  - When creating L3 EtherChannel, create the logical (port-channel) interface first

```
interface port-channel 20
 no switchport
 ip address [ip address] [mask]
 ip pim sparse-mode
!
interface range teng1/1/8 , teng2/1/8 , teng1/2/8 , teng2/2/8
 channel-protocol lacp
 channel-group 20 mode active
 macro apply EgressQoS
```

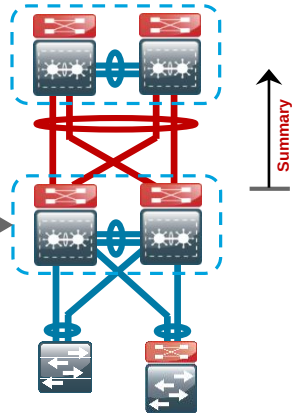
- Configure EtherChannel Member Interfaces
  - Configure the physical interfaces to tie to the logical port-channel

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)



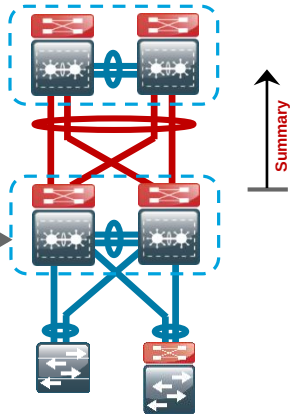
- As networks grow, IP address summarization is used
  - To reduce bandwidth required for routing updates
  - To reduce convergence time around a link failure
  - Summarize all subnets in the distribution layer to the rest of the network

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

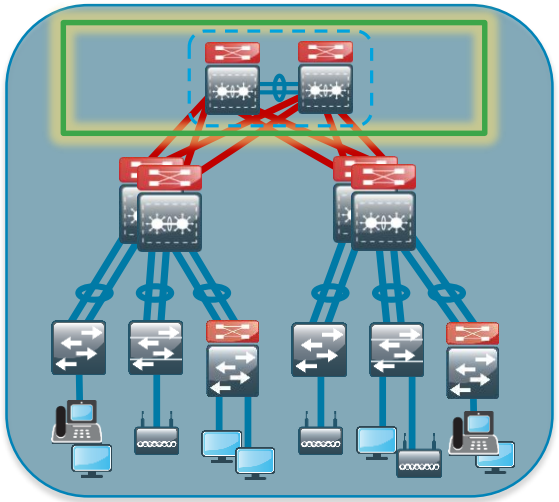
Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
- Core Layer Deployment
  - Attributes and platform
  - Global Options
- Conclusion

Core Layer Attributes

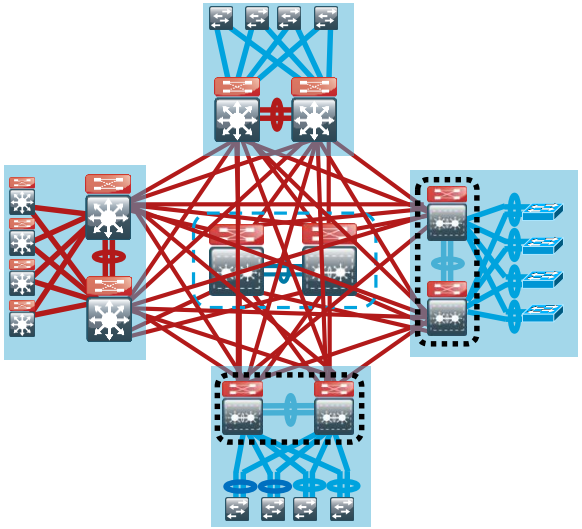
LAN Core Layer

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



- 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

Do I need a Core Layer?



Core Layer Platform

Catalyst 6500/6807 (VSS) w/ Supervisor 2T

- Resilient LAN Core platform with redundant supervisor and SSO support, and load sharing power supplies
- Quad-Supervisor SSO available
- Wide Range of connectivity from Gigabit Ethernet, GEC, 10 Gb Ethernet, 10-GEC, and 40 Gb Ethernet
- Up to 220G/slot (6807-XL / Sup 2T)
- Consistent IOS interface and feature set with rest of LAN
- VSS and Multi-Chassis EtherChannel for highly resilient connectivity
- Scalable distributed forwarding

- Core based on two physically separate switches, one logical switch (VSS) – simplified configuration with highest performance and resiliency
- All connectivity to Core is dual homed links or EtherChannels – designed for high speed ranging from Gigabit Ethernet, GEC, 10 Gigabit Ethernet,10 GEC, and 40 Gigabit Ethernet
- Additional resiliency available with Quad-Supervisor Virtual Switching System Stateful Switchover (VS4O)

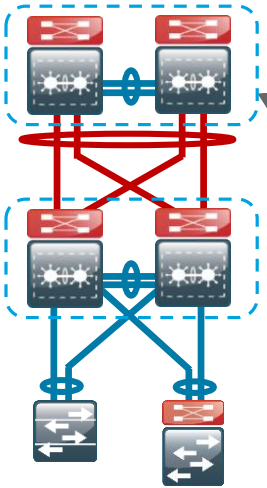
Agenda

- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
- Core Layer Deployment
  - Attributes and platform
  - Global Options
- Conclusion

In-Band Management Interface

LAN Core Layer

- The loopback interface is the preferred way to manage when using in-band access
  - Logical interface
  - Always available as long as device is operational
  - Commonly a host address (32-bit address mask)
- Bind SNMP, SSH, TACACS and PIM processes to Loopback interface address for optimal resiliency



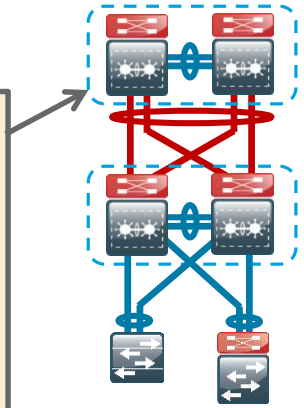
```
interface loopback 0
 ip address 10.1.1.1 255.255.255.255
!
snmp-server trap-source loopback 0
ip ssh source-interface loopback 0
ip pim register-source loopback 0
ip tacacs source-interface loopback 0
```

Core Layer IP Unicast Routing - EIGRP

LAN Core Layer

- Enable EIGRP for address space in use for core
  – just as was done in the distribution
- However…
  - No passive interfaces in Core
    – route to everything from the core
- Remember to…
  - Enable authentication of neighbor routing protocol communication
  - Enable NSF

```
key chain EIGRP-KEY
 key 1
  key-string [key]
router eigrp LAN
address-family ipv4 unicast autonomous-system 100
    network [network] [inverse mask]
    eigrp router-id [ip address of loopback 0]
    nsf
  exit-address-family
  af-interface default
    authentication mode md5
    authentication key-chain EIGRP-KEY
   exit-af-interface
```

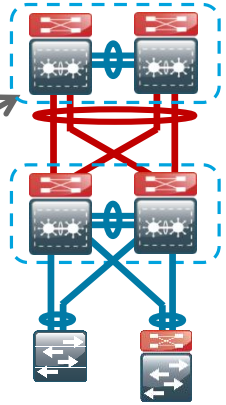


Core Layer IP Unicast Routing - OSPF

LAN Core Layer

- Enable OSPF for address space in use for core
  – just as was done in the distribution
  - Core is OSPF Area 0
- However…
  - No passive interfaces in Core
    – route to everything from the core
- Remember to…
  - Enable authentication of neighbor routing protocol communication
  - Enable NSF

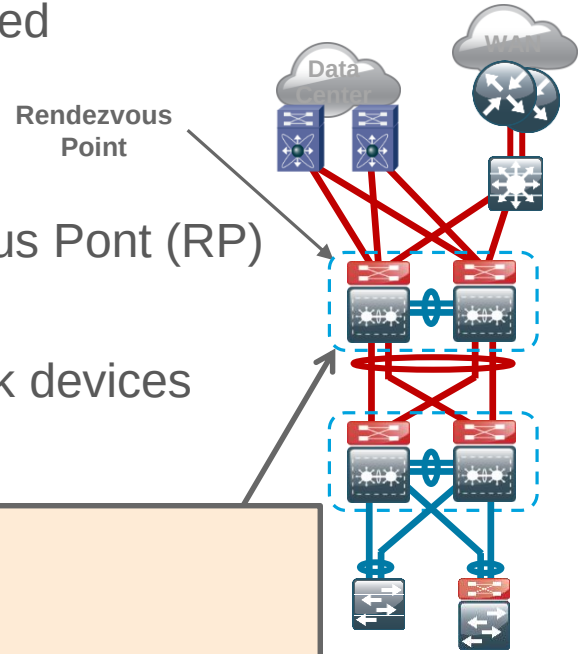
```
interface [interface]
 ip ospf message-digest-key [key id] md5 [key]
router ospf 100
 router-id [ip address of loopback 0]
 nsf
 area 0 authentication message-digest
 network [network] [inverse mask] area 0
```



Resilient IP Multicast Routing – VSS Core

LAN Core Layer

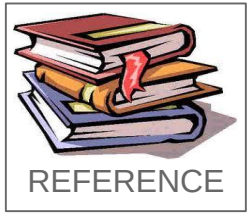
- IP Multicast allows a single IP data stream to be replicated by the infrastructure (Routers and Switches)
- IP PIM Sparse-Mode
- Every Layer 3 switch and router points to the Rendezvous Pont (RP)
  - RP placed centrally in the network (core)
- Auto-RP used for dynamic RP announcement to network devices
- RP resiliency is critical to IP Multicast operation
  - VSS SSO ensures RP availability




```
interface loopback 1
 ip address 10.1.1.2 255.255.255.255
 ip pim sparse-mode
!
access-list 10 permit 239.1.0.0 0.0.255.255
ip pim send-rp-announce Loopback1 scope 32 group-list 10
ip pim send-rp-discovery Loopback1 scope 32
```

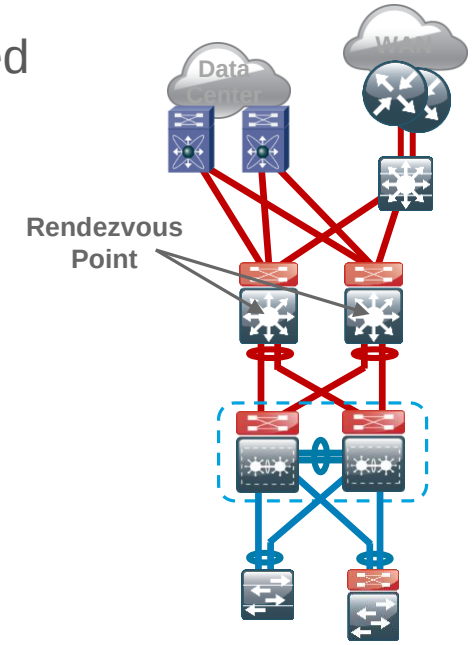
Announce “I (10.1.1.2) will be an RP” →
Discovers RPs and tells best to AutoRP listeners →

Resilient IP Multicast RP – Two Box Core



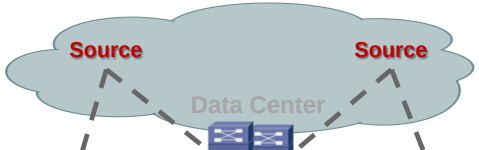
LAN Core Layer

- When the core isn't a single logical platform
- IP Multicast allows a single IP data stream to be replicated by the infrastructure (Routers and Switches)
- IP PIM Sparse-Mode is used
  - Sparse-mode uses a Rendezvous Point(RP) to allow IP Multicast receivers to find IP Multicast Sources
  - Place IP Multicast RP in the center or Core of the network
- Auto-RP used for dynamic RP announcement to network devices
- RP resiliency is critical to IP Multicast operation
  - Multiple RP redundancy methods
  - Design uses Anycast RP for simplicity and fast failover



Anycast RP Operation & Configuration

Resilient IP Multicast



ip pim auto-rp listener

ip pim auto-rp listener

RP1
10.1.1.1

MSDP

RP2
10.1.1.1

SA

SA

```
interface loopback 0
 ip address 10.1.1.2 255.255.255.255
 ip pim sparse-mode

interface loopback 1
 ip address 10.1.1.1 255.255.255.255
!
ip msdp peer 10.1.1.3 connect-source loopback 0
ip msdp originator-id loopback 0
!
access-list 10 permit 239.1.0.0 0.0.255.255
ip pim send-rp-announce Loopback1 scope 32 group-list 10
!
ip pim send-rp-discovery Loopback0 scope 32
```

```
interface loopback 0
   ip address 10.1.1.3 255.255.255.255
   ip pim sparse-mode

interface loopback 1
 ip address 10.1.1.1 255.255.255.255
!
ip msdp peer 10.1.1.2 connect-source loopback 0
ip msdp originator-id loopback 0
!
access-list 10 permit 239.1.0.0 0.0.255.255
ip pim send-rp-announce Loopback1 scope 32 group-list 10
!
ip pim send-rp-discovery Loopback0 scope 32
```

Discovers RP and tells AutoRP listeners

Announce “I will be an RP (10.1.1.1)”

ip pim auto-rp listener

Receiver

Receiver

Discovers RP and tells AutoRP listeners

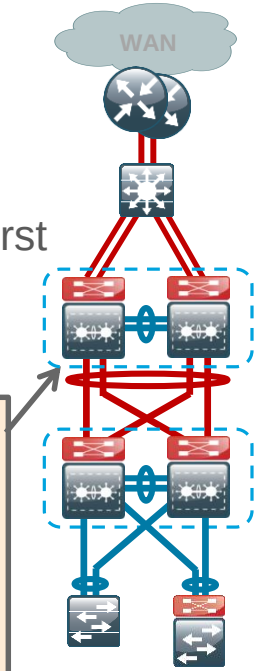
Announce “I will be an RP (10.1.1.1)”

REFERENCE

Layer 3 Connectivity to Distribution Layer

LAN Core Layer

- Links from Core Layer are Layer 3 links (no SVIs)
- Use MEC to VSS in distribution layer
- Configure Layer 3 EtherChannel interface
  - When creating L3 EtherChannel, create the logical (port-channel) interface first
- Configure EtherChannel Member Interfaces
  - Configure the physical interfaces to tie to the logical port-channel
- Dual home to WAN or Data Center to Core



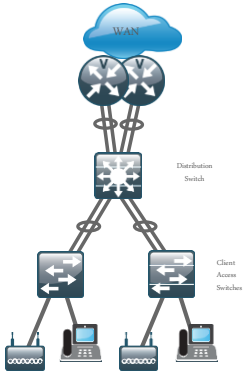

```
interface port-channel 20
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
!
interface range teng1/1/8 , teng2/1/8 , teng1/2/8 , teng2/2/8
  channel-protocol lacp
  channel-group 20 mode active
  macro apply EgressQoS
  no shutdown
```

Agenda

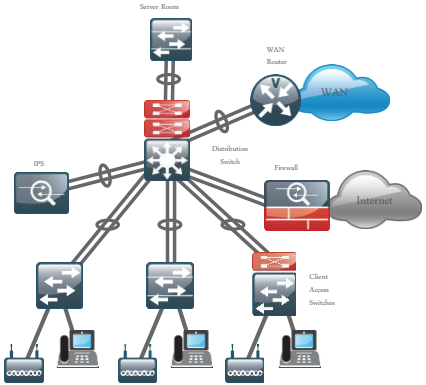
- Introduction to the Campus Wired LAN CVD
- Access Layer Deployment
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion

You Now Have the Tools to Build This!

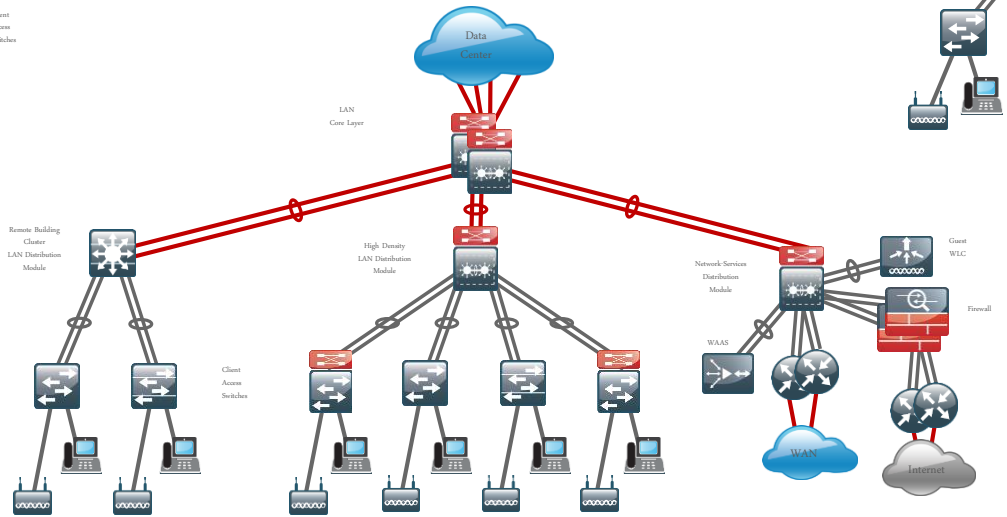
Two-Tier Remote-Site LAN



Two-Tier Collapsed LAN Core



Three-Tier LAN Design



Summary

- The Cisco Validated Design provides a design framework for the wired campus with step-by-step deployment processes based on the cumulative Cisco leading practices
- Access Layer
  - Consistent LAN Access Layer across the network (small site to large campus)
  - Supports both layer 2 and layer 3 application needs
  - Secure boundary and ready for advanced technologies
- Distribution Layer
  - Simplified single logical platform with resilient and scalable design
  - Etherchannel for resiliency and scalability
- Core Layer
  - Scalable, resilient Layer 3 VSS core for simplified topology and easier configuration

Resiliency, scalability, and flexibility
– easily deployed throughout the network.

Cisco live!

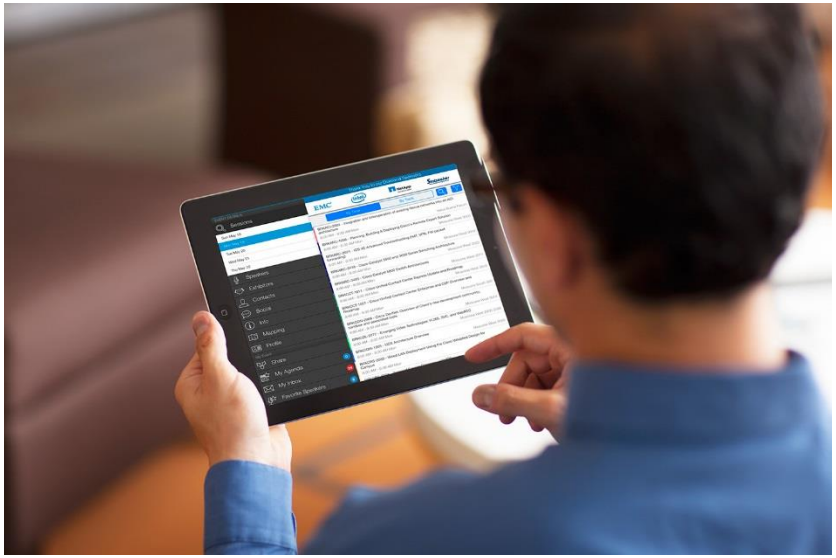
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could Be a Winner

- Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)
- Send a tweet and include
  - Your favorite speaker’s Twitter handle @ccie5060
  - Two hashtags: #CLUS #MyFavoriteSpeaker
- You can submit an entry for more than one of your “favorite” speakers
- Don’t forget to follow @CiscoLive and @CiscoPress
- View the official rules at http://bit.ly/CLUSwin

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.
- Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.



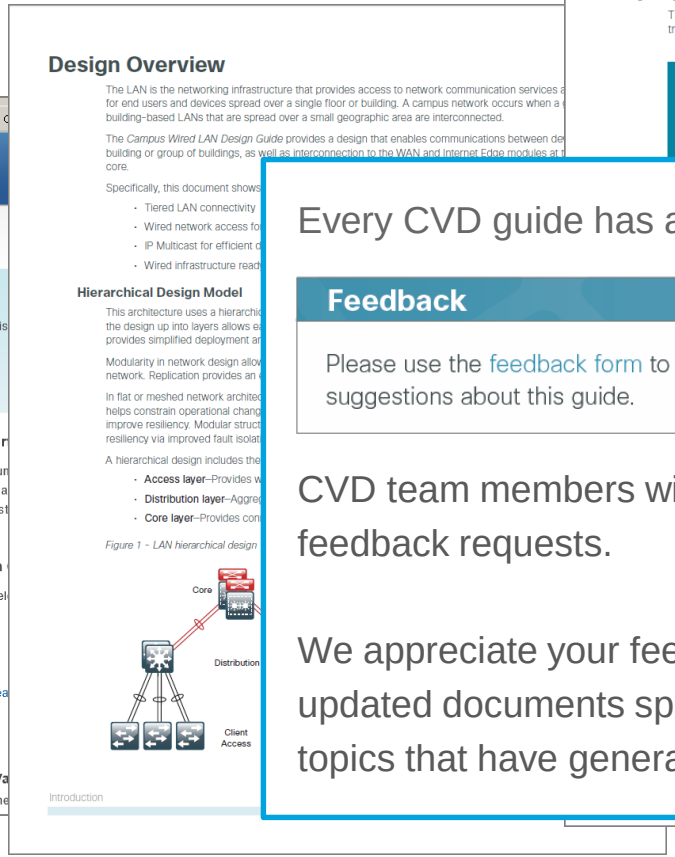
Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

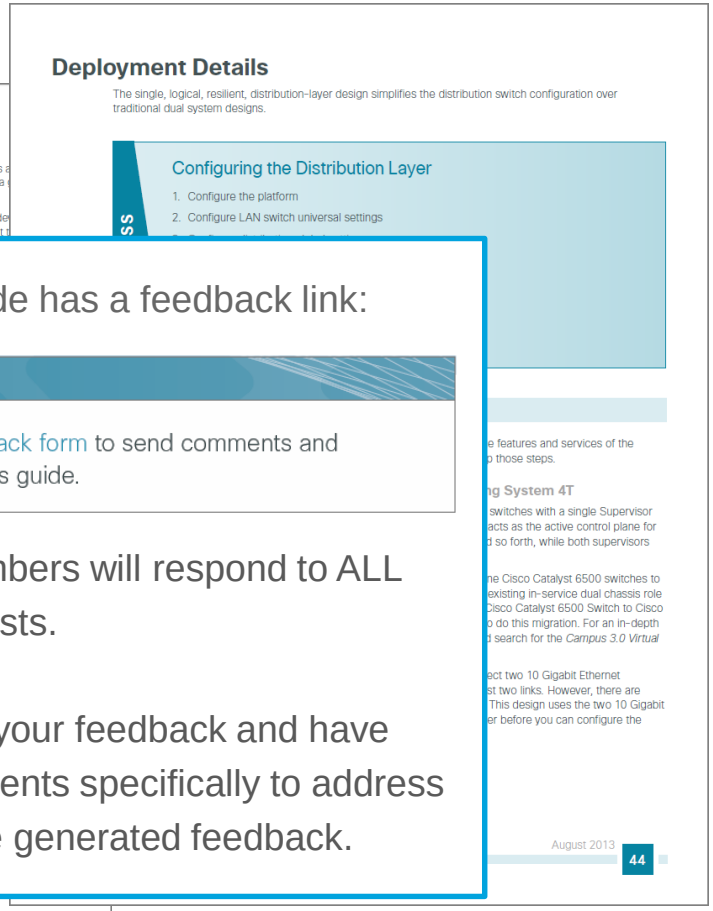
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions

Published Design Guides

www.cisco.com/go/cvd





Every CVD guide has a feedback link:

Feedback

Please use the feedback form to send comments and suggestions about this guide.

CVD team members will respond to ALL feedback requests.

We appreciate your feedback and have updated documents specifically to address topics that have generated feedback.

Thank you

TOMORROW starts here.

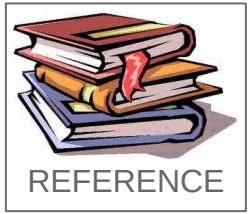
www.cisco.com/go/cvd

Related Sessions

- BRKRST-2040: WAN and Remote-Site Deployment using Cisco Validated Designs
- BRKCRS-2501: Campus QoS Design – Simplified
- BRKCRS-3035: Advanced Enterprise Campus Design: Virtual Switching System (VSS)
- BRKCRS-3502 - Advanced Enterprise Campus Design: Instant Access
- BRKRST-2301:Enterprise IPv6 Deployment
- BRKSEC-3003: Advanced IPv6 Security in the LAN

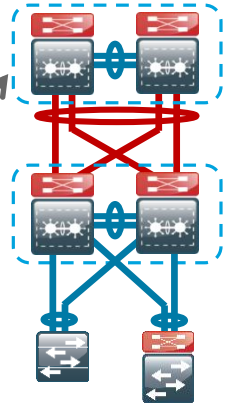
IP Unicast Routing – Very Large Scale EIGRP

LAN Core Layer



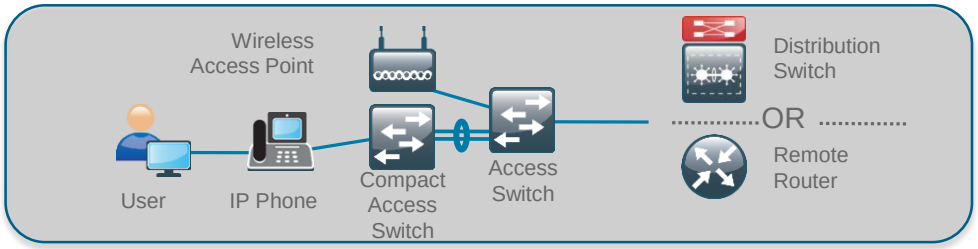
- Enable additional network summarization and optimization
  - Summarize the default route towards the distribution
  - Add floating summary to account for the local discard route
  - Predefinition of a static metric for summary also eliminates computing and updates for any additions and changes to components of summary – still allows for withdrawal when all components lost

```
router eigrp LAN
  address-family ipv4 unicast autonomous-system 100
    network [network] [inverse mask]
    eigrp router-id [ip address of loopback 0]
    nsf
  af-interface [interface]
    summary-address 0.0.0.0 0.0.0.0
  exit-af-interface
  topology base
    summary-metric 0.0.0.0/0 [bandwidth] [delay] [reliability] [load] [mtu] distance 250
  ex-af-topology
  exit-address-family
```



Extended Access Layer – Compact Switch

Additional Option



- Extend the Access Layer with Cisco feature set, including FHS
  - Applications: Retail, education, hospitality, conference room
- Cisco Catalyst 3560CPD-8PT-L and 2960CPD-8PT-L
  - Can be powered by upstream access switch via PoE
  - Optional external power supply for non-PoE applications or resiliency
- Cisco Catalyst Compact Switch options available to use internal power supply for up to 8 or 12 ports of PoE delivering a maximum of 124 watts.

Powering Options	Power from Uplink (nominal)	Catalyst 2960CPD Available PoE	Catalyst 3560CPD Available PoE
1 PoE	15.4 watts	0 watts	-
2 PoE	30.8 watts	7 watts	0 watts
1 PoE+	30 watts	7 watts	0 watts
1 PoE+ and 1 PoE	45.4 watts	15.4 watts	0 watts
2 PoE+	60 watts	22.4 watts	15.4 watts
1 UPOE	60 watts	30.8 watts	23.8 watts
Aux Power Input (Aux with UPOE uplink)	-	22.4 watts (30.8 W)	15.4 watts (23.8 W)