Cisco Live!
July 10-14, 2016 • Las Vegas, NV
Your Time Is Now
Campus Wired LAN Deployment Using Cisco Validated Designs

Dana Daum, Communications Architect
BRKCRS-1500
Agenda

• Introduction to the Campus Wired LAN Deployment CVD
• Access Layer Deployment
• Distribution Layer Deployment
• Core Layer Deployment
• Conclusion
BRKCRS-1500 Abstract: Campus Wired LAN Deployment Using Cisco Validated Designs

This session is an introduction to LAN design and deployment best practices covered in the Campus Wired LAN design and deployment guides - part of the Cisco Validated Design (CVD) body of work. 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.

Though introductory, attendees for this session will benefit from an understanding of LAN switching and routing fundamentals equivalent to a CCNA level for a brief exploration of some intermediate topics.
Agenda

• Introduction to the Campus Wired LAN Deployment 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 do I do it quickly?

How do I manage it?

How do I put it all together?
The Cisco Validated Design – provides a framework for design and deployment guidance based on common use cases.

From “Classic” CVDs… …to Modular CVDs, White Papers and Tools

LAN Deployment - Process Flow Chart

Each layer follows the same process

1. **Platform**
   - Configure platform specific features for resiliency and Quality of Service

2. **LAN Switch Universal**
   - Enable features and functionality common to all switches in the design

3. **Role in the Network**
   - Enable features and functionality required for the role the switch is serving in the network

4. **Service or Function**
   - Enable features and functionality required to provide connectivity (client access, uplink connections, etc.)
Validated Design and Best Practice Auditing
Cisco Active Advisor

Provides:
- Security Advisories (PSIRTs and Field Notices)
- End-of-life & End-of-support dates
- Warranty & service contract status
- Feature usage

Enhances the Cisco product experience
- Improves network with Best Practices Advisories
- Shortens deployment time of new products
- Takes complexity out of Cisco’s products

Free cloud-based service

Agentless – nothing to download or install

BRKNMS-1300: Scan. Analyze. Improve! Reduce Risk and Improve Network Health with Free cloud-based Service
Also in Education Zone Tuesday afternoon and Cisco DNA Demo Theater Monday-Wednesday morning/afternoon.

www.CiscoActiveAdvisor.com
LAN Deployment Principles

- Ease of Deployment
- Flexibility and Scalability
- Easy to Manage
- Advanced Technology Ready
- Resiliency and Security
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

Maps well to our session agenda!
Campus Wired LAN Design Options (1 Core, 2x Dist+Acc)

- Traditional Multilayer Campus
  - Logical Topology
  - Physical Topology
  - Protocols / Tuning
  - Design Notes
  - BRKCRS-2031

- Layer 3 Routed Access
  - Logical Topology
  - Physical Topology
  - L3 Planning Limited L2
  - Design Notes
  - BRKCRS-3036

- L2 Access / Simplified Distribution
  - Logical Topology
  - Physical Topology
  - Flexible, Easy, Scalable
  - Design Notes
  - BRKCRS-1500

- Campus Fabric
  - Logical Topology
  - Physical Topology
  - Flexible, Tools to Simplify
  - Design Notes
  - BRKCRS-3800

CiscoLive!
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 Deployment 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

• 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

© 2016  Cisco and/or its affiliates. All rights reserved. Cisco Public
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

<table>
<thead>
<tr>
<th>Catalyst 4500-E with Supervisor 8-E / 8L-E / 7L-E</th>
<th>Catalyst 3850 and Catalyst 3650</th>
<th>Catalyst 2960-X and Catalyst 2960-XR</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Modular switch with 1:1 redundancy for all critical systems (supervisors, power supplies, fans)</td>
<td>• Fixed configuration stackable switch with central config and control</td>
<td>• Fixed configuration stackable switch with central config and control</td>
</tr>
<tr>
<td>• Stateful switchover provides subsecond supervisor recovery</td>
<td>• Stateful switchover provides subsecond recovery</td>
<td>• Up to 8 switches in a stack</td>
</tr>
<tr>
<td>• Multiple Ethernet Connectivity options (fiber or copper with various densities)</td>
<td>• Modular Uplinks (3850), power supplies, and fans</td>
<td>• FlexStack+ 80G stacking (Stack Module Required)</td>
</tr>
<tr>
<td>• Quad Sup RPR (new)</td>
<td>• StackWise480 and StackPower (3850), StackWise160 (3650)</td>
<td>• Stack or stack member failure recovery max 1-2 seconds</td>
</tr>
<tr>
<td>• In-Service Software Upgrades</td>
<td>• Up to 9 switches in a stack</td>
<td>• PoE and PoE+</td>
</tr>
<tr>
<td>• PoE, PoE+, and UPOE</td>
<td>• PoE, PoE+, UPOE</td>
<td>• Redundant Power Supply and L3 Access option (XR)</td>
</tr>
<tr>
<td>• Energy Efficient Ethernet</td>
<td>• UADP – Wireless Capable</td>
<td></td>
</tr>
<tr>
<td>• Sup8-E – UADP Wireless</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agenda

• Introduction to the Campus Wired LAN Deployment 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 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

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

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

```
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.

```
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.
Quality of Service Overview for LAN CVDs

Example 8-Class Model

<table>
<thead>
<tr>
<th>Voice / Real Time Video</th>
<th>Signaling / Network Control</th>
<th>Multimedia Conferencing</th>
<th>Multimedia Streaming</th>
<th>Transactional Data</th>
<th>Bulk Data</th>
<th>Scavenger</th>
<th>Best Effort</th>
</tr>
</thead>
</table>

- 8-Class Model is used as the current basis for the LAN deployment (this will likely change over time)
- 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

Quality of Service Deployment

Macros Ease the Deployment Process for Platform-Specific Commands

Macros Used Later in the Deployment Process:

1. **AccessEdgeQoS Macro**
   - Applied on all client facing interfaces

2. **EgressQoS Macro**
   - Applied on all other interfaces

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 Deployment 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

```plaintext
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.

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

Optionally, secure vty and SNMP access
```
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]
serve 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
```
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.

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 Deployment 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

```plaintext
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)

- 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.

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

Configure in the global configuration:

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

Configure on the client interface:

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

Example DHCP Snooping Binding Table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:56:BA:13:DB</td>
<td>10.4.80.10</td>
<td>10</td>
<td>GigabitEthernet2/0/1</td>
</tr>
</tbody>
</table>

Client
MAC=00:50:56:BA:13:DB
IP Addr=10.4.80.10

DHCP Snooping Diagram
ARP Inspection
Client Facing Interface Configuration

Example DHCP Snooping Binding Table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:56:BA:13:DB</td>
<td>10.4.80.10</td>
<td>10</td>
<td>GigabitEthernet2/0/1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:56:BA:13:DB</td>
<td>10.4.80.10</td>
<td>10</td>
<td>GigabitEthernet2/0/1</td>
</tr>
</tbody>
</table>

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

Configure on the switch at the global level:

```
spanning-tree portfast bpdu-guard default
```

- 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 Deployment 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

```bash
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.
```
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 member interfaces.

```
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 Deployment 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
  - 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 RPVST+ for edge protection
Catalyst 6500/6807 Supervisor 6T/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 Catalyst 6840-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, 8 (VSS) Catalyst 4500-X (VSS)
- Physically separate chassis, line cards, and power supplies, with fixed/modular options
- VSS-two physical chassis into a single logical entity
- SSO between chassis
- 4500-E Quad Sup RPR (new)
- Used to aggregate a smaller number of Gigabit or 10 Gigabit access layer switches
- In Service Software Updates (ISSU)

Catalyst 3850-12S Catalyst 3850- (12/24/48)XS (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 Deployment 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

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

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
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 renames 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.
“Is there an easier way to enable VSS?”

Use Easy VSS to configure from a single console port

Prerequisites:
- Switches running same software with feature support (4K:3.6E, 6K:15.2(1)SY1)
- Links to be used for VSLs up with CDP communication

1) 6K - Enable Easy VSS feature, convert, and reload

```
VSS-Sw1# switch virtual easy
VSS-Sw1# switch convert mode easy links
Local Interface      Remote Interface  Hostname
    TenGigabit3/4      TenGigabit3/4  VSS-Sw2
    TenGigabit4/4      TenGigabit4/4  VSS-Sw2
VSS-Sw1# switch convert mode easy links T3/4 T4/4 domain 100
VSS-Sw1(config)# switch virtual domain 100
VSS-Sw1(config-vs-domain)# mac-address use-virtual
VSS-Sw1# copy running-config startup-config
VSS-Sw1# reload
```

2) 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)#
```

3) 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
```
Agenda

- Introduction to the Campus Wired LAN Deployment 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

```
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
```
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

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

---

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

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

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

**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**

**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
Agenda

• Introduction to the Campus Wired LAN Deployment 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

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

```yaml
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
```
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
```

- 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

- Enable EIGRP for the core-facing interface (disable passive-interface)
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 Deployment 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
### Catalyst 6807/6500 (VSS) w/ Supervisor 6T/2T
- LAN Core platform with consistent IOS interface and feature set as rest of LAN allowing single logical and resilient platform using Virtual Switching System (VSS)
- Redundant supervisor and SSO support, VSS, and Quad-Supervisor SSO available (VS4O), and load sharing power supplies
- Wide Range of connectivity from Gigabit Ethernet, GEC, 10 Gb Ethernet, 10-GEC, and 40 Gb Ethernet
- Up to 440G/slot (6807-XL / Sup 6T)
- VSS and Multi-Chassis EtherChannel for highly resilient connectivity and scalable distributed forwarding

### Nexus 7700 / 7000 (Independent Chassis)
- Alternate LAN Core platform allowing independent control planes and a consolidated DC and LAN core possible through Virtual Device Contexts (VDC)
- Resilient supervisor and SSO support, and load sharing power supplies
- Wide Range of connectivity from Gigabit Ethernet, GEC, High Density 10 Gb Ethernet, 10-GEC, 40Gb and 100Gb Ethernet
- In Service Software Upgrades
- Data Center NX-OS heritage
Agenda

- Introduction to the Campus Wired LAN Deployment 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

```plaintext
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
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 (such as Nexus)

• 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

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 10.1.1.1 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

Announce “I will be an RP (10.1.1.1)”

MSDP

Source

Data Center

Source

RP1

10.1.1.1

RP2

10.1.1.1

Receiver

Receiver

ip pim auto-rp listener

ip pim auto-rp listener

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 10.1.1.1 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

Announce “I will be an RP (10.1.1.1)”

Discovers RP and tells AutoRP listeners

Discovers RP and tells AutoRP listeners
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

```plaintext
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 Deployment CVD
- Access Layer Deployment
- Distribution Layer Deployment
- Core Layer Deployment
- Conclusion
You Now Have the Tools to Build This!

Two-Tier Remote-Site LAN

Three-Tier LAN Design

Two-Tier Collapsed LAN Core
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, and alternative Nexus 7K option

  Resiliency, scalability, and flexibility
  – easily deployed throughout the network.
Look for the feedback link in the guides:

**Feedback**

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

Team members will respond to ALL feedback requests.

We appreciate your feedback and have updated documents specifically to address topics that have generated feedback.
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 through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

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
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions
Please join us for the Service Provider Innovation Talk featuring:

Yvette Kanouff | Senior Vice President and General Manager, SP Business
Joe Cozzolino | Senior Vice President, Cisco Services

Thursday, July 14th, 2016
11:30 am - 12:30 pm, In the Oceanside A room

What to expect from this innovation talk
• Insights on market trends and forecasts
• Preview of key technologies and capabilities
• Innovative demonstrations of the latest and greatest products
• Better understanding of how Cisco can help you succeed

Register to attend the session live now or watch the broadcast on cisco.com
Thank you
Cisco live!
July 10-14, 2016 • Las Vegas, NV
www.cisco.com/go/cvd
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

Two 10 GbE links for VSL

Dual 40 GbE links to core from each VSS Node

Two 10 GbE links for VSL?

Two 40 GbE links for VSL?
Catalyst 6500 VSS – Physical Connections

LAN Distribution Layer

Dual 10 GbE links to core from each VSS Node

Dual 40 GbE links to core from each VSS Node

Two 10 GbE links for VSL

Two 10 GbE links for VSL
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 Connectivity Option – new switch versions now available

- 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.

<table>
<thead>
<tr>
<th>Powering Options</th>
<th>Power from Uplink nominal</th>
<th>Catalyst 2960CPD Available PoE</th>
<th>Catalyst 3560CPD Available PoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PoE</td>
<td>15.4 watts</td>
<td>0 watts</td>
<td>-</td>
</tr>
<tr>
<td>2 PoE</td>
<td>30.8 watts</td>
<td>7 watts</td>
<td>0 watts</td>
</tr>
<tr>
<td>1 PoE+</td>
<td>30 watts</td>
<td>7 watts</td>
<td>0 watts</td>
</tr>
<tr>
<td>1 PoE+ and 1 PoE</td>
<td>45.4 watts</td>
<td>15.4 watts</td>
<td>0 watts</td>
</tr>
<tr>
<td>2 PoE+</td>
<td>60 watts</td>
<td>22.4 watts</td>
<td>15.4 watts</td>
</tr>
<tr>
<td>1 UPOE</td>
<td>60 watts</td>
<td>30.8 watts</td>
<td>23.8 watts</td>
</tr>
<tr>
<td>Aux Power Input</td>
<td>-</td>
<td>22.4 watts (30.8 W)</td>
<td>15.4 watts (23.8 W)</td>
</tr>
</tbody>
</table>
  (Aux with UPOE uplink)
Cisco Live!
July 10-14, 2016 • Las Vegas, NV
Your Time Is Now