CISCO VALIDATED DESIGN

Campus LAN Layer 2 Access with Simplified Distribution Deployment Guide

October 2015

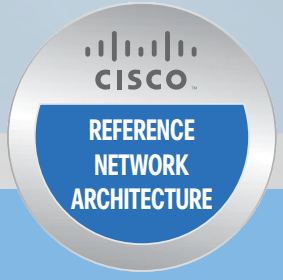


Table of Contents

Introduction

The guide describes how to deploy a wired network access with ubiquitous capabilities that scale from small environments (for instance, those environments with one to just a few LAN switches) to a large, campus-size LAN. Resiliency, security, and scalability are included to provide a robust communications environment. Quality of service (QoS) is integrated to ensure the base architecture can support a multitude of applications including low latency, drop-sensitive multimedia applications, that coexist with data applications on a single network.

The campus LAN architecture is designed to meet the needs of organizations with wired LAN connectivity requirements that range from a small, remote-site LAN to a large, multi-building location. The purpose of a campus network is to support arbitrary device connectivity for workers and users in the office and business spaces or meeting places of a building, such as for laptops, telephones, printers, and video conferencing systems. This is in contrast to the highly controlled connectivity for servers in a data center or machine and device connectivity in an industrial network or a WAN.

Many organizations have campus LAN requirements that include both wired and wireless access connected to a distribution layer, and some organizations have requirements to add a core or use alternative access and distribution designs. Deployment guidance presented in this guide focuses on a Layer 2 access connected to a simplified distribution layer. Other deployment alternatives are outside the scope of this guide, with many alternatives covered in Design Zone at http://cisco.com/go/designzone.

Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

As you review this guide, you may find it useful to understand the IP addressing and VLAN assignments used. Although your design requirements may differ, by addressing the various distribution layers at a location with contiguous IP address space, you can summarize the IP address range to the rest of the network. This design uses VLAN assignments that reflect the third octet of the IP address range for a given access layer switch for ease of reference. Alternatively, many organizations may choose to reuse the same VLAN IDs in each distribution—use and document the method that makes the most sense for your organization. The LAN Core IP addressing is a combination of 30-bit subnets for point-to-point Layer 3 links, and 32-bit host addresses for loopback addresses.

Table 1 *IP addressing for Campus Wired LAN Technology Design Guide*

Address block	Access VLAN	IP addressing	Usage
Distribution #1	100	10.4.0.0/24	Data-Access Switch 1
10.4.0.0/20	101	10.4.1.0/24	Voice-Access Switch 1
	102	10.4.2.0/24	Data-Access Switch 2
	103	10.4.3.0/24	Voice-Access Switch 2
	Continue through 113	10.4.4.0/24–10.4.13.0/24	alternate Data and Voice
	115	10.4.15.0/25	Management
	None	10.4.15.128/32–10.4.15.255/32	Distribution Loopback Interfaces

table continued on next page

table continued from previous page

Address block	Access VLAN	IP addressing	Usage
Distribution #2 10.4.64.0/20	164	10.4.64.0/24	Data-Access Switch 1
	165	10.4.65.0/24	Voice-Access Switch 1
	166	10.4.66.0/24	Data-Access Switch 2
	167	10.4.67.0/24	Voice-Access Switch 2
	Continue through 177	10.4.68.0/24–10.4.77.0/24	alternate Data and Voice
	179	10.4.79.0/25	Management
	None	10.4.79.128/32–10.4.79.255/32	Distribution Loopback Interfaces
Distribution #3 10.4.80.0/20	180	10.4.80.0/24	Data-Access Switch 1
	181	10.4.81.0/24	Voice-Access Switch 1
	182	10.4.82.0/24	Data-Access Switch 2
	183	10.4.83.0/24	Voice-Access Switch 2
	Continue through 193	10.4.84.0/24–10.4.93.0/24	alternate Data and Voice
	195	10.4.95.0/25	Management
	None	10.4.95.128/32–10.4.95.255/32	Distribution Loopback Interfaces
Distribution #4 10.4.96.0/20	196	10.4.96.0/24	Data-Access Switch 1
	197	10.4.97.0/24	Voice-Access Switch 1
	198	10.4.98.0/24	Data-Access Switch 2
	199	10.4.99.0/24	Voice-Access Switch 2
	Continue through 209	10.4.100.0/24–10.4.109.0/24	alternate Data and Voice
	211	10.4.111.0/25	Management
	None	10.4.111.128/32–10.4.111.255/32	Distribution Loopback Interfaces
Distribution #5 10.4.112.0/20	212	10.4.112.0/24	Data-Access Switch 1
	213	10.4.113.0/24	Voice-Access Switch 1
	214	10.4.114.0/24	Data-Access Switch 2
	215	10.4.115.0/24	Voice-Access Switch 2
	Continue through 225	10.4.116.0/24–10.4.125.0/24	alternate Data and Voice
	227	10.4.127.0/25	Management
	None	10.4.127.128/32–10.4.127.255/32	Distribution Loopback Interfaces
Core 10.4.40.0/24	None	10.4.40.0/30–10.4.40.124/30	Core to Distribution Links
	None	10.4.40.128/32–10.4.40.255/32	Core Loopback Interfaces

Layer 2 LAN Access Deployment

ACCESS LAYER PLATFORMS

Wiring Closets Requiring up to 48 Ports

Cisco Catalyst 2960-X and 3650 Series are economical 10/100/1000 Ethernet fixed-port switches that provide flexibility and common features required for wiring closets that can be supported by a single fixed port switch. Cisco Catalyst 2960-X and 3650 are available in both PoE+ and non-power-supplying versions and have optional support for stacking.

Cisco Catalyst 3650 additional capabilities include support for dual replaceable redundant power supplies, dual redundant fans, and enhanced enterprise options such as Cisco TrustSec and NetFlow. The Cisco Catalyst 3650 has an integrated wireless controller which optionally can be enabled for converged wired and wireless access.

Wiring Closets Requiring Greater than 48 Ports

When a wiring closet requires greater interface density than can be provided by a single switch, an intelligent stack of fixed configuration switches or a modular switch is recommended.

Intelligent stacks or modular Ethernet switches provide the following major benefits:

- **Single point of management**—All switches in the stack are managed as one.
- **Built-in redundancy and high availability**—The high-bandwidth dedicated stack connections provide redundant communication for each stack member.
- **Scalable to fit network needs**—As the need for additional access interfaces grows, adding a new switch to a stack or a module to a modular switch is easy.

The following series of Cisco Catalyst switches are used in this design when intelligent stacking or a modular deployment is required in a single access layer in a wiring closet: Cisco Catalyst 2960-X, 3650, 3850, and 4500E Series.

Cisco Catalyst 2960-X Series are fixed-configuration, stackable, 10/10/1000 Ethernet switches, with PoE+ and non-power-supplying versions designed for entry-level enterprise, midmarket, and remote site networks.

- Cisco FlexStack+ is implemented by adding a stacking module to the Cisco Catalyst 2960-X Series Switch. This enables up to eight Catalyst 2960-X series switches to be stacked together. Cisco FlexStack+ links are full duplex 20-Gbps links with typical recovery time between 1-2 seconds.

Cisco Catalyst 3650 Series and Catalyst 3850 Series Switches are fixed-port, stackable, 10/100/1000 Ethernet switches, with PoE+ and non-power-supplying versions, which provide enhanced switching performance and resiliency through StackWise-160 (Cisco Catalyst 3650) or StackWise-480 and StackPower technologies (Cisco Catalyst 3850), with Flexible NetFlow capabilities on all ports.

- Cisco Catalyst 3650 stacking is implemented with an optional stacking module. Switches stack together using StackWise-160 mode with up to nine switches in single stack-ring.
- Cisco Catalyst 3850 Series Switches have built-in stacking capability, and stack together using StackWise-480 mode with up to nine switches in single stack-ring.
- Cisco StackPower technology increases system-level resiliency during catastrophic power failure on a stack-member switch. Cisco StackPower enables power redundancy across a group of four Cisco Catalyst 3850 Series Switches within same stack. This allows the flexible arrangement of power supplies in the stack, and enables a zero-footprint redundant power supply deployment and intelligent load shedding.
- Cisco 3650 Series Switches have fixed uplinks that can be configured as Gigabit Ethernet or 10-Gigabit Ethernet.
- Cisco 3850 Series Switches have modular uplinks that can be configured as Gigabit Ethernet or 10-Gigabit Ethernet.
- Cisco Catalyst 3650 and Cisco Catalyst 3850 Series supports Stateful Switchover, which allows a switch in the active role in a stack to rapidly switchover to a switch in the standby role with minimum disruption to the network.
- With appropriate licenses, the Cisco Catalyst 3650 and Cisco Catalyst 3850 Series hardware supports wireless LAN controller functionality in order to support a unified access policy for converged wired and wireless designs.

Cisco Catalyst 4500E Series are modular switches that support multiple Ethernet connectivity options, including 10/100/1000 Ethernet, 100-Megabit fiber, Gigabit fiber, and 10-Gigabit fiber. The Catalyst 4500E Series Switches also have an upgradable supervisor module that enables future functionality to be added with a supervisor module upgrade while maintaining the initial investment in the chassis and the modules.

- All key switching and forwarding components are located on the supervisor module; upgrading the supervisor upgrades the line cards.
- The Cisco Catalyst 4500E Series Supervisor Engine 7-E and Supervisor Engine 7L-E have uplink interfaces that can be configured as Gigabit Ethernet or 10-Gigabit interfaces, allowing organizations to easily increase bandwidth in the future. The Supervisor Engine 8-E includes eight 10-Gigabit interfaces on board, along with integrated wireless LAN controller hardware which can be enabled in the future, and extends the range of performance up to 48-Gbps per slot and 928 Gbps system switching capacity.
- The Cisco Catalyst 4500E Series provides maximum PoE flexibility with support of IEEE 802.3af, 802.3at, and now Cisco UPOE, and supplies up to 60 watts per port of power over Ethernet. Cisco UPOE line cards are backward compatible to earlier PoE and PoE+ connected end points as well.
- The Cisco Catalyst 4507R+E chassis supports redundant supervisor modules and power supplies, which increases system availability by providing 1:1 redundancy for all critical systems. When configured with dual Supervisor modules, Stateful Switchover, which allows a supervisor switchover to occur with minimum disruption to the network.
- With a dual Supervisor Engine system, the entire software upgrade process is simplified by using In-Service Software Upgrade (ISSU). Not only does ISSU help eliminate errors in the software upgrade process, but additional checks are incorporated that allow the new software version to be tested and verified before completing the upgrade.

PROCESS

Configuring the Access Layer

1. Configure the platform
2. Configure LAN switch universal settings
3. Configure access switch global settings
4. Configure client connectivity
5. Connect to distribution or WAN router

Procedure 1 Configure the platform

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you do not have a platform listed for an option, skip that option and its steps.

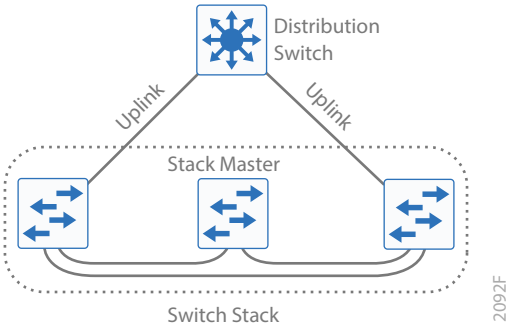
Option 1: Configure the Cisco Catalyst 2960-X

Step 1: If you are configuring a stack of switches, set the stack master switch.

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

When there are multiple Cisco Catalyst 2960-X Series Switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master. When three or more switches are configured as a stack, configure the stack master switch functionality on a switch that does not have uplinks configured.

Figure 1 *Stack master placement in a switch stack*



If you configure stack master switch priority on a Cisco Catalyst 2960-X switch stack, a single reload is required to force the stack master to operate on the switch that you configured with the highest priority. Reload the switch stack after all of your configuration is complete for this entire "Configuring the Access Layer" process.

Step 2: If you are configuring a stack, run the **stack-mac persistent timer 0** command. This ensures that the original stack master MAC address is used by any switch in the stack that takes the stack master role after a switchover.

```
Switch(config)#stack-mac persistent timer 0
```

The default behavior when the stack master switch fails is for the newly active stack master switch to assign a new stack MAC address. This new MAC address assignment can cause the network to reconverge because the link aggregation control protocol (LACP) and many other protocols rely on the stack MAC address and must restart.

Step 3: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. This design uses EtherChannels extensively because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load-balancing option.

```
port-channel load-balance src-dst-ip
```

Step 4: For each platform, define two macros that you will use in later procedures to apply the platform specific QoS configuration. This makes consistent deployment of QoS easier.

```
macro name AccessEdgeQoS
 auto qos voip cisco-phone
@
!
macro name EgressQoS
 mls qos trust dscp
 queue-set 1
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
@
```

Option 2: Configure the Cisco Catalyst 3650 and 3850 platform

Step 1: To configure a Cisco Catalyst 3650 or 3850 stack, use the CLI global exec mode (not configuration mode) to set the preferred active switch and the preferred hot-standby switch.

```
switch [switch number] priority 15
switch [switch number] priority 14
```

When there are multiple Cisco Catalyst 3650 or 3850 Series Switches configured in a stack, one of the switches takes the ACTIVE switch role, and another member takes the STANDBY HOT role. Upon reload, the switch configured with the highest priority assumes the active role, and a switch with the next-best priority is selected for the STANDBY HOT role. If this is a new configuration, only the active switch console is active during the initial configuration. When three or more switches are configured as a stack, configure the active switch functionality on a switch without infrastructure uplink connections. When four or more switches are configured as a stack, configure the standby switch functionality on a switch without infrastructure uplink connections.

Step 2: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. This design uses EtherChannels extensively because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load-balancing option.

```
port-channel load-balance src-dst-mixed-ip-port
```

Step 3: For each platform, define two macros that you will use in later procedures to apply the platform-specific QoS configuration. This makes consistent deployment of QoS easier.

Tech Tip

The match statements in the class-maps can be combined into one line. However, listing them separately provides additional per-DSCP counters available from SNMP and from the following verification command.

```
show policy-map interface
table-map policed-dscp
 map from 0 to 8
 map from 10 to 8
 map from 18 to 8
 map from 24 to 8
 map from 46 to 8
 default copy
!
class-map match-any CISCO-PHONE-VOICE
  match cos 5
class-map match-any CISCO-PHONE-SIGNALING
  match cos 3
!
class-map match-any PRIORITY-QUEUE
  match  dscp ef
class-map match-any VIDEO-PRIORITY-QUEUE
  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
  match  dscp af42
  match  dscp af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match  dscp af31
  match  dscp af32
  match  dscp af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-any BULK-SCAVENGER-DATA-QUEUE
  match  dscp af11
  match  dscp af12
  match  dscp af13
  match  dscp cs1
!
policy-map CISCO-PHONE
 class CISCO-PHONE-VOICE
    set dscp ef
   police cir 128000 bc 8000
     conform-action transmit
     exceed-action set-dscp-transmit dscp table policed-dscp
 class CISCO-PHONE-SIGNALING
    set dscp cs3
   police cir 32000 bc 8000
     conform-action transmit
     exceed-action set-dscp-transmit dscp table policed-dscp
 class class-default
    set dscp default
!
policy-map 2P6Q3T
 class PRIORITY-QUEUE
    priority level 1
    police rate percent 10
```

```
 class VIDEO-PRIORITY-QUEUE
    priority level 2
    police rate percent 20
 class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
 class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af43 percent 80
    queue-limit dscp af42 percent 90
    queue-limit dscp af41 percent 100
 class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af33 percent 80
    queue-limit dscp af32 percent 90
    queue-limit dscp af31 percent 100
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af23 percent 80
    queue-limit dscp af22 percent 90
    queue-limit dscp af21 percent 100
 class BULK-SCAVENGER-DATA-QUEUE
    bandwidth remaining percent 5
    queue-buffers ratio 10
    queue-limit dscp values af13 cs1 percent 80
    queue-limit dscp values af12 percent 90
    queue-limit dscp values af11 percent 100
 class class-default
    bandwidth remaining percent 25
    queue-buffers ratio 25
!
macro name AccessEdgeQoS
 trust device cisco-phone
```

```
 service-policy input CISCO-PHONE
 service-policy output 2P6Q3T
@
!
macro name EgressQoS
 service-policy output 2P6Q3T
@
```

Step 4: Configure the Cisco Catalyst 3650 or 3850 stack to automatically upgrade the software of new switches introduced into the stack to the level of the active switch, allowing full stack operability.

```
Switch(config)#software auto-upgrade enable
```

Step 5: If you are using a Cisco Catalyst 3850 with StackPower technology, ensure enough power is available during any power supply failure in order to support the entire stack during the degraded mode of operation, and configure the non-default redundant mode of operation for each switch in the stack.

```
Switch(config)#stack-power stack PowerStack-1
Switch(config-stackpower)#mode redundant
Switch(config)#stack-power switch 1
Switch(config-stackpower)# stack PowerStack-1
Switch(config)#stack-power switch 2
Switch(config-stackpower)# stack PowerStack-1
```

Option 3: Configure the Cisco Catalyst 4507R+E platform

Step 1: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. EtherChannels are used extensively in this design because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load balancing option.

```
port-channel load-balance src-dst-ip
```

Step 2: For each platform, define two macros that you will use in later procedures to apply the platform-specific QoS configuration. This makes consistent deployment of QoS easier.

```
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
  match  dscp af42
  match  dscp af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match  dscp af31
  match  dscp af32
  match  dscp af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-any BULK-DATA-QUEUE
  match  dscp af11
  match  dscp af12
  match  dscp 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
 auto qos voip cisco-phone
@
!
macro name EgressQoS
 service-policy output 1P7Q1T
@
```

Step 3: When a Cisco Catalyst 4507R+E is configured with two Supervisor Engine 7L-E, 7-E, or 8-E modules, configure the switch to use stateful switchover (SSO) when moving the primary supervisor functionality between modules. SSO synchronizes active process information as well as configuration information between supervisor modules, which enables a fast transparent data plane failover.

```
redundancy
  mode sso
```

Tech Tip

To enable SSO mode you must have a license level of ipbase or entservices operating on the switch supervisors. You can check the current license level of operation with a **show version** command.

Procedure 2 Configure LAN switch universal settings

Within this design, there are features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.

This procedure provides examples for some of those settings. The actual settings and values will depend on your current network configuration.

Table 2 Common network services used in the deployment examples

Setting	Value
Domain Name	cisco.local
Active Directory, DNS, DHCP Server	10.4.48.10
Authentication Control System	10.4.48.15
Network Time Protocol Server	10.4.48.17

Step 1: Configure the device hostname to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: If the switch VLAN Trunking Protocol (VTP) mode has been changed from default, configure VTP transparent mode. This design uses VTP transparent mode because the benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior resulting from operational error.

VTP allows network managers to configure a VLAN in one location of the network and have that configuration dynamically propagate out to other network devices. However, in most cases, VLANs are defined once during switch setup with few, if any, additional modifications.

```
vtp mode transparent
```

Step 3: Enable Rapid Per-VLAN Spanning-Tree (PVST+). Rapid PVST+ provides an instance of RSTP (802.1w) per VLAN. Rapid PVST+ greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D).

Although this architecture is built without any Layer 2 loops, you should still enable spanning tree with the most up-to-date network safeguards. By enabling spanning tree, you ensure that if any physical or logical loops are accidentally configured, no actual layer 2 loops occur.

```
spanning-tree mode rapid-pvst
```

Step 4: Enable Unidirectional Link Detection (UDLD) as the default for fiber ports.

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected interface and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree loops, black holes, and non-deterministic forwarding. In addition, UDLD enables faster link failure detection and quick reconvergence of interface trunks, especially with fiber, which can be susceptible to unidirectional failures.

```
udld enable
```

Step 5: Enable the recovery mechanism to allow ports disabled as a result of errors to automatically clear the err-disable status and attempt a recovery to operational behavior and connected status. Enabling the recovery mechanism avoids having to intervene manually by using the CLI to shutdown and enable the port after the cause of the error is cleared. By default, the recovery mechanism waits five minutes to attempt clearing of the interface err-disable status.

```
errdisable recovery cause all
```

Step 6: Configure DNS for host lookup.

At the command line of a Cisco IOS device, it is helpful to be able to type a domain name instead of the IP address for a destination.

```
ip name-server 10.4.48.10
```

Step 7: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

The SSH and HTTPS protocols enable secure management of the LAN device. Both protocols are encrypted for privacy, and the unencrypted protocols, Telnet and HTTP, are turned off. Enabling HTTPS automatically generates a cryptographic key to use the service. When SSH is configured after HTTPS, you do not have to explicitly generate the cryptographic key that SSH requires, unless you wish to change the default key size.

Secure Copy (SCP) provides a secure and authenticated method for copying configuration and image files by making use of SSH as a secure transport. Enable SCP to allow secure file management with the device to avoid the use of less secure protocols such as TFTP and FTP.

Specify the transport preferred none on vty lines in order to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name server is unreachable, long timeout delays may occur for mistyped commands.

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

Step 8: Enable Simple Network Management Protocol (SNMP) in order to allow the network infrastructure devices to be managed by a Network Management System (NMS), and then configure SNMPv2c both for a read-only and a read-write community string.

```
snmp-server community [SNMP read-only name] ro
snmp-server community [SNMP read-write name] rw
```

Step 9: If your network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
ip access-list standard MANAGEMENT
  permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class MANAGEMENT in
!
snmp-server community [SNMP read-only name] ro MANAGEMENT
snmp-server community [SNMP read-write name] rw MANAGEMENT
```

The Cisco Catalyst 3650 and 3850 Series Switches have an additional keyword to be added to the access-class, which allows console access from other switch members to not be affected.

```
line vty 0 15
  access-class MANAGEMENT in vrf-also
```

Caution

If you configure an access-list on the vty interface, you may lose the ability to use SSH to log in from one device to the next for hop-by-hop troubleshooting.

Step 10: Configure local login and password.

The local login account and password provide basic device access authentication to view platform operation. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the use of plain text passwords when viewing configuration files. The **aaa new-model** command enables new access control commands and functions, and causes the local username and password on the router to be used in the absence of other AAA statements.

```
username admin secret [user password]
enable secret [enable password]
service password-encryption
aaa new-model
```

By default, https access to the switch uses the enable password for authentication.

Step 11: If you want to reduce operational tasks per device, configure centralized user authentication by using the TACACS+ protocol to authenticate management logins on the infrastructure devices to the authentication, authorization and accounting (AAA) server.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
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
```

Step 12: Configure a synchronized clock by programming network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```
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
```

The **ntp update-calendar** command configures the switch to update the hardware clock from the ntp time source periodically. Since not all switches have a hardware clock, this command is not supported by all devices.

Procedure 3 Configure access switch global settings

The access layer devices use VLANs to separate traffic from different devices into the following logical networks:

- 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.

  Both the data and the voice VLAN are configured on all user-facing interfaces.
- The management VLAN provides in-band access to the network for the switches management interface. The management VLAN is not configured on any user-facing interface and the VLAN interface of the switch is the only member.

Step 1: Configure VLANs on the switch.

Configure the data, voice, and management VLANs on the switch so that connectivity to clients, IP phones, and the in-band management interfaces can be configured. These are the most common examples, and organizations can reduce or increase VLANs for access segmentation as needed to support security systems, IP cameras, Wireless LANs, etc.

```
vlan [data vlan]
  name Data
exit
vlan [voice vlan]
  name Voice
exit
vlan [management vlan]
  name Management
exit
```

Tech Tip

If the switch is the only switch at the site and is directly connected to a router or firewall, do not configure a management VLAN. Instead, use the data VLAN for both data and switch management. When you use this configuration, the next step requires that you also configure the in-band management interface VLAN using the data VLAN ID. For example:

```
interface vlan [data vlan]
  description In-band switch management using data VLAN
  ip address [ip address] [mask]
  no shutdown
```

Step 2: Configure the switch with an IP address so that it can be managed via in-band connectivity.

```
interface vlan [management vlan]
  ip address [ip address] [mask]
  no shutdown
ip default-gateway [default router]
```

Do not use the **ip default-gateway** command on Cisco Catalyst 4500 because it has IP routing enabled by default and this command will not have any effect. Instead use the following command on the Cisco Catalyst 4500.

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

Step 3: Configure DHCP snooping and enable it on the data and voice VLANs. The switch intercepts and safeguards DHCP messages within the VLAN. This ensures that an unauthorized DHCP server cannot serve up addresses to end-user devices.

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

Step 4: Configure ARP inspection on the data and voice VLANs.

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

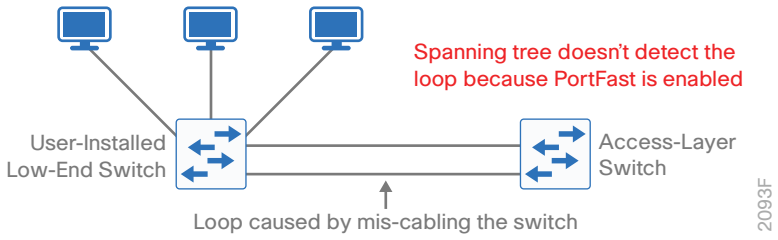
Step 5: Configure the Bridge Protocol Data Unit (BPDU) Guard global setting to protect PortFast-enabled interfaces.

```
spanning-tree portfast bpduguard default
```

This automatically disables any PortFast-enabled interface if it receives BPDUs protecting against an accidental topology loop which could cause data packet looping and disrupt switch and network operation. You configure the PortFast feature for interfaces in a later step.

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

Figure 2 *Scenario that BPDU Guard protects against*



Step 6: Configure the IPv6 First Hop Security global policy for host ports. This global policy is referenced by the access-layer port configuration to intercept and drop IPv6 router advertisements from connected devices. Blocking the advertisements mitigates intentional and unintentional denial-of-service attacks and man-in-the-middle attacks among devices connected to the access layer, and is beneficial regardless of the use of IPv4 or IPv6 routing configuration in the rest of the network.

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

Tech Tip

Default configurations and default options may not be displayed when you use the **show running-configuration** command. To see the configuration including default options, you can use the **all** option and filter the results as you desire. For example, to see the previous configuration with the default device-role that is applied, enter the following command:

```
show running-config all | section raguard
```

Procedure 4 Configure client connectivity

To make configuration easier when the same configuration is applied to multiple interfaces on the switch, use the **interface range** command. This command allows you to issue a command once and have it apply to many interfaces at the same time. Since most of the interfaces in the access layer are configured identically, it can save a lot of time. For example, the following command allows you to enter commands on all 24 interfaces (Gig 0/1 to Gig 0/24) simultaneously.

```
interface range GigabitEthernet 0/1-24
```

Step 1: Configure switch interfaces to support clients and IP phones.

The host interface configurations support PCs, phones, or wireless access points. Inline power is available on switches that support 802.3AF/AT for capable devices.

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

Step 2: Because only end-device connectivity is provided at the access layer, optimize the interface for device connectivity by applying the switchport host command.

```
  switchport host
```

This command does three things: it applies switchport access mode participation as an access port in a VLAN; it enables PortFast, which moves the interface directly into spanning-tree forwarding state, reducing the time it takes for the interface to start forwarding packets; and it also removes any existing channel-group configuration, which is incompatible with an access configuration.

Step 3: Reduce the length of time used for computing interface load average statistics. Reducing the time allows you to display more current and instantaneous data, which is useful for quickly observing interface load value changes during traffic bursts.

```
load-interval 30
```

Step 4: Configure 11 MAC addresses to be active on the interface at one time; additional MAC addresses are considered to be in violation, and their traffic will be dropped.

```
switchport port-security maximum 11
switchport port-security
```

The number of MAC addresses allowed on each interface is specific to the organization. However, the popularity of virtualization applications, IP phones, and passive hubs on the desktop drives the need for the number to be larger than one might guess at first glance. This design uses a number that allows flexibility in the organization while still protecting the network infrastructure.

Step 5: Set an aging time to remove learned MAC addresses from the secured list after 2 minutes of inactivity.

```
switchport port-security aging time 2
switchport port-security aging type inactivity
```

The timeout you choose is an arbitrary time. You may tune the time to fit your environment. Using aggressive timers can impact the switch CPU, so use caution when lowering this from the default value defined on your switch.

Step 6: Configure the restrict option to drop traffic from MAC addresses that are in violation, but do not shut down the port. This configuration ensures that an IP phone can still function on this interface when there is a port security violation.

```
switchport port-security violation restrict
```

Step 7: Configure DHCP snooping and ARP inspection on the interface to process 100 packets per second of traffic on the port.

```
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
```

The packets per second rate that you choose is an arbitrary rate. You may tune this value to fit your environment.

Step 8: Configure IP Source Guard on the interface. IP Source Guard is a means of preventing IP spoofing.

```
ip verify source
```

If you have a Cisco Catalyst 4500, use the following command instead because Catalyst 4500 requires an additional keyword for the **ip verify source** command.

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

Step 9: Attach the IPv6 First Hop Security policy to the interface. This configuration uses the IPv6 FHS global policy you previously created for devices connecting to the access layer.

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

Step 10: Enable QoS by applying the access edge QoS macro that was defined in the platform configuration procedure. This macro generates a QoS configuration appropriate for the platform.

```
macro apply AccessEdgeQoS
```

All client-facing interfaces allow for an untrusted PC and/or a trusted Cisco IP phone to be connected to the switch and automatically set QoS parameters. When a Cisco IP Phone is connected, trust is extended to the phone and any device that connects to the phone will be considered untrusted and all traffic from that device will be remarked to best-effort or class of service (CoS) 0.

Tech Tip

When you apply this macro, device-specific QoS using is applied and a service policy is imposed on the interface. An example policy application to the interface may look like:

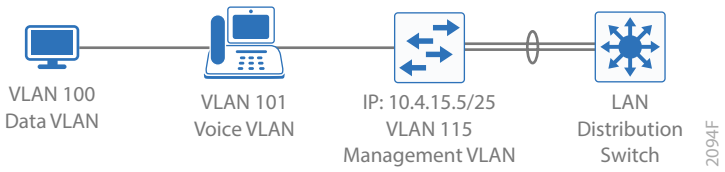
```
service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
```

In this case, the policy-map called by the service-policy comes preconfigured in the software running on the platform.

Step 11: If the access switch is a Cisco Catalyst 2960-X, increase the buffers for the default queue. This modification of the global QoS settings improves the ability to handle high bandwidth bursty traffic in the default queue, by overriding one of the settings previously applied using the AccessEdgeQoS macro. In global configuration mode, add the following command:

```
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

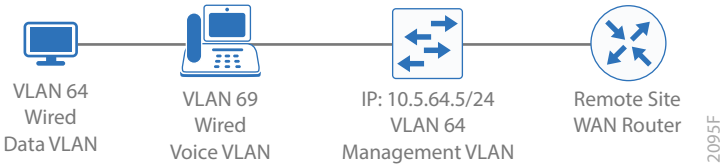
Example: Connected to Distribution Switch




```
vlan 100
  name Data
vlan 101
  name Voice
vlan 115
  name Management
!
interface vlan 115
  description In-band Management
  ip address 10.4.15.5 255.255.255.0
```

```
  no shutdown
!
ip default-gateway 10.4.15.1
!
ip dhcp snooping vlan 100,101
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 100,101
!
spanning-tree portfast bpduguard default
!
ipv6 nd raguard policy HOST_POLICY
  device-role host
!
interface range GigabitEthernet 1/0/1-24
  switchport access vlan 100
  switchport voice vlan 101
  switchport host
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip arp inspection limit rate 100
  ip dhcp snooping limit rate 100
  ip verify source
  ipv6 nd raguard attach-policy HOST_POLICY
  macro apply AccessEdgeQoS
!
! Next QoS Command for Cisco Catalyst 2960-X
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

Example: Connected to WAN Router at a small site




```
vlan 64
  name WiredData
vlan 69
  name WiredVoice
!
interface vlan 64
  description In-band Management to WAN Router
  ip address 10.5.64.5 255.255.255.0
  no shutdown
!
ip default-gateway 10.5.64.1
!
ip dhcp snooping vlan 64,69
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 64,69
!
spanning-tree portfast bpduguard default
!
ipv6 nd raguard policy HOST_POLICY
  device-role host
!
interface range GigabitEthernet 1/0/1-24
  switchport access vlan 64
  switchport voice vlan 69
  switchport host
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
```

```
  ip arp inspection limit rate 100
  ip dhcp snooping limit rate 100
  ip verify source
  ipv6 nd raguard attach-policy HOST_POLICY
  macro apply AccessEdgeQoS
!
! Next QoS Command for Cisco Catalyst 2960-X
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

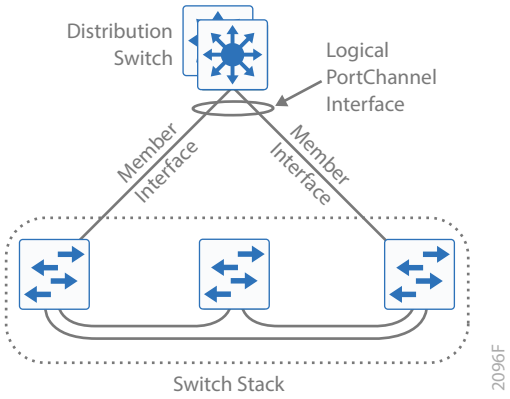
Procedure 5 Connect to distribution or WAN router

Access layer devices can be one component of a larger LAN and connect to a distribution switch, or, in the case of a small remote site, might be the only LAN device and connect directly to a WAN device. Unless the access layer device is a single fixed configuration switch connecting to a WAN router, Layer 2 EtherChannels are used to interconnect the devices in the most resilient method possible.

When using EtherChannel, the member interfaces should be on different switches in the stack or different modules in the modular switch for the highest resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. This allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Figure 3 *EtherChannel example*



Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two.

This procedure details how to connect any access layer switch (Cisco Catalyst 4500, 3850, 3650, or 2960-X) or to a distribution switch or WAN router. Where there are differences for configuring a specific switch, the differences are called out in the step. If the upstream device is not a distribution switch (such as a remote site connection to a router) use Option 2 with an interface type that is appropriate for the deployment.

Option 1: Configure EtherChannel to distribution switch

This design uses Layer 2 EtherChannels to connect all access layer switches to the distribution layer. When connecting to another switch, use two links or a multiple of two links distributed for maximum resiliency. The example shows a configuration with four links.

Step 1: If you are using LACP, follow this step, and then proceed to step 3. If instead you are using PAgP, skip this step and follow Step 2.

Set Link Aggregation Control Protocol negotiation to active on both sides in order to ensure a proper EtherChannel is formed. Also, apply the egress QoS macro that was defined in the platform configuration procedure in order to ensure that traffic is prioritized appropriately.

Cisco Catalyst 2960-X Series Switches do not require the **switchport** command, and the Cisco Catalyst 4500 does not use the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to Distribution Layer Port 1
interface [interface type] [port 2]
  description Link to Distribution Layer Port 2
interface [interface type] [port 3]
  description Link to Distribution Layer Port 3
interface [interface type] [port 4]
  description Link to Distribution Layer Port 4
!
interface range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  switchport
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
```

Step 2: If you are using PAgP instead of LACP, follow this step.

Set Cisco Port Aggregation Protocol negotiation to preferred on both sides in order to ensure a proper EtherChannel is formed. Also, apply the egress QoS macro that was defined in the platform configuration procedure in order to ensure traffic is prioritized appropriately.

Cisco Catalyst 2960-X Series Switches do not require the **switchport** command, and the Cisco Catalyst 4500 does not use the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to Distribution Layer Port 1
```

```
interface [interface type] [port 2]
  description Link to Distribution Layer Port 2
interface [interface type] [port 3]
  description Link to Distribution Layer Port 3
interface [interface type] [port 4]
  description Link to Distribution Layer Port 4
!
interface range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  switchport
  channel-protocol pagp
  channel-group [number] mode desirable
  logging event link-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
```

Step 3: Configure the VLAN trunk interface to the upstream device.

An 802.1Q trunk is used for the connection to this upstream device, which allows the uplink to provide Layer 3 services to all the VLANs defined on the access layer switch. Using a trunk even for a single access VLAN allows for easier VLAN additions in the future. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access switch. Set DHCP Snooping and ARP Inspection to trust.

Because the upstream device is a distribution switch, you use an EtherChannel—the interface type is port-channel and the number must match channel-group configured for the member link physical interfaces.

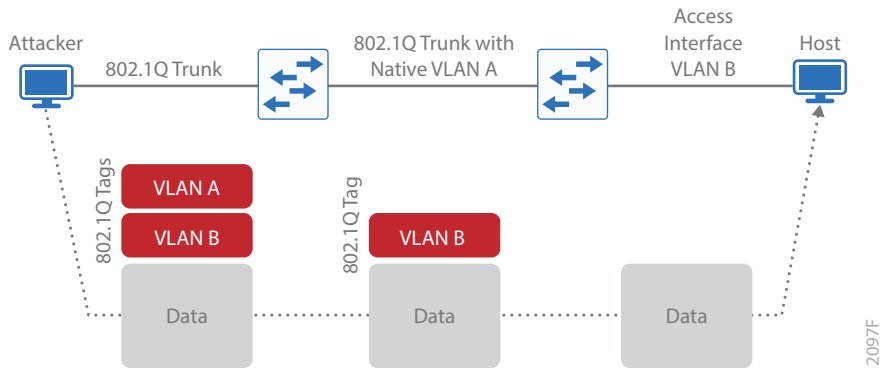
```
interface [interface type] [number]
  description EtherChannel Link to Distribution Layer
  switchport trunk allowed vlan [data vlan],[voice vlan],
    [management vlan]
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  logging event trunk-status
  no shutdown
  load-interval 30
exit
```

If the interface type is not a port-channel, you must configure an additional command **macro apply EgressQoS** on the interface.

In the next step, you mitigate VLAN hopping on the trunk for switch-to-switch connections.

There is a remote possibility that an attacker can create a double 802.1Q encapsulated packet. If the attacker has specific knowledge of the 802.1Q native VLAN, a packet could be crafted that when processed, the first or outermost tag is removed when the packet is switched onto the untagged native VLAN. When the packet reaches the target switch, the inner or second tag is then processed and the potentially malicious packet is switched to the target VLAN.

Figure 4 *VLAN hopping attack*



At first glance, this appears to be a serious risk. However, the traffic in this attack scenario is in a single direction and no return traffic can be switched by this mechanism. Additionally, this attack cannot work unless the attacker knows the native VLAN ID.

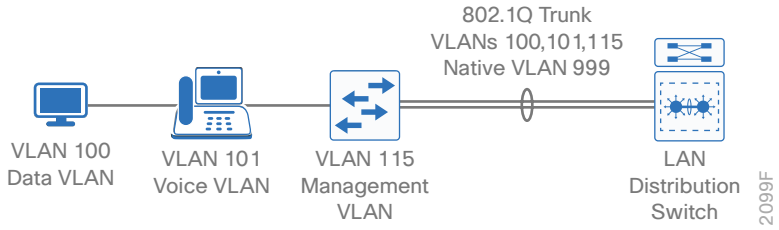
Step 4: Configure an unused VLAN on all switch-to-switch 802.1Q trunk links from access layer to distribution layer. This configuration mitigates the remote risk of a VLAN hopping attack. Choosing an arbitrary, non-default, unused VLAN assignment for the native VLAN reduces the possibility that a double 802.1Q-tagged packet can hop VLANs. If you are running the recommended EtherChannel uplink to the LAN access layer switch, configure the **switchport trunk native vlan** on the port-channel interface.

```
vlan 999
  name AntiVLANhopping
exit
!
interface [port-channel] [number]
  switchport trunk native vlan 999
```

Step 5: After leaving configuration mode, save the running configuration that you have entered so it will be used as the startup configuration file when your switch is reloaded or power-cycled.

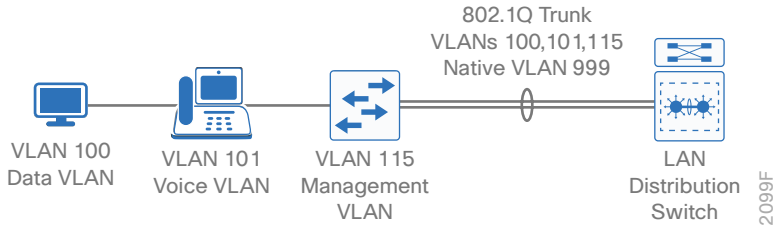
```
copy running-config startup-config
```

Example: Option 1, with LACP




```
vlan 999
  name AntiVLANhopping
!
interface GigabitEthernet 1/0/25
  description Link to Distribution Layer port 1
interface GigabitEthernet 3/0/25
  description Link to Distribution Layer port 2
interface GigabitEthernet 1/0/26
  description Link to Distribution Layer port 3
interface GigabitEthernet 3/0/26
  description Link to Distribution Layer port 4
!
interface range GigabitEthernet 1/0/25, GigabitEthernet 3/0/25, GigabitEthernet
1/0/26, GigabitEthernet 3/0/26
  logging event link-status
  logging event bundle-status
  channel-protocol lacp
  channel-group 1 mode active
  load-interval 30
  macro apply EgressQoS
!
interface Port-channel 1
  description EtherChannel to Distribution Layer
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100,101,115
  switchport mode trunk
  logging event trunk-status
  ip arp inspection trust
  ip dhcp snooping trust
  load-interval 30
  no shutdown
```

Example: Option 1, with PAgP




```
vlan 999
  name AntiVLANhopping
!
interface GigabitEthernet 1/0/25
  description Link to Distribution Layer port 1
interface GigabitEthernet 3/0/25
  description Link to Distribution Layer port 2
interface GigabitEthernet 1/0/26
  description Link to Distribution Layer port 3
interface GigabitEthernet 3/0/26
  description Link to Distribution Layer port 4
!
interface range GigabitEthernet 1/0/25, GigabitEthernet 3/0/25, GigabitEthernet
1/0/26, GigabitEthernet 3/0/26
  logging event link-status
  logging event bundle-status
  channel-protocol pagp
  channel-group 1 mode desirable
  load-interval 30
  macro apply EgressQoS
!
interface Port-channel 1
  description EtherChannel to Distribution Layer
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100,101,115
  switchport mode trunk
  logging event trunk-status
  ip arp inspection trust
  ip dhcp snooping trust
  load-interval 30
  no shutdown
```

Option 2: Configure Connection to WAN router

If your access layer switch is a single fixed configuration switch connecting to a single remote-site router without using EtherChannel, you can skip Step 1.

Step 1: Configure EtherChannel member interfaces.

When connecting to a network infrastructure device that does not support LACP, like a router, set the **channel-group mode** to be forced on.

Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

Cisco Catalyst 2960S and 2960-X do not require the **switchport** command, and the Cisco Catalyst 4500 does not use the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to Router Port 1
interface [interface type] [port 2]
  description Link to Router Port 2
!
interface range [interface type] [port 1], [interface type] [port 2]
  switchport
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
```

Step 2: Configure the VLAN trunk interface to the upstream device.

An 802.1Q trunk is used for the connection to this upstream device, which allows the router to provide Layer 3 services to all the VLANs defined on the access layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access switch. Set DHCP snooping and ARP Inspection to trust.

When using EtherChannel, the interface type is port-channel, and the number must match channel-group configured in Step 1 in this procedure. For deployments other than EtherChannel, interface type is one appropriate for your deployment.

```
interface [interface type] [number]
  description Trunk Interface to Router
  switchport trunk allowed vlan [data vlan],[voice vlan],[optional transit vlan]
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
```

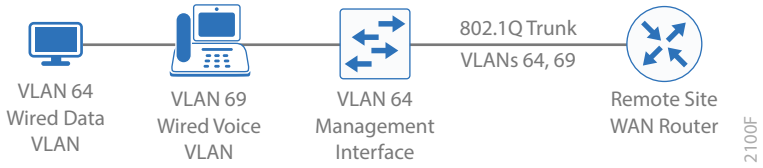
```
spanning-tree portfast trunk
logging event link-status
logging event trunk-status
load-interval 30
no shutdown
```

If the interface type is not a port-channel, you must configure additional commands **switchport** and **macro apply EgressQoS** on the interface.

Step 3: Save the running configuration that you have entered so it will be used as the startup configuration file when your switch is reloaded or power-cycled.

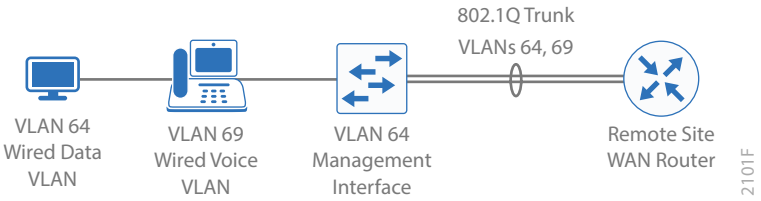
```
copy running-config startup-config
```

Example: Option 2, without EtherChannel




```
interface GigabitEthernet 1/0/24
  description Link to WAN Router
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69,99
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  spanning-tree portfast trunk
  macro apply EgressQoS
  no shutdown
```

Example: Option 2, with EtherChannel




```
interface GigabitEthernet 1/0/25
  description Link to WAN Router Port 1
interface GigabitEthernet 3/0/25
  description Link to WAN Router Port 2
!
interface range GigabitEthernet 1/0/25, GigabitEthernet 3/0/25
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  channel-group 1 mode on
  macro apply EgressQoS
!
interface Port-channel 1
  description EtherChannel to WAN Router
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  spanning-tree portfast trunk
  load-interval 30
  no shutdown
```

Simplified Distribution Layer Deployment

DISTRIBUTION LAYER PLATFORMS

You can use multiple platforms to deploy the simplified distribution layer design. Physically, the distribution layer can be a Cisco Catalyst 6500 Virtual Switching System (VSS), a Cisco Catalyst 4500-X VSS, a highly available Cisco Catalyst 4507R+E switch pair in VSS mode, or a stack of Cisco Catalyst 3850 switches. It is important to note that although each switch has different physical characteristics, each appears to the rest of the network as a single node and provides a fully resilient design.

Cisco Catalyst 6807-XL and 6500-E VSS

The Cisco Catalyst 6500-E and 6807-XL chassis with the Supervisor Engine 2T are the premier distribution layer platforms.

- Cisco Catalyst 6807-XL VSS uses two physical chassis with Cisco Catalyst 6500 Supervisor Engine 2T, which offers a per slot switching capacity of 220 Gbps in the Cisco Catalyst 6807-XL chassis, and delivers hardware-enabled scalability and features. The performance is increased over the same Supervisor Engine in the 6500-E chassis enabling the system to provide 40-Gigabit Ethernet connectivity and growth capability for future 100-gigabit Ethernet connectivity.
- Cisco Catalyst 6500 VSS uses Cisco Catalyst 6500 Supervisor Engine 2T, which offers per slot switching capacity of 80 Gbps in the Cisco Catalyst 6500-E Series chassis and delivers hardware-enabled scalability and features. This level of performance enables the system to provide 40-gigabit Ethernet uplinks for core layer connectivity.
- Adding an additional Cisco Catalyst 6500 Supervisor Engine 2T to each chassis in the VSS pair for a total of four supervisors creates a Quad-Supervisor SSO (VS4O) configuration, offering the ability to have an in-chassis standby supervisor capability. The in-chassis standby enables Enhanced Fast Software Upgrades (eFSU) for minimal downtime during software upgrades, along with the ability to recover from a degraded state of performance upon loss of a supervisor, without human intervention.
- Cisco 6500 Supervisor Engine 2T supports the line cards with Distributed Forwarding Card 4-E (DFC4-E), including the WS-X6816-10G, WS-X6908-10G, and WS-X6904-40G-2T, which provide enhanced hardware capabilities. The WS-X6908-10G provides eight 10-Gbps Ethernet ports with 1:1 oversubscription. The WS-X6904-40G-2T provides up to four 40-Gbps Ethernet ports or up to sixteen 10-Gbps Ethernet ports using modular adapters and can be programmed to run in 2:1 or 1:1 oversubscription mode.
- The Supervisor Engine 2T supports DFC4-A based line cards, including the WS-X6824 and WS-X6848, to provide gigabit Ethernet ports. The WS-X6724 and WS-X6748 gigabit Ethernet cards are also supported when installed with CFC or DFC4-A modules.
- The Supervisor Engine 2T-based switch enhances support for Cisco TrustSec (CTS) by providing MacSec encryption and role-based access control lists (RBACL), and delivers improved control plane policing to address denial-of-service attacks.
- VSS effectively allows the merging of two physical chassis into a logical entity that can be operated as a single device. This configuration provides redundant chassis, supervisors, line cards, and power supplies and can provide the highest density of the product options for Gigabit Ethernet, 10 Gigabit Ethernet, and 40-Gigabit EtherChannel uplinks using Cisco Multi-chassis EtherChannel (MEC).

- Provides Stateful Switch-Over (SSO) to synchronize infrastructure and forwarding state between chassis, along with Non-Stop Forwarding (NSF) for graceful-restart of L3 routing protocols, in the event of a chassis failure. Also allows Enhanced Fast Software Upgrades (EFSU) with In-Service Software Upgrades (ISSU) for minimizing downtime for system upgrades.
- The Cisco Catalyst 6500-E and 6807-XL chassis with the Supervisor Engine 2T are the premier distribution layer platforms. They allow for high density aggregation of wiring closets connected with Gigabit Ethernet and 10-Gigabit Ethernet, while providing an advanced feature set and the highest resiliency of the available platforms.

Cisco Catalyst 6880-X VSS

- Cisco Catalyst 6880-X VSS uses Cisco Catalyst 6880-X Series extensible fixed aggregation switch, with the Cisco Catalyst 6500 feature set in a small form factor.
- The Cisco Catalyst 6800-X Series is a resilient chassis offering N+1 redundant fans and 1+1 resilient power supplies, along with the capability for two switches to be paired into a resilient single logical Virtual Switching System.
- The base chassis comes with 16 SFP+ ports supporting 1-Gigabit Ethernet and 10-Gigabit Ethernet services, and an additional four slots available for extensible port cards to allow for future growth. For example, adding C6880-X-16P10G 16-port 10-Gigabit Ethernet cards enables up to a total of 80-ports of 10-Gigabit Ethernet in the chassis. The chassis is also designed with the capability to support 40-Gigabit Ethernet and 100-Gigabit Ethernet, with future port cards, and a backplane capable of delivering 220-Gbps per slot.
- Provides Stateful Switch-Over (SSO) to synchronize infrastructure and forwarding state between chassis, along with Non-Stop Forwarding (NSF) for graceful-restart of L3 routing protocols, in the event of a chassis failure. Also allows Enhanced Fast Software Upgrades (EFSU) with In-Service Software Upgrades (ISSU) for minimizing downtime for system upgrades.
- Cisco Catalyst 6880-X is the premier fixed distribution layer platform in this design. It allows for medium density aggregation of Gigabit Ethernet and 10 Gigabit Ethernet connected wiring closets, while providing an advanced feature set and the highest resiliency of the available platforms.

Cisco Catalyst 4500-X VSS

- Cisco Catalyst 4500-X Series switch family includes 32-port 10-Gigabit Ethernet and 16-port 10-Gigabit Ethernet switches both with a slot for adding an optional 8-port 10-Gigabit Ethernet module.
- Cisco Catalyst 4500-X Series has resiliency capabilities including redundant hot swappable fans and power supplies, in addition to the capability for two switches to be paired into a resilient single logical Virtual Switching System.
- Provides Stateful Switchover to synchronize infrastructure and forwarding state between chassis, along with Nonstop Forwarding for graceful-restart of L3 routing protocols in the event of a chassis failure, which also allows In-Service Software Upgrade (ISSU) functionality for the system.
- Cisco Catalyst 4500-X Series can be used at locations where there is a smaller number of Gigabit Ethernet or 10 Gigabit Ethernet connected wiring closets that need to be aggregated.

Cisco Catalyst 4507R+E VSS

- The Cisco Catalyst 4507R+E switch supports redundant supervisors, line cards, and power supplies. In this design, two 4507R+E chassis are paired into a resilient single logical Virtual Switching System distribution layer platform. The Cisco Catalyst 4500 Supervisor Engine 7-E has the ability to provide a medium density of Gigabit Ethernet and even 10-Gigabit Ethernet EtherChannel links to the access layer.
- Provides Stateful Switchover between supervisors in the VSS pair, to synchronize infrastructure and forwarding state between chassis, along with Nonstop Forwarding for graceful-restart of L3 routing protocols in the event of a chassis failure, which also allows In-Service Software Upgrade (ISSU) functionality for the system.

Cisco Catalyst 3850 Stack

- Cisco Catalyst 3850 Series Switches are fixed-port Ethernet switches, with SFP-based versions for fiber connectivity recommended in the distribution layer. For resiliency, you configure the Cisco Catalyst 3850 Series Switches as a stack, and then configure and manage the stack as a single unit.
- Cisco Catalyst 3850 Series Switches have built-in stacking capability and stack together using StackWise-480 mode with up to nine switches in single stack-ring.
- Cisco StackPower technology increases system-level resiliency during catastrophic power failure on a stack-member switch. Cisco StackPower enables power redundancy across a group of four Cisco Catalyst 3850 Series Switches within same stack. This allows the flexible arrangement of power supplies in the stack and enables a zero-footprint redundant power supply deployment and intelligent load shedding.
- Cisco 3850 Series Switches have modular uplinks that can be configured as Gigabit Ethernet or 10-Gigabit Ethernet.
- Cisco Catalyst 3850 Series supports Stateful Switchover, which allows a switch in the active role in a stack to rapidly switchover to a switch in the standby role with minimum disruption to the network.
- With appropriate licenses, the Cisco Catalyst 3850 Series hardware supports wireless LAN controller functionality in order to support a unified access policy for converged wired and wireless designs with up to 40-Gbps of wireless capacity per switch.

PROCESS

Configuring the Distribution Layer

1. Configure the platform
2. Configure LAN switch universal settings
3. Configure distribution global settings
4. Configure IPv4 unicast routing
5. Configure IPv4 Multicast routing
6. Configure IPv4 Multicast Dynamic RP
7. Connect to access layer
8. Connect to LAN core or WAN router

Procedure 1 Configure the platform

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you do not have a platform listed for an option, skip that option and its steps. Some platforms have multiple options.

Option 1: Convert Cisco Catalyst 6807-XL, 6500-E, 6880-X, 4500E, and 4500-X to Virtual Switching System using Easy-VSS

Cisco Catalyst 6807-XL and 6500-E Virtual Switching System merges two physical 6807-XL or 6500-E switches together as a single logical switch using a single or optionally dual Cisco Supervisor Engine 2T modules in each physical switch. Cisco Catalyst 6880-X Virtual Switching System merges two physical 6880-X switches together as a single logical switch. The Cisco Catalyst 4500E and the Cisco Catalyst 4500-X Virtual Switching Systems merge two switches together as a single logical switch, using two Cisco Catalyst 4500E Series or two Cisco Catalyst 4500-X Series switches, respectively. A Supervisor module in the 6500-E and 4500E or built-in Supervisor hardware in the 6880-X and 4500-X acts as the active control plane for both chassis by controlling protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) Spanning Tree, CDP, and so forth, while supervisor hardware in each chassis actively switches packets.

You use the Easy-VSS feature on two VSS-capable devices in order to merge them into a VSS pair. This deployment uses software that has support for Easy-VSS. This software is listed in the appendix.

Step 1: Configure a temporary hostname on each switch so you can keep track of your configuration steps, and enable the Easy-VSS feature. In a later step after the conversion is complete, you apply a replacement hostname to the merged VSS configuration.

On the standalone switch #1:

```
Router#config t
Router#(config)#hostname VSS-Sw1
VSS-Sw1(config)#switch virtual easy
```

On the standalone switch #2:

```
Router#config t
Router#(config)#hostname VSS-Sw2
VSS-Sw2(config)#switch virtual easy
```

Step 2: Identify and enable connectivity between at least two switch port pairs to use for the Virtual Switch Link (VSL) interconnection, with at least one link on the Supervisor or base hardware.

On the standalone switch #1:

```
VSS-Sw1(config)#interface range Ten3/4 , Ten4/4
VSS-Sw1(config-if-range)#no shut
VSS-Sw1(config-if-range)#end
```

On the standalone switch #2:

```
VSS-Sw2(config)#interface range Ten3/4 , Ten4/4
VSS-Sw2(config-if-range)#no shut
VSS-Sw2(config-if-range)#end
```

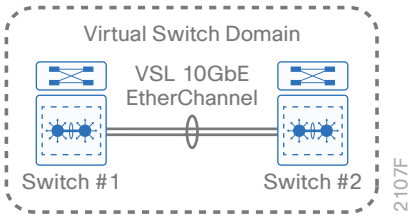
Tech Tip

With the links established, Cisco Discovery Protocol shares neighbor information used for next steps. The global **cdp run** and the per-interface **cdp enable** default commands must not be disabled or the conversion cannot be completed with Easy-VSS.

After the switches establish CDP communication across the links to be used for the VSL, you complete the remaining configuration steps from switch #1.

Step 3: Identify a unique domain ID to be used for this step to form a VSS pair. Each switch in the pair must have a matching domain ID, and if there are multiple VSS pairs, the domain ID selected for the pair should be unique. In this example, the domain number is 100. Each switch is also given a unique identifier within the domain, switch 1 or switch 2. The switch that initiates the Easy-VSS conversion is switch 1.

Figure 5 *VSS domain*



Step 4: At the enable prompt (that is, not in configuration mode) on the standalone switch #1, use the following command with the question mark:

```
VSS-Sw1# switch convert mode easy-virtual-switch links ?
  Local Interface        Remote Interface      Hostname
  TenGigabitEthernet3/4  TenGigabitEthernet3/4   VSS-Sw2
  TenGigabitEthernet4/4  TenGigabitEthernet4/4   VSS-Sw2
VSS-Sw1#switch convert mode easy-virtual-switch links
```

The CLI outputs the interfaces available to select.

Step 5: Use the VSL interfaces and complete the command, giving the VSS pair a unique domain ID, and then when prompted allow the conversion to proceed.

```
VSS-Sw1# switch convert mode easy-virtual-switch links Ten3/4 Ten4/4 domain 100
This command will convert all interface names
to naming convention "interface-type switch-number/slot/port",
removes configurations under switch virtual domain,
save the running config to startup-config and
reload current and peer switches
Do you want to proceed? [yes/no]: yes
VSS-Sw1#
*Jun 26 00:47:57.207: Master: connecting to standby ...
*Jun 26 00:47:57.207: Master: Provisioning ...
Domain ID 100 config will take effect only
after the exec command 'switch convert mode virtual' is issued
WARNING: Interface Port-channel255 placed in restricted config mode. All extra-
neous configs removed!
 Interface TenGigabitEthernet1/5
Interface TenGigabitEthernet1/5 set to default configuration
 Interface TenGigabitEthernet5/5
Interface TenGigabitEthernet5/5 set to default configuration
Converting interface names
```

```
Building configuration...
[OK]
Saved startup config:
System Initializing ...
```

Both switches reload. The switch pair negotiates using VSLP over the VSL and becomes a VSS, with one of the switches resolved as the ACTIVE supervisor for the merged VSS switch. You must enter all configuration commands in the following steps on the single active switch console. The other physical chassis in the VSS pair contains the STANDBY HOT supervisor with a console port that displays the Standby prompt.

Step 6: Use the following command to verify that both switches can see each other, that they are in SSO mode, and that the second supervisor is in STANDBY HOT status.

```
VSS-Sw1#show switch virtual redundancy
```

The two Cisco Catalyst switches are now operating as a single VSS system.

Step 7: Use configuration mode to rename the switch hostname for the VSS pair.

```
VSS-Sw1(config)#hostname D6500-VSS
D6500-VSS(config)#
```

The VSL allows the switches to communicate and stay in synchronization. The VSS uses the Stateful Switchover (SSO) redundancy facility to keep the control plane synchronized between the two switches. As a result, the VSS appears to devices in adjoining layers as a single switch with a single MAC address.

Step 8: Configure dual-active detection mechanism.

```
D6500-VSS(config)#interface range gigabit1/7/48, gigabit2/7/48
D6500-VSS(config-if-range)#dual-active fast-hello
D6500-VSS(config-if-range)#no shutdown
%VSDA-SW2_SPSTBY-5-LINK_UP: Interface Gi2/7/48 is now dual-active detection
capable
%VSDA-SW1_SP-5-LINK_UP: Interface Gi1/7/48 is now dual-active detection capable
```

In the event that the VSL is severed (that is, all links are down), or for any reason communication is lost over the VSL (such as excessive high CPU utilization), both switches would assume the active control plane role, thus creating a dual-active condition, which can result in network instability. To prevent a dual-active scenario from causing an outage in the network, VSS supports multiple unique dual-active detection and recovery mechanisms.

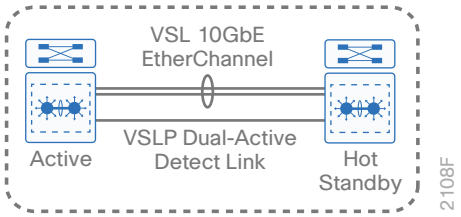
The dual-active detection mechanisms are used to trigger a VSS recovery mode. In the VSS recovery mode, only one switch chassis is allowed to remain active. The other switch (the previous VSS active switch) enters recovery mode and shuts down all of its interfaces except the VSL interfaces, thereby preventing instability in the network. After the VSL is repaired and communication over the VSL is reestablished, then the VSS reloads the switch in recovery mode and returns the VSS to a normal operating state.

You can use the following methods to detect this dual-active condition:

- Ethernet Fast-Hello (VSLP) link
- Enhanced Port Aggregation Protocol (PAgP) hellos with an adjacent switch

This design uses the Fast-Hello (VSLP) link for dual-active detection in this stage. Enhanced PAgP can be added to the design when bringing up PAgP EtherChannel links. The Fast-Hello link is a Gigabit Ethernet interface on each VSS switch chassis and connects them together (similar to a VSL connection) in a back-to-back fashion. This link does not require high bandwidth because it is only a detection link with control plane hellos on it.

Figure 6 VSLP



Step 9: Configure the system virtual MAC address.

Step 10: Set a virtual MAC address for the VSS system so that either active supervisor will use the same MAC address pool, regardless of which supervisor is active, even across a system reload.

```
D6500-VSS(config)# switch virtual domain 100
D6500-VSS(config-vs-domain)# mac-address use-virtual
Configured Router mac address is different from operational value. Change will
take effect after the configuration is saved and the entire Virtual Switching
System (Active and Standby) is reloaded.
```

By default, the VSS system uses the default chassis-based MAC-address pool assigned to the switch that is resolved to be the active switch when the switches initialize. As a result of events such as stateful switchover, the MAC may change.

Step 11: Configure standby chassis post-boot delayed port operation.

Ensure that the standby chassis is fully synchronized with the active chassis after rebooting before bringing up interfaces and attracting traffic.

```
D6500-VSS(config)# switch virtual domain 100
D6500-VSS(config-vs-domain)# standby port delay 300
D6500-VSS(config-vs-domain)# standby port bringup 1 2
```

Step 12: Save and reload the switch.

Save the running configuration and then reload the entire system (both chassis).

```
copy running-config startup-config
reload
```

When the switches initialize after this final reload, the VSS configuration is complete.

Option 2: Configure Cisco Catalyst 6807-XL, 6500-E, or 6880-X Virtual Switching System

Step 1: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. EtherChannels are used extensively in this design because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load balancing option.

```
port-channel load-balance vlan-src-dst-mixed-ip-port
```

Step 2: Configure QoS.

On the Cisco Catalyst 6500 Supervisor Engine 2T based switches and Cisco Catalyst 6880-X switches, QoS is enabled by default and policies for interface queuing are defined by attached service policies. The QoS policies are now defined using Cisco Common Classification Policy Language (C3PL), which is similar to Modular QoS CLI to reduce operational complexity.

All interface connections in the distribution and core are set to trust differentiated services code point (DSCP) markings. Even though this design is configured to trust DSCP markings, it is a best practice to ensure proper mapping of CoS to DSCP for VoIP. This mapping is accomplished by overriding the default mapping of CoS 5 "voice bearer traffic" to DSCP 40, with DSCP 46, which is the EF per-hop behavior for voice.

This egress QoS policy is configured to accommodate the 10-Gigabit and 40-Gigabit Ethernet ports on cards which use a 1P7Q4T queuing architecture.

```
! Enable port-based QoS
auto qos default
! Class maps for 1P7Q4T 10Gbps and 40Gbps ports service policy
class-map type lan-queuing match-any PRIORITY-QUEUE
  match dscp ef
  match dscp cs5
  match dscp cs4
  match cos 5
class-map type lan-queuing match-any CONTROL-MGMT-QUEUE
  match dscp cs7
  match dscp cs6
  match dscp cs3
  match dscp cs2
  match cos 3 6 7
class-map type lan-queuing match-any MULTIMEDIA-CONFERENCING-QUEUE
  match dscp af43
  match dscp af42
  match dscp af41
  match cos 4
```

```
class-map type lan-queuing match-any MULTIMEDIA-STREAMING-QUEUE
  match dscp af33
  match dscp af32
  match dscp af31
class-map type lan-queuing match-any TRANSACTIONAL-DATA-QUEUE
  match dscp af23
  match dscp af22
  match dscp af21
  match cos 2
class-map type lan-queuing match-any BULK-DATA-QUEUE
  match dscp af13
  match dscp af12
  match dscp af11
class-map type lan-queuing match-any SCAVENGER-QUEUE
  match dscp cs1
  match cos 1
!
policy-map type lan-queuing 1P7Q4T
 class PRIORITY-QUEUE
  priority
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 14
  queue-buffers ratio 10
class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 14
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 38 percent 70 100
  random-detect dscp 36 percent 80 100
  random-detect dscp 34 percent 90 100
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 14
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 30 percent 70 100
  random-detect dscp 28 percent 80 100
```

```
  random-detect dscp 26 percent 90 100
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 14
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 22 percent 70 100
  random-detect dscp 20 percent 80 100
  random-detect dscp 18 percent 90 100
 class BULK-DATA-QUEUE
  bandwidth remaining percent 6
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 14 percent 70 100
  random-detect dscp 12 percent 80 100
  random-detect dscp 10 percent 90 100
 class SCAVENGER-QUEUE
  bandwidth remaining percent 2
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 8 percent 80 100
class class-default
  queue-buffers ratio 25
  random-detect dscp-based aggregate
  random-detect dscp values 0 1 2 3 4 5 6 7 percent 80 100
  random-detect dscp values 9 11 13 15 17 19 21 23 percent 80 100
  random-detect dscp values 25 27 29 31 33 35 37 39 percent 80 100
  random-detect dscp values 41 42 43 44 45 47 49 50 percent 80 100
  random-detect dscp values 51 52 53 54 55 57 58 59 percent 80 100
  random-detect dscp values 60 61 62 63 percent 80 100
!
table-map cos-discard-class-map
 map from 0 to 0
 map from 1 to 8
 map from 2 to 16
 map from 3 to 24
 map from 4 to 32
```

```
 map from 5 to 46
 map from 6 to 48
 map from 7 to 56
!
macro name EgressQoS
  service-policy type lan-queuing output 1P7Q4T
@
```

Step 3: If you are using Gigabit Ethernet cards supported in VSS mode on Cisco Catalyst 6500-XLand 6807-E Supervisor Engine 2T based switches, configure an additional QoS policy for the Gigabit Ethernet ports.

A separate egress QoS policy is configured to accommodate the Gigabit Ethernet cards, which use a 1P3Q8T queuing architecture supporting COS-based queuing. This policy does not apply to the Cisco Catalyst 6880-X platforms.

```
! Class maps for 1P3Q8T 1Gb ports service policy
class-map type lan-queuing match-any PRIORITY-QUEUE-GIG
 match cos 5 4
class-map type lan-queuing match-any CONTROL-AND-STREAM-MEDIA
 match cos 7 6 3 2
class-map type lan-queuing match-any BULK-DATA-SCAVENGER
 match cos 1
!
policy-map type lan-queuing 1P3Q8T
 class PRIORITY-QUEUE-GIG
  priority
  queue-buffers ratio 15
 class CONTROL-AND-STREAM-MEDIA
  bandwidth remaining percent 55
  queue-buffers ratio 40
class BULK-DATA-SCAVENGER
  bandwidth remaining percent 10
  queue-buffers ratio 20
  random-detect cos-based
  random-detect cos 1 percent 80 100
 class class-default
  queue-buffers ratio 25
  random-detect cos-based
  random-detect cos 0 percent 80 100
```

```
!
macro name EgressQoSOneGig
  service-policy type lan-queuing output 1P3Q8T
@
```

Option 3: Configure Cisco Catalyst 4500E VSS and 4500-X VSS platforms

Step 1: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. EtherChannels are used extensively in this design because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load balancing option.

```
port-channel load-balance src-dst-ip
```

Step 2: For each platform, define a macro that you will use in later procedures in order to apply the platform-specific QoS configuration. This makes consistent deployment of QoS easier.

```
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 af43
  match  dscp af42
  match  dscp af41
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match  dscp af33
  match  dscp af32
  match  dscp af31
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af23
  match  dscp af22
  match  dscp af21
class-map match-any BULK-DATA-QUEUE
  match  dscp af13
```

```
  match  dscp af12
  match  dscp af11
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 EgressQoS
 service-policy output 1P7Q1T
@
```

Step 3: Save the running configuration.

```
copy running-config startup-config
```

Option 4: Configure the Cisco Catalyst 3850 platform

Step 1: To configure a Cisco Catalyst 3850 stack, use the CLI global exec mode (not configuration mode) to set the preferred active switch.

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

When there are multiple Cisco Catalyst 3850 Series Switches configured in a stack, one of the switches takes the ACTIVE switch role and another member takes the STANDBY HOT role. Upon reload, the switch configured with the highest priority assumes the active role. If this is a new configuration, only the active switch console is active during the initial configuration. When two or more switches are configured as a stack, configure the active switch functionality on a switch of your preference.

Step 2: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. EtherChannels are used extensively in this design because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load balancing option.

```
port-channel load-balance src-dst-mixed-ip-port
```

Step 3: To make consistent deployment of QoS easier, each distribution platform defines a macro that will be used in later procedures to apply the platform specific QoS configuration.

Tech Tip

The match statements in the class-maps can be combined into one line. However, listing them separately provides additional per-DSCP counters available from SNMP and from the following verification command.

```
show policy-map interface
class-map match-any PRIORITY-QUEUE
  match  dscp ef
class-map match-any VIDEO-PRIORITY-QUEUE
  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
  match  dscp af42
  match  dscp af43
```

```
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match  dscp af31
  match  dscp af32
  match  dscp af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-any BULK-SCAVENGER-DATA-QUEUE
  match  dscp af11
  match  dscp af12
  match  dscp af13
  match  dscp cs1
!
policy-map 2P6Q3T
 class PRIORITY-QUEUE
    priority level 1
    police rate percent 10
 class VIDEO-PRIORITY-QUEUE
    priority level 2
    police rate percent 20
 class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
 class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af43 percent 80
    queue-limit dscp af42 percent 90
    queue-limit dscp af41 percent 100
 class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af33 percent 80
    queue-limit dscp af32 percent 90
    queue-limit dscp af31 percent 100
```

```
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af23 percent 80
    queue-limit dscp af22 percent 90
    queue-limit dscp af21 percent 100
 class BULK-SCAVENGER-DATA-QUEUE
    bandwidth remaining percent 5
    queue-buffers ratio 10
    queue-limit dscp values af13 cs1 percent 80
    queue-limit dscp values af12 percent 90
    queue-limit dscp values af11 percent 100
 class class-default
    bandwidth remaining percent 25
    queue-buffers ratio 25
!
macro name EgressQoS
 service-policy output 2P6Q3T
@
```

Step 4: Configure Cisco Catalyst 3850 stack to automatically upgrade the software of new switches introduced into the stack to the level of the active switch, allowing full stack operability.

```
Switch(config)#software auto-upgrade enable
```

Step 5: If you are using a Cisco Catalyst 3850 with StackPower technology, ensure enough power is available during any power supply failure to support the entire stack during the degraded mode of operation, and configure the non-default redundant mode of operation for each switch in the stack.

```
Switch(config)#stack-power stack PowerStack-1
Switch(config-stackpower)#mode redundant
Switch(config)#stack-power switch 1
Switch(config-stackpower)# stack PowerStack-1
Switch(config)#stack-power switch 2
```

Procedure 2 Configure LAN switch universal settings

In this design, there are features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.

This procedure provides examples for some of those settings. The actual settings and values will depend on your current network configuration.

Table 3 Common network services used in the design examples

Setting	Value
Domain Name	cisco.local
Active Directory, DNS, DHCP Server	10.4.48.10
Authentication Control System	10.4.48.15
Network Time Protocol Server	10.4.48.17
EIGRP Named Mode Configuration Name	CAMPUS
EIGRP AS or OSPF AS	100
Multicast Range	239.1.0.0/16

Step 1: Configure the device hostname to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: If the switch VTP mode has been changed from default, configure VTP transparent mode. This design uses VTP transparent mode because the benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior resulting from operational error.

VLAN Trunking Protocol (VTP) allows network managers to configure a VLAN in one location of the network and have that configuration dynamically propagate out to other network devices. However, in most cases, VLANs are defined once during switch setup with few, if any, additional modifications.

```
vtp mode transparent
```

Step 3: Enable Rapid Per-VLAN Spanning-Tree (PVST+). Rapid PVST+ provides an instance of RSTP (802.1w) per VLAN. Rapid PVST+ greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D).

Although this architecture is built without any Layer 2 loops, you should still enable spanning tree with the most up-to-date network safeguards. By enabling spanning tree, you ensure that if any physical or logical loops are accidentally configured, no actual layer 2 loops occur.

```
spanning-tree mode rapid-pvst
```

Step 4: Set the distribution layer switch to be the spanning-tree root for all VLANs on access layer switches or appliances that you are connecting to the distribution switch.

```
spanning-tree vlan 1-4094 root primary
```

Step 5: Enable Unidirectional Link Detection (UDLD) as the default for fiber ports.

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected interface and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree loops, black holes, and non-deterministic forwarding. In addition, UDLD enables faster link failure detection and quick reconvergence of interface trunks, especially with fiber, which can be susceptible to unidirectional failures.

```
udld enable
```

Step 6: Enable the recovery mechanism to allow ports disabled as a result of errors to automatically clear the err-disable status and attempt a recovery to operational behavior and connected status. Enabling the recovery mechanism avoids having to intervene manually by using the CLI to shutdown and enable the port after the cause of the error is cleared. By default, the recovery mechanism waits five minutes to attempt clearing of the interface err-disable status.

```
errdisable recovery cause all
```

Step 7: Configure DNS for host lookup.

At the command line of a Cisco IOS device, it is helpful to be able to type a domain name instead of the IP address for a destination.

```
ip name-server 10.4.48.10
```

Step 8: Configure device management protocols.

The SSH and HTTPS protocols enable secure management of the LAN device. Both protocols are encrypted for privacy, and the unencrypted protocols, Telnet and HTTP, are turned off. Enabling HTTPS automatically generates a cryptographic key to use the service. When SSH is configured after HTTPS, you do not have to explicitly generate the cryptographic key that SSH requires, unless you wish to change the default key size.

Secure Copy (SCP) provides a secure and authenticated method for copying configuration and image files by making use of SSH as a secure transport. Enable SCP to allow secure file management with the device to avoid the use of less secure protocols such as TFTP and FTP.

Specify the transport preferred none on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name server is unreachable, long timeout delays may occur for mistyped commands.

```
no ip http server
ip http secure-server
ip domain-name cisco.local
ip ssh version 2
ip scp server enable
!
```

```
line vty 0 15
  transport input ssh
  transport preferred none
```

Step 9: Enable Simple Network Management Protocol (SNMP) in order to allow the network infrastructure devices to be managed by a Network Management System (NMS), and then configure SNMPv2c both for a read-only and a read-write community string.

```
snmp-server community [SNMP read-only name] ro
snmp-server community [SNMP read-write name] rw
```

Step 10: If your network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
ip access-list standard MANAGEMENT
  permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class MANAGEMENT in
!
snmp-server community [SNMP read-only name] ro MANAGEMENT
snmp-server community [SNMP read-write name] rw MANAGEMENT
```

The Cisco Catalyst 3850 Series Switch has an additional keyword to be added to the access-class, which allows console access from other switch members to not be affected.

```
line vty 0 15
  access-class MANAGEMENT in vrf-also
```

Caution

If you configure an access-list on the vty interface, you may lose the ability to use ssh to log in from one device to the next for hop-by-hop troubleshooting.

Step 11: Configure local login and password

The local login account and password provides basic device access authentication to view platform operation. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the use of plain text passwords when viewing configuration files. The **aaa new-model** command enables new access control commands and functions, and causes the local username and password on the router to be used in the absence of other AAA statements.

```
username admin secret [user password]
enable secret [enable password]
service password-encryption
aaa new-model
```

By default, https access to the switch will use the enable password for authentication.

Step 12: If you want to reduce operational tasks per device, configure centralized user authentication by using the TACACS+ protocol to authenticate management logins on the infrastructure devices to the AAA server.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
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
```

Step 13: Configure a synchronized clock by programming network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```
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
```

The **ntp update-calendar** command configures the switch to update the hardware clock from the ntp time source periodically. Since not all switches have a hardware clock, this command is not supported by all devices.

Procedure 3 Configure distribution global settings

Step 1: Configure BPDU Guard globally to protect PortFast-enabled interfaces.

In some scenarios, a service appliance that requires **spanning-tree portfast** may be connected to the distribution layer. When an interface is set for portfast, BPDU guard protects against an accidental connection of another switch into a PortFast-enabled interface, which could cause a catastrophic undetected spanning-tree loop.

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

Disable the interface if another switch is plugged into the PortFast-enabled interface.

```
spanning-tree portfast bpduguard default
```

On the Cisco Catalyst 6500 and Catalyst 6800 Series Switches, the global BPDU Guard command is slightly different.

```
spanning-tree portfast edge bpduguard default
```

Step 2: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the IP address block that the distribution switch summarizes to the rest of the network.

```
interface Loopback0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

The need for the **ip pim sparse-mode** command will be explained further in Step 3 of Procedure 5, "Configure IPv4 Multicast routing".

Step 3: If you have an out-of-band management network, configure an out-of-band management interface and route to the management network.

```
interface Gig1/3/2
  ip address [ip address] [mask]
ip route [out-of-band-network] [mask] [gateway]
```

Out-of-band networks allow for additional access capabilities when recovering from problems that affect traffic flow to an in-band management interface.

Step 4: If you are using VSS and have interfaces used to connect to an out-of-band management network, exclude them from being shutdown during a recovery from a dual-active state. Configure the out-of-band management interfaces with their IP addresses first, and then add them to the list of excluded interfaces in the VSS domain.

```
D6500-VSS(config)# switch virtual domain 100
D6500-VSS(config-vs-domain)# dual-active exclude interface [switch 1 OOB interface]
D6500-VSS(config-vs-domain)# dual-active exclude interface [switch 2 OOB interface]
```

Step 5: Configure the system processes to use the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback 0
ip ssh source-interface Loopback 0
ip pim register-source Loopback 0
ip tacacs source-interface Loopback 0
ntp source Loopback 0
```

Procedure 4 Configure IPv4 unicast routing

The single logical distribution layer design, when configured with VSS, uses Stateful Switchover and Nonstop Forwarding to provide sub-second failover in the event of a supervisor data or control plane failure. This ability reduces packet loss in switchover to redundant logic and keeps packets flowing when the data plane is still intact to adjacent nodes. In the stack-based distribution layer approach, a single logical control point still exists and the master control plane in a stack can fail over to another member in the stack providing near-second or sub-second resiliency.

When the supervisor or master switch of a distribution platform switches over from the active to the hot-standby supervisor or switch, it will continue switching IP data traffic flows in hardware. However, the device in the active role requires time to reestablish control plane two-way peering with IP routing neighbors and avoid the peer router from tearing down adjacencies due to missed hellos that would cause a reroute and disruption of traffic. To allow this time for the device taking over the active role to recover, there is a Nonstop Forwarding (NSF) setting for the routing protocol to wait for the dual supervisor peer switch to recover. The neighboring router is said to be NSF-aware if it has a newer release of Cisco IOS Software that recognizes an NSF peer. All of the platforms used in this design are NSF-aware for the routing protocols in use.

The distribution layer switch is configured to enable NSF for the routing protocol in use so that it can signal a peer when it switches over from a previously active to a hot-standby device, to allow the peering neighbor time to reestablish the IP routing protocol relationship to that node. No tuning of the default NSF timers is needed in this network. Nothing has to be configured for an NSF-aware peer router.

Option 1: Configure EIGRP unicast routing

Enhanced Interior Gateway Routing Protocol (EIGRP) is the IP unicast routing protocol used in this design because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks. If you use OSPF as an alternative to EIGRP, choose Option 2.

Step 1: Enable EIGRP named mode for the IP address space that the network will be using. If needed for your network, you can enter multiple network statements. Enable all routed links to be passive by default. The Loopback 0 IP address is used for the EIGRP router ID to ensure maximum resiliency. Because routing functionality is bounded at the distribution and not extended into the access layer, every distribution is configured as a stub network, optimizing performance. The summary keyword allows summary routes to be advertised and summarization is used whenever possible.

Tech Tip

There are situations where a layer-3 distribution switch cannot be an EIGRP stub network, such as in a WAN aggregation or for an Internet edge distribution. Those situations are addressed in the guides for those configurations.

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  network 10.4.0.0 0.1.255.255
  eigrp router-id [ip address of loopback 0]
  eigrp stub summary
  nsf
 exit-address-family
```

Option 2: Configure OSPF unicast routing

Open Shortest Path First (OSPF) can be used instead of EIGRP for networks where OSPF is required for compatibility. If you configured EIGRP in the previous procedure, you can skip this option.

Step 1: Enable OSPF for the IP address space that the network will be using. If needed for your network, you can enter multiple network statements. Enable all routed links to be passive by default. The Loopback 0 IP address is used for the OSPF router ID to ensure maximum resiliency. Each distribution gets a unique non-zero area number, which is configured as a totally stubby area to optimize performance. An OSPF totally stubby area only has a single default route out to the rest of the network, which is the case for a distribution switch.

Tech Tip

There are situations where a layer 3 distribution switch cannot be an OSPF totally stubby network, such as in a WAN aggregation. Those situations are addressed in the WAN guides for those configurations.

```
router ospf 100
 router-id [IP address of loopback 0]
 nsf
 area [unique area number] stub no-summary
 passive-interface default
 network 10.4.0.0 0.0.15.255 area [unique area number]
 network 10.4.40.0 0.0.0.255 area 0
```

Step 2: Revert from the latest default routing protocol behavior and enable the traditional Cisco IOS software-based route install and purge behavior.

```
no ip routing protocol purge-interface
```

You use this configuration for deterministic sub-second convergence without the requirement for advanced fine-tuning of the OSPF routing protocol. The enterprise campus network design uses a physical full mesh and Cisco VSS and MEC technology, so the forwarding and rerouting decision process is hardware-driven, negating the benefit of the newer default configuration.

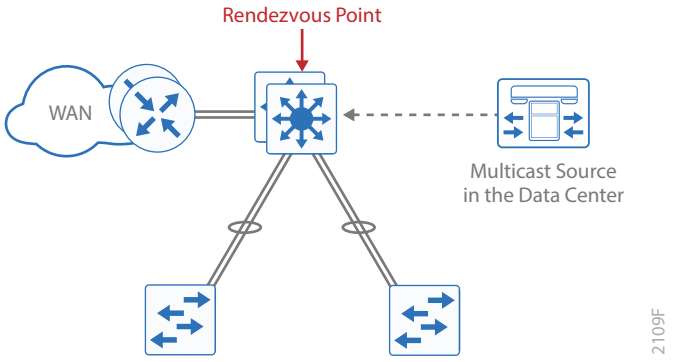
Procedure 5 Configure IPv4 Multicast routing

IP Multicast allows a single IP data stream to be replicated by the infrastructure (that is, routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony Music on Hold and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as a Rendezvous Point (RP) to map the receivers to active sources so they can join their streams.

The RP is a control plane operation that should be placed in the core of the network or close to the IP Multicast sources on a pair of Layer 3 switches or routers. IP Multicast routing begins at the distribution layer if the access layer is Layer 2 and provides connectivity to the IP Multicast RP. In designs without a core layer, the distribution layer will perform the RP function.

Figure 7 *Rendezvous point placement in the network*



This design is based on sparse mode multicast operation.

Step 1: Configure IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Step 2: Configure the switch to discover the IP Multicast RP.

Every Layer 3 switch and router is configured to discover the IP Multicast RP with AutoRP in this design—other alternatives are not covered. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
ip pim accept-rp auto-rp
```

Step 3: Configure ip pim sparse-mode. All Layer 3 interfaces in the network should be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

Example: Procedures 3-5 with EIGRP

```
spanning-tree portfast bpduguard default
!
interface Loopback 0
  ip address 10.4.15.254 255.255.255.255
  ip pim sparse-mode
!
snmp-server trap-source Loopback 0
ip ssh source-interface Loopback 0
ip pim register-source Loopback 0
ip tacacs source-interface Loopback 0
```

```
ntp source Loopback 0
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  network 10.4.0.0 0.1.255.255
  eigrp router-id 10.4.15.254
  eigrp stub summary
  nsf
 exit-address-family
!
```

Example: Procedures 3-5 with OSPF

```
spanning-tree portfast bpduguard default
!
interface Loopback 0
  ip address 10.4.15.254 255.255.255.255
  ip pim sparse-mode
!
snmp-server trap-source Loopback 0
ip ssh source-interface Loopback 0
ip pim register-source Loopback 0
ip tacacs source-interface Loopback 0
ntp source Loopback 0
!
no ip routing protocol purge-interface
!
router ospf 100
 router-id 10.4.15.254
 nsf
 area 0 authentication message-digest
 area 1 stub no-summary
 area 1 range 10.4.0.0 255.255.240.0
 passive-interface default
```

```
 no passive-interface Port-channel30
 network 10.4.0.0 0.0.15.255 area 1
 network 10.4.40.0 0.0.0.255 area 0
ip multicast-routing
ip pim autorp listener
!
```

Procedure 6 Configure IPv4 Multicast Dynamic RP

(Optional)

In networks without a core layer, you can place the RP function on the distribution layer. If a core layer does exist, configure the RP function as part of your core deployment.

Every Layer 3 switch and router must know the address of the IP Multicast RP, including the core switches that are serving as the RP. This design uses AutoRP to announce candidate RPs, which are the core switches, to the rest of the network.

Step 1: Configure loopback interface for RP.

Configure a second loopback interface to be used as the RP interface. The interface uses a host address mask (32 bits). All routers then point to this common IP address on **loopback 1** for the RP.

```
interface Loopback 1
 ip address 10.4.15.253 255.255.255.255
 ip pim sparse-mode
```

Tech Tip

Although you could use an existing loopback interface, adding a new interface increases the ability to rapidly adapt to future requirements which may drive a change in the location of the RP.

For example, if your RP is currently configured on a distribution layer, you may want to move the RP when you add a core. Configuring the RP address on the loopback interface at the new location with the same IP address used on Loopback 1 in this procedure and establishing IP Multicast and MSDP peering enables the migration. All remote routers should still point to the same RP address, which simplifies the move and reduces disruption to the IP Multicast environment.

Step 2: Configure AutoRP candidate RP.

The **send-rp-announce** command in conjunction with the **group-list** option advertises the RP address, with the multicast range the device is willing to serve, as a candidate RP to the AutoRP mapping agents.

```
access-list 10 permit 239.1.0.0 0.0.255.255
ip pim send-rp-announce Loopback 1 scope 32 group-list 10
```

Step 3: Configure AutoRP mapping agent.

The AutoRP mapping agent listens for candidate RPs and then advertises to the rest of the network the list of available RPs. The **send-rp-discovery** command enables this switch to act as an AutoRP mapping agent. The RPs that are announced are limited by an access list.

```
ip access-list standard RP-NETS
  permit 10.4.40.0 0.0.0.255
  permit 10.4.48.0 0.0.0.255
ip pim send-rp-discovery Loopback0 scope 32
ip pim rp-announce-filter rp-list RP-NETS
```

Step 4: Filter any rogue multicast sources from overloading the router control plane.

Apply an ACL to the rendezvous point that allows only acceptable addresses for sources of multicast traffic and the destination multicast addresses they serve.

```
ip access-list extended MCAST-SOURCES
permit ip [source network] [source mask] 239.1.0.0 0.0.255.255
  deny ip any any
ip pim accept-register list MCAST-SOURCES
```

Procedure 7 Connect to access layer

The resilient, single, logical, distribution layer switch design is based on a hub-and-spoke or star design. The links to access layer switches and connected routers are Layer 2 EtherChannels. Links to other distribution layers, and the optional core are Layer 3 links or Layer 3 EtherChannels.

When using EtherChannel, the member interfaces should be on different switches in the stack or different modules in the modular switch for the highest resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. This allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two.

If this distribution layer will be used as a network-services aggregation block, you likely will not have an access layer to connect.

Step 1: Configure VLANs.

Configure all VLANs for the access layer switches that you are connecting to the distribution switch.

```
vlan [data vlan]
  name Data
exit
vlan [voice vlan]
  name Voice
exit
vlan [management vlan]
  name Management
exit
```

Step 2: If there is no external central site DHCP server in the network, you can provide DHCP service in IOS by configuring the IOS DHCP server. This function can also be useful at a remote-site where you want to provide local DHCP service and not depend on the WAN link to an external central site DHCP server.

```
ip dhcp excluded-address 10.4.100.1 10.4.100.10
ip dhcp pool access
  network 10.4.100.0 255.255.255.0
  default-router 10.4.100.1
  domain-name cisco.local
  dns-server 10.4.48.10
```

The example configuration provides IP addresses via the IOS based DHCP service for the subnet 10.4.100.0/24 and prevents the server from assigning reserved addresses .1-.10.

Step 3: Configure EtherChannel member interfaces.

This design uses Layer 2 EtherChannels to connect all access layer switches to the distribution layer and thereby create the hub-and-spoke resilient design that eliminates spanning-tree loops. Add links in multiples of two and distribute as much as possible across physical components of the platform. A configuration is shown using four member links for additional resiliency.

Connect the access layer EtherChannel uplinks to separate switches in the distribution layer Virtual Switching System or stack.

Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

Option 1: Configure EtherChannel Using LACP

Cisco Catalyst 4500 and 4500-X Series Switches do not use the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to {your device here} Port 1
interface [interface type] [port 2]
  description Link to {your device here} Port 2
interface [interface type] [port 3]
  description Link to {your device here} Port 3
interface [interface type] [port 4]
  description Link to {your device here} Port 4
!
interface range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  switchport
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
  !6K platforms with 1-Gigabit Ethernet cards use alternative
  !macro apply EgressQoSOneGig
```

Tech Tip

The Cisco Catalyst 6500 and 6800 Series Switches have two egress QoS macros: EgressQoSOneGig, which is used for Gigabit Ethernet ports, and EgressQoS, which is used for 10-Gigabit or 40-Gigabit Ethernet ports. All other distribution layer platforms have a single egress QoS macro, which applies to all Ethernet ports, including Gigabit Ethernet and 10-Gigabit Ethernet.

Option 2: Configure EtherChannel Using PAgP

Step 1: Set Cisco Port Aggregation Protocol negotiation to *preferred* on both sides in order to ensure a proper EtherChannel is formed. Also, apply the egress QoS macro that was defined in the platform configuration procedure in order to ensure traffic is prioritized appropriately.

Cisco Catalyst 4500 and 4500-X Series Switches do not use the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to {your device here} Port 1
interface [interface type] [port 2]
  description Link to {your device here} Port 2
interface [interface type] [port 3]
  description Link to {your device here} Port 3
interface [interface type] [port 4]
  description Link to {your device here} Port 4
!
interface range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  switchport
  channel-protocol pagp
  channel-group [number] mode preferred
  logging event link-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
  !6K platforms with 1-Gigabit Ethernet cards use alternative
  !macro apply EgressQoSOneGig
```

Tech Tip

The Cisco Catalyst 6500 and 6800 Series Switches have two egress QoS macros: EgressQoSOneGig, which is used for Gigabit Ethernet ports, and EgressQoS, which is used for 10-Gigabit or 40-Gigabit Ethernet ports. All other distribution layer platforms have a single egress QoS macro, which applies to all Ethernet ports, including Gigabit Ethernet and 10-Gigabit Ethernet.

Step 2: If the port-channel is on a VSS device connected to an access layer and you wish to use it for an additional method of dual-active detection available with Enhanced PAgP, configure the VSS domain with the additional method.

```
switch virtual domain 100
  dual-active detection pagp trust channel-group [number]
```

Step 3: Configure the VLAN trunk interface to the access layer.

An 802.1Q trunk is used for the connection to the access layer, which allows the distribution switch to provide Layer 3 services to all the VLANs defined on the access layer switch. Prune the VLANs on the trunk to only the VLANs that are active on the access switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Procedure 7, Step 3.

```
interface [port-channel] [number]
  description EtherChannel Link to {your device here}
  switchport trunk allowed vlan [data vlan],[voice vlan],
    [management vlan]
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  no shutdown
  exit
```

If the interface type is not port-channel, then the additional command macro apply EgressQoS must also be configured on the interface.

Next, mitigate VLAN hopping on the trunk for switch-to-switch connections.

There is a remote possibility that an attacker can create a double 802.1Q encapsulated packet. If the attacker has specific knowledge of the 802.1Q native VLAN, they could create a packet that when processed, removes the first or outermost tag when the packet is switched onto the untagged native VLAN. When the packet reaches the target switch, the inner or second tag is then processed and the potentially malicious packet is switched to the target VLAN.

At first glance, this appears to be a serious risk. However, the traffic in this attack scenario is in a single direction and no return traffic can be switched by this mechanism. Additionally, this attack cannot work unless the attacker knows the native VLAN ID.

Step 4: Configuring an unused VLAN on all switch-to-switch 802.1Q trunk links from access layer to distribution layer removes the remote risk of this type of attack. By choosing an arbitrary, non-default, unused VLAN assignment for the native VLAN, you reduce the possibility that a double 802.1Q-tagged packet can hop VLANs.

```
vlan 999
  name AntiVLANhopping
exit
!
interface [port-channel] [number]
  switchport trunk native vlan 999
```

Step 5: Configure Layer 3.

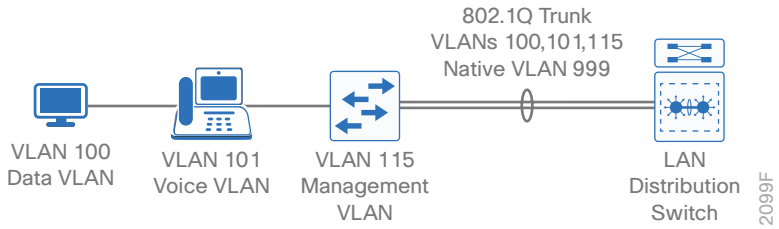
Configure a VLAN interface (SVI) for every access layer VLAN so devices in the VLAN can communicate with the rest of the network.

Use the **ip helper-address** command to allow remote DHCP servers to provide IP addresses for this network. The address that the **helper** command points to is the central DHCP server. If you have more than one DHCP server, you can list multiple helper commands on an interface.

```
interface vlan [number]
  ip address [ip address] [mask]
  ip helper-address [dhcp server ip]
  ip pim sparse-mode
  no shutdown
```

If you configured the IOS DHCP server function on this distribution layer switch in Step 2 of this procedure, the **ip helper-address** is not needed on the VLAN interface.

Example: Access switch VLAN deployment




```
vlan 100
  name Data
vlan 101
  name Voice
vlan 115
  name Management
vlan 999
  name AntiVLANhopping
spanning-tree vlan 1-4094 root primary
!
interface GigabitEthernet 1/1/1
  description Link to Access Switch Port 1
interface GigabitEthernet 2/1/1
  description Link to Access Switch Port 2
interface GigabitEthernet 1/1/2
  description Link to Access Switch Port 3
```

```
interface GigabitEthernet 2/1/2
  description Link to Access Switch Port 4
!
interface range GigabitEthernet 1/1/1, GigabitEthernet 2/1/1, GigabitEthernet
1/1/2, GigabitEthernet 2/1/2
  switchport
  channel-protocol lacp
  channel-group 10 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
  no shutdown
!
interface Port-channel 10
  description EtherChannel Link to Access Switch
  switchport trunk native vlan 999
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100,101,115
  switchport mode trunk
  load-interval 30
  no shutdown
!
interface vlan 100
  ip address 10.4.0.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface vlan 101
  ip address 10.4.1.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface vlan 115
  ip address 10.4.15.1 255.255.255.128
  ip pim sparse-mode
```

Procedure 8 Connect to LAN core or WAN router

Any links to connected WAN routers or a LAN core layer should be Layer 3 links or Layer 3 EtherChannels. The LAN design does not extend Layer 2 VLANs beyond the distribution layer.

Option 1: Connect distribution layer switch to WAN router

When the LAN distribution layer connects to a WAN router this may present a number of scenarios:

- The distribution layer switch is a collapsed core HQ location connecting to one or more WAN headend routers.
- The distribution layer switch is collapsed core for a larger remote site with multiple WAN routers for survivability.
- The distribution layer switch is a WAN aggregation switch with a number of WAN headend routers connected to it for a modular block connecting to a LAN Core switch.

Because of the number of combinations, further investigation may be necessary to adjust for the LAN connectivity that matches your deployment scenario.

Option 2: Connect distribution layer switch to LAN core switch

Step 1: Configure the Layer 3 interface.

If you are using an EtherChannel to connect to the LAN core, the interface type is port-channel and the number must match the channel-group number you will configure in Step 3. When configuring a Layer 3 EtherChannel, the logical port-channel interface is configured prior to configuring the physical interfaces associated with the EtherChannel.

If you are configuring a Catalyst 6800 or 6500 Series platform, optimize the EtherChannel recovery for multicast by using the **platform multicast forwarding fast-redirect** command.

```
interface [interface type] [number]
  description Link to {your device here}
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
! next multicast optimization for Catalyst 6K only
  platform multicast forwarding fast-redirect
  logging event link-status
  carrier-delay msec 0
  load-interval 30
  no shutdown
```

If the interface type is not a port-channel, then an additional command **macro apply EgressQoS** must also be configured on the interface.

Step 2: If the routing protocol you are using is OSPF, you add the router neighbor authentication configuration to the interface. The chosen password must match the neighbor peer, and you do additional OSPF authentication configuration in a later step.

```
interface [interface type] [number]
 ip ospf message-digest-key 1 md5 [neighbor key]
 ip ospf network point-to-point
```

In this design, the OSPF routers are always directly connected as the only two neighbors on a link, so to reduce processing and complexity, the network type is changed to point-to-point on the neighbor links.

Step 3: If you want to run EtherChannel links to the core layer, configure the EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the **channel-group** command. The number for the port-channel and channel-group must match.

Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure that traffic is prioritized appropriately, and apply IP interface dampening on the routing interfaces. This improves network stability during instances of multiple interface flaps.

Cisco Catalyst 4500 Series Switches do not use the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to {your device here} Port 1
interface [interface type] [port 2]
  description Link to {your device here} Port 2
interface [interface type] [port 3]
  description Link to {your device here} Port 3
interface [interface type] [port 4]
  description Link to {your device here} Port 4
!
interface range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  no switchport
  carrier-delay msec 0
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  dampening
  macro apply EgressQoS
  no shutdown
```

Tech Tip

The Cisco Catalyst 6500 Series Switches have two egress QoS macros: EgressQoSOneGig, which is used for Gigabit Ethernet ports, and EgressQoS, which is used for 10-Gigabit or 40-Gigabit Ethernet ports. All other distribution layer platforms have a single egress QoS macro, which applies to all Ethernet ports, including Gigabit Ethernet and 10-Gigabit Ethernet.

Step 4: Configure IP address summarization on the links to the core.

As networks grow, the number of IP subnets or routes in the routing tables grows as well. You configure IP summarization on links where logical boundaries exist in order to reduce the amount of bandwidth, processor speed, and memory necessary to carry large route tables and to reduce convergence time around a link failure. If the connected device provides connectivity to another piece of the network (for example, the WAN, Internet, or LAN core), configure summarization.

EIGRP Summarization

```
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [interface type] [number]
   summary-address 10.4.0.0 255.255.240.0
  exit-af-interface
 exit-address-family
```

OSPF Summarization

```
router ospf 100
 area [unique area number] range 10.4.0.0 255.255.240.0
```

Tech Tip

If you have multiple address blocks that are not contiguous and can't be aggregated into a single summary, you can add additional EIGRP summary-address statements or OSPF area range statements, as appropriate. If this is a distribution switch at a WAN remote site, you need to complete additional steps on the remote-site router for any summary address, as described in related WAN design guides.

Step 5: Configure router neighbor authentication, and override passive interface configuration for links to the core.

After you have configured the Layer 3 interfaces and Layer 3 port-channels connecting to other Layer 3 devices, allow the routing protocol to form neighbor relationships with MD5 authentication across these interfaces to establish peering adjacencies and exchange route tables.

Unlike EIGRP named mode configuration, OSPF neighbor authentication also requires a configuration attached directly to the Layer-3 interfaces, thus additional router neighbor authentication configuration is completed as part of the prior Layer-3 interface configuration steps.

EIGRP Neighbor Authentication

```
key chain EIGRP-KEY
 key 1
  key-string [neighbor key]
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface [interface type] [number]
   authentication mode md5
   authentication key-chain EIGRP-KEY
   no passive-interface
  exit-af-interface
 exit-address-family
```

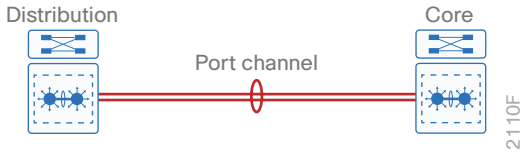
OSPF Neighbor Authentication

```
router ospf 100
 area 0 authentication message-digest
 no passive-interface [interface type] [number]
```

Step 6: Save the running configuration that you have entered so it will be used as the startup configuration file when your switch is reloaded or power-cycled.

```
copy running-config startup-config
```

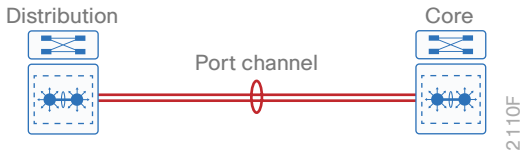
Example: Distribution to Core PortChannel configuration–EIGRP




```
interface Port-channel 30
  description EtherChannel Link to Core Switch
  no switchport
  ip address 10.4.40.10 255.255.255.252
  ip pim sparse-mode
  load-interval 30
  no shutdown
!
```

```
interface range FortyGigabitEthernet 1/2/1, FortyGigabitEthernet 2/2/1,
FortyGigabitEthernet 1/3/1, FortyGigabitEthernet 2/3/1
  description EtherChannel Link to Core Switch
  no switchport
  carrier-delay msec 0
  channel-group 30 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
  no shutdown
!
key chain EIGRP-KEY
 key 1
  key-string [neighbor key]
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  af-interface Port-channel30
   summary-address 10.4.0.0 255.255.240.0
   authentication mode md5
   authentication key-chain EIGRP-KEY
   no passive-interface
  exit-af-interface
  network 10.4.0.0 0.1.255.255
  eigrp router-id 10.4.40.254
  eigrp stub summary
  nsf
 exit-address-family
!
```

Example: Distribution to Core PortChannel configuration–OSPF




```
interface Port-channel 30
  description EtherChannel Link to Core Switch
  no switchport
  ip address 10.4.40.10 255.255.255.252
  ip pim sparse-mode
  ip ospf message-digest-key 1 md5 [neighbor key]
  ip ospf network point-to-point
 no shutdown
!
interface range FortyGigabitEthernet 1/2/1, FortyGigabitEthernet 2/2/1,
FortyGigabitEthernet 1/3/1, FortyGigabitEthernet 2/3/1
  description EtherChannel Link to Core Switch
  no switchport
  carrier-delay msec 0
  channel-group 30 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
  no shutdown
!
!
router ospf 100
 router-id 10.4.15.254
 nsf
.
```

```
area 0 authentication message-digest
area 1 stub no-summary
area 1 range 10.4.0.0 255.255.240.0
passive-interface default
no passive-interface Port-channel30
network 10.4.0.0 0.0.15.255 area 1
network 10.4.40.0 0.0.0.255 area 0
```

Appendix A: Product List

LAN ACCESS LAYER

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.7.1E(15.2.3E1) IP Base
	Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps	WS-X45-SUP8-E	
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.7.1E(15.2.3E1) IP Base
	Cisco Catalyst 4500E Supervisor Engine 7L-E, 520Gbps	WS-X45-SUP7L-E	
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.7.1E(15.2.3E1) IP Base
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink	WS-C3650-24PD	3.7.1E(15.2.3E1) IP Base
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	
	Cisco Catalyst 3650 Series Stack Module	C3650-STACK	
	Cisco Catalyst 2960-X Series 24 10/100/1000 Ethernet and 2 SFP+ Uplink	WS-C2960X-24PD	15.2(3)E1 LAN Base
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	
Standalone Access Layer Switch	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	3.7.1E(15.2.3E1) IP Base

LAN DISTRIBUTION LAYER

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.2(1)SY1 IP Services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	15.2(1)SY1 IP Services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 48-port GigE Mod (SFP)	WS-X6748-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
Extensible Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6880-X Extensible Fixed Aggregation Switch (Standard Tables)	C6880-X-LE	15.2(1)SY1 IP Services
	Cisco Catalyst 6800 Series 6880-X Multi Rate Port Card (Standard Tables)	C6880-X-LE-16P10G	

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.7.1E(15.2.3E1) Enterprise Services
	Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps	WS-X45-SUP8-E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500-X Series 32 Port 10GbE IP Base Front-to-Back Cooling	WS-C4500X-32SFP+	3.7.1E(15.2.3E1) Enterprise Services
Stackable Distribution Layer Switch	Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet	WS-C3850-12S	3.7.1E(15.2.3E1) IP Services
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	

LAN CORE LAYER

Functional Area	Product Description	Part Numbers	Software
Modular Core Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.2(1)SY1 IP Services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 8-port 10GbE Fiber Module w/ DFC4	WS-X6908-10G-2T	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 48-port GbE SFP Fiber Module w/DFC4	WS-X6848-SFP-2T	
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	15.2(1)SY1 IP Services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 8-port 10GbE Fiber Module w/ DFC4	WS-X6908-10G-2T	
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	

Appendix B: Changes

This is the first publication of this guide.

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.