



CVD



Campus Wired LAN

TECHNOLOGY DESIGN GUIDE

August 2013



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency.....	2
Introduction	3
Technology Use Cases	3
Use Case: Connecting Wired Devices to an Organization’s Network.....	3
Use Case: LAN and Services Interconnection to Scale within a Physical Site.....	4
Design Overview.....	5
Hierarchical Design Model.....	5
Access Layer.....	6
Distribution Layer.....	8
Core Layer	11
Quality of Service (QoS)	12
Access Layer	13
Design Overview.....	13
Infrastructure Security Features.....	13
Common Design Method to Simplify Installation and Operation.....	14
Features to Support Voice and Video Deployment	15
Access Layer Platforms	15
Wiring Closets Requiring up to 48 Ports.....	15
Wiring Closets Requiring Greater than 48 Ports	15
Deployment Details	17
Configuring the Access Layer	18
Distribution Layer	37
Design Overview.....	37
Traditional Distribution Layer Design	38
Routed Access Distribution Layer Design	39
Simplified Distribution Layer Design.....	39
Distribution Layer Roles	40

Distribution Layer Platforms	42
Cisco Catalyst 6500 VSS 4T	42
Cisco Catalyst 4507R+E Switch.....	43
Cisco Catalyst 3750-X Stack.....	43
Deployment Details	44
Configuring the Distribution Layer	44
Core Layer.....	71
Design Overview.....	71
Core Layer Platform.....	72
Cisco Catalyst 6500 VSS 4T	72
Deployment Details	73
Configuring the Core.....	73
Appendix A: Product List.....	90
Appendix B: Device Configuration Files.....	92

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-  
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

For the most recent CVD guides, see the following site:

<http://www.cisco.com/go/cvd>

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Connecting Wired Devices to an Organization's Network**—Wired devices use Ethernet for access to services and communication at an organization's remote sites and headquarters. Deployed with efficiency and consistency on LANs, the devices incorporate security, reliability, and manageability.
- **LAN and Services Interconnection to Scale within a Physical Site**—At a larger site with increasing numbers of devices, a highly available hierarchical network interconnects an organization's devices and services, for scale and growth. This network aids manageability, operational efficiency, and resiliency, while minimizing complexity.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Ethernet wired access and device interconnection using Cisco Catalyst switches
- Hierarchical local area network design model, including access, distribution, and core layers, with simplified design options using Virtual Switching System (VSS)
- Advanced technology support for voice and video, including quality of service (QoS) marking and treatment
- Security, including management authentication and Catalyst Infrastructure Security Features (CISF)
- Unicast routing using Enhanced Interior Gateway Routing Protocol (EIGRP) and multicast routing using Protocol Independent Multicast (PIM) sparse mode

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks

Related CVD Guides



Campus Wireless LAN
Technology Design Guide



Device Management Using
ACS Technology Design Guide



To view the related CVD guides,
click the titles or visit the following site:
<http://www.cisco.com/go/cvd>

Introduction

The *Campus Wired LAN Design Guide* describes how to design a wired network access with ubiquitous capabilities that scale from small environments with one to 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 that 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.

Technology Use Cases

The *Campus Wired LAN Design Guide* addresses the requirements of organizations when designing Local Area Networks (LANs) for their data communications needs. The guidance offered is useful for greenfield designs, for optimizing existing networks, and as a reference design offering operational consistency for an organization as its LAN grows. The scope of coverage applies to small, remote-site LANs with a single router up to large multi-building campuses with a routed core supporting connectivity to multiple-routed distribution modules.

The *Campus Wired LAN Design Guide* addresses four primary wired LAN requirements shared by organizations, including the need to:

- Offer reliable access to organization resources
- Minimize time required to absorb technology investments
- Provide a productive and consistent user experience
- Reduce operation costs

Use Case: Connecting Wired Devices to an Organization's Network

Organizations of all sizes have a need to connect data devices used by their employees such as desktop computers, laptops, and IP phones enabling communications with resources such as printers, business applications systems, voice and video endpoints and conference bridges, along with Internet accesses, for interaction with partners and customers. Ethernet is the ubiquitous wired technology to make these communication connections. Using this guide, a LAN design of a few Ethernet interconnected devices can scale up to many thousands of devices in a multi-building campus over time.

This design guide enables the following network capabilities when connecting wired devices to an organization's network:

- **Consistent user experience**—Uses consistent design methodology in order to allow small remote sites with just a few Ethernet connections to be able to use the same access switch configurations as large campus Ethernet designs
- **Network security**—Protects the network and users from malicious attacks by applying security using Catalyst Infrastructure Security Features (CISF), secure communication to devices, and integrating external authentication, authorization, and accounting (AAA) services
- **Protection of multimedia and critical applications traffic**—Enables critical applications and rich media communications, such as streaming and interactive voice and video media, through the use of end-to-end quality of service (QoS) enforcement, marking, and transmission policies, ensuring appropriate network treatment of all types of business communications
- **Rapid deployment**—Offers a choice of platforms with a range of power over Ethernet (PoE) support for deployment of media endpoints, such as phones and cameras, aided by in-line power technology
- **Manageability**—Allows the ability for network components to be managed from a central management network
- **Reliable connectivity**—Uses a Layer 2 LAN access design with resilient components and links for loop-free connections in order to ensure communications remain dependable, without wasted resources, such as unused links caused by spanning tree port blocking

Use Case: LAN and Services Interconnection to Scale within a Physical Site

As an organization grows, the network must grow to accommodate the increased number of devices connecting to the network, as well as offer connectivity to additional services components of increased size.

This design guide enables the following network capabilities supporting LAN and services interconnection within a physical site:

- **Reduced design complexity**—Uses replicable LAN access building blocks for Ethernet connectivity, network modularity concepts, and network hierarchy in order to allow network design to be assembled in a consistent approach to the scale that is dictated by organization growth
- **Connectivity to IP services**—Uses resilient connectivity to a Layer 3 campus distribution or site router
- **Ability to scale to large topologies**—Includes a design option of a resilient routed core, using a single pair of core devices, based on Virtual Switching System technology
- **High availability**—Offers resilient platform options and use of resilient connectivity configurations, allowing for maintenance of components without disruption of network services and mitigating single link disconnections from disrupting business communication
- **Operational efficiency**—Uses consistent configurations across all areas of the network, increasing speed to deployment and reducing risk of configuration mistakes

Design Overview

The LAN is the networking infrastructure that provides access to network communication services and resources for end users and devices spread over a single floor or building. A campus network occurs when a group of building-based LANs that are spread over a small geographic area are interconnected.

The *Campus Wired LAN Design Guide* provides a design that enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and Internet Edge modules at the network core.

Specifically, this document shows you how to design the network foundation and services to enable

- Tiered LAN connectivity
- Wired network access for employees
- IP Multicast for efficient data distribution
- Wired infrastructure ready for multimedia services

Hierarchical Design Model

This architecture uses a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to focus on specific functions, which simplifies the design and provides simplified deployment and management.

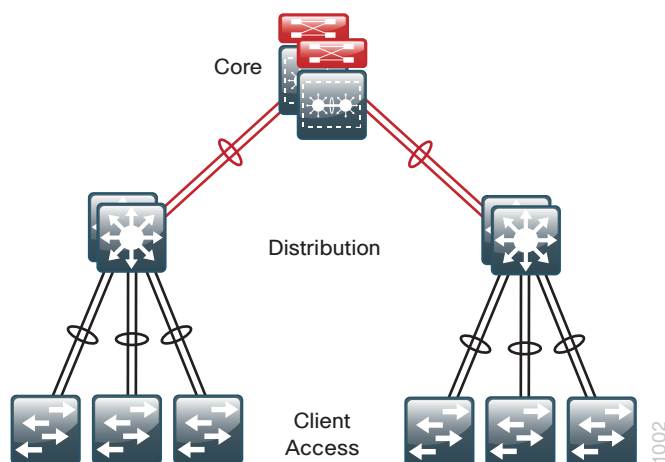
Modularity in network design allows you to create design elements that can be replicated throughout the network. Replication provides an easy way to scale the network as well as a consistent deployment method.

In flat or meshed network architectures, changes tend to affect a large number of systems. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage as well as improve resiliency. Modular structuring of the network into small, easy-to-understand elements also facilitates resiliency via improved fault isolation.

A hierarchical design includes the following three layers:

- **Access layer**—Provides workgroup/user access to the network.
- **Distribution layer**—Aggregates access layers and provides connectivity to services.
- **Core layer**—Provides connection between distribution layers for large LAN environments.

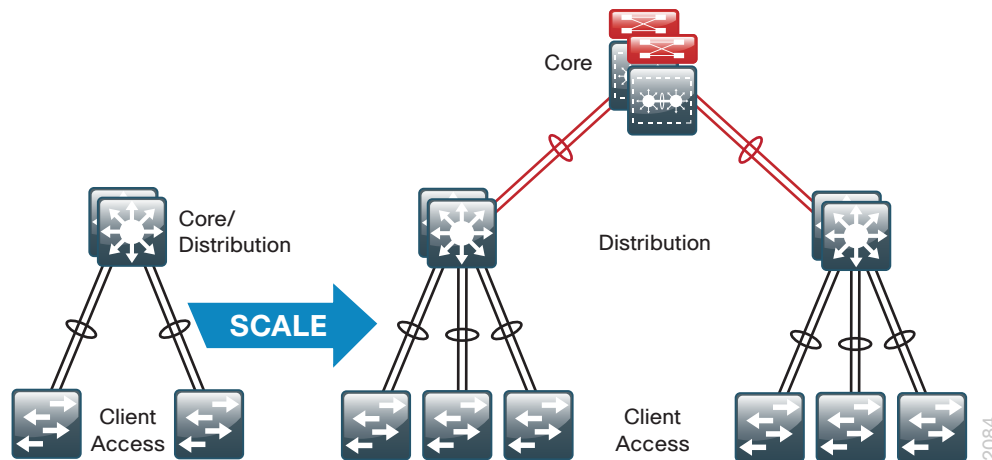
Figure 1 - LAN hierarchical design



The three layers—access, distribution, and core—each provide different functionality and capability to the network. Depending on the characteristics of the site where the network is being deployed, you might need one, two, or all three of the layers. For example, a remote site supporting only 10 users will only require an access layer. A site that occupies a single building might only require the access and distribution layers, while a campus of multiple buildings will most likely require all three layers.

Regardless of how many layers are implemented at a site, the modularity of this design ensures that each layer will always provide the same services, and in this architecture, will use the same design methods.

Figure 2 - Scalability by using a modular design



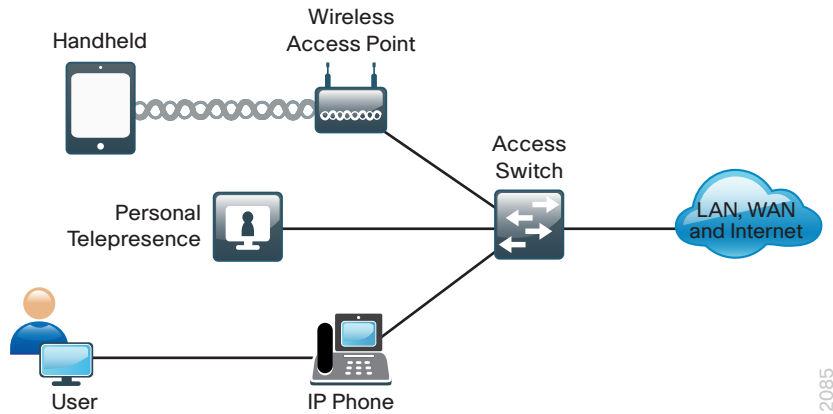
Access Layer

The access layer is the point at which user-controlled and user-accessible devices are connected to the network. The access layer provides both wired and wireless connectivity and contains features and services that ensure security and resiliency for the entire network.

Device Connectivity

The access layer provides high-speed user-controlled and user-accessible device connectivity. Once expensive options, high-speed access technologies like Gigabit Ethernet and 802.11n wireless are now standard configurations on end-user devices. While an end-user device in most cases will not use the full capacity of these connections for long periods of time, the ability to burst up to these high speeds when performing routine tasks does help make the network a transparent part of an end-users day-to-day job. The longer someone has to wait to back up their machine, send an email, or open a file off an internal web page the harder it is for the network to be transparent.

Figure 3 - Access layer connectivity



It is common for many different types of devices to connect at the access layer. Personal computers, IP phones, wireless access points, and IP video surveillance cameras all might connect to the same access layer switch. Since it can be beneficial for performance, management, and security reasons to segment these different devices, the access layer provides the capability to support many logical networks on one physical infrastructure.

Resiliency and Security Services

In general, the goal of the resiliency and security services in the infrastructure is to ensure that the network is available for use without impairment for everyone that needs it. Because the access layer is the connection point between the network and client devices, it plays a role in ensuring the network is protected from human error and from malicious attacks. This protection includes making sure the devices connecting to the network do not attempt to provide services to any end users that they are not authorized for, that they do not attempt to take over the role of any other device on the network, and, when possible, that they verify the device is allowed on the network.

Enabling these services in the access layer contributes not only to the overall security of the network, but also to the resiliency and availability of the network.

Advanced Technology Capabilities

Finally, the access layer provides a set of network services that support advanced technologies. Voice and video are commonplace in today's organizations and the network must provide services that enable these technologies. This includes providing specialized access for these devices, ensuring the traffic from these devices is not impaired by others, and providing efficient delivery of traffic that is needed by many devices in the network.

Distribution Layer

The distribution layer serves many important services for the LAN. The primary function is to serve as an aggregation point for multiple access layer switches in a given location or campus. In a network where connectivity needs to traverse the LAN end-to-end, whether between different access layer devices or from an access layer device to the WAN, the distribution layer facilitates this connectivity.

Scalability

In any network where multiple access layer devices exist at a location to serve end-user connectivity, it becomes impractical to interconnect each access switch as the access layer grows beyond two or three switches.

The distribution layer provides a logical point to summarize addressing and to create a boundary for protocols and features necessary for the access layer operation. Another benefit of the distribution layer boundary is that it creates fault domains that serve to contain failures or network changes to those parts of the network directly affected.

The end result to the organization is that the distribution layer can lower the cost of operating the network by making it more efficient, by requiring less memory, and by processing resources for devices elsewhere in the network. The distribution layer also increases network availability by containing failures to smaller domains.

Reduce Complexity and Increase Resiliency

This design uses a simplified distribution layer design, which consists of a single logical entity that can be implemented using a pair of physically separate switches operating as one device, a physical stack of switches operating as one device, or a single physical device with redundant components.

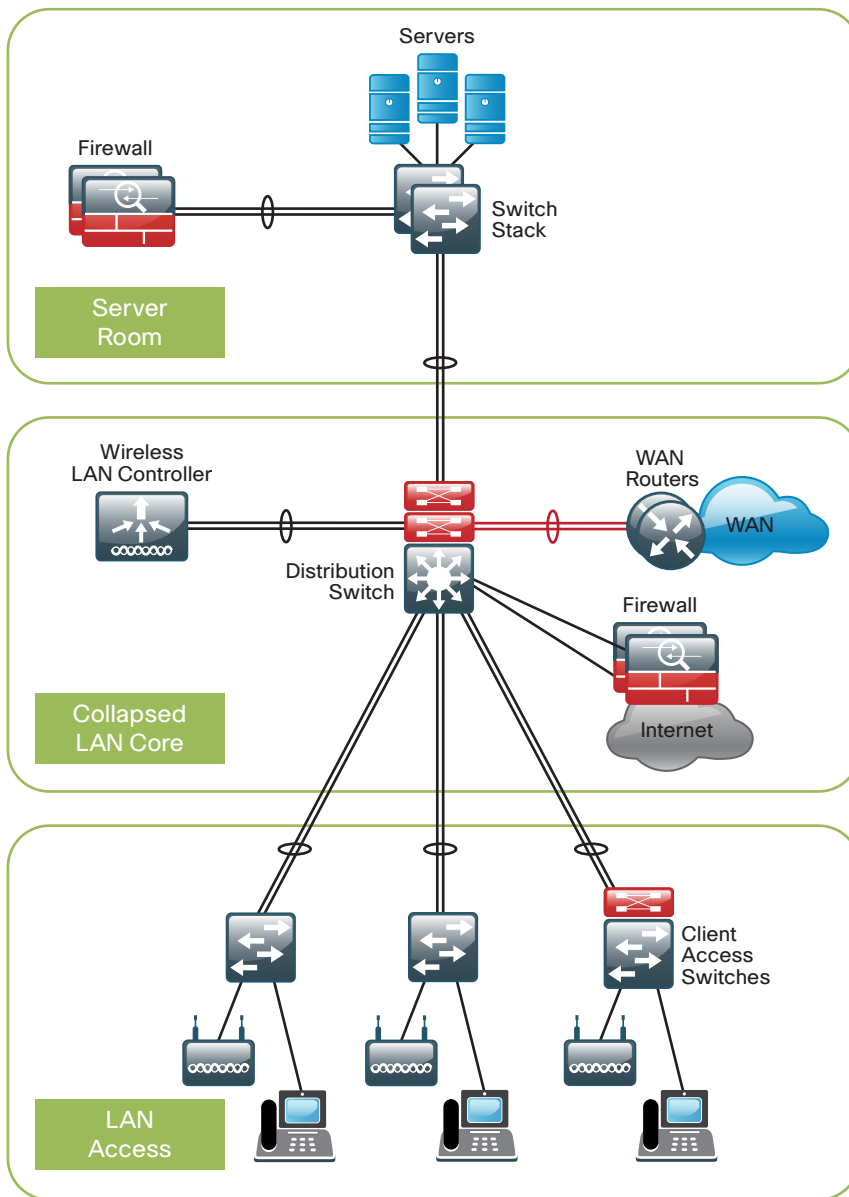
The benefit to the organization is the reduced complexity of configuring and operating the distribution layer as fewer protocols are required and little or no tuning is needed to provide near-second or sub-second convergence around failures or disruptions.

The design resiliency is provided by physically redundant components like power supplies, supervisors, and modules, as well as stateful switchover to redundant logical control planes. Reduced complexity and consistent design lower the operational cost of configuring and maintaining the network.

Flexible Design

The distribution layer provides connectivity to network-based services, to the WAN, and to the Internet Edge. Network-based services can include and are not limited to Wide Area Application Services (WAAS), and wireless LAN controllers. Depending on the size of the LAN, these services and the inter-connection to the WAN and Internet Edge may reside on a distribution layer switch that also aggregates the LAN access layer connectivity. This is also referred to as a “collapsed core” design because the distribution serves as the Layer 3 aggregation layer for all devices.

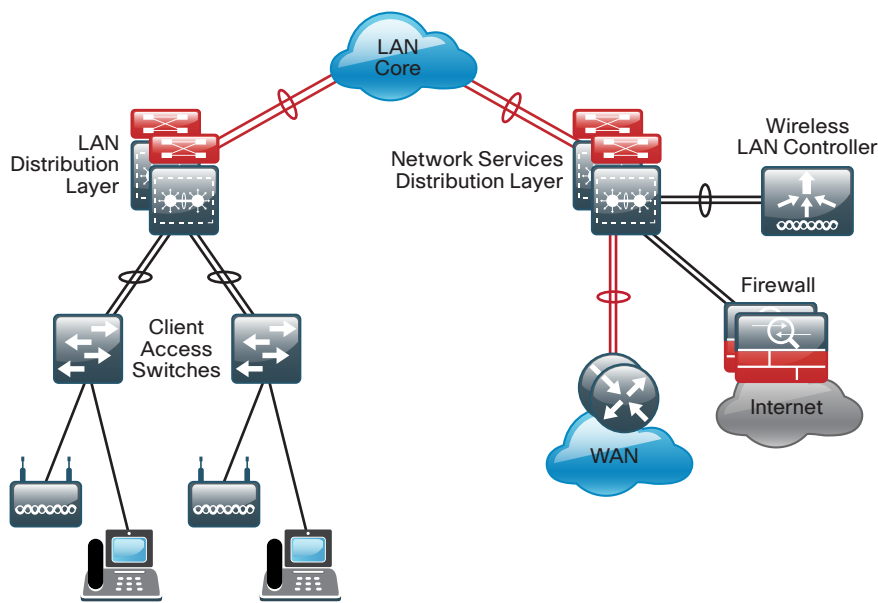
Figure 4 - Two tier design: Distribution layer functioning as a collapsed Core



Larger LAN designs require a dedicated distribution layer for network-based services connectivity versus sharing one with access layer devices. As the density of WAN routers, WAAS controllers, Internet Edge devices, and wireless LAN controllers grows, the ability to connect to a single distribution layer switch becomes hard to manage. There are a number of factors that drive LAN design with multiple distribution layer modules:

- The number of ports and port speed that the distribution layer platform can provide affects network performance and throughput.
- Network resilience is a factor when all LAN and network-based services rely on a single platform, regardless of that platform's design, it can present a single point of failure or an unacceptably large failure domain.
- Change control and frequency affects resilience. When all LAN, WAN, and other network services are consolidated on a single distribution layer, operational or configuration errors can affect all network operation.
- Geographic dispersion of the LAN access switches across many buildings in a larger campus facility would require more fiber optic interconnects back to a single collapsed core.

Figure 5 - Network-services distribution layer



2087

Like the access layer, the distribution layer also provides QoS for application flows to guarantee critical applications and multimedia applications perform as designed.

Core Layer

In a large LAN environment there often arises a need to have multiple distribution layer switches. One reason for this is that when access layer switches are located in multiple geographically dispersed buildings, you can save costly fiber-optic runs between buildings by locating a distribution layer switch in each of those buildings. As networks grow beyond three distribution layers in a single location, organizations should use a core layer to optimize the design.

Another reason to use multiple distribution layer switches is when the number of access layer switches connecting to a single distribution layer exceeds the performance goals of the network designer. In a modular and scalable design, you can colocate distribution layers for data center, WAN connectivity, or Internet Edge services.

In environments where multiple distribution layer switches exist in close proximity and where fiber optics provide the ability for high-speed interconnect, a core layer reduces the network complexity, as shown in the following two figures.

Figure 6 - LAN topology with a core layer

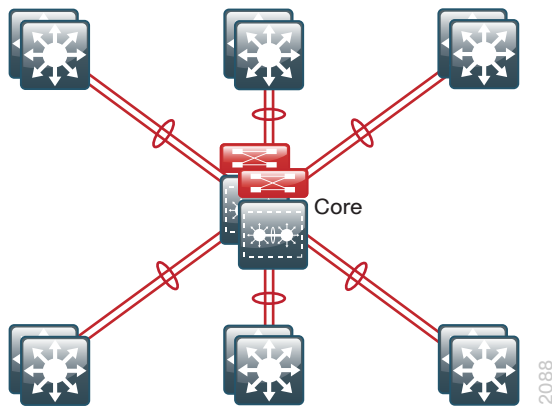
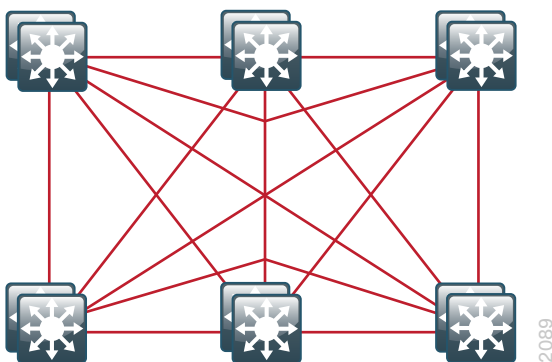


Figure 7 - LAN topology without a core layer



The core layer of the LAN is a critical part of the scalable network, and yet it is one of the simplest by design. The distribution layer provides the fault and control domains, and the core represents the 24x7x365 nonstop connectivity between them, which organizations must have in the modern business environment where connectivity to resources to conduct business is critical.

In this design, the core layer is based on two physically separate switches, which behave as one logical device. Connectivity to and from the core is Layer 3 only, which drives increased resiliency and stability. In a campus core-layer design where Cisco Catalyst 6500s are used, a Catalyst 6500 VSS Layer-3 core design is an alternative to the two-box core used in the design.



Reader Tip

For an in-depth VSS configuration guide and configuration options, go to www.cisco.com and search for the Campus 3.0 Virtual Switching System Design Guide.

Quality of Service (QoS)

Because real-time traffic is very sensitive to delay and drop, organizations need to provide special handling for it on the network. The network must ensure that this type of traffic is handled with priority so that the stream of audio or video is not interrupted.

QoS allows the organization to define different traffic types and to create more deterministic handling for real-time traffic. QoS is especially useful in congestion handling, where a full communications channel might prevent voice or video streams from being intelligible at the receiving side. It is important to note, however, that QoS does not create bandwidth; rather, it takes bandwidth from one class (that is, generally the default traffic class) to give some bandwidth to another class.

Within this design the approach to using QoS capabilities is to keep the QoS profiles as simple as necessary to meet the goals for supporting applications that need special delivery. The primary goals of implementing QoS within the network are:

- Support and ensure first out-the-door service for supported, real-time applications.
- Provide business continuance for business-critical applications.
- Provide fairness between all other applications when congestion occurs.
- Build a trusted edge around the network to guarantee that users cannot inject their own arbitrary priority values and to allow the organization to trust marked traffic throughout the network.

To accomplish these goals, the design uses a three-step approach to implementing QoS across the network as follows:

- Establish a limited number of traffic classes (that is, one to eight classes) within the network that need special handling (for example, real-time voice, real-time video, high-priority data, interactive traffic, batch traffic, and default classes).
- Classify applications into the traffic classes.
- Apply special handling to the traffic classes to achieve intended network behavior.

In this design, QoS configurations are as simple as possible, and are applied only to those applications that require special handling.

This approach establishes a solid, scalable, and modular framework to implement QoS across the entire network.

Access Layer

Design Overview

The access layer is the point at which user-controlled and user-accessible devices are connected to the network and it is the one architecture component that is found in every LAN.

Infrastructure Security Features

Because the access layer is the connection point between network-based services and client devices it plays an important role in protecting other users, the application resources, and the network itself from human error and malicious attacks. Network resiliency and security in the access layer is achieved through the use of Cisco Catalyst Infrastructure Security Features (CISF) including DHCP snooping, IP Source Guard, port security, and Dynamic ARP Inspection.

MAC flooding attacks are used to force a LAN switch to flood all their traffic out to all the switch interfaces. Port security limits the number of MAC addresses that can be active on a single port to protect against such attacks.

Port security lets you to configure Layer 2 interfaces to allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN.

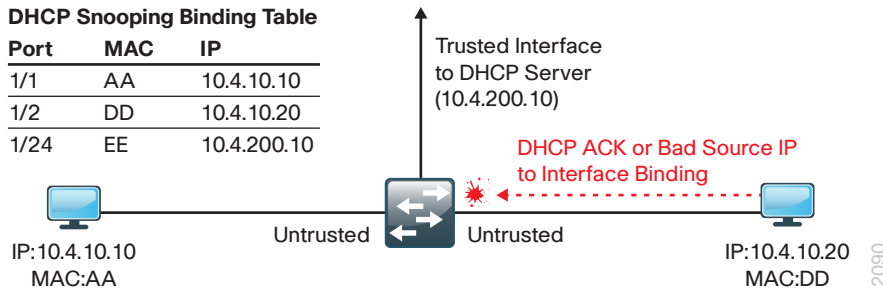
The number of MAC addresses that the device secures on each interface is configurable. For ease of management, the device can learn the addresses dynamically. Using the dynamic learning method, the device secures MAC addresses while ingress traffic passes through the interface. If the address is not yet secured and the device has not reached any applicable maximum, it secures the address and allows the traffic. The device ages dynamic addresses and drops them when the age limit is reached.

DHCP snooping is a DHCP security feature that filters and rate-limits DHCP traffic from untrusted sources. An untrusted source is any interface on the switch not specifically configured as a known DHCP server or path towards a known DHCP server, including all client-facing interfaces, allowing DHCP replies to be blocked from those interfaces.

The DHCP snooping feature helps simplify management and troubleshooting by tracking MAC address, IP address, lease time, binding type, VLAN number, and interface information that correspond to the local untrusted interfaces on the switch. DHCP snooping stores this information in the DHCP binding table, which is then used as a reference for comparison against observed traffic.

Dynamic ARP inspection (DAI) mitigates ARP poisoning attacks. An ARP poisoning attack is a method by which an attacker sends false ARP information to a local segment. This information is designed to poison the ARP cache of devices on the LAN, allowing the attacker to execute man-in-the-middle attacks.

Figure 8 - DHCP snooping and ARP inspection



DAI uses the data generated by the DHCP snooping feature and intercepts and validates the IP-to-MAC address relationship of all ARP packets on untrusted interfaces. ARP packets that are received on trusted interfaces are not validated and invalid packets on untrusted interfaces are discarded.

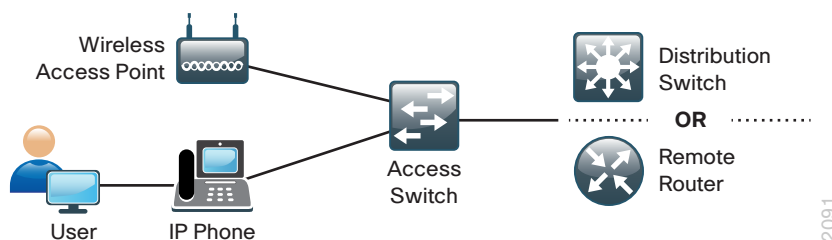
IP Source Guard is a means of preventing a packet from using an incorrect source IP address to obscure its true source, also known as *IP spoofing*. IP Source Guard uses information from DHCP snooping to dynamically configure a port access control list (PACL) on the interface that denies any traffic from IP addresses that are not in the DHCP binding table.

Common Design Method to Simplify Installation and Operation

To provide consistent access capabilities and simplify network deployment and operation, the design uses a common deployment method for all access layer devices, whether they are located in the headquarters or at a remote site. To reduce complexity, the access layer is designed so that you can use a single interface configuration for a standalone computer, an IP phone, an IP phone with an attached computer, or a wireless access point.

The LAN access layer provides high-speed connections to devices via 10/100/1000 Ethernet with both Gigabit and 10-Gigabit uplink connectivity options. The 10 Gigabit uplinks also support Gigabit connectivity to provide flexibility and help business continuity during a transition to 10 Gigabit Ethernet. The LAN access layer is configured as a Layer 2 switch, with all Layer 3 services being provided either by the directly-connected distribution layer or router.

Figure 9 - Access layer overview



Features to Support Voice and Video Deployment

Voice and video are enabled in the access layer via network services such as Power over Ethernet (PoE), QoS, multicast support, and Cisco Discovery Protocol with the voice VLAN.

PoE enables devices such as IP Phones, wireless access points, virtual desktops, and security cameras to be powered by the access layer device. This removes the expense of installing or modifying building power to support devices in difficult to reach locations and allows for the consolidation of back-up power supplies and Uninterruptable Power Supplies (UPSs) to the access closet.

To support the increasing requirements of devices powered by the network, all of the access layer devices support the IEEE 802.3at standard, also known as PoE+. The devices, and or line cards support all the previous implementations of PoE up to 15 watts per port as well as the new IEEE 802.3at implementation of up to 30 watts per port. For the most demanding PoE environments, like virtual desktops, the Catalyst 4500 in the access layer has the ability to provide up to 60 watts of power per port with Cisco Universal Power Over Ethernet (UPOE) over the same cable plant as you use for PoE+.

Cisco Discovery Protocol supports voice and video device integration into the access layer. Cisco IP Phones that are plugged into the access layer communicate bidirectionally with the access layer switch via Cisco Discovery Protocol. Cisco Discovery Protocol provides the IP Phone with configuration information and provides the access layer switch with the IP Phones power requirements and the ability to selectively prioritize traffic from the IP Phone.

Access Layer Platforms

Wiring Closets Requiring up to 48 Ports

Cisco Catalyst 2960-S and 3560-X Series are both 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-S and 3560-X are available in both PoE+ and non-power-supplying versions.

In addition to the capabilities supported by Catalyst 2960-S (other than stacking), Catalyst 3560-X supports dual redundant power supplies, dual redundant fans, modular uplinks, an upgradable Cisco IOS feature set, and enhanced enterprise capabilities such as Cisco TrustSec, Medianet, and Cisco IOS Sensor, where IOS Sensor may be a required component for configuring Bring Your Own Device (BYOD). With the addition of a 10-Gigabit Ethernet Services Module, Catalyst 3560-X also supports Flexible NetFlow and Cisco TrustSec MACsec.

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-speed 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: Cisco Catalyst 2960-S, 3750-X, 3850, and 4500E Series.

Cisco Catalyst 2960-S 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 switch. This enables up to four Catalyst 2960-S series switches to be stacked together.
- Cisco FlexStack links are full duplex 10 Gigabit Ethernet links with recovery time between 1-2 seconds.

Cisco Catalyst 3750-X Series are fixed-port, stackable, 10/100/1000 Ethernet switches, with PoE+ and non-power-supplying versions, that provide enhanced resiliency through StackWise Plus and StackPower technologies.

- Cisco StackWise Plus enables up to nine Cisco Catalyst 3750-X switches to be stacked together using a 64-Gbps stack interconnect with rapid failure recovery.
- Cisco StackPower shares power across the Cisco Catalyst 3750-X switch 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 3750-X Series have modular uplinks and support upgrading the Cisco IOS feature set and enhanced enterprise capabilities like TrustSec, Flexible NetFlow, Medianet, and Cisco IOS Sensor, to ensure that the switch functionality grows as the organization grows.

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

- Catalyst 3850 switches stack together using StackWise-480 mode with up to four switches in single stack-ring in the initial software release. The ability to stack beyond four physical switches will be supported in future Cisco IOS software releases.
- 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 Cisco Catalyst 3850 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 have modular uplinks that can be configured as Gigabit Ethernet or 10-Gigabit Ethernet.
- 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 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 4500 E-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 4500 E-Series switches also have an upgradable supervisor module which 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 Catalyst 4500 E-Series Supervisor 7-E and Supervisor 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 Catalyst 4500 E-Series provides maximum PoE flexibility with support of IEEE 802.3af, 802.3at, and now Cisco UPOE that supplies up to 60 watts per port of PoE. UPOE line cards are backward compatible to earlier PoE and PoE+ connected end points as well.
- The Catalyst 4507R+E chassis supports redundant supervisor modules and power supplies, which increases system availability by providing 1:1 redundancy for all critical systems.

- The Catalyst 4507R+E supports stateful switchover which allows a supervisor switchover to occur with minimum disruption to the network.
- The entire software upgrade process is simplified 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.

Deployment Details

As you review the *Campus Wired LAN Design 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. 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 Design Guide

Distribution Block	VLAN	IP Addressing	Usage
LAN Access A	100	10.4.0.x/24	Data-Access Switch 1
	101	10.4.1.x/24	Voice-Access Switch 1
	102	10.4.2.x/24	Data-Access Switch 2
	103	10.4.3.x/24	Voice-Access Switch 2
	Continue through 113	10.4.4.x - .13.x	alternate Data and Voice
	114	10.4.14.x/24	Available
	115	10.4.15.x/24	Management
LAN Access B	164	10.4.64.x/24	Data-Access Switch 1
	165	10.4.65.x/24	Voice-Access Switch 1
	166	10.4.66.x/24	Data-Access Switch 2
	167	10.4.67.x/24	Voice-Access Switch 2
	Continue through 177	10.4.68.x - .77.x	alternate Data and Voice
	178	10.4.78.x/24	Available
	179	10.4.79.x/24	Management
LAN Access C	180	10.4.80.x/24	Data-Access Switch 1
	181	10.4.81.x/24	Voice-Access Switch 1
	182	10.4.82.x/24	Data-Access Switch 2
	183	10.4.83.x/24	Voice-Access Switch 2
	Continue through 193	10.4.84.x - .93.x	alternate Data and Voice
	194	10.4.94.x/24	Available
	195	10.4.95.x/24	Management
Core	None	10.4.40.x	Core to Distribution Links

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 in the following steps, you can skip those steps.

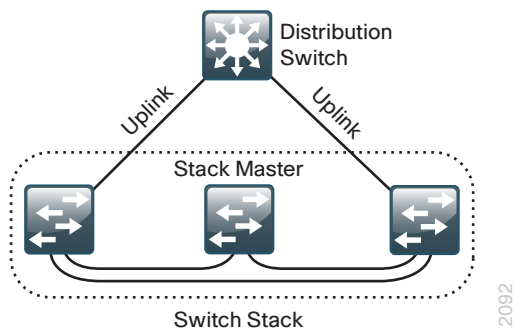
Option 1: Configure the Catalyst 2960-S, 3560-X, and 3750-X

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

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

When there are multiple Catalyst 2960-S or 3750-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 10 - Stack master placement in a switch stack



If you configure stack master switch priority on a Cisco Catalyst 2960-S or Cisco 3750-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. This command does not apply to the Catalyst 3560-X switch.

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

```
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 Catalyst 3850 platform

Step 1: If you are configuring a Catalyst 3850 stack, use the CLI global exec mode to set the preferred active switch.

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

For the Catalyst 3850, this setting is part of ROMMON, and does not appear in the configuration. When there are multiple Catalyst 3850 Series switches configured in a stack, one of the switches takes the role of the active switch. 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 dialog. When three or more Catalyst 3850s are configured as a stack, configure the active switch functionality on a switch that does not have uplinks configured.

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 cs5 cs4
class-map match-any CONTROL-MGMT-QUEUE
  match dscp cs7 cs6 cs3 cs2
class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
  match dscp af41 af42 af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match dscp af31 af32 af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match dscp af21 af22 af23
class-map match-any BULK-DATA-QUEUE
```

```

    match dscp af11 af12 af13
class-map match-any SCAVENGER-QUEUE
    match dscp cs1
!
policy-map 2P6Q3T
    class PRIORITY-QUEUE
        priority level 1 percent 30
    class CONTROL-MGMT-QUEUE
        bandwidth remaining percent 10
        queue-limit dscp cs2 percent 80
        queue-limit dscp cs3 percent 90
        queue-limit dscp cs6 percent 100
    class MULTIMEDIA-CONFERENCING-QUEUE
        bandwidth remaining percent 10
        queue-buffers ratio 10
    class MULTIMEDIA-STREAMING-QUEUE
        bandwidth remaining percent 10
        queue-buffers ratio 10
    class TRANSACTIONAL-DATA-QUEUE
        bandwidth remaining percent 10
        queue-buffers ratio 10
    class BULK-DATA-QUEUE
        bandwidth remaining percent 4
    class SCAVENGER-QUEUE
        bandwidth remaining percent 1
        queue-buffers ratio 10
    class class-default
        bandwidth remaining percent 25
        queue-buffers ratio 25
!

macro name AccessEdgeQoS
    auto qos voip cisco-phone
@
!
macro name EgressQoS
    service-policy output 2P6Q3T
@

```

Option 3: Configure the Catalyst 4507R+E platform

Step 1: 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 cs5 cs4
class-map match-any CONTROL-MGMT-QUEUE
    match dscp cs7 cs6 cs3 cs2

```

```

class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
  match dscp af41 af42 af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match dscp af31 af32 af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match dscp af21 af22 af23
class-map match-any BULK-DATA-QUEUE
  match dscp af11 af12 af13
class-map match-any SCAVENGER-QUEUE
  match dscp cs1
!
policy-map 1P7Q1T
  class PRIORITY-QUEUE
    priority
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
  class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    dbl
  class BULK-DATA-QUEUE
    bandwidth remaining percent 4
    dbl
  class SCAVENGER-QUEUE
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
    dbl
!
macro name AccessEdgeQoS
  auto qos voip cisco-phone
@
!
macro name EgressQoS
  service-policy output 1P7Q1T
@

```

Step 2: When a Catalyst 4507R+E is configured with two Supervisor 7L-Es, configure the switch to use Stateful Switchover (SSO) when moving the primary supervisor functionality between modules. To enable a fast transparent data plane failover, SSO synchronizes active process information as well as configuration information between supervisor modules.

```

redundancy
  mode sso

```

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 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 that is due to 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 must still enable spanning tree. 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: 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.

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

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.

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.

```
ip domain-name cisco.local
crypto key generate rsa modulus 2048
ip ssh version 2
no ip http server
ip http secure-server
!
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 cisco RO
snmp-server community cisco123 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.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



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, and in a Catalyst 3850 stack you may lose the ability to log in from the console ports of non-active (standby and member) switches.

Step 10: 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 password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

By default, https access to the switch will use 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 Authentication, Authorization and Accounting (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 SecretKey
!
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.

```
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, configure the in-band management interface on the data VLAN.

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 the 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 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]
```

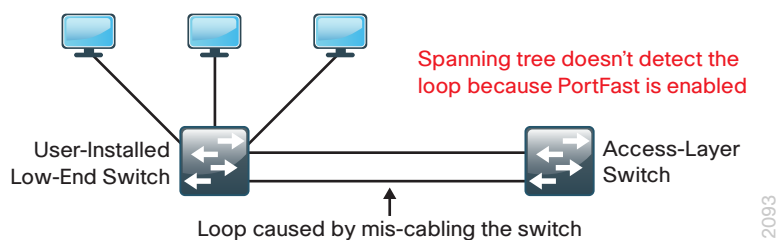
Step 5: Configure BPDU Guard globally to protect PortFast-enabled interfaces. This protects PortFast-enabled interfaces by disabling the port if another switch is plugged into the port.

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

BPDU guard protects against a user plugging a switch into an access port, 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.

Figure 11 - Scenario that BPDU Guard protects against



Procedure 4 Configure client connectivity

To make configuration easier when the same configuration will be 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, enable PortFast. PortFast shortens the time it takes for the interface to go into a forwarding state by disabling 802.1q trunking and channel group negotiation.

```
switchport host
```

Step 3: Enable QoS by applying the access edge QoS macro that was defined in the platform configuration procedure.

```
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.

Next, configure port security on the interface.

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
```

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
```

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

```
ip verify source
```

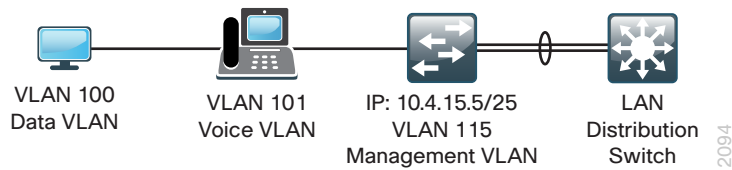
The Catalyst 4500 does not support the **ip verify source** command. Instead, use the following command:

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

Step 9: If the access switch is a Cisco Catalyst 3750-X, 3560-X, or 2960-S, increase the buffers for the default queue. This modification of the global QoS settings improves the ability to handle high bandwidth bursty traffic. In global configuration mode, add the following command:

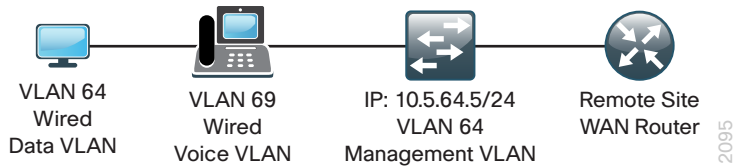
```
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

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
!
interface range GigabitEthernet 1/0/1-24
  switchport access vlan 100
  switchport voice vlan 101
  switchport host
  macro apply AccessEdgeQoS
  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
!
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

Example: Connected to WAN Router



```
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 10.5.69.1
!
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
!
interface range GigabitEthernet 1/0/1-24
  switchport access vlan 64
  switchport voice vlan 69
  switchport host
  macro apply AccessEdgeQoS
  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
!
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

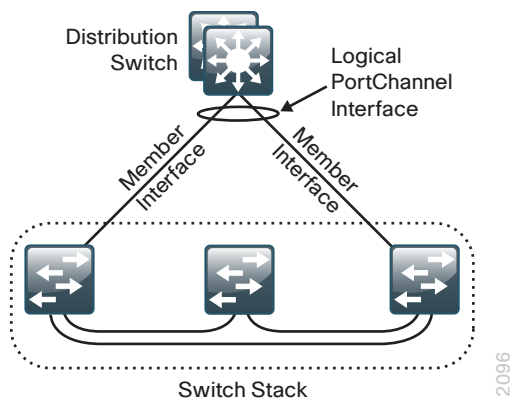
Procedure 5 Connect to distribution or WAN router

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 12 - 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, 3750-X, 3560-X, or 2960-S) to a distribution switch or WAN router. Where there are differences for configuring a specific switch, it will be called out in the step.

Option 1: Configure EtherChannel to distribution switch

Step 1: Configure EtherChannel member interfaces.

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

Cisco Catalyst 2960S does 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 range [interface type] [port 1] , [interface type] [port 2]
  switchport
```



```

macro apply EgressQoS
channel-protocol lacp
channel-group [number] mode active
logging event link-status
logging event trunk-status
logging event bundle-status

```

Step 2: Configure the trunk.

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. 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 will be port-channel and the number must match channel-group configured in Step 1.

The Catalyst 3750 requires the **switchport trunk encapsulation dot1q** command.

```

interface [interface type] [number]
description EtherChannel link to Distribution Layer
switchport trunk allowed vlan [data vlan],[voice vlan],
[mgmt vlan]
switchport mode trunk
ip arp inspection trust
ip dhcp snooping trust
logging event link-status
logging event trunk-status
no shutdown

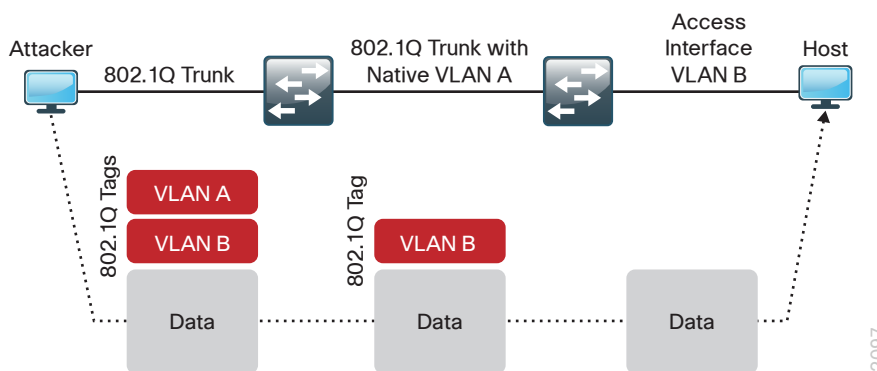
```

If the interface type is not a port-channel, you must configure an additional command **macro apply EgressQoS** 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, 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 13 - 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 3: To remove the remote risk of this type of attack, configure an unused VLAN on all switch-to-switch 802.1Q trunk links from access layer to distribution layer. 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 4: 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
```

Step 5: If you have configured your access-layer Cisco Catalyst 2960-S or Cisco Catalyst 3750-X switch stack for an EtherChannel link to the distribution layer switch, reload your switch stack now to ensure proper operation of EtherChannel. A single reload of a newly configured switch is necessary to ensure that EtherChannel operates with other features configured on the switch stack.

```
reload
```

Option 2: Configure EtherChannel 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 does 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
  macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 2: Configure the trunk.

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 will be port-channel, and the number must match channel-group configured in Step 1 in Option 2: of this procedure.

The Catalyst 3750 requires the **switchport trunk encapsulation dot1q** command.

```
interface [interface type] [number]
  description EtherChannel link to Router
  switchport trunk allowed vlan [data vlan],[voice vlan]
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  spanning-tree portfast trunk
  logging event link-status
  logging event trunk-status
  no shutdown
```

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

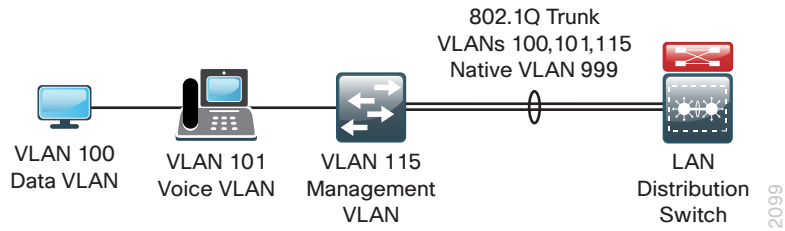
Step 3: Save the running configuration that you have entered so it will be used as the startup configuration file when your switch is reloaded or power-cycled.

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

Step 4: If you have configured your access layer Cisco Catalyst 2960-S or Cisco Catalyst 3750-X switch stack for EtherChannel to the WAN router, reload your switch stack now to ensure proper operation of EtherChannel. A single reload of a newly configured switch is necessary to ensure that EtherChannel operates with other features configured on the switch stack.

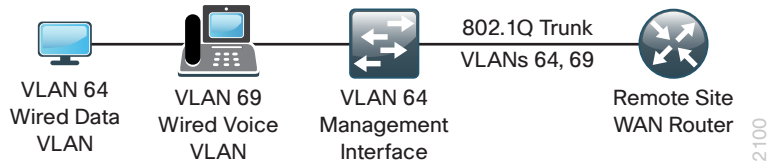
```
reload
```

Example: Procedure 5, Option 1



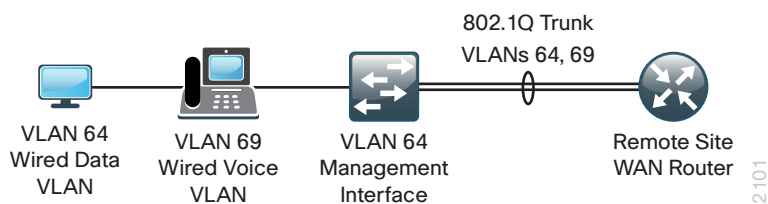
```
vlan 999
  name AntiVLANhopping
!
interface GigabitEthernet 1/0/25
  description Link to Distribution Layer port 1
interface GigabitEthernet 3/0/25
  description Link to Distribution Layer port 2
!
interface range GigabitEthernet 1/0/25, GigabitEthernet 3/0/25
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  channel-protocol lacp
  channel-group 1 mode active
!
interface Port-channel 1
  description Etherchannel to Distribution Layer
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100,101,115
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  no shutdown
```

Example: Procedure 5, Option 2



```
interface GigabitEthernet 1/0/24
  description Link to WAN Router
  macro apply EgressQoS
  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
  no shutdown
```

Example: Procedure 5, 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
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  channel-group 1 mode on
!
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
  no shutdown
```

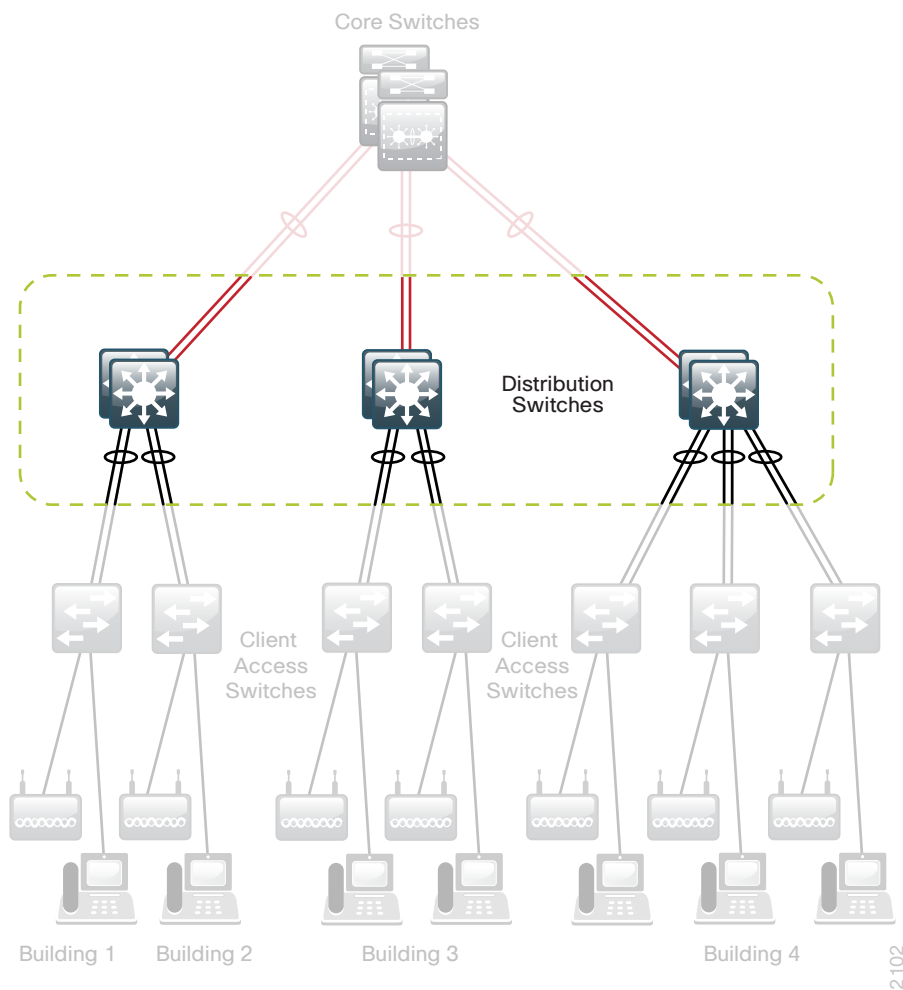
Distribution Layer

Design Overview

The primary function of the distribution layer is to aggregate access layer switches in a given building or campus. The distribution layer provides a boundary between the Layer 2 domain of the access layer and the Layer 3 domain that provides a path to the rest of the network. This boundary provides two key functions for the LAN. On the Layer 2 side the distribution layer creates a boundary for Spanning Tree Protocol limiting propagation of Layer 2 faults. On the Layer 3 side the distribution layer provides a logical point to summarize IP routing information before it enters the network and reduce IP route tables for easier troubleshooting and faster recovery from failures.

The LAN distribution layer uses a simplified distribution layer design that is easier to operate and troubleshoot than the traditional and routed access designs.

Figure 14 - Distribution layer overview



Traditional Distribution Layer Design

Traditional LAN designs use a multitier approach with Layer 2 from the access layer to the distribution layer, where the Layer 3 boundary exists. The connectivity from the access layer to the distribution layer can result in either a loop-free or looped design.

In the traditional network design, the distribution layer has two standalone switches for resiliency. It is recommended that you restrict a Layer 2 VLAN to a single wiring closet or access uplink pair to reduce or eliminate topology loops that Spanning Tree Protocol must block and that are a common point of failure in LANs. Restricting a VLAN to a single switch provides a loop-free design, but it does limit network flexibility.

To create a resilient IP gateway for VLANs in this design, you must use first-hop redundancy protocols, which provide hosts with a gateway IP for a VLAN on a healthy switch. Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) are the most common gateway redundancy protocols, but they only allow hosts to send data out one of the access uplinks to the distribution layer. Gateway Load Balancing Protocol (GLBP) does provide greater uplink utilization for traffic exiting the access layer by balancing load from hosts across multiple uplinks, but you can only use it in a non-looped topology.

All of these redundancy protocols require that you fine tune the default settings to allow for subsecond network convergence.

Some organizations require the same Layer 2 VLAN be extended to multiple access layer closets to accommodate an application or service. The looped design causes spanning tree to block links, which reduces the bandwidth from the rest of the network and can cause slower network convergence.

Figure 15 - Traditional loop-free design with a VLAN per access switch

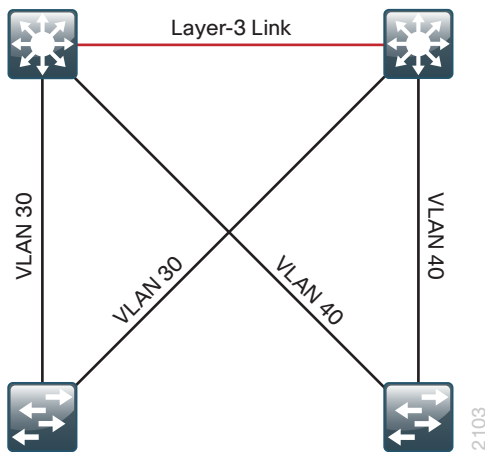
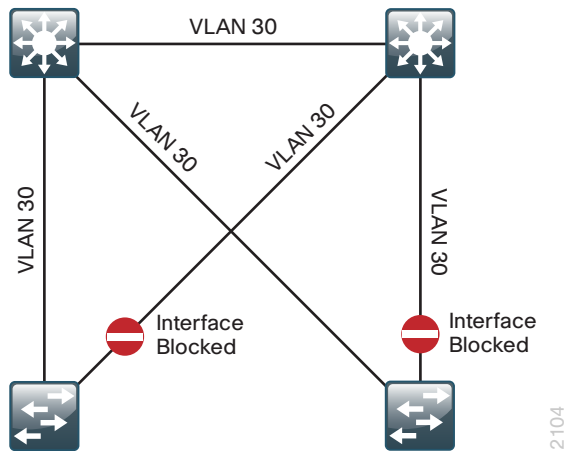


Figure 16 - Traditional looped design with VLANs spanning access switches



Routed Access Distribution Layer Design

In another approach to access and distribution layer design, you can use Layer 3 all the way to the access layer. The benefits of this design are that you eliminate spanning tree loops and reduce protocols because the IP gateway is now the access switch. Because there are no spanning tree blocking links, you can use both uplinks to the access layer and increase effective bandwidth available to the users.

The challenge with the routed access layer design is that the Layer 2 domains are confined to a single access closet, which limits flexibility for applications that require Layer 2 connectivity that extends across multiple access closets.

Simplified Distribution Layer Design

The distribution layer design in the LAN design uses multiple physical switches that act as a single logical switch or a single, highly-redundant physical switch. One advantage of this design is that spanning tree dependence is minimized, and all uplinks from the access layer to the distribution are active and passing traffic. Even in the distributed VLAN design, spanning tree blocked links due to looped topologies are eliminated. You reduce dependence on spanning tree by using EtherChannel to the access layer with dual-homed uplinks. This is a key characteristic of this design and you can load balance up to eight links if needed for additional bandwidth.

Figure 17 - Simplified design with a VLAN per access switch

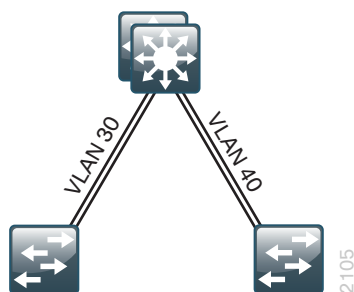
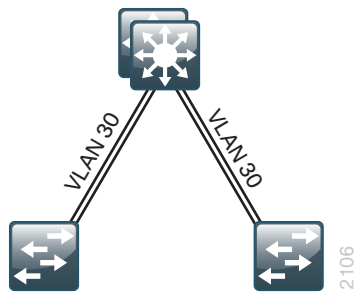


Figure 18 - Simplified design with VLANs spanning access switches



EtherChannel is a logical interface that can use a control plane protocol to manage the physical members of the bundle. It is better to run a channel protocol instead of using forced-on mode because a channel protocol performs consistency checks for interfaces programmed to be in the channel and provides protection to the system from inconsistent configurations. Cisco Catalyst switches provide both Port Aggregation Protocol (PAgP), which is a widely deployed Cisco designed protocol, and Link Aggregation Protocol (LACP) based on IEEE 802.3ad. This design uses LACP for EtherChannel because it is the only protocol supported in a Catalyst 3750 cross-stack configuration and can be used in all configurations in this design.

There are several other advantages to the simplified distribution layer design. You no longer need IP gateway redundancy protocols like HSRP, VRRP, and GLBP because the default IP gateway is now on a single logical interface and resiliency is provided by the distribution layer switch or switches. Also, the network will converge faster now that it is not depending on spanning tree to unblock links when a failure occurs because EtherChannel provides fast subsecond failover between links in an uplink bundle.

The topology of the network from the distribution layer to the access layer is logically a hub-and-spoke topology, which reduces complexity of design and troubleshooting. The hub-and-spoke topology design provides a more efficient operation for IP Multicast in the distribution layer because there is now a single logical designated router to forward IP Multicast packets to a given VLAN in the access layer.

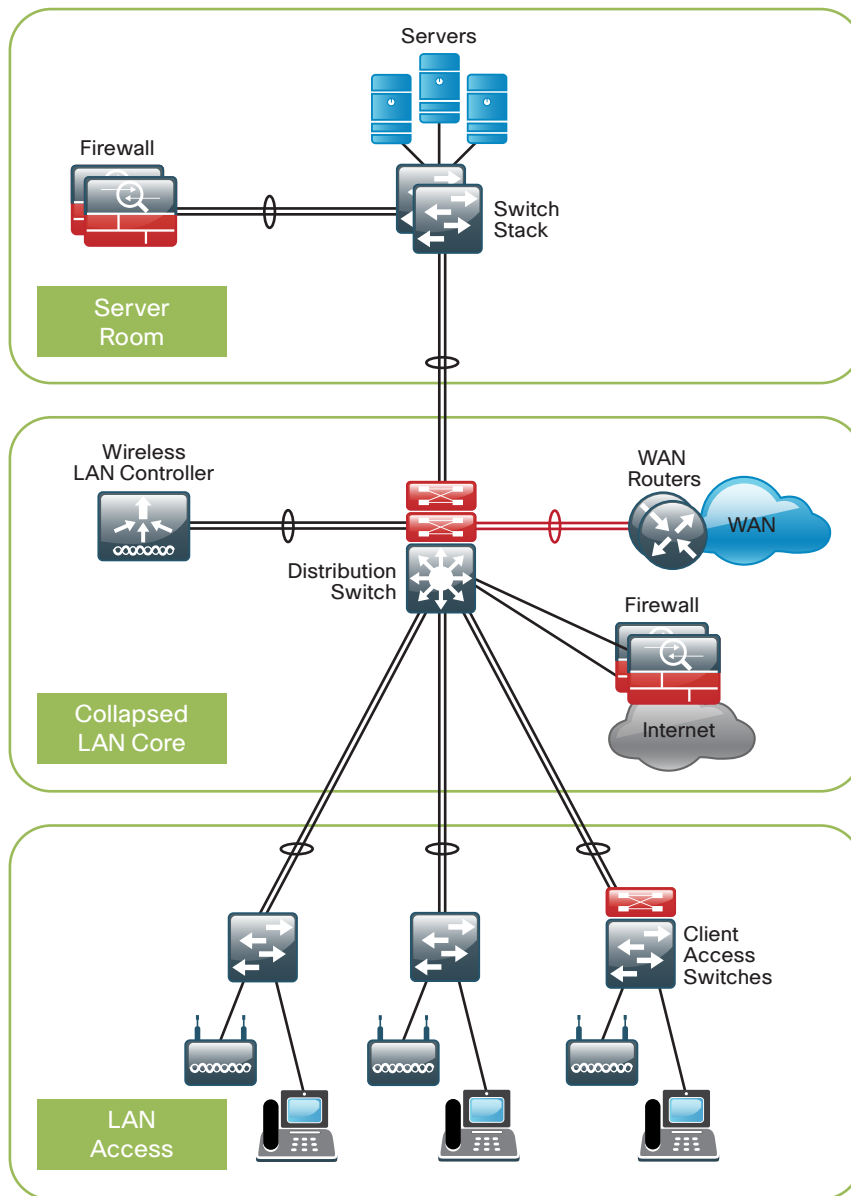
Finally, by using the single logical distribution layer design, there are fewer boxes to manage, which reduces the amount of time spent on ongoing provisioning and maintenance.

Distribution Layer Roles

Much emphasis has been placed on the distribution layer as the access layer aggregation point because this is the most common role. The distribution layer serves other roles in LAN designs.

In many smaller locations, the WAN head end and Internet Edge terminate at the headquarters location, along with a server farm or small data center and the LAN access for user connectivity. In these situations a single distribution layer or “collapsed core” design may be appropriate to allow the network to stay within budget limits while serving a smaller LAN access environment. Although the port density and configuration complexity may not be an issue, operational complexity of supporting many functions on one device must be monitored as the organization grows.

Figure 19 - Two tier Collapsed LAN Core design

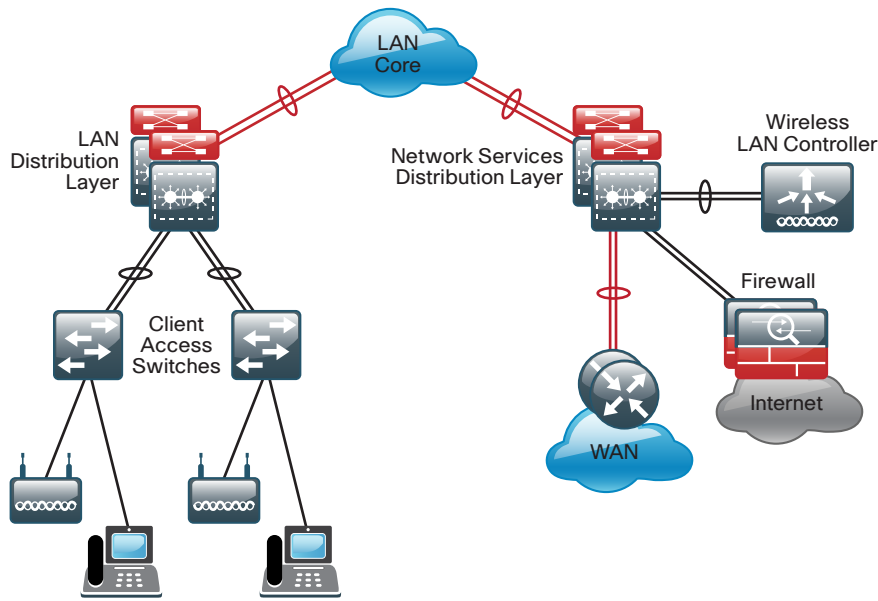


In larger LAN locations where the access layer density along with the number of network-service devices and WAN routers exceeds platform density or operational complexity additional distribution layer modules can break up the design.

The addition of a separate “services” distribution layer provides:

- Modular growth for high densities of WAN headend routers and WAN services like WAAS appliance.
- Wireless LAN controller termination in a central location for larger campus populations.
- Fault domains separate from the LAN access for a more resilient overall network.
- IP address summarization from WAN or Internet Edge toward the core of the network.

Figure 20 - Network services distribution layer



Whether the distribution layer role in your network design is serving as purely LAN access aggregation, a collapsed core, or network-services aggregation, the distribution layer configuration provides the processes and procedures to prepare this layer of the LAN for your application.

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) 4T, a highly available Cisco Catalyst 4507R+E switch, or a stack of Cisco Catalyst 3750-X 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 6500 VSS 4T

- Cisco Catalyst 6500 VSS 4T uses Cisco Catalyst 6500 Supervisor Engine 2T, which increases the per slot switching capacity to 80 Gbps, delivers better scalability, and provides enhanced hardware-enabled features. The increased performance enables the system to provide 40-gigabit Ethernet uplinks for core layer connectivity.
- Cisco 6500 Supervisor 2T supports the line cards enabled for Policy Feature Card 4 (PFC4), including the WS-X6816-10G WS-X6908-10G and WS-X6904-40G-2T, which provide enhanced capabilities. The WS-X6908-10G provides eight 10Gb Ethernet ports with 1:1 oversubscription. The WS-X6904-40G-2T provides up to four 40Gb Ethernet ports or up to sixteen 10Gb Ethernet ports using modular adapters for 10Gb or 40Gb Ethernet applications and can be programmed to run in 2:1 or 1:1 oversubscription mode. The WS-X6824 and WS-X6848 PFC4-based cards providing gigabit Ethernet ports are supported. The WS-X6724- and WS-X6748-based gigabit Ethernet cards are supported with CFC or DFC4A modules installed.

- The Supervisor 2T-based switch enhances support for Cisco TrustSec (CTS) by providing MacSec encryption and role-based access control (RBAC) lists, and delivers improved control plane policing to address denial-of-service attacks.
- Effectively allows the clustering 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 now 40 Gigabit Ethernet EtherChannel uplinks using Cisco Multi-chassis EtherChannel.
- Provides stateful switchover between supervisors in each chassis for Nonstop Forwarding in the event of a failure and provides Enhanced Fast Software Upgrades for minimizing downtime for upgrades.
- The premier distribution layer platform in this design. It allows for high 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 4507R+E Switch

- Cisco Catalyst 4507R+E switch has redundant supervisors, line cards, and power supplies. In this design, Cisco uses a single 4507R+E chassis configured with resilient components as a distribution layer platform. The Supervisor 7E 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 which is critical to Nonstop Forwarding in the event of a failure and allows in-service software upgrades for the system.
- Use it at locations where there is only a small number of Gigabit Ethernet or 10 Gigabit Ethernet connected wiring closets that need to be aggregated.

Cisco Catalyst 3750-X Stack

- Configured as a single unit, but has independent load-sharing power supplies and processor for each switch in the StackWise Plus stack. The LAN architecture uses a pair of stacked 3750X-12S-E switches that provide Layer 2 and Layer 3 switching. The switches use Small Form-Factor Pluggable (SFP) transceivers for a port-by-port option of copper or fiber optic Gigabit Ethernet EtherChannel uplinks to access closets.
- Cisco StackWise Plus enables up to nine Cisco Catalyst 3750-X switches to be stacked together using a 64-Gbps stack interconnect with rapid failure recovery.
- Cisco StackPower shares power across the Cisco Catalyst 3750-X switch 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 3750-X Series have modular uplinks for connectivity to the core layer at Gigabit or 10 Gigabit Ethernet speeds, and support upgrading the IOS feature set and enhanced enterprise capabilities like TrustSec and Medianet, to ensure that the switch functionality grows as the organization grows.
- Use it at locations where there is only a small number of gigabit connected wiring closets that need to be aggregated.

Deployment Details

The single, logical, resilient, distribution-layer design simplifies the distribution switch configuration over traditional dual system designs.

PROCESS

Configuring the Distribution Layer

1. Configure the platform
2. Configure LAN switch universal settings
3. Configure distribution global settings
4. Configure IP unicast routing
5. Configure IP Multicast routing
6. Configure IP Multicast 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 in the following steps, you can skip those steps.

Option 1: Configure Cisco Catalyst 6500 Virtual Switching System 4T

Cisco Catalyst 6500 Virtual Switching System 4T clusters two physical 6500 switches with a single Supervisor 2T in each switch together as a single logical switch. One of the supervisors acts as the active control plane for both chassis by controlling protocols such as EIGRP, Spanning Tree, CDP, and so forth, while both supervisors actively switch packets in each chassis.

The following configuration example shows you how to convert two standalone Cisco Catalyst 6500 switches to a Virtual Switching System (VSS). If you are migrating your switches from an existing in-service dual chassis role to a VSS system, go to www.cisco.com and search on “Migrate Standalone Cisco Catalyst 6500 Switch to Cisco Catalyst 6500 Virtual Switching System” for information that describes how to do this migration. For an in-depth VSS configuration guide and configuration options, go to www.cisco.com and search for the *Campus 3.0 Virtual Switching System Design Guide*.

When you set up the Cisco Catalyst 6500 Virtual Switching System 4T, connect two 10 Gigabit Ethernet links between the chassis to provide the Virtual Switch Link (VSL). Use at least two links. However, there are restrictions on which 10 Gigabit Ethernet interfaces you can use for the VSL. This design uses the two 10 Gigabit Ethernet interfaces on each supervisor. You must cable the interfaces together before you can configure the VSS.

Step 1: Convert standalone 6500s to VSS.

Configure a hostname on each switch so you can keep track of your programming steps.

On the Catalyst 6500 standalone switch #1:

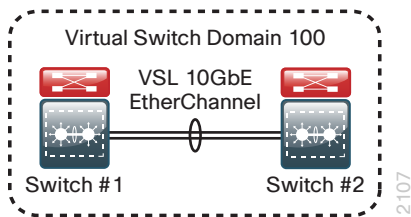
```
Router#config t  
Router#(config)#hostname VSS-Sw1
```

On the Catalyst 6500 standalone switch #2:

```
Router#config t  
Router#(config)#hostname VSS-Sw2
```

Each VSS switch pair must have a unique domain assigned that the pair shares. In this example, the domain number is 100. Each switch is also given a unique number in the domain, switch 1 or switch 2.

Figure 21 - VSS domain



On the standalone switch #1:

```
VSS-Sw1 (config)#switch virtual domain 100  
VSS-Sw1 (config-vs-domain)# switch 1
```

On the standalone switch #2:

```
VSS-Sw2 (config)#switch virtual domain 100  
VSS-Sw2 (config-vs-domain)# switch 2
```

Step 2: Configure the Virtual Switch Link (VSL).

The VSL is a critical component of the Virtual Switching System. Use unique port-channel numbers on each switch even though they connect to each other because both switches will soon become a single logical switch. This example uses port-channel number 101 on switch 1 and port-channel number 102 on switch 2. You must configure **channel-group mode on** for the VSL port channel. For the physical interfaces of the VSL EtherChannel, this example uses the 10 Gigabit Ethernet interfaces on the supervisor.

On standalone switch #1:

```
VSS-Sw1 (config) #interface port-channel 101
VSS-Sw1 (config-if) #switch virtual link 1
VSS-Sw1 (config-if) #no shutdown
VSS-Sw1 (config) #interface range tengigabit 5/4-5
VSS-Sw1 (config-if) #channel-group 101 mode on
VSS-Sw1 (config-if) #no shutdown
```

On standalone switch #2:

```
VSS-Sw2 (config) #interface port-channel 102
VSS-Sw2 (config-if) #switch virtual link 2
VSS-Sw2 (config-if) #no shutdown
VSS-Sw2 (config) #interface range tengigabit 5/4-5
VSS-Sw2 (config-if) #channel-group 102 mode on
VSS-Sw2 (config-if) #no shutdown
```

At this point you should be able to see that port-channel 101 and 102 are up, and both links are active on standalone switch #1 and standalone switch #2 respectively. The switches are not in VSS mode yet.

```
VSS-Sw1# show etherchannel 101 port
VSS-Sw2# show etherchannel 102 port
```

The previous two commands show the same output below.

```
Ports in the group:
-----
Port: Te5/4
-----
Port state = Up Mstr In-Bndl
...
Port: Te5/5
-----
Port state = Up Mstr In-Bndl
...
```

Step 3: Enable virtual mode operation.

Now that a port-channel has been established between the switches, convert each switch to virtual mode operation. At the enable prompt (that is, not in configuration mode) on each switch, enter the following commands for each switch.

On standalone switch #1:

```
VSS-Sw1# switch convert mode virtual
```

On standalone switch #2:

```
VSS-Sw2# switch convert mode virtual
```

When asked if you want to proceed, answer yes.

Each switch now renumbers its interfaces from interface y/z (where y is the slot number and z is the interface number) to interface x/y/z (where x is the switch number, y is the module number in that switch, and z is the interface on that module). This numbering scheme allows the two chassis to be addressed and configured as a single system from a single supervisor, which is the supervisor with the active control plane.

Once the configuration changes, it prompts you to save the configuration to bootflash. Press Return <CR> or Enter to accept the destination filename and location on each switch.

Both switches reload and become a VSS and one of the switches is resolved as the ACTIVE supervisor for the VSS cluster. All configuration commands now must be entered on the single active switch console; the standby switch console displays the Standby prompt.

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
```

Confirm that the two Catalyst 6500 switches are now operating as a single VSS system by using configuration mode to rename the switch hostname.

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


Step 4: Configure dual-active detection mechanism.

A critical aspect of the Cisco Catalyst 6500 VSS 4T is the control plane and data plane operating models. From a control plane standpoint the VSS uses an active-standby operating model. This means that one supervisor becomes the active control plane for the entire VSS while the other supervisor becomes the standby. The control plane handles protocol operations like EIGRP peering, route table updates, and spanning tree BPDUs. On the dataplane side, both supervisors are actively forwarding traffic in an active-active operating model. The VSL allows the supervisors to communicate and stay in synchronization. The VSS uses the Stateful Switchover (SSO) redundancy facility to keep the controlplane synchronized between the two supervisors.

In the event that the VSL is severed (that is, all links), or for any other reason communication is lost over the VSL, both supervisors would assume the active control plane role, thus creating a dual-active condition which can result in network instability.

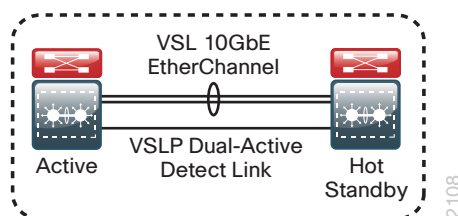
To prevent the dual-active scenario from causing an outage in the network, VSS supports multiple different dual-active detection mechanisms. The dual-active detection mechanisms are used to trigger a VSS recovery mode. In the VSS recovery mode only one supervisor is allowed to remain active, the other supervisor which is in recovery mode, shuts down all of its' interfaces except the VSL interfaces, thereby preventing instability in the network. Once the VSL is repaired, and communication over the VSL is reestablished, then the VSS would reload the supervisor that was in the recovery mode and return the VSS to a normal operating state.

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

- Ethernet Fast-Hello (VSLP) packet mode link
- Enhanced Port Aggregation Protocol (PAgP) hellos between an adjacent switch to the VSS

This design uses the Fast-Hello (VSLP) packet mode link for dual-active detection. To configure the link, use a Gigabit Ethernet interface on each VSS switch chassis and cable 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 22 - VSLP



```
D6500-VSS(config)# switch virtual domain 100
D6500-VSS(config-vs-domain)#dual-active detection fast-hello
D6500-VSS(config)#interface range gigabit1/1/24, gigabit2/1/24
D6500-VSS(config-if-range)#dual-active fast-hello
D6500-VSS(config-if-range)#no shutdown
%VSDA-SW2_SPSTBY-5-LINK_UP: Interface Gi2/1/24 is now dual-active detection capable
%VSDA-SW1_SP-5-LINK_UP: Interface Gi1/1/24 is now dual-active detection capable
```

Step 5: Configure the system virtual MAC address.

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. 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 config is saved and the entire Virtual Switching System (Active
and Standby) is reloaded.
```

Step 6: 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 programming is complete.

Step 7: If you are using the Cisco Catalyst 6900 Series 40-Gigabit Ethernet Interface Module with FourX adapters to convert CFP ports into four 10-Gigabit Ethernet ports, configure the switch to enable the line card to use 10-Gigabit Ethernet functionality for the associated port-group. After converting to VSS, the **switch** parameter is required.

```
D6500-VSS(config)# hw-module switch [switch] slot [slot] operation-mode port-
group [port-group] TenGigabitEthernet
```

Step 8: Configure QoS.

On the Catalyst 6500 Supervisor 2T based 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.

Two separate egress QoS policies are configured for the Catalyst 6500 to accommodate the 10-Gigabit and 40-Gigabit Ethernet cards which use a 1P7Q4T queuing architecture, and the Gigabit Ethernet cards which use a 1P3Q8T queuing architecture.

```
! Enable port-based QoS
auto qos default
! Class maps for 1P7Q4T 10Gb and 40Gb 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 af41 af42 af43
    match cos 4
class-map type lan-queuing match-any MULTIMEDIA-STREAMING-QUEUE
    match dscp af31 af32 af33
class-map type lan-queuing match-any TRANSACTIONAL-DATA-QUEUE
    match dscp af21 af22 af23
    match cos 2
class-map type lan-queuing match-any BULK-DATA-QUEUE
    match dscp af11 af12 af13
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
    random-detect dscp-based
    random-detect dscp 16 percent 60 70
    random-detect dscp-based
    random-detect dscp 24 percent 70 80
    random-detect dscp-based
    random-detect dscp 48 percent 80 90
    random-detect dscp-based
    random-detect dscp 56 percent 90 100
class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 14
    queue-buffers ratio 10
    random-detect dscp-based
    random-detect dscp 38 percent 70 80
    random-detect dscp-based
    random-detect dscp 36 percent 80 90
    random-detect dscp-based
    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 80
    random-detect dscp-based
    random-detect dscp 28 percent 80 90

```

```

    random-detect dscp-based
    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 80
    random-detect dscp-based
    random-detect dscp 20 percent 80 90
    random-detect dscp-based
    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 80
    random-detect dscp-based
    random-detect dscp 12 percent 80 90
    random-detect dscp-based
    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
!
! 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
        random-detect cos-based
        random-detect cos 2 percent 60 70
        random-detect cos-based
        random-detect cos 3 percent 70 80
        random-detect cos-based
        random-detect cos 6 percent 80 90
        random-detect cos-based
        random-detect cos 7 percent 90 100
    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 EgressQoS_TenOrFortyGig
    service-policy type lan-queuing output 1P7Q4T
@
!
macro name EgressQoS
    service-policy type lan-queuing output 1P3Q8T
@

```

Option 2: Configure the Catalyst 4507R+E platform

Step 1: For each platform, define a macro 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 cs5 cs4
class-map match-any CONTROL-MGMT-QUEUE
  match dscp cs7 cs6 cs3 cs2
class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
  match dscp af41 af42 af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match dscp af31 af32 af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match dscp af21 af22 af23
class-map match-any BULK-DATA-QUEUE
  match dscp af11 af12 af13
class-map match-any SCAVENGER-QUEUE
  match dscp cs1
!
policy-map 1P7Q1T
  class PRIORITY-QUEUE
    priority
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
  class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    dbl
  class BULK-DATA-QUEUE
    bandwidth remaining percent 4
    dbl
  class SCAVENGER-QUEUE
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
    dbl
!
macro name EgressQoS
  service-policy output 1P7Q1T
@
```

Step 2: When you configure a Catalyst 4507R+E with two Supervisor Engine 7-Es, configure the switch to use Stateful Switchover (SSO) when moving the primary supervisor functionality between modules. To enable a fast transparent data plane failover, SSO synchronizes active process information as well as configuration information between supervisor modules.

```
redundancy
mode sso
```

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.

Option 3: Configure the Catalyst 3750-X platform

Step 1: When there are multiple switches configured in a stack, one of the switches controls the operation of the stack. This switch 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.

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

If you configure stack master switch priority on Cisco 3750-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 Distribution Layer” process.

Step 2: By default, the newly active stack master switch assigns a new stack MAC address when the stack master switch fails. This new MAC address assignment can cause the network to reconverge because LACP and many other protocols rely on the stack MAC address and must restart. As such, you should use the **stack-mac persistent timer 0** command to ensure that the original master MAC address remains the stack MAC address after a failure.

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

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. Since AutoQoS might not be configured on this device, manually configure the global QoS settings by running the following commands:

```
mls qos map policed-dscp 0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
```

```

mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 1
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@
!

```

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 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 that is due to 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.

```
ntp 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 must still enable spanning tree. 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: 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.

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

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.

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.

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.

```
ip domain-name cisco.local
crypto key generate rsa modulus 2048
ip ssh version 2
no ip http server
ip http secure-server
!
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 cisco RO
snmp-server community cisco123 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.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



Caution

If you configure an access-list on the vty interface, you may lose the ability to use ssh to login 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 password clisco123
enable secret clisco123
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 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 Authentication, Authorization and Accounting (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 SecretKey
!
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 Catalyst 6500 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 IP Multicast routing”.

Step 3: 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 IP unicast routing

Enhanced IGRP (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.

The single logical distribution layer design uses stateful switchover and nonstop forwarding to provide subsecond 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 subsecond resiliency.

When the supervisor or master switch of a distribution platform switches over from the active to the hot-standby supervisor, it will continue switching IP data traffic flows in hardware. However, the supervisor requires time to reestablish control plane two-way peering with EIGRP 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 supervisor 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 IOS 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 must be configured to enable NSF for the protocol in use so that it can signal a peer when it switches over to a hot-standby supervisor for the peering neighbor to allow it time to reestablish the EIGRP protocol 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.

Step 1: Enable EIGRP for the IP address space that the network will be using. If needed for your network, you can enter multiple network statements. Disable auto summarization of the IP networks and 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.

```
ip routing
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 no auto-summary
 passive-interface default
 eigrp router-id [ip address of loopback 0]
 nsf
```

Cisco Catalyst 6500 does not require the **ip routing** command because it is enabled by default on that platform.



Tech Tip

Verify that **eigrp stub connected summary** is not configured in your EIGRP routing instance. This command may have been automatically configured if you have changed platform licensing from an ip base capable image.

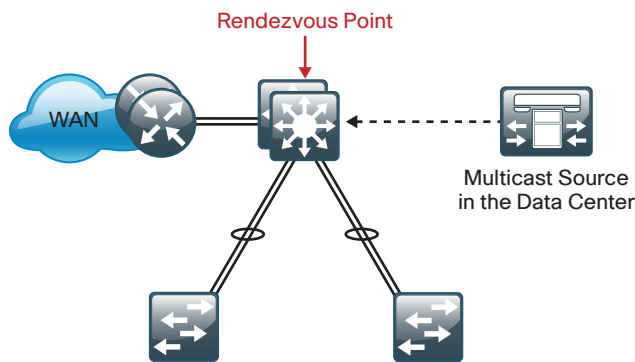
Procedure 5 Configure IP multicast routing

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 23 - 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
```

Cisco Catalyst 3750 Series switches instead require the **ip multicast-routing distributed** command.

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

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. 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
```

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

```
ip pim sparse-mode
```

Example

```
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
!
ip routing
!
router eigrp 100
  network 10.4.0.0 0.1.255.255
  no auto-summary
  passive-interface default
  eigrp router-id 10.4.15.254
  nsf
!
ip multicast-routing
ip pim autorp listener
!
```

Procedure 6 Configure IP multicast RP

(Optional)

In networks without a core layer, the RP function can be placed on the distribution layer. If a core layer does exist follow the IP Multicast Procedure 4 in the core layer section to configure the RP function.

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
```

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.

```
ip pim send-rp-discovery Loopback0 scope 32
```

In the event you add a core layer to your existing network and the RP is currently configured on a distribution layer, you may want to move the RP to the core. You can do this by configuring the RP address on the loopback 1 interfaces at the new location with the same ip address used on loopback 1 in this procedure, then enable and establish IP Multicast and MSDP peering.

All remote routers should still point to the same RP address, which simplifies the move and reduces disruption to the IP Multicast environment.

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.

Cisco 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.

Connect the access layer EtherChannel uplinks to separate switches in the distribution layer switches or stack, and in the case of Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

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

Cisco Catalyst 4500 does 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 range [interface type] [port 1], [interface type] [port 2]
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```



Tech Tip

The Catalyst 6500 has two egress QoS macros: EgressQoS, which is used for Gigabit Ethernet ports, and EgressQoSSTenOrFortyGig, 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 a trunk.

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 Step 3 .

The Catalyst 3750 requires the **switchport trunk encapsulation dot1q** command.

```
interface [port-channel] [number]
  description EtherChannel link to {your device here}
  switchport trunk allowed vlan [data vlan],[voice vlan],
    [mgmt vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

If the interface type is not portchannel, 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 5: To remove the remote risk of this type of attack is to configure an unused VLAN on all switch-to-switch 802.1Q trunk links from access layer to distribution layer. 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 6: Configure Layer 3.

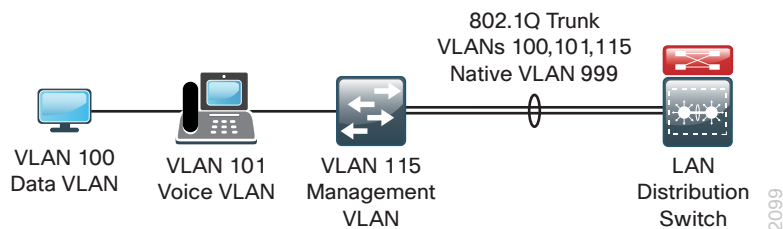
Configure a VLAN interface (SVI) for every access layer VLAN so devices in the VLAN can communicate with the rest of the network.

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 range GigabitEthernet 1/1/1, GigabitEthernet 2/1/1
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group 10 mode active
  logging event link-status
  logging event trunk-status
```

```

logging event bundle-status
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
  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 10.4.15.1 255.255.255.0
  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 will be 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.

```
interface [interface type] [number]
  description Link to {your device here}
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
  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: 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 EIGRP summarization.

```
ip summary-address eigrp 100 [network] [mask]
```

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

Cisco Catalyst 4500 does 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 range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  no switchport
  macro apply EgressQoS
  carrier-delay msec 0
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```



Tech Tip

The Catalyst 6500 has two egress QoS macros: EgressQoS, which is used for Gigabit Ethernet ports, and EgressQoSSTenOrFortyGig, 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 the EIGRP interface.

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

```
router eigrp 100
  no passive-interface [interface type] [number]
```

Step 5: 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



```
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 summary-address eigrp 100 10.4.0.0 255.255.240.0
  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
  macro apply EgressQoS TenOrFortyGig
  carrier-delay msec 0
  channel-group 30 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
router eigrp 100
  no passive-interface Port-channel 30
```

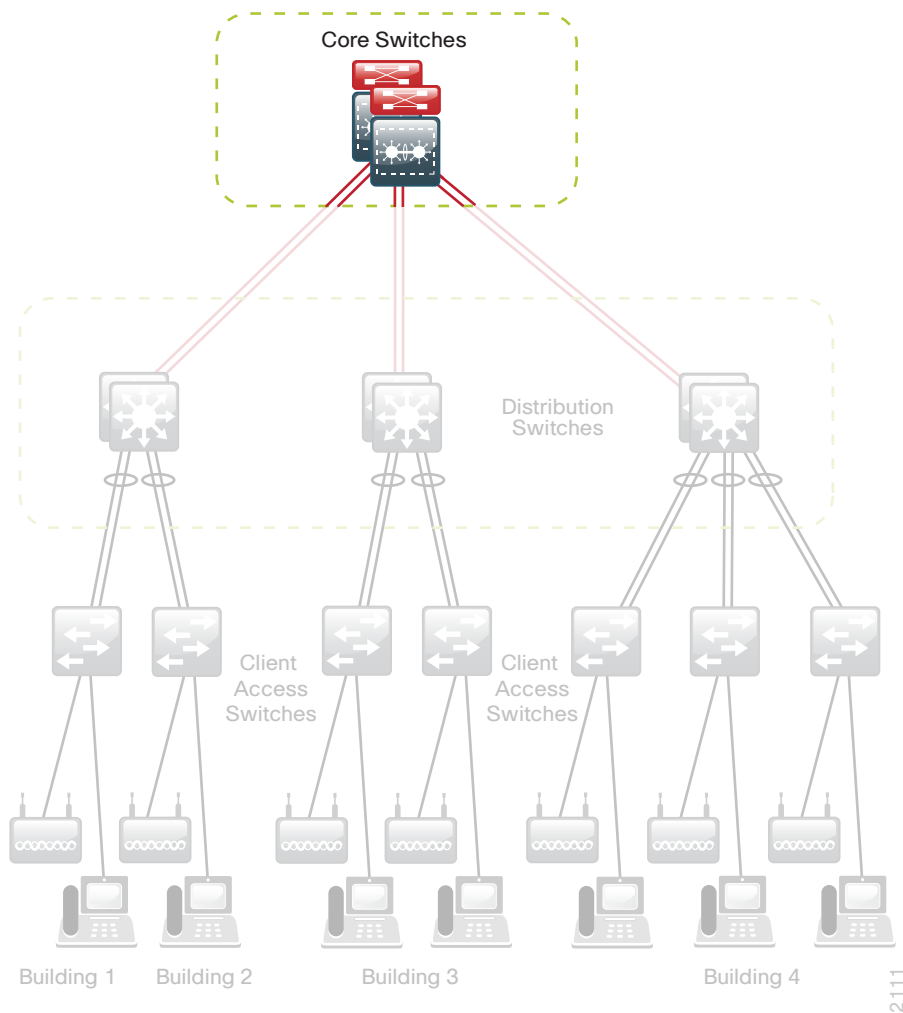
Core Layer

Design Overview

The core layer of the LAN is a critical part of the scalable network, yet by design, is one of the simplest. Like the distribution layer aggregates connectivity for multiple access layer switches, the core layer aggregates connectivity when there are multiple distribution blocks. As networks grow beyond three distribution blocks in a single location, a core layer should be used to optimize the design.

Beyond the simple aggregation of connectivity, the core layer serves to reduce the number of paths between distribution layers, which in turn lowers the time required to converge the network after a failure. By upgrading bandwidth between a distribution layer and the core, multiple distribution layer blocks can benefit from the increase versus the need to upgrade the bandwidth to every other device in a design without a core. The core layer is especially relevant to designs where the data center resources might be colocated with the LAN.

Figure 24 - Core layer overview



In large modular and scalable LAN designs, a core layer is used to aggregate multiple user connectivity distribution layer blocks and network-services distribution layer blocks. In designs with a colocated data center, the core provides high speed fan-out connectivity to the rest of the network. The core layer also serves as the connection between the Wide Area Network (WAN) and Internet Edge distribution layer blocks. Because of this central point of connectivity for all data flows, the core is part of the backbone IP routing address space and is designed to be highly resilient to protect from component-, power-, or operational-induced outages. The core layer should not contain highly complex or high touch services that require constant care and tuning, to avoid downtime required by complex configuration changes, increased software upgrades for new services, or links that toggle up/down as part of normal operations like user endpoint connectivity.

The core layer in this design is based on two physically separate switches, which behave as a single logical device using Cisco Virtual Switching System (VSS) like the Cisco Catalyst 6500 VSS in the distribution layer does. Connectivity to and from the core should be Layer 3 only. No VLANs should span the core to drive increased resiliency and stability.

The core is built on dual switches to provide redundant logic, line cards, hardware, and power for the backbone operation. Each distribution layer block, router, or other appliance connecting to the core should be connected with an EtherChannel with at least one link to each core switch. This approach provides load sharing of IP traffic across links of the multichassis EtherChannel for traffic traversing the core, and fast failover based on EtherChannel without waiting for routing protocol topology changes to propagate the network.

The core is designed to be high speed and provides for connectivity ranging from Gigabit Ethernet to 40 Gigabit Ethernet, and Gigabit EtherChannel up to 40 Gigabit EtherChannel. The core can provide non-blocking bandwidth based on design and configuration. EtherChannel links homed to a switch should be spread across line cards when possible.

The supervisor modules for the core switches in a VSS pair operate in an active/standby mode for Stateful Switchover (SSO) operation to protect the core operation in the event that a control plane hardware or software failure occurs. The core switches are Nonstop Forwarding (NSF) aware to provide enhanced resiliency for any dual supervisor connected devices and NSF capable if provisioned with dual supervisors per switch.

Core Layer Platform

Cisco Catalyst 6500 VSS 4T

- Cisco Catalyst 6500 VSS 4T uses two physical chassis with Cisco Catalyst 6500 Supervisor Engine 2T, which increases the per slot switching capacity to 80 Gbps, delivers better scalability, and provides enhanced hardware-enabled features. The increased performance enables the system to provide 40-gigabit Ethernet links for core layer connectivity.
- Cisco 6500 Supervisor 2T supports the line cards enabled for Policy Feature Card 4 (PFC4), including the WS-X6816-10G, WS-X6908-10G, and WS-X6904-40G-2T, which provide enhanced capabilities. The WS-X6908-10G provides eight 10-Gb Ethernet ports with 1:1 oversubscription. The WS-X6904-40G-2T provides up to four 40-Gb Ethernet ports or up to sixteen 10-Gb Ethernet ports using modular adapters for 10-Gb or 40-Gb Ethernet applications and can be programmed to run in 2:1 or 1:1 oversubscription mode. The WS-X6824 and WS-X6848 PFC4-based cards providing gigabit Ethernet ports are supported. The WS-X6724- and WS-X6748-based gigabit Ethernet cards are supported with CFC or DFC4A modules installed.
- The Supervisor 2T-based switch enhances support for Cisco TrustSec (CTS) by providing MacSec encryption and role-based access control (RBAC) lists, and delivers improved control plane policing to address denial-of-service attacks.

- The Cisco Catalyst 6500 VSS 4T effectively allows the clustering 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 now 40-Gigabit Ethernet EtherChannel links using Cisco Multi-chassis EtherChannel.
- Stateful switchover is provided between supervisors in each chassis for Cisco Nonstop Forwarding in the event of a failure, and Enhanced Fast Software Upgrades minimizes downtime for upgrades.
- The premier core layer platform in this design allows for high density aggregation of Gigabit Ethernet, 10-Gigabit Ethernet, and 40-Gigabit Ethernet connected distribution modules, while providing an advanced feature set and the highest resiliency available.

Deployment Details

The core layer uses a Cisco Catalyst 6500 VSS design for resiliency.

PROCESS

Configuring the Core

1. Configure the platform
2. Configure LAN switch universal settings
3. Configure the core switch global settings
4. Configure IP Multicast routing
5. Connect to distribution layer

Procedure 1 Configure the platform

Cisco Catalyst 6500 Virtual Switching System 4T clusters two physical 6500 switches with a single Supervisor 2T in each switch together as a single logical switch. One of the supervisors acts as the active control plane for both chassis by controlling protocols such as EIGRP, Spanning Tree, CDP, and so forth, while both supervisors actively switch packets in each chassis.

The following configuration example shows you how to convert two standalone Cisco Catalyst 6500 switches to a Virtual Switching System (VSS). If you are migrating your switches from an existing in-service dual chassis role to a VSS system, go to www.cisco.com and search on “Migrate Standalone Cisco Catalyst 6500 Switch to Cisco Catalyst 6500 Virtual Switching System” for information that describes how to do this migration. For an in-depth VSS configuration guide and configuration options, go to www.cisco.com and search for the *Campus 3.0 Virtual Switching System Design Guide*.

When you set up the Cisco Catalyst 6500 Virtual Switching System 4T, connect two 10-Gigabit Ethernet links between the chassis to provide the Virtual Switch Link (VSL). Use at least two links. However, there are restrictions on which 10-Gigabit Ethernet interfaces you can use for the VSL. This design uses the two 10-Gigabit Ethernet interfaces on each supervisor. You must cable the interfaces together before you can configure the VSS.

Step 1: Convert standalone 6500s to VSS by configuring a hostname on each switch so you can keep track of your programming steps.

On the Catalyst 6500 standalone switch #1:

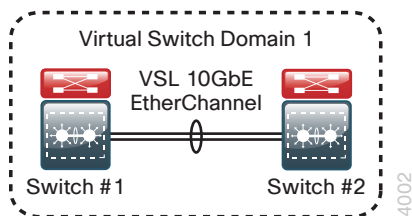
```
Router#config t  
Router#(config)#hostname VSS-Sw1
```

On the Catalyst 6500 standalone switch #2:

```
Router#config t  
Router#(config)#hostname VSS-Sw2
```

Each VSS switch pair must have a unique domain assigned that the pair shares. In this example, the domain number is 1. Each switch is also given a unique number in the domain, switch 1 or switch 2.

Figure 25 - VSS domain



On the standalone switch #1:

```
VSS-Sw1(config)#switch virtual domain 1  
VSS-Sw1(config-vs-domain)# switch 1  
VSS-Sw1(config-vs-domain)# exit  
VSS-Sw1(config)#
```

On the standalone switch #2:

```
VSS-Sw2(config)#switch virtual domain 1  
VSS-Sw2(config-vs-domain)# switch 2  
VSS-Sw2(config-vs-domain)# exit  
VSS-Sw2(config)#
```

Step 2: Configure the Virtual Switch Link (VSL).

The VSL is a critical component of the Virtual Switching System. Use unique port-channel numbers on each switch even though they connect to each other because both switches will soon become a single, logical switch. This example uses port-channel number 101 on switch 1 and port-channel number 102 on switch 2. You must configure **channel-group mode on** for the VSL port channel. For the physical interfaces of the VSL EtherChannel, this example uses the 10-Gigabit Ethernet interfaces on the supervisor.

On standalone switch #1:

```
VSS-Sw1 (config) #interface port-channel 101
VSS-Sw1 (config-if) #switch virtual link 1
VSS-Sw1 (config-if) #no shutdown
VSS-Sw1 (config) #interface range tengigabit 5/4-5
VSS-Sw1 (config-if) #channel-group 101 mode on
VSS-Sw1 (config-if) #no shutdown
```

On standalone switch #2:

```
VSS-Sw2 (config) #interface port-channel 102
VSS-Sw2 (config-if) #switch virtual link 2
VSS-Sw2 (config-if) #no shutdown
VSS-Sw2 (config) #interface range tengigabit 5/4-5
VSS-Sw2 (config-if) #channel-group 102 mode on
VSS-Sw2 (config-if) #no shutdown
```

At this point you should be able to see that port-channel 101 and 102 are up, and both links are active on standalone switch #1 and standalone switch #2, respectively. The switches are not in VSS mode yet.

```
VSS-Sw1# show etherchannel 101 port
VSS-Sw2# show etherchannel 102 port
```

The previous two commands show the same output below.

```
Ports in the group:
-----
Port: Te5/4
-----
Port state = Up Mstr In-Bndl
...
Port: Te5/5
-----
Port state = Up Mstr In-Bndl
...
```

Step 3: Enable virtual mode operation.

Now that a port-channel has been established between the switches, convert each switch to virtual mode operation. At the enable prompt (that is, not in configuration mode) on each switch, enter the following commands for each switch.

On standalone switch #1:

```
VSS-Sw1# switch convert mode virtual
```

On standalone switch #2:

```
VSS-Sw2# switch convert mode virtual
```

When asked if you want to proceed, answer yes.

Each switch now renumbers its interfaces from interface y/z (where y is the slot number and z is the interface number) to interface x/y/z (where x is the switch number, y is the module number in that switch, and z is the interface on that module). This numbering scheme allows the two chassis to be addressed and configured as a single system from a single supervisor, which is the supervisor with the active control plane.

Once the configuration changes, it prompts you to save the configuration to bootflash. Accept the destination filename and location on each switch by pressing **Return <CR>** or **Enter**.

Both switches reload and become a VSS and one of the switches is resolved as the ACTIVE supervisor for the VSS cluster. All configuration commands now must be entered on the single active switch console; the standby switch console displays the VSS-Sw1-sdby standby switch prompt.

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
```

Confirm that the two Catalyst 6500 switches are now operating as a single VSS system by using configuration mode to rename the switch hostname.

```
VSS-Sw1 (config)#hostname C6500-VSS  
C6500VSS (config)#
```

Step 4: Configure dual-active detection mechanism.

A critical aspect of the Cisco Catalyst 6500 VSS 4T is the control plane and data plane operating models. From a control plane standpoint, the VSS uses an active-standby operating model. This means that one supervisor becomes the active control plane for the entire VSS while the other supervisor becomes the standby. The control plane handles protocol operations like EIGRP peering, route table updates, and spanning tree BPDUs. On the dataplane side, both supervisors are actively forwarding traffic in an active-active operating model. The VSL allows the supervisors to communicate and stay in synchronization. The VSS uses the Stateful Switchover (SSO) redundancy facility to keep the controlplane synchronized between the two supervisors.

In the event that the VSL is severed (that is, all links), or for any other reason communication is lost over the VSL, both supervisors would assume the active control plane role, thus creating a dual-active condition that can result in network instability.

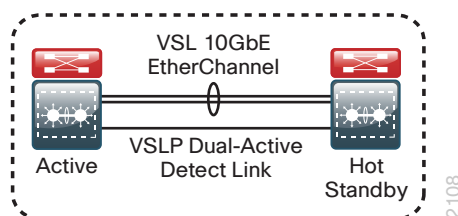
In order to prevent the dual-active scenario from causing an outage in the network, VSS supports multiple dual-active detection mechanisms. The dual-active detection mechanisms trigger a VSS recovery mode. In the VSS recovery mode, only one supervisor is allowed to remain active, the other supervisor, which is in recovery mode, shuts down all of its interfaces except the VSL interfaces, thereby preventing instability in the network. Once the VSL is repaired, and communication over the VSL is reestablished, the VSS reloads the supervisor that was in the recovery mode and returns the VSS to a normal operating state.

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

- Virtual Switch Link Protocol (VSLP) Ethernet Fast-Hello packet mode link
- Enhanced Port Aggregation Protocol (PAgP) hellos between an adjacent switch to the VSS

This design uses the Fast-Hello (VSLP) packet mode link for dual-active detection. Configure the link by using a Gigabit Ethernet interface on each VSS switch chassis and cabling 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 26 - VSLP



```
C6500-VSS(config)# switch virtual domain 1
C6500-VSS(config-vs-domain)#dual-active detection fast-hello
C6500-VSS(config)#interface range gigabit1/1/24, gigabit2/1/24
C6500-VSS(config-if-range)#dual-active fast-hello
C6500-VSS(config-if-range)#no shutdown
%VSDA-SW1-5-LINK_UP: Interface Gi1/1/24 is now dual-active detection capable
%VSDA-SW2_STBY-5-LINK_UP: Interface Gi2/1/24 is now dual-active detection capable
```

Step 5: Configure the system virtual MAC address.

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. 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.

```
C6500-VSS(config)# switch virtual domain 1
C6500-VSS(config-vs-domain)# mac-address use-virtual
Configured Router mac address is different from operational value. Change will
take effect after config is saved and the entire Virtual Switching System (Active
and Standby) is reloaded.
```

Step 6: 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 programming is complete.

Step 7: If you are using the Cisco Catalyst 6900 Series 40-Gigabit Ethernet Interface Module with FourX adapters to convert CFP ports into four 10-Gigabit Ethernet ports, configure the switch to enable the line card to use 10-Gigabit Ethernet functionality for the associated port-group. After converting to VSS, the **switch** parameter is required.

```
C6500-VSS(config)# hw-module switch [switch] slot [slot] operation-mode port-
group [port-group] TenGigabitEthernet
```

Step 8: Configure QoS.

On the Catalyst 6500 Supervisor 2T based 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, in order 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.

Configure two separate egress QoS policies for the Catalyst 6500 in order to accommodate the 10-Gigabit and 40-Gigabit Ethernet cards, which use a 1P7Q4T queuing architecture, and the Gigabit Ethernet cards, which use a 1P3Q8T queuing architecture.

```
! Enable port-based QoS
auto qos default
! Class maps for 1P7Q4T 10Gb and 40Gb 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 af41 af42 af43
    match cos 4
class-map type lan-queuing match-any MULTIMEDIA-STREAMING-QUEUE
    match dscp af31 af32 af33
class-map type lan-queuing match-any TRANSACTIONAL-DATA-QUEUE
    match dscp af21 af22 af23
    match cos 2
class-map type lan-queuing match-any BULK-DATA-QUEUE
    match dscp af11 af12 af13
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
        random-detect dscp-based
        random-detect dscp 16 percent 60 70
        random-detect dscp-based
        random-detect dscp 24 percent 70 80
        random-detect dscp-based
        random-detect dscp 48 percent 80 90
        random-detect dscp-based
        random-detect dscp 56 percent 90 100
    class MULTIMEDIA-CONFERENCING-QUEUE
        bandwidth remaining percent 14
        queue-buffers ratio 10
        random-detect dscp-based
        random-detect dscp 38 percent 70 80
        random-detect dscp-based
        random-detect dscp 36 percent 80 90
        random-detect dscp-based
        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 80
        random-detect dscp-based
        random-detect dscp 28 percent 80 90
        random-detect dscp-based

```



```

    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 80
    random-detect dscp-based
    random-detect dscp 20 percent 80 90
    random-detect dscp-based
    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 80
    random-detect dscp-based
    random-detect dscp 12 percent 80 90
    random-detect dscp-based
    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
!
! 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
    random-detect cos-based
    random-detect cos 2 percent 60 70
    random-detect cos-based
    random-detect cos 3 percent 70 80
    random-detect cos-based
    random-detect cos 6 percent 80 90
    random-detect cos-based
    random-detect cos 7 percent 90 100
  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 EgressQoS_TenOrFortyGig
  service-policy type lan-queuing output 1P7Q4T
@
!
macro name EgressQoS
  service-policy type lan-queuing output 1P3Q8T
@

```

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 these settings. The actual settings and values depend on your current network configuration.

Table 4 - 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 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 that is due to 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 must still enable spanning tree. 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 convergence of interface trunks, especially with fiber, which can be susceptible to unidirectional failures.

```
udld enable
```

Step 5: 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.

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

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.

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.

```
ip domain-name cisco.local
crypto key generate rsa modulus 2048
ip ssh version 2
no ip http server
ip http secure-server
!
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 cisco RO
snmp-server community cisco123 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.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



Caution

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

Step 10: 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 password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

By default, https access to the switch will use 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 Authentication, Authorization and Accounting (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 SecretKey
!
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
```

Procedure 3 Configure the core switch global settings

Step 1: Configure the in-band management interface.

The loopback interface for Cisco Layer 3 devices 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. Layer 3 process and features are also bound to the loopback interface to ensure resiliency of the processes. The loopback address is commonly a host address with a 32-bit address mask and has been allocated out of the core network address range. This example includes the **ip pim sparse-mode** command that will be explained further in Procedure 4.

```
interface loopback 0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

Step 2: 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 Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

Step 3: Configure IP unicast routing

Enable EIGRP for the IP address space that the network will be using and disable auto summarization of the IP networks. If needed for your network, you can enter multiple network statements. The Loopback 0 IP address is used for the EIGRP router ID to ensure maximum resiliency.

```
router eigrp 100
  network 10.4.0.0 0.1.255.255
  no auto-summary
  eigrp router-id [ip address of loopback 0]
```

Procedure 4 Configure IP Multicast routing

IP Multicast allows a single IP data stream to be sent from a single source to multiple receivers and be replicated by the infrastructure (that is, routers and switches). Using IP Multicast is much more efficient than multiple 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 an RP to map 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. This design, which is based on the pim sparse mode multicast operation, uses the resiliency inherent in a VSS configuration for a simple yet scalable way to provide a highly resilient RP environment.

Step 1: Enable PIM.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Step 2: Configure a second loopback interface for RP functions on the core VSS switch. All routers point to this IP address on **loopback 1** for the RP. You configure the RP address from the core IP address space. Creating the RP on a second loopback interface allows for flexibility for potential RP migrations using Anycast RP operation.

```
interface Loopback 1
 ip address 10.4.40.252 255.255.255.255
 ip pim sparse-mode
```

Step 3: Configure AutoRP candidate RPs.

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 Loopback1 scope 32 group-list 10
```

Step 4: 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 the core switches to act as AutoRP mapping agents.

```
ip pim send-rp-discovery Loopback1 scope 32
```

Step 5: Configure devices to listen to AutoRP announcements.

All Layer 3 switches and routers in the organization, including the RP switches, must be configured to listen to the AutoRP announcements from the mapping agents.

```
ip pim autorp listener
```

Devices other than the Cisco Catalyst 6500 use the command **ip pim auto-rp listener**.

In the event you add a core layer to your existing network and the RP is currently configured on a distribution layer, you may want to move the RP to the core.

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
C6500-VSS (config-if) #ip pim sparse-mode
```

Procedure 5 Connect to distribution layer

In this design, links to the core VSS are configured as point-to-point Layer 3 routed EtherChannels. When using Cisco Catalyst 6500 VSS 4T system in the campus, Cisco recommends that all peer-connected links are EtherChannel links, with EtherChannel members distributed between the physical switches in the VSS. EtherChannel to the Catalyst 6500 VSS provides for optimal forwarding because a packet that is received on the switch will be forwarded out a link on that same switch in normal operation instead of traversing the VSL connection.

Other benefits of EtherChannel to any single physical or logical device are that it makes it easier for you to grow bandwidth without changing the topology and that a single link failure uses EtherChannel recovery versus using ECMP or a routing topology change to reroute the data flows for fastest recovery.

Since the core links are point-to-point routed links, use 30-bit IP address subnets and masks and do not use Switched Virtual Interfaces (SVI).

Step 1: Configure the Layer 3 interface.

When using an EtherChannel to connect to a distribution layer platform, the interface type will be portchannel and the number must match the channel-group number you will configure in Step 2. When configuring a Layer 3 EtherChannel the logical port-channel interface is configured prior to configuring the physical interfaces associated with the EtherChannel.

```
interface [interface type] [number]
  description Link to {your device here}
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
  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 you are connecting to the same distribution layer switch with multiple links, you can use a portchannel for added bandwidth over a single logical link. Configure the physical interfaces to tie to the logical port channel by using the **channel-group** command. The number for the port channel and channel group will match.

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



Tech Tip

The Catalyst 6500 has two egress QoS macros: EgressQoS, which is used for Gigabit Ethernet ports, and EgressQoSSTenOrFortyGig, which is used for 10-Gigabit or 40-Gigabit Ethernet ports.

```
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 range [interface type] [port 1], [interface type] [port 2],
[interface type] [port 3], [interface type] [port 4]
  no switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```

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: Core to distribution port-channel configuration



```
interface Port-channel 30
  description EtherChannel link to Distribution Switch
  no switchport
  ip address 10.4.40.9 255.255.255.252
  ip pim sparse-mode
  no shutdown
!
interface range FortyGigabitEthernet 1/3/1, FortyGigabitEthernet 1/3/3,
FortyGigabitEthernet 2/3/1, FortyGigabitEthernet 2/3/3
  description EtherChannel link to Distribution Switch
  no switchport
  macro apply EgressQoS TenOrFortyGig
  carrier-delay msec 0
  channel-group 30 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
```

Appendix A: Product List

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	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 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE2 LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY IP Services license
	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 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1- 2SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE2 IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

LAN Core Layer

Functional Area	Product Description	Part Numbers	Software
Modular Core Layer Switch	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY IP services license
	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 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	

Appendix B: Device Configuration Files

To view the configuration files from the CVD lab devices that we used to test this guide, please go to the following URL:

<http://cvddocs.com/fw/Rel2-215>

Feedback

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)