Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-168

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

Discrete Manufacturing LAN Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). 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 shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

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 SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide 1
- Cisco SBA Solutions 1
- Route to Success 1
- About This Guide 1

Introduction 2
- Related Reading 2
- Design Goals 2

Discrete Manufacturing LAN Overview 3
- Architecture Overview 3
- Network Services 6

Distribution/Core Layer 10
- Business Overview 10
- Technology Overview 10
- Deployment Details 12
  - Configuring the Distribution/Core Layer 12

Access Layer 21
- Business Overview 21
- Technology Overview 21
- Deployment Details 23
  - Configuring the Access Layer 23
  - Connecting the Access Layer to the Distribution/Core Layer 32

Operations and Server Room 39
- Business Overview 39
- Technical Overview 39
- Deployment Details 41
  - Configuring the Server Room 41
  - Connecting the Server Room to the Distribution/Core Layer 46

Appendix A: Product List 50

Appendix B: Configuration Files 53
- Distribution/Core-Layer Configurations 53
- Access Layer Configurations 64
- Server Room Configuration 77

What's In This SBA Guide

Cisco SBA Solutions

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

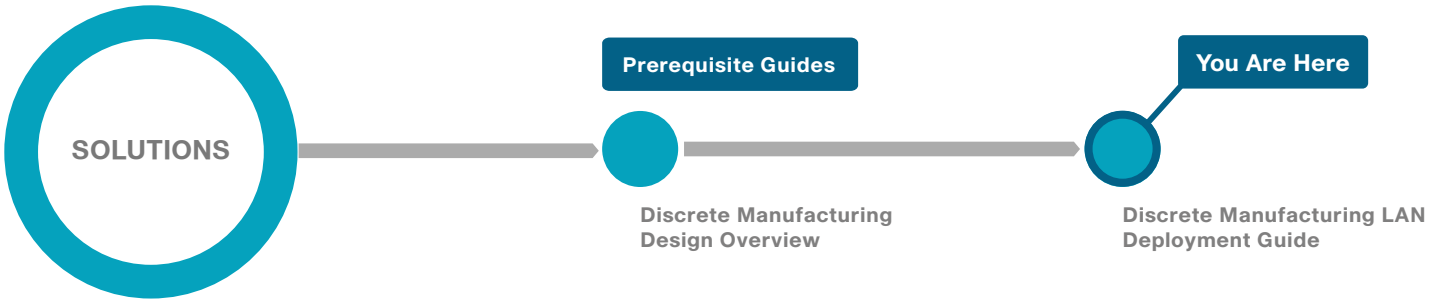
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

The *Cisco SBA—Solutions Discrete Manufacturing LAN Deployment Guide* describes how to deploy wired network access that scales from small environments with one to a few LAN switches to a large LAN. Resiliency, high availability, segmentation, security, and scalability are included in order to provide a robust communications environment. Quality of service (QoS) and multicast management are integrated in order to ensure that the base architecture can support a multitude of applications, including latency- and jitter-sensitive industrial automation and control system (IACS) applications that coexist with enterprise data applications on a single network.

The Cisco Smart Business Architecture (SBA) discrete manufacturing LAN architecture is designed for connectivity requirements that range from a small plant to up to 2,500 connected devices at a single plant location.

Cisco SBA—Solutions Discrete Manufacturing networks is a solid network foundation designed to provide networks with up to 2,500 connected devices the flexibility to support new devices or network services without re-engineering the network. This is a prescriptive, out-of-the-box deployment guide that is based on best-practice design principles and that delivers resiliency, security, flexibility, and scalability.

Related Reading

The *Discrete Manufacturing Design Overview* orients you to the overall Cisco SBA design and explains the requirements that were considered when selecting specific products.

The *Discrete Manufacturing Security Deployment Guide* focuses on deploying firewall, intrusion prevention system, and VPN services in the DMZ, between the enterprise and industrial Ethernet networks.

Design Goals

This architecture is based on requirements gathered from customers, partners, and Cisco field personnel for organizations with up to 2,500 connected manufacturing devices. Based on this input, the Cisco SBA discrete manufacturing design focuses on ease of deployment and scalability as the primary requirements of a manufacturing organization.

Because plant facilities range in size and organizations may have multiple plants of varying sizes, and because IT expertise may be limited in a manufacturing environment, ease of deployment is considered to be a critical network requirement. This architecture uses a small number of standard designs for common portions of the network. This allows the support staff to more effectively design services for the network and then to implement and support the network. The modular design not only simplifies deployment, but it enhances scalability by providing a set of standard, global building blocks that can be assembled in order to meet your organization's requirements.

Many of the design's plug-in modules look identical for several service areas, allowing you to use the same support methods for multiple areas of network, providing additional consistency and scalability. To ensure that interfaces between the plug-ins are well defined, the plug-in modules use the standard hierarchical design model that is composed of core, distribution, and access layers. This allows for easy replication and enhanced scalability.

Discrete Manufacturing LAN Overview

Industrial automation and control system (IACS) is a term that describes the automation and control applications typically found on the plant floor. IACSs perform the automated tasks and processes that make up the production environment, and they consist of devices such as programmable automation controllers, human machine interfaces, drives, motors, sensors, actuators, and I/O units. An IACS would typically include the network infrastructure that connects the other IACS devices. For more on IACSs, see the *Cisco SBA—Solutions Discrete Manufacturing Design Overview*.

The purpose of the architecture and the network services used in this guide is to provide a single, reliable industrial Ethernet network infrastructure that enables easy communication and access to IACSs, their devices, and the critical information that flows between them.

Architecture Overview

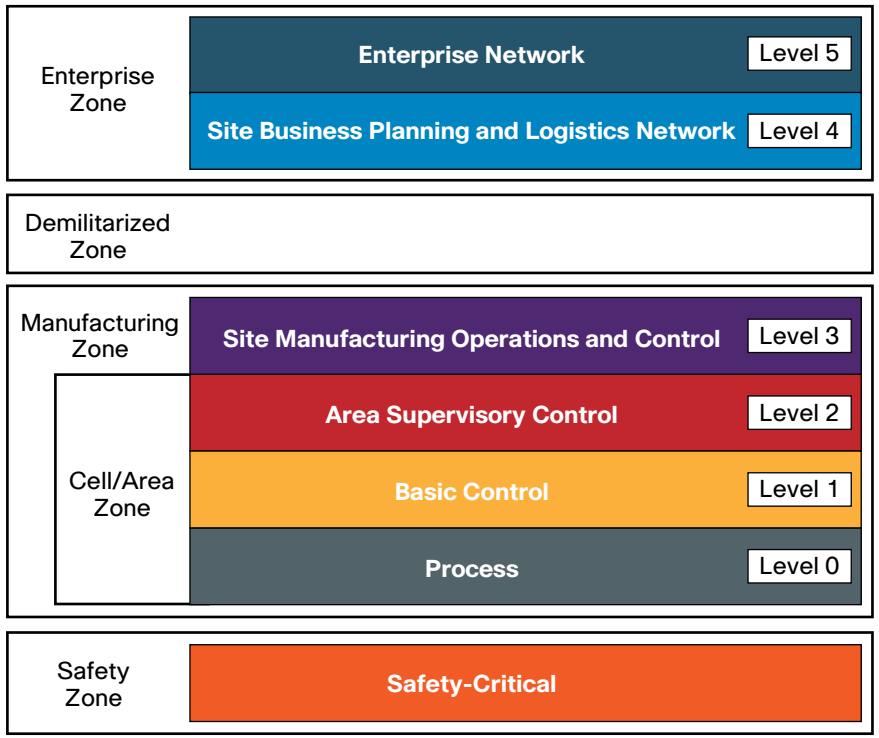
The discrete manufacturing LAN design model combines the zones of the converged industrial Ethernet network architecture with the layers of the Cisco SBA LAN hierarchical design model in order to meet the design goals of a highly scalable, resilient, secure, and easy-to-deploy standard industrial Ethernet network.

Converged Industrial Ethernet Network Architecture

A converged industrial Ethernet network consolidates all device and control management functions into a single, standards-based infrastructure that is converged with the enterprise network through a demilitarized zone (DMZ). The converged industrial Ethernet network is divided into the following functional zones and their levels of operations:

- Enterprise zone—Is analogous to the Cisco SBA enterprise network. Although important, these services may not be viewed as critical to the industrial Ethernet network or the plant-floor operations. This level is typically under the management and control of the IT department.
- Demilitarized zone—Consists of firewalls that ensure separation between the Manufacturing zone and the Enterprise zone. This separation protects the real-time availability and security of the industrial Ethernet network. For more information about the Demilitarized zone and security, see the *Discrete Manufacturing Security Deployment Guide*.
- Manufacturing zone—Contains the Cell/Area zones and site's manufacturing operation and control equipment. All of the IACS applications, devices, and controllers critical to monitoring and controlling the plant-floor IACS operations are in this zone, and it is the highest level of the industrial Ethernet network.

Figure 1 - Zones and levels of operation



- **Cell/Area zone**—Is a functional area within the plant facility. It may be as small as a single controller and its associated devices on a process skid, or it may be multiple controllers on an assembly line. Each plant facility defines the Cell/Area zone demarcation differently, but most plants have multiple Cell/Area zones.
- **Safety zone**—Consists of the safety systems that provide predictable, fail-safe shutdown of IACS applications in order to protect personnel, the environment, and the applications themselves.

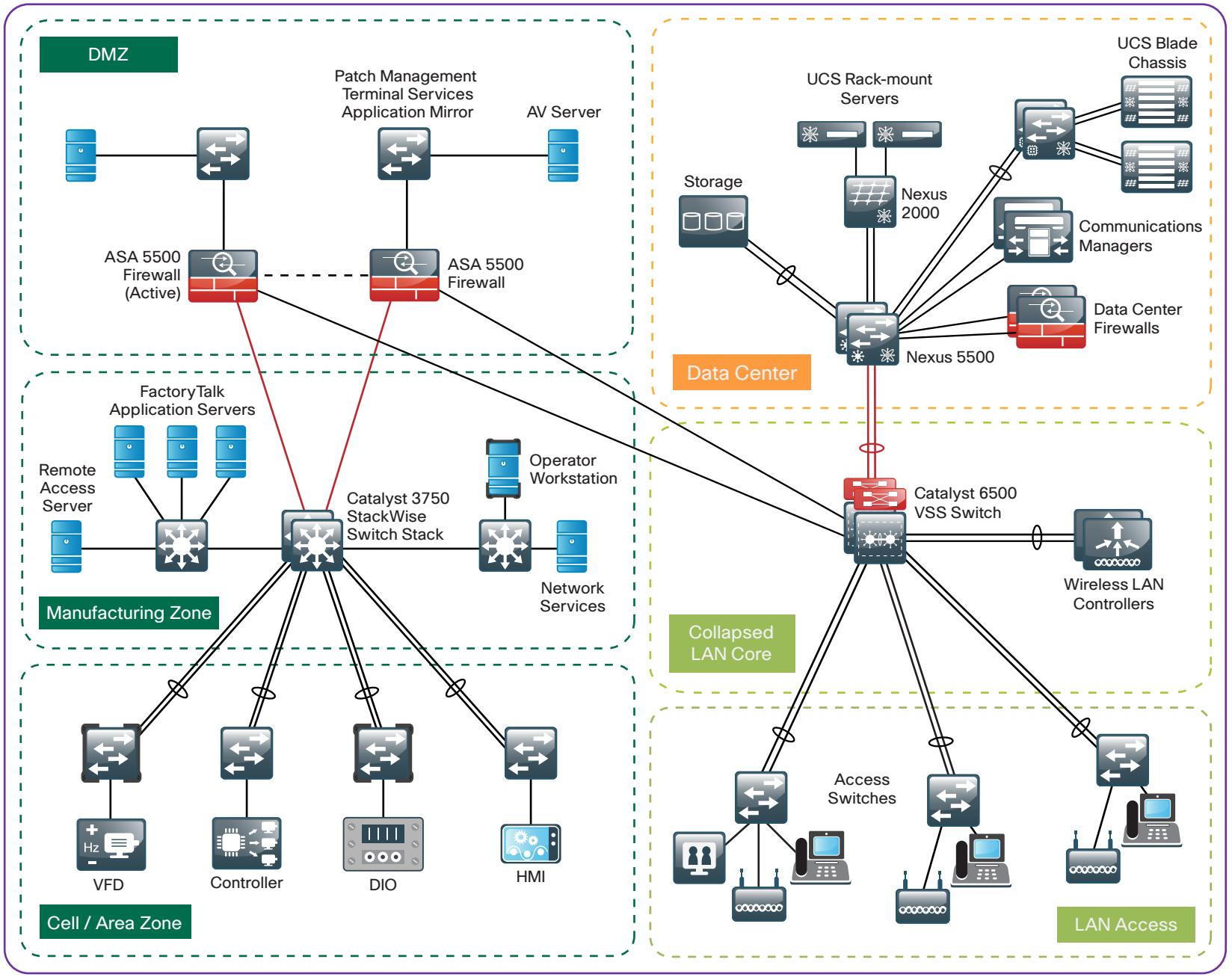
Reader Tip

For more detailed information about the architecture of a converged industrial Ethernet network and its design considerations, please refer to the *Discrete Manufacturing Design Overview*.

Notes

The following figure shows the architecture of a converged industrial Ethernet network and the relationship between the zones and the enterprise network.

Figure 2 - Converged industrial Ethernet network architecture



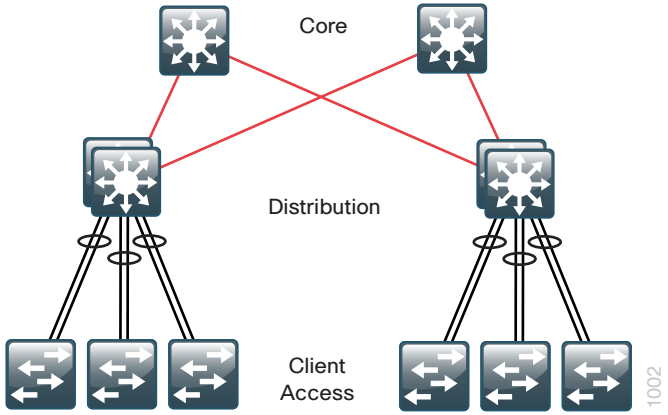
Hierarchical LAN Design Model

Cisco SBA uses a hierarchical design model to divide the design into modular groups, or *layers*. Breaking the design up into layers allows each layer to focus on specific functions, which simplifies the design, provides simplified deployment and management, and enhances scalability.

The hierarchical design model includes the following three layers:

- Access layer—Provides workgroup or 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 3 - Cisco SBA LAN hierarchical design model

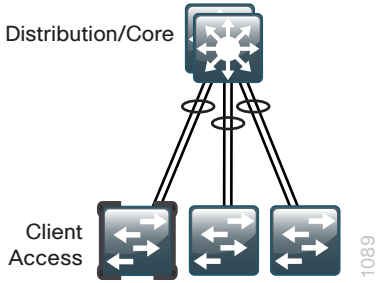


Reader Tip

For more information about the Cisco SBA hierarchical design model, see the "Architecture Overview" chapter of the *Cisco SBA—Borderless Networks LAN Deployment Guide*.

In the discrete manufacturing LAN design model, the distribution layer and the core layer are combined into one layer, called the *distribution/core layer*. This layer consists of the Manufacturing zone operations, and it provides interconnectivity between the systems in in the Manufacturing zone and between the Cell/Area zones, and it also provides access to the DMZ.

Figure 4 - Combined distribution/core layer model



In the discrete manufacturing design model, the *access layer* consists of the Cell/Area zone operations, and this is where all the IACS devices are connected. This layer carries most of the critical IACS traffic, and most of that traffic does not even leave the Cell/Area zone in which it originates.

Network Services

This section describes the key services the network provides for proper functioning of the systems and applications that rely upon it.

Redundant Star Topology

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

Reader Tip

For more information about the redundant star topology and its recommended resiliency protocols, see the *Discrete Manufacturing Design Overview*.

Protocols

The following protocols are used throughout the LAN deployment process:

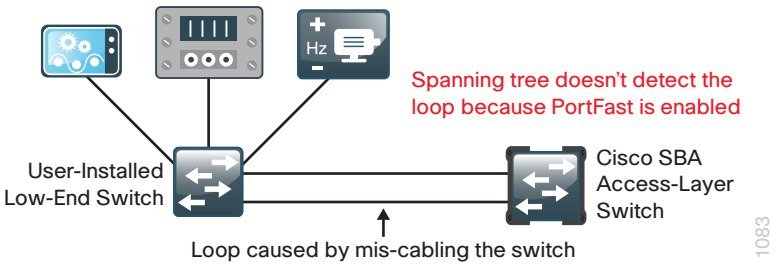
- Link Aggregation Control Protocol (LACP)—Performs consistency checks for interfaces programmed to be in the channel, and it provides protection to the system from inconsistent configurations. This design model uses LACP because it is the only EtherChannel protocol that can be used in all configurations in this design.
- 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. This deployment uses VTP transparent mode because the benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error.
- Rapid Per VLAN Spanning Tree Plus (RPVST+)—Provides an instance of RSTP (802.1w) per VLAN. It greatly improves the detection of indirect failures or linkup restoration events over classic Spanning Tree Protocol (802.1D). Although this architecture is built without any Layer 2 loops, you must still enable RPVST+ in order to ensure that if any physical or logical loops are accidentally configured, no actual Layer 2 loops occur.
- Unidirectional Link Detection Protocol (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-optic cables, which can be susceptible to unidirectional failures.
- 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 LAN devices. Both protocols are encrypted for privacy, and the nonsecure protocols, Telnet and HTTP, are turned off.
- Simple Network Management Protocol (SNMP)—Is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite.
- Enhanced Interior Gateway Routing Protocol (EIGRP)—Is the IP unicast routing protocol used in this design because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks.
- Dynamic Host Configuration Protocol (DHCP)—Enables communication between network devices on an IP network. *DHCP snooping* is a feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. In this design, DHCP snooping is enabled on the access-layer port interfaces that are connected to IP phones and workstations.
- Network Time Protocol (NTP)—Synchronizes timekeeping among a set of distributed time servers and clients. A local NTP server typically references a more accurate clock feed.
- TACACS+—Authenticates management logins to infrastructure devices against an authentication, authorization, and accounting (AAA) server. Use of this protocol and AAA services is optional in this deployment.

BPDU Guard

The PortFast Bridge Protocol Data Unit (BPDU) guard feature is a Spanning Tree Protocol enhancement that improves switch network reliability, manageability, and security. BPDU guard protects against a user plugging a switch into an access port or into a PortFast-enabled interface, which could cause a catastrophic undetected spanning-tree loop.

If a PortFast-enabled 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 PortFast-enabled interface receives a BPDU.

Figure 5 - Scenario that BPDU guard protects against



Segmentation

Each Cell/Area zone should be a subnet with a defined VLAN. Careful consideration should be given when designing an industrial Ethernet network, identifying which IACS devices belong to which Cell/Area zone, and minimizing the size of the Cell/Area zone. When segmenting Cell/Area zones for your organization, follow the guidance in the *Discrete Manufacturing Design Overview*.

Prioritization and QoS

Quality of service (QoS) refers to network control mechanisms that can provide various priorities to network traffic or data flows. In a converged industrial Ethernet network, it is important that the network assign priority to the IACS traffic in order to deliver improved performance for these applications.

QoS can be challenging to configure and maintain, but the template, platform-specific approach in this guide makes it much easier and adds significant value to the overall availability and reliability of the data transmission on the industrial Ethernet network. If changes are made to the QoS settings used in this guide, verify the configuration in a lab in order to ensure it operates as expected prior to deployment in production.

IP Multicast and IGMP

Multicast traffic is an important consideration of a Cell/Area zone because it is used by many of the key IACS communication protocols, and Internet Group Management Protocol (IGMP) is the standard method to manage multicast traffic. IGMP enables the network infrastructure to understand which endpoints are interested in which multicast data, enabling the network infrastructure to forward messages only to those endpoints that want them.

The key multicast management recommendation is to enable the IGMP process in the Cell/Area zone. To enable and configure IGMP, it is recommended that you:

- Configure the IGMP querier on the distribution/core-layer switch and ensure the distribution/core-layer switch has the lowest IP address in the subnet, statically defined.
- Configure Protocol Independent Multicast (PIM) sparse mode on all Layer 3 interfaces. It builds unidirectional shared trees that are rooted at a rendezvous point (RP) per group, and it scales well.
- Configure Layer 3 switches in the distribution/core layer to use Anycast RP, which provides load-sharing and redundancy in PIM sparse mode networks.

IP Addressing

Use of IPv6 is very limited and not widely supported by IACS applications at this time. IPv4 is still the most commonly deployed address space and will remain so for some time inside of industrial Ethernet networks with the use of Network Address Translation (NAT) and newer IPv4-to-IPv6 translation techniques. IPv4 is used in this deployment.

For ease of use and to simplify security policies, it is recommended that in the Manufacturing zone, you use a private contiguous block of addresses that is not in use in the enterprise network.

Reader Tip

For more information on IPv4 and IPv6 addressing design, please refer to the following:

Cisco SBA—Borderless Networks IPv4 Addressing Guide
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_IPv4AddressingGuide-Feb2013.pdf

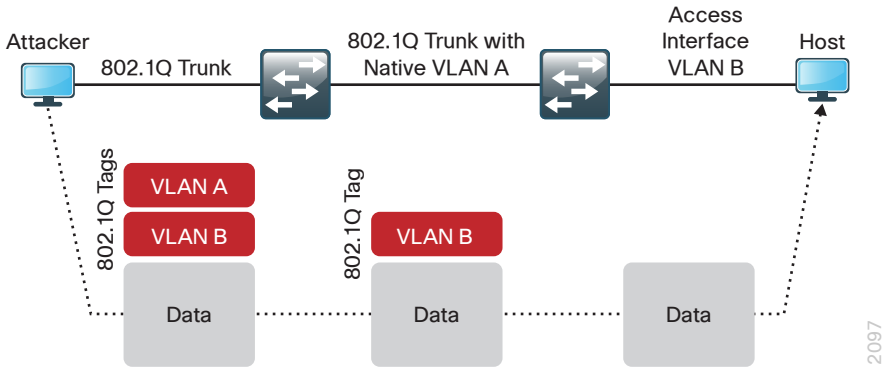
Cisco SBA—Borderless Networks IPv6 Addressing Guide
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_IPv6AddressingGuide-Feb2013.pdf

802.1Q Trunking

An 802.1Q trunk is used for connections to upstream devices, which allows the uplink to provide Layer 3 services to all VLANs on the downstream switch.

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. This attack is known as a *VLAN-hopping attack*.

Figure 6 - 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.

In order to mitigate the remote risk of a VLAN-hopping attack, you configure an unused VLAN on all switch-to-switch 802.1Q trunk links. By using a hard-to-guess, unused VLAN for the native VLAN, you reduce the possibility that a double 802.1Q-encapsulated packet can hop VLANs.

AAA services

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. A local AAA user database is also defined on each network infrastructure device in order to provide a fallback authentication source in case the centralized AAA server is unavailable. This deployment guide provides optional instructions for configuring AAA services for management logins to infrastructure devices.

Reader Tip

The AAA server used in this architecture is Cisco Secure Access Control System (ACS). Configuration of Secure ACS is discussed in the *Device Management Using ACS Deployment Guide*.

Distribution/Core Layer

Business Overview

The challenge for a plant organization is to provide reliable access between the plant operation services (for example, a manufacturing execution system or an asset manager) and the Cell/Area functional zones. As the number of Cell/Area zones at a plant grows, it creates the need to aggregate the connectivity at a common point. One of the benefits of aggregation is that you can reduce costs by reducing the number of interconnections from each Cell/Area access-layer switch to the rest of the network, which is used to get to the applications and resources hosted in the center of the network or across the WAN.

Traditional IACS network design used physical networks that were separate from the enterprise Ethernet network. To reduce costs, organizations must create a single multi-use network infrastructure on a single physical infrastructure per site. The dominant Internetwork protocol in use in networks today is IP, which allows a routed network topology, but some applications require that network-connected endpoints be Layer 2 adjacent. IT must work to design networks that accommodate the IACS application requirements without sacrificing the reliability or scalability of the network. The goal of the network foundation architecture is to provide a design that supports an ever-increasing number of services required from the LAN and to control the increasing complexity of delivering those services, without eliminating essential functionality.

Technology Overview

The distribution/core layer provides interconnectivity between the operations and server-room systems in in the Manufacturing zone and between the Cell/Area zones, and it also provides access to the DMZ. In a typical hierarchical network, the distribution/core layer connects the systems by routing traffic between the various VLANs.

The layer's network infrastructure provides services such as the following:

- Routing based upon a chosen routing protocol
- IGMP querier
- Default gateway
- Root switch (if running Spanning Tree Protocol).

The distribution/core layer also enables scalability. If new lines or zones are added to an industrial Ethernet network, they can be connected to the distribution/core layer without disrupting ongoing operations in the Cell/Area or Manufacturing zones.

The primary function of the distribution/core layer is to aggregate access-layer switches in a given building; additionally in plant designs, the distribution/core layer also connects to the plant-edge DMZ and operations and server-room segments. The distribution/core 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/core layer creates a boundary for Spanning Tree Protocol, limiting propagation of Layer 2 faults. On the Layer 3 side, the distribution/core layer is a logical point to summarize IP routing information before it enters the network and to reduce IP route tables for easier troubleshooting and faster failure recovery.

Distribution/Core Layer Design

The distribution layer design in the Cisco SBA discrete manufacturing design model uses multiple physical switches that act as a single logical switch or a single, highly redundant physical switch. This design minimizes spanning-tree dependence, and all uplinks from the access layer to the distribution/core layer are active and passing traffic. Spanning-tree links that are blocked due to looped topologies are eliminated. You reduce dependence on Spanning Tree Protocol by using EtherChannel to the access layer and using 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.

EtherChannel is a logical interface that can use a control plane protocol in order to manage the physical members of the bundle. It is recommended that you run a channel protocol instead of using forced-on mode. A channel protocol performs consistency checks for interfaces programmed to be in the channel, and it 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 Control Protocol (LACP) based on IEEE 802.3ad. This design uses LACP for EtherChannel because it is the only protocol that can be used in all configurations in this design.

There are several other advantages to the simplified distribution/core layer design. Due to the default IP gateway being located on a logical interface and to the resiliency provided by the distribution/core layer switch, you no longer need IP gateway redundancy protocols such as Hot Standby Router Protocol, Virtual Router Redundancy Protocol, and Gateway Load Balancing Protocol. Also, the network converges faster now that it is not depending on Spanning Tree Protocol in order to unblock links when a failure occurs, because EtherChannel provides fast failover between links in an uplink bundle. Finally, by using the single logical distribution/core layer design, there are fewer boxes to manage, which reduces the amount of time spent on ongoing provisioning and maintenance.

The network design from the distribution layer to the access layer is a redundant star topology design that reduces complexity and troubleshooting. The single, logical designated router forwards IP Multicast packets to a designated VLAN in the access layer, providing more efficient operation for IP Multicast in the distribution/core layer.

Distribution/Core Layer Roles

Much emphasis has been placed on the distribution/core layer as the access-layer aggregation point because this is the most common role. The distribution/core layer serves other roles in the Cisco SBA for discrete manufacturing LAN deployments.

The distribution/core layer in industrial Ethernet environments typically connects to the access layer, server and operations systems, and plant-edge DMZ.

The distribution/core layer provides:

- Communication routing within the Cell/Area and Manufacturing zones.
- Multicast management querier function for Cell/Area zones.
- Modular growth for plant access-layer switches.
- Separated fault domains for the access layer, server room, and plant-edge DMZ.
- IP address summarization for the plant.

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

Distribution/Core Layer Platforms

You can use multiple platforms in order to deploy the simplified distribution/core layer design. Physically, the distribution/core layer can be a highly available Cisco Catalyst 4507R+E switch or a stack of Cisco Catalyst 3750-X Series switches. It is important to note that although each platform has different physical characteristics, each appears to the rest of the network as a single node and provides a fully resilient design.

Cisco Catalyst 4507R+E Switch

Cisco Catalyst 4507R+E switches have redundant supervisors, line cards, and power supplies. In this design, Cisco uses a single Catalyst 4507R+E chassis configured with resilient components as a distribution/core layer platform. Cisco Catalyst 4500 Supervisor Engine 7-E has the ability to provide the access layer a medium density of 1-Gigabit and 10-Gigabit Ethernet EtherChannel uplinks.

The Cisco Catalyst 4507R+E chassis also provides Cisco Stateful Switchover (SSO). SSO is critical to Cisco Nonstop Forwarding, which continues to forward IP packets even in the event of a switchover or failure, and SSO also allows in-service software upgrades for the system. SSO enables a fast, transparent data-plane failover by synchronizing active process information and configuring information between supervisor modules.

Cisco Catalyst 3750-X Series Switch Stack

The Cisco Catalyst 3750-X Series switch stack is configured as a single unit, but it has independent load-sharing power supplies and a processor for each switch in the Cisco StackWise Plus stack. The Cisco SBA discrete manufacturing architecture uses a pair of stacked Cisco Catalyst 3750X-12S-E switches that provide Layer 2 and Layer 3 switching. The following are some of the benefits of using the Cisco Catalyst 3750-X Series switch stack:

- For EtherChannel uplinks to access closets, the switches use Small Form-Factor Pluggable transceivers for a port-by-port option of copper or fiber-optic Gigabit Ethernet.
- Cisco StackWise Plus enables up to nine Cisco Catalyst 3750-X Series switches to be stacked together by using a 64-Gbps stack interconnect, providing subsecond failure recovery.
- Cisco StackPower shares power across the Cisco Catalyst 3750-X Series 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 Catalyst 3750-X Series switches have modular uplinks for connectivity at 1-Gigabit or 10-Gigabit Ethernet speeds, and they support upgrading the Cisco IOS feature set.

Deployment Details

The single, logical, resilient, distribution/core-layer design simplifies the distribution/core-layer switch configuration.

Process

Configuring the Distribution/Core Layer

1. Configure the distribution/core platform
2. Configure switch universal settings
3. Configure switch global settings
4. Configure IP unicast routing
5. Configure IP Multicast routing
6. Configure the IP Multicast RP

Procedure 1 Configure the distribution/core platform

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you are using a Cisco Catalyst 4507R+E chassis for the platform, complete Option 1. If you are using a Cisco Catalyst 3750-X Series switch stack for the platform, complete Option 2.

Option 1. Using a Cisco Catalyst 4507R+E switch

Step 1: Create class maps that differentiate the various types of manufacturing and voice traffic.

```
class-map match-any CONTROL-MGMT-QUEUE
  match cos  3
class-map match-any SCAVENGER-QUEUE
  match cos  1
class-map match-any CIP-PTP-General
  match cos  5  6
class-map match-any PRIORITY-QUEUE
  match cos  7
```

Step 2: Configure QoS parameters and policy maps that define how traffic is prioritized as it passes through the network.

```
policy-map 1P5Q1T
  class PRIORITY-QUEUE
    priority
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 40
  class CIP-PTP-General
    bandwidth remaining percent 40
  class SCAVENGER-QUEUE
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 18
    dbl
!
policy-map 1P5Q1T-PC
  class PRIORITY-QUEUE
    police cir 200000000 conform-action transmit exceed-action
drop
```

Tech Tip

When the **police cir** [rate in bps] command is used on port channels, the rate must be calculated based on the speed of the link being used. For example, on a port channel consisting of four 1-Gbps links on which you wanted to police traffic to 10% of the aggregate bandwidth, you take the total bandwidth, 4 Gbps or 4,000,000,000 bps, multiply by 10%, or 0.1, and get the rate 400,000,000 bps.

Step 3: Configure the macros that apply the QoS parameters, as defined by the class maps and policy maps, to the port-channel interfaces.

```
macro name CiscoIEEgress
 service-policy output 1P5Q1T
@
macro name CiscoIEEgress-PC
 service-policy output 1P5Q1T-PC
@
```

Step 4: If you have two Cisco Catalyst 4500 Supervisor Engine 7-Es and if the license level for the switch supervisors is ipbase or entservices, configure the switch to use Cisco Stateful Switchover (SSO) when moving the primary supervisor functionality between modules.

```
redundancy
  mode sso
```

Tech Tip

You can check the current license level of operation with the **show version** command.

Option 2. Using a Cisco Catalyst 3750-X Series switch stack

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*. If three or more switches are configured as the stack, configure the stack-master switch functionality on a switch that does not have uplinks configured.

By default, the 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. This configuration preserves the original stack-master MAC address in order prevent convergence issues.

If you are using a Cisco Catalyst 3750-X Series switch stack, a single reboot is required in order to force the stack master to operate on the switch that you configured with the highest priority. Reboot the switch stack after all of the distribution/core-layer switch configuration is complete.

Step 1: Assign a stack-master switch.

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

Step 2: Ensure that the original master MAC address remains the stack MAC address after a failure.

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

Step 3: Configure QoS parameters that define how traffic is prioritized as it passes through the network.

```
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4
5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34
35 36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42
44 45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54
56 57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31
43 46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30
32 33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39
40 41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51
52 53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61
62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47
48 55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos
```

Step 4: Create a macro that applies the platform-specific QoS configuration. This macro is used in later procedures and eases consistent deployment of QoS.

```
macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
```

Procedure 2 Configure 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 system settings simplify and secure the management of the industrial Ethernet network.

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

Table 1 - Common network services used in the deployment examples

Network parameter	Cisco SBA value
Domain name	cisco.local
Active Directory, DNS, DHCP server	10.13.48.10
Cisco Secure ACS	10.13.48.15
Network Time Protocol server	10.13.48.17
EIGRP Autonomous System	101
Multicast range	239.1.0.0/16

In this procedure, you configure a local login account and password that provide basic device access authentication in order 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. By default, HTTPS access to the switch uses the enable password for authentication.

Reader Tip

For more information about the protocols used in this procedure, see the "Protocols" section of the "Discrete Manufacturing LAN Overview" chapter.

Step 1: On the distribution/core layer switch, configure the device hostname. This makes it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure VTP transparent mode.

```
vtp mode transparent
```

Step 3: Enable RPVST+.

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

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

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

Step 5: Enable UDLD.

```
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.

```
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 10.13.48.10
```

Step 8: Configure HTTPS and SSH device management protocols, and then specify the **transport preferred none** command on vty lines.

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

Tech Tip

The **transport preferred none** command prevents errant connection attempts from the CLI prompt, and without it, long timeout delays may occur for mistyped commands if the IP name server is unreachable.

Step 9: Enable SNMP in order to allow the network infrastructure devices to be managed by a Network Management System, 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 and you want to increase network security, use an access list to limit the networks that can access your device. In this example, only devices on the 10.13.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.13.48.0 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 router to the next, for hop-by-hop troubleshooting.

Step 11: Configure a local login and password.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 12: If you want to use AAA services for centralized user authentication, use TACACS+ protocol in order to authenticate management logins to infrastructure devices.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.13.48.15
  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: Program network devices to synchronize to a local NTP server in the network, and then configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```
ntp server 10.13.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Tech Tip

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 switch global settings

Step 1: On the distribution/core-layer switch, configure Bridge Protocol Data Unit (BPDU) guard globally. This protects PortFast-enabled interfaces.

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

Reader Tip

For more information about BPDU guard, see the "BPDU Guard" section of the "Discrete Manufacturing LAN Overview" chapter.

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 in order 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/core-layer switch summarizes to the rest of the network.

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

Step 3: Configure the SNMP,SSH, TACACS, and PIM processes to use the loopback interface address.

```
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
```

Step 4: Save the running configuration that you have entered as the startup configuration file. When the distribution/core-layer switch is reloaded or power-cycled, this configuration is used.

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

Step 5: If the distribution/core-layer switch is a Cisco Catalyst 3750-X Series switch stack, reload your switch stack. This ensures that EtherChannel operates with other features configured on the switch stack and that the switch with the highest priority becomes the master of the stack.

```
reload
```

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/core layer design uses Cisco Stateful Switchover and Cisco Nonstop Forwarding in order to provide subsecond failover in the event of a supervisor data or control-plane failure. This feature reduces packet loss during a control plane switchover and keeps packets flowing when the data plane is still intact to adjacent nodes. In the stack-based distribution/core 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/core 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 to avoid the peer router from tearing down adjacencies due to missed hellos, which would cause a reroute and traffic disruption. To allow this time for the supervisor to recover, the routing protocol's Cisco Nonstop Forwarding (NSF) setting waits for the dual-supervisor peer switch to recover. The neighboring router is *NSF-aware* if it has a newer release of Cisco 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/core layer switch must be configured to enable Cisco NSF for the protocol in use. In the event of a switchover to a hot-standby supervisor, NSF signals a peer to allow the supervisor time to reestablish the EIGRP protocol to that node. You do not need to tune the default NSF timers in this network, and no additional configuration is required in order to set up the NSF-aware function for the peer router.

Step 1: On the distribution/core-layer switch, 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.

```
ip routing
!
router eigrp 101
  network 10.13.0.0 0.0.255.255
  no auto-summary
  passive-interface default
  eigrp router-id [ip address of loopback 0]
  nsf
```

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

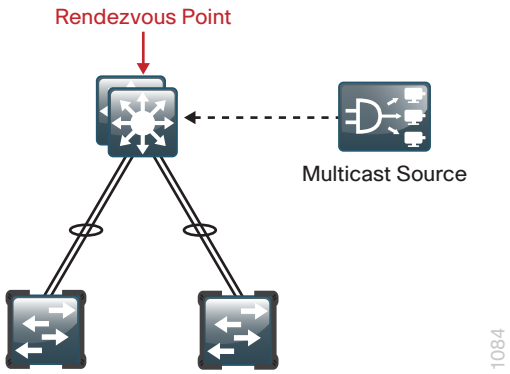
IP Multicast allows a single IP data stream to be replicated by the infrastructure (that is, routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple, individual unicast streams or a broadcast stream that would propagate everywhere, and IP Multicast is essential to the operation of many industrial Ethernet network protocols.

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/core layer if the access layer is Layer 2 and provides connectivity to the IP Multicast RP.

Every Layer 3 switch and router must be configured to discover the IP Multicast RP by using AutoRP. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

Figure 7 - Rendezvous point placement in the network



In this design, which is based on sparse-mode Multicast operation, Cisco uses Anycast RP to provide a simple yet scalable way to provide a highly resilient RP environment.

Step 1: If you are using a Cisco Catalyst 4507R+E chassis, on the platform, in global configuration mode, configure IP Multicast routing.

```
ip multicast-routing
```

If you are using a Cisco Catalyst 3750-X Series switch stack, on the platform, in global configuration mode, configure IP Multicast routing.

```
ip multicast-routing distributed
```

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

```
ip pim autorp listener
```

Step 3: Configure sparse-mode IP Multicast operation for all Layer 3 interfaces in the network.

```
ip pim sparse-mode
```

Example

```
spanning-tree portfast bpduguard default
!
interface Loopback 0
  ip address 10.13.15.254 255.255.255.255
  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 101
  network 10.13.0.0 0.0.255.255
  no auto-summary
  passive-interface default
  eigrp router-id 10.13.15.254
  nsf
!
ip multicast-routing
ip pim autorp listener
!
```

Procedure 6 Configure the IP Multicast RP

Every Layer 3 switch and router must know the address of the IP Multicast RP, including the distribution/core layer switches that are serving as the RP. This design uses AutoRP to announce candidate RPs, which are the distribution/core layer switches, to the rest of the network. The *AutoRP-mapping agent* listens for candidate RPs and then advertises the list of available RPs to the rest of the network.

Step 1: On the distribution/core-layer switch, 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 10.13.15.253 255.255.255.255
 ip pim sparse-mode
```

Step 2: Configure the AutoRP candidate RP by issuing the **send-rp-announce** command in conjunction with the **group-list** option. This advertises the RP address, with the IP 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 3: Configure the AutoRP-mapping agent by issuing the **send-rp-discovery** command. This enables this switch to act as an AutoRP-mapping agent.

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

Notes

Access Layer

Business Overview

To conduct business in today's competitive global economy, organizations rely on the flow of information. They must provide a dispersed workforce with access to applications and communication tools that support the manufacturing business and operations among internal and external associates.

Traditional IACS networks do not support the flexibility that organizations need in order to control IT expenses and streamline operations. Traditional, proprietary systems create multiple networks in the same space. These networks have separate power, cabling, and communication requirements, and they have multiple sets of spares, skill requirements, and support programs. Most importantly, IACS networks segregate the critical Cell/Area zones and IACS systems, making them hard to reach and difficult to get information from.

The ability to move information around the organization is critical; no longer will siloed IACS networks suffice. By ensuring that users, regardless of their location, have the ability to access this information or push communications by using an increasingly diverse set of communications devices, the organization is able to help the workforce become more productive. This ability increases original equipment effectiveness (OEE), reduces downtime in the plant, and reduces the cost of deployment and operations. The security, speed, reliability, and availability of the transport are critical to success.

IACS devices are precise, and meeting the timing requirements, including latency and jitter sensitivity, is essential to ensuring that plant floor operations run smoothly and efficiently. In the industrial Ethernet network, 80–90% of the Cell/Area zone traffic is local and occurs between IACS devices. Because this communication occurs in the access layer, it is critical that the network and physical infrastructure of the access layer are highly available and resilient, and the IACS traffic must be prioritized appropriately in order to prevent costly delay or outages.

Technology Overview

The access layer is composed of the Cell/Area zones, and this is where all the IACS devices are connected. This layer carries most of the critical IACS traffic. Although the traffic may not leave the Cell/Area zone or VLAN, because a Cell/Area zone may span several access-layer switches, the distribution/core layer switch plays critical roles, such as acting as IGMP querier and default gateway and providing interconnectivity between the VLANs.

This chapter focuses on the configuration of the access-layer switches, those with end-devices connected to them and with uplinks that carry traffic to other parts of the network.

The Cell/Area zone access-layer switches are the ingress and egress points for the IACS traffic. The access-layer switches provide:

- Resilient interconnectivity to the rest of the industrial Ethernet network.
- Security for end-devices by assigning them to a VLAN.
- Management of Multicast traffic by passing it to subscribing end-devices.
- Monitoring and prevention of inadvertent loops that would impact network services.
- Protection from broadcast storms and other forms of unwanted traffic.
- Quality of service (QoS) that gives priority to critical IACS traffic throughout its journey in the industrial Ethernet network.

The Cell/Area zone access layer is the point at which IACS devices are connected to the network, and it is one architecture component that is found in every industrial Ethernet LAN.

Deployment Method

To provide consistent access capabilities and simplify network deployment and operation, the design uses a common deployment method for all access-layer devices. To reduce complexity, the access layer is designed so that you can use a single interface configuration for an IACS device, standalone computer, an IP phone, or a wireless access point.

The LAN access layer provides high-speed connections to devices via 10/100/1000 Ethernet with both 1-Gigabit and 10-Gigabit uplink connectivity options. The 10-Gigabit uplinks also support 1-Gigabit connectivity in order to provide flexibility and help business continuity during the transition to 10-Gigabit Ethernet. The LAN access layer is configured as a Layer 2 switch, with all Layer 3 services being provided by the directly connected distribution/core layer.

Wiring Closet Equipment

Wiring closet components can vary depending on the manufacturing environment and IACS requirements. Use the following information to select equipment that is appropriate for your organization.

For Harsh Environments

Cisco Industrial Ethernet (IE) 2000 and 3000 Series switches allow for a variety of interfaces and configurations, are extendable from 4-port to 24-port combinations, and offer a variety of 10/100/1000 Ethernet copper and fiber-optic options. The Cisco IE 2000 and 3000 Series switches feature a design with extended environmental ratings, convection cooling, DIN-rail mounting, redundant 24VDC power input, alarm relays, and surge and noise immunity.

Up to 48 Ports

Cisco Catalyst 2960-S and 3560-X Series switches 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 Series switches are available in both Power over Ethernet Plus (PoE+) and non-powered versions.

In addition to the capabilities supported by Cisco Catalyst 2960-S Series switches, Cisco Catalyst 3560-X Series switches support modular uplinks, an upgradable Cisco IOS feature set, and enhanced capabilities such as Cisco TrustSec and medianet, but it does not support stacking.

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.

Cisco Catalyst 2960-S or 3750-X Series switches are used in this design when intelligent stacking or a modular deployment is required.

Cisco Catalyst 2960-S Series are fixed-configuration, stackable, 10/10/1000 Ethernet switches, with PoE+ and non-powered 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 a recovery time between 1–2 seconds.

Cisco Catalyst 3750-X Series are fixed-port, stackable, 10/100/1000 Ethernet switches, with PoE+ and non-powered versions, and they provide enhanced resiliency through the following technologies:

- **Cisco StackWise Plus**—Enables up to nine Cisco Catalyst 3750-X Series switches to be stacked together by using a 64-Gbps stack interconnect, providing near subsecond failure recovery.
- **Cisco StackPower**—Shares power across the Cisco Catalyst 3750-X Series 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 Catalyst 3750-X Series switches have modular uplinks, support upgrading the Cisco IOS feature set, and provide enhanced capabilities such as Cisco TrustSec and medianet. These features ensure that the switch functionality grows as the organization grows.

Deployment Details

As you review the *Discrete Manufacturing LAN Deployment 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. For ease of reference, this design uses VLAN assignments that reflect the third octet of the IP address range for a given access-layer switch.

Table 2 - VLANs and IP address assignments for a single distribution block

VLAN	IP addressing	Cell/Area zone	Usage
100	10.13.0.x/24	1	IACS devices
101	10.13.1.x/24	1	Workstations
102	10.13.2.x/24	1	Voice
103	10.13.3.x/24	2	IACS devices
104	10.13.4.x/24	2	Workstations
105	10.13.5.x/24	2	Voice
106	10.13.6.x/24	3	IACS devices
107	10.13.7.x/24	3	Workstations
108	10.13.8.x/24	3	Voice
Continue through 114	10.13.9-114.x/24	—	—
115	10.13.15.x/25	—	Management

Process

Configuring the Access Layer

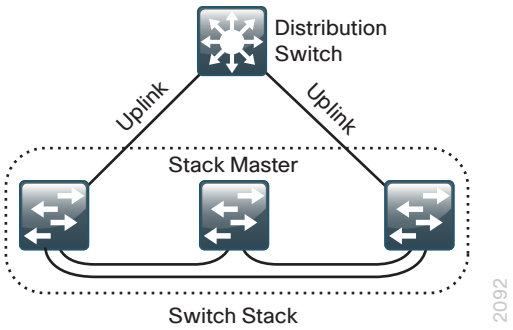
1. Configure the access-layer platform
2. Configure switch universal settings
3. Configure switch global settings
4. Configure IACS interface
5. Configure workstation and voice interface

Procedure 1 Configure the access-layer platform

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you are using a Cisco Catalyst 3560-X or 3750-X Series switch or if you are using a Cisco Industrial Ethernet 2000 or 3000 Series switch, complete Option 1 of this procedure. If you are using a Cisco Catalyst 2960-S switch, complete Option 2.

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*. If three or more switches are configured as the stack, configure the stack-master switch functionality on a switch that does not have uplinks configured.

Figure 8 - Stack master placement in a switch stack



By default, the 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. This configuration preserves the original stack-master MAC address in order prevent convergence issues.

At the end of the "Configuring Access-Layer Switch Services" process, a single reboot of the switch stack is required in order to force the stack master to operate on the switch that you configured with the highest priority.

Option 1. Using a Cisco Catalyst 3560-X or 3750-X Series switch or using a Cisco IE 2000 or 3000 Series switch

Step 1: If you are using the Cisco Catalyst 3750-X Series switch stack, set the stack master switch.

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

If you are not using the Cisco Catalyst 3750-X Series switch, proceed to Step 3.

Step 2: If you are using the Cisco Catalyst 3750-X Series switch stack, ensure that the original master MAC address remains the stack MAC address after a failure.

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

Step 3: Create access lists and class maps that differentiate the various types of manufacturing and voice traffic.

```
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any

ip access-list extended default-data-acl
 permit ip any any

class-map match-all CIP-Implicit_dscp_55
 match access-group 101
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_43
 match access-group 103
class-map match-all CIP-Implicit_dscp_any
 match access-group 104
class-map match-all CIP-Other
 match access-group 105
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all 1588-PTP-General
  match access-group 107

class-map match-all voip-data
  match ip dscp ef
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all voip-control
  match ip dscp cs3
```

Step 4: Configure QoS parameters and policy maps that define how traffic is prioritized as it passes through the network.

```
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
```

```
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4
5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34
35 36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42
44 45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54
56 57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31
43 46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30
32 33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39
40 41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51
52 53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61
62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47
48 55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos

policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
  set ip dscp 55
  class CIP-Implicit_dscp_47
  set ip dscp 47
  class CIP-Implicit_dscp_43
  set ip dscp 43
  class CIP-Implicit_dscp_any
  set ip dscp 31
  class CIP-Other
   set ip dscp 27
  class 1588-PTP-Event
   set ip dscp 59
  class 1588-PTP-General
   set ip dscp 47

policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
```

Step 5: Configure three macros that will be applied to different kinds of access ports. These macros are used in later procedures and ease consistent deployment of QoS.

```
macro name CiscoIEPhone
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 service-policy input Voice-Map
@

macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@

macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
```

Option 2. Using a Cisco Catalyst 2960-S Series switch or switch stack

Step 1: Set the stack master switch.

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

Step 2: Ensure that the original master MAC address remains the stack MAC address after a failure.

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

Step 3: Create access lists and class maps that differentiate the various types of manufacturing and voice traffic.

```
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any

ip access-list extended default-data-acl
 permit ip any any

class-map match-all CIP-Implicit_dscp_55
 match access-group 101
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_43
 match access-group 103
class-map match-all CIP-Implicit_dscp_any
 match access-group 104
class-map match-all CIP-Other
 match access-group 105
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all 1588-PTP-General
  match access-group 107

class-map match-all voip-data
  match ip dscp ef
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all voip-control
  match ip dscp cs3
```

Step 4: Configure QoS parameters and policy maps that define how traffic is prioritized as it passes through the network.

```
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
```

```
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30
32 33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39
40 41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51
52 53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61
62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47
48 55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos

policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
  set ip dscp 55
  class CIP-Implicit_dscp_47
  set ip dscp 47
  class CIP-Implicit_dscp_43
  set ip dscp 43
  class CIP-Implicit_dscp_any
  set ip dscp 31
  class CIP-Other
   set ip dscp 27
  class 1588-PTP-Event
   set ip dscp 59
  class 1588-PTP-General
   set ip dscp 47

policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
```

Step 5: Configure three macros that will be applied to different kinds of access ports. These macros are used in later procedures and ease consistent deployment of QoS.

```
macro name CiscoIEPhone
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 service-policy input Voice-Map
@

macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@

macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
```

Procedure 2 Configure 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 depend on your current network configuration.

Table 3 - Common network services used in the deployment examples

Network parameter	Cisco SBA value
Domain name	cisco.local
Active Directory, DNS, DHCP server	10.13.48.10
Cisco Secure ACS	10.13.48.15
NTP server	10.13.48.17

In this procedure, you configure a local login account and password that provide basic device access authentication in order 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. By default, HTTPS access to the switch uses the enable password for authentication.

Reader Tip

For more information about the protocols used in this procedure, see the "Protocols" section of the "Discrete Manufacturing LAN Overview" chapter.

Step 1: On the access-layer switch, configure the device hostname. This makes it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure VTP transparent mode.

```
vtp mode transparent
```

Step 3: Enable RPVST+.

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

Step 4: Enable Unidirectional Link Detection (UDLD).

```
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.

```
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 10.13.48.10
```

Step 7: Configure HTTPS and SSH device management protocols, and then specify the **transport preferred none** command on vty lines.

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

Tech Tip

The **transport preferred none** command prevents errant connection attempts from the CLI prompt, and without it, long timeout delays may occur for mistyped commands if the IP name server is unreachable.

Step 8: Enable SNMP in order to allow the network infrastructure devices to be managed by a Network Management System, 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 and you want to increase network security, use an access list to limit the networks that can access your device. In this example, only devices on the 10.13.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.13.48.0 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 router to the next, for hop-by-hop troubleshooting.

Step 10: Configure a local login and password.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 11: If you want to use AAA services for centralized user authentication, use TACACS+ protocol in order to authenticate management logins to infrastructure devices.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.13.48.15
  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: Program network devices to synchronize to a local NTP server in the network, and then configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```
ntp server 10.13.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 3 Configure switch global settings

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

- The IACS VLAN provides network connectivity for industrial automation devices such as the following: programmable automation controllers (PAC), variable frequency drives (VFD), human machine interfaces (HMI), and distributed input/output (DIO) devices.
- The workstation VLAN enables network access for PCs on the factory floor.
- The voice VLAN provides network access for IP phones.
- The management VLAN provides in-band network access for the switch's management interface.

In a Cell/Area zone, IACS devices, workstations, and IP phones should not share the same VLAN. User-facing interfaces are configured with both the workstation VLAN and the voice VLAN. The management VLAN is not configured on any user-facing interface, and the VLAN interface of the switch is the only member.

Step 1: On the access-layer switch, configure the IACS, workstation, voice, and management VLANs.

```
vlan [IACS vlan]
  name CZ1-IACS
vlan [Workstation vlan]
  name CZ1-Workstation
vlan [Voice vlan]
  name CZ1-Voice
vlan [Management vlan]
  name Management
```

Step 2: Configure an IP address for the switch. This allows management via in-band connectivity.

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

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

```
ip dhcp snooping vlan [Workstation vlan],[Voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

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

```
ip arp inspection vlan [Workstation vlan],[Voice vlan]
```

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

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

Reader Tip

For more information about BPDU guard, see the "BPDU Guard" section of the "Discrete Manufacturing LAN Overview" chapter.

Example

```
vlan 100
  name CZ1-IACS
vlan 101
  name CZ1-Workstation
vlan 102
  name CZ1-Voice
vlan 115
  name Management
!
interface Vlan 115
  description In-band Management
  ip address 10.13.15.5 255.255.255.128
  no shutdown
!
ip default-gateway 10.13.15.1
!
ip dhcp snooping vlan 101,102
no ip dhcp snooping information option
ip dhcp snooping
!
ip arp inspection vlan 101,102
spanning-tree portfast bpduguard default
```

Procedure 4 Configure IACS interface

The host port configuration described below supports PAC, VFD, HMI, and DIO devices.

To make configuration easier, when you apply the same configuration 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. Because 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 (GigabitEthernet0/1 to GigabitEthernet0/24) simultaneously.

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

Step 1: On the access-layer switch, configure the switch interface to support IACS devices.

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

Step 2: Because only end-device connectivity is provided at the access layer, enable PortFast. By disabling 802.1Q trunking and channel group negotiation, PortFast shortens the time it takes for the interface to go into a forwarding state.

```
switchport host
```

Step 3: Apply the CiscoEtherNetIP QoS macro that was defined in Procedure 1, "Configure the access-layer platform."

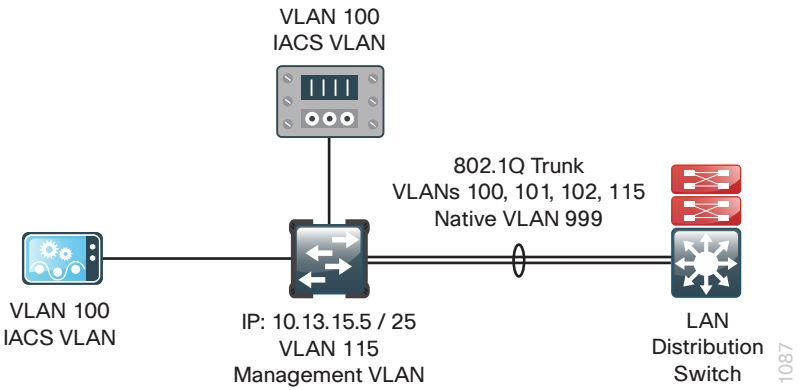
```
macro apply CiscoEtherNetIP
```

Step 4: Limit the storm control rate. This prevents LAN interfaces from being disrupted by *broadcast storms*, which occur when broadcast packets flood the subnet and create excessive traffic that degrades network performance.

```
storm-control broadcast level 3.00 1.00
```

Example

Figure 9 - IACS devices connected to the access layer




```
interface range FastEthernet 1/1-4
  description Cell/Area Zone - IACS Access Port
  switchport access vlan 100
  switchport host
  macro apply CiscoEtherNetIP
  storm-control broadcast level 3.00 1.00
```

Procedure 5 Configure workstation and voice interface

The host interface configurations support workstations or IP phones. Inline power is available on switches that support 802.3af/at for capable devices.

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 11 MAC addresses, which allows flexibility in the organization while still protecting the network infrastructure. Additional MAC addresses are considered to be in violation, and their traffic is dropped.

Step 1: On the access-layer switch, configure the switch interfaces to support clients and IP phones.

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

Step 2: Because only end-device connectivity is provided at the access layer, enable PortFast. By disabling 802.1Q trunking and channel-group negotiation, PortFast shortens the time it takes for the interface to go into a forwarding state.

```
switchport host
```

Step 3: Apply the CiscoIEPhone QoS macro that was defined in Procedure 1, "Configure the access-layer platform."

```
macro apply CiscoIEPhone
```

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

Next, you configure port security on the interface.

Step 4: Configure 11 MAC addresses to be active on the interface at one time.

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

Step 5: Set an aging time that removes 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 not to 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.

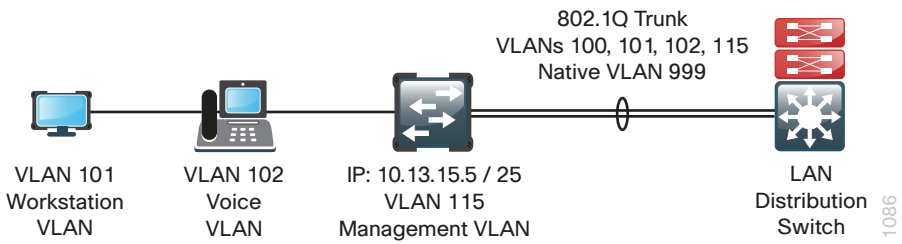
```
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
```

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

```
ip verify source
```

Example

Figure 10 - Workstation and IP phone connected to the access layer




```
interface range GigabitEthernet 1/0/1-24
 description Cell/Area Zone - Workstation/VoIP Access Port
 switchport access vlan 101
 switchport voice vlan 102
 switchport host
 macro apply CiscoIEPhone
 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
```

Process

Connecting the Access Layer to the Distribution/Core Layer

1. Create access-layer EtherChannel uplinks
2. Configure distribution/core-layer downlinks

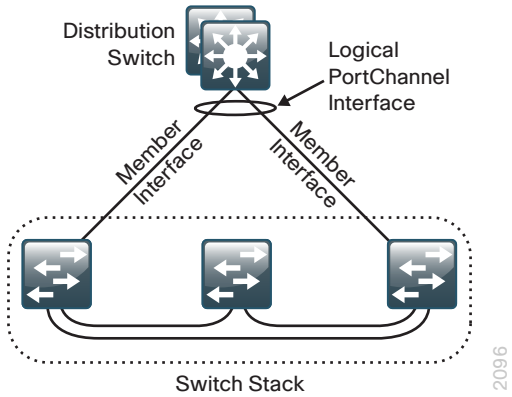
Procedure 1 Create access-layer EtherChannel uplinks

In this design, which users a redundant star topology, access-layer devices are a component of a larger LAN and are connected to the distribution/core-layer switch. Layer 2 EtherChannels are used to interconnect the devices in the most resilient method possible.

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

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 11 - 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.

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.

This procedure details how to connect any Cisco SBA discrete manufacturing access-layer switch (Cisco Catalyst 3750-X, Catalyst 3560-X, Catalyst 2960-S, Cisco IE 2000, or IE 3000) to a distribution/core-layer switch. Where there are differences for configuring a specific switch model, it is called out in the step.

Step 1: On the access-layer switch, set LACP negotiation to active, and then apply the CiscoIEEgress QoS macro that was defined in Procedure 1, "Configure the access-layer platform." This configures the EtherChannel member interfaces and ensures traffic is prioritized appropriately.

If the access-layer switch is a Cisco Catalyst 2960-S Series switch, the **switchport** command is not required.

```
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 CiscoIEEgress
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 2: Configure an 802.1Q trunk, prune the VLANs on the trunk to only the VLANs that are active on the access-layer switch, and then set DHCP snooping and ARP inspection to trust. The interface type is port-channel, and the number must match the channel group configured in Step 1.

If the access-layer switch is a Cisco Catalyst 3750-X or 3560-X Series switch, the **switchport trunk encapsulation dot1q** command is required.

```
interface Port-channel [number]
  description EtherChannel link to Distribution Layer
  switchport trunk allowed vlan [IACS vlan],
[Workstation vlan],[Voice vlan],[Management vlan]
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  logging event trunk-status
  no shutdown
```

Step 3: Configure an unused VLAN on all switch-to-switch 802.1Q trunk links from the access layer to the distribution/core layer, and then set the native VLAN for the access-layer uplink 802.1Q trunk to the VLAN you just created. Choosing an arbitrary, non-default, unused VLAN assignment for the native VLAN reduces the possibility of a VLAN-hopping attack.

```
vlan 999
!
interface Port-channel [number]
  switchport trunk native vlan 999
```

Reader Tip

For more information about VLAN-hopping attacks, see the "802.1Q Trunking" section of the "Discrete Manufacturing LAN Overview" chapter.

Step 4: Save the running configuration that you have entered as the startup configuration file. When the access-layer switch is reloaded or power-cycled, this configuration is used.

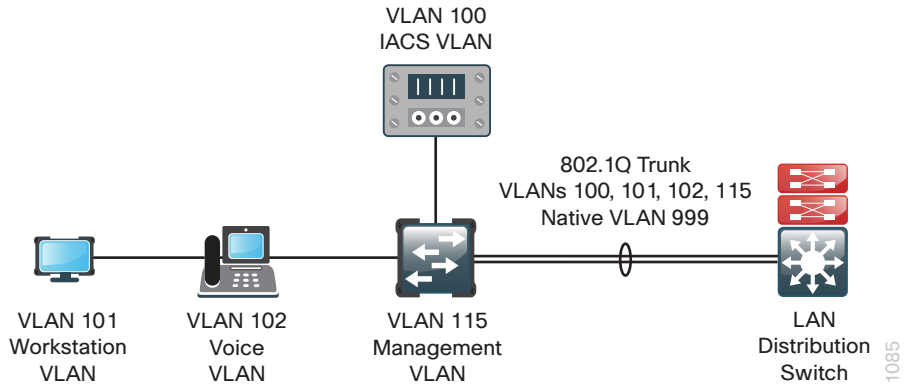
```
copy running-config startup-config
```

Step 5: If the access-layer switch is a Cisco Catalyst 2960-S or Cisco Catalyst 3750-X Series switch stack, reload your switch stack. This ensures that EtherChannel operates with other features configured on the switch stack and that the switch with the highest priority becomes the master of the stack.

```
reload
```

Example

Figure 12 - Access-layer switch EtherChannel connection to distribution/core-layer switch




```
vlan 999
!
interface GigabitEthernet 1/1
  description Link to Distribution Layer port 1
interface GigabitEthernet 1/2
  description Link to Distribution Layer port 2
!
interface range GigabitEthernet 1/1/1, GigabitEthernet 1/1/2
  macro apply CiscoIEEgress
  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 allowed vlan 100,101,102,115
  switchport mode trunk
  switchport trunk native vlan 999
  ip arp inspection trust
  ip dhcp snooping trust
  no shutdown
```

Procedure 2 Configure distribution/core-layer downlinks

The resilient, single, logical, distribution/core layer switch design is based on a redundant star topology that eliminates spanning-tree loops. The links to access-layer switches and connected routers are Layer 2 EtherChannels.

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

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 you add them in multiples of two.

An 802.1Q trunk is used for the connection to the access layer, which allows the distribution/core-layer switch to provide Layer 3 services to all the VLANs defined on the access-layer switch.

Step 1: On the distribution/core-layer switch, configure VLANs for the access-layer switches that you are connecting to the distribution/core-layer switch.

```
vlan [IACS vlan]
  name CZ1-IACS
vlan [Workstation vlan]
  name CZ1-Workstation
vlan [Voice vlan]
  name CZ1-Voice
vlan [Management vlan]
  name Management
```

Step 2: If there is no external, central-site DHCP server in the network and you want to provide DHCP service, configure DHCP service in Cisco IOS on the distribution/core-layer switch. 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 10.13.1.1 10.13.1.10
ip dhcp excluded-address 10.13.2.1 10.13.2.10
ip dhcp pool CZ1-Workstation
  network 10.13.1.0 255.255.255.0
  default-router 10.13.1.1
  domain-name cisco.local
  dns-server 10.13.48.10
!
ip dhcp pool CZ1-Voice
  network 10.13.2.0 255.255.255.0
  default-router 10.13.2.1
  domain-name cisco.local
  dns-server 10.13.48.10
```

The example configuration provides IP addresses via the Cisco IOS-based DHCP service for the subnets 10.13.1.0/24 10.13.2.0/24 and prevents the server from assigning reserved addresses .1-.10.

Step 3: Connect the access-layer EtherChannel uplinks to separate switches or switch modules in the distribution/core layer. On the distribution/core-layer switch, set LACP negotiation to active on all EtherChannel member interfaces, and then apply the QoS macro that was defined in Procedure 1, "Configure the distribution/core platform." This configures EtherChannel member interfaces and ensures traffic is prioritized appropriately.

If you are using a Cisco Catalyst 4507R+E chassis, connect the EtherChannel uplinks to separate modules. This provides additional resiliency.

```
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 CiscoIEEgress
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 4: If you are using a Cisco Catalyst 3750-X Series switch stack, on the distribution/core-layer switch, configure an 802.1Q trunk, and then prune the VLANs on the trunk to only the VLANs that are active on the access-layer switch. The interface type is port-channel, and the number must match the channel group configured in Step 3.

```
interface Port-channel [number]
  description EtherChannel link to {your device here}
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [IACS vlan],
[Workstation vlan],[Voice vlan],[Management vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

If you are using a Cisco Catalyst 4507R+E switch, on the distribution/core-layer switch, configure an 802.1Q trunk, and then prune the VLANs on the trunk to only the VLANs that are active on the access-layer switch. The interface type is port-channel, and the number must match the channel group configured in Step 3.

```
interface Port-channel [number]
  description EtherChannel link to {your device here}
  macro apply CiscoIEEgress-PC
  switchport trunk allowed vlan [IACS vlan],
[Workstation vlan],[Voice vlan],[Management vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

Step 5: Configure an unused VLAN on all switch-to-switch 802.1Q trunk links from the access layer to the distribution/core layer, and then set the native VLAN for the access-layer uplink 802.1Q trunk to the VLAN you just created. By using a hard-to-guess, unused VLAN for the native VLAN, you reduce the risk of a VLAN-hopping attack.

```
vlan 999
!
interface Port-channel [number]
  switchport trunk native vlan 999
```

Reader Tip

For more information about VLAN-hopping attacks, see the "802.1Q Trunking" section of the "Discrete Manufacturing LAN Overview" chapter.

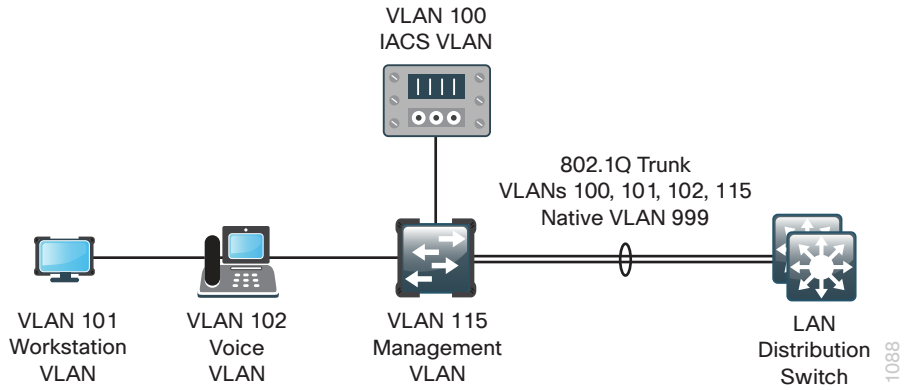
Step 6: For every access-layer VLAN, configure a switched virtual interface (SVI). This enables devices in the VLAN to communicate with the rest of the network.

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.

If you completed Step 2 in order to enable the Cisco IOS DHCP server function on the distribution/core layer switch, the **ip helper-address** command is not needed on the VLAN interface.

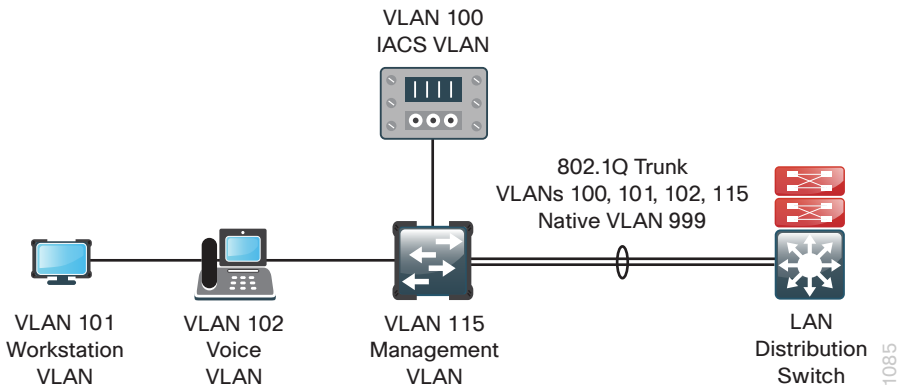
```
interface Vlan [number]
  ip address [ip address] [mask]
  ip helper-address [dhcp server ip]
  ip pim sparse-mode
  no shutdown
```

Example: Cisco Catalyst 3750-X Series switch stack



```
vlan 100
  name CZ1-IACS
vlan 101
  name CZ1-Workstation
vlan 102
  name CZ1-Voice
vlan 115
  name Management
vlan 999
spanning-tree vlan 1-4094 root primary
!
interface GigabitEthernet 1/0/1
  description Link to Access Switch port 1
interface GigabitEthernet 3/0/1
  description Link to Access Switch port 2
!
interface range GigabitEthernet 1/0/1, GigabitEthernet 3/0/1
  switchport
  macro apply  CiscoIEEgress
  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 encapsulation dot1q
  switchport trunk allowed vlan 100,101,102,115
  switchport mode trunk
  switchport trunk native vlan 999
  no shutdown
!
interface Vlan 100
description Cell Zone 1 IACS VLAN
  ip address 10.13.0.1 255.255.255.0
  ip helper-address 10.13.48.10
  ip pim sparse-mode
!
interface Vlan 101
description Cell Zone 1 Workstation VLAN
  ip address 10.13.1.1 255.255.255.0
  ip helper-address 10.13.48.10
  ip pim sparse-mode
!
interface Vlan 102
description Cell Zone 1 Voice VLAN
  ip address 10.13.2.1 255.255.255.0
  ip helper-address 10.13.48.10
  ip pim sparse-mode
!
interface Vlan 115
description Management VLAN
  ip address 10.13.15.1 255.255.255.128
  ip helper-address 10.13.48.10
  ip pim sparse-mode
```

Example: Cisco Catalyst 4507R+E chassis




```
vlan 100
  name CZ1-IACS
vlan 101
  name CZ1-Workstation
vlan 102
  name CZ1-Voice
vlan 115
  name Management
vlan 999
spanning-tree vlan 1-4094 root primary
!
interface GigabitEthernet 1/1
  description Link to Access Switch port 1
interface GigabitEthernet 2/1
  description Link to Access Switch port 2
!
interface range GigabitEthernet 1/1, GigabitEthernet 2/1
  switchport
  macro apply  CiscoIEEgress
  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
  macro apply CiscoIEEgress-PC
  switchport trunk allowed vlan 100,101,102,115
  switchport mode trunk
  switchport trunk native vlan 999
  no shutdown
!
interface Vlan 100
description Cell Zone 1 IACS VLAN
  ip address 10.13.0.1 255.255.255.0
  ip helper-address 10.13.48.10
  ip pim sparse-mode
!
interface Vlan 101
description Cell Zone 1 Workstation VLAN
  ip address 10.13.1.1 255.255.255.0
  ip helper-address 10.13.48.10
  ip pim sparse-mode
!
interface Vlan 102
description Cell Zone 1 Voice VLAN
  ip address 10.13.2.1 255.255.255.0
  ip helper-address 10.13.48.10
  ip pim sparse-mode
!
interface Vlan 115
description Management VLAN
  ip address 10.13.15.1 255.255.255.128
  ip helper-address 10.13.48.10
  ip pim sparse-mode
```

Operations and Server Room

Business Overview

The operation and server-room network connects the Manufacturing zone (Level 3) applications, servers, and control-engineering workstations to the industrial Ethernet network. This network interconnects with the rest of the network via the distribution/core layer, giving the Level 3 applications access to the devices and data residing in the IACS systems.

The guideline for converged industrial Ethernet network design is that applications critical to plant operations should be placed in the industrial Ethernet network, segmented from the enterprise network. The systems, applications, and databases may be replicated or share data with applications in the Enterprise zone via the DMZ. Applications typically found in the operation and server-room network include:

- Production schedule and manufacturing execution systems
- Plant asset managers
- Plant historians and reporting applications
- Control-engineering workstations and programming applications
- Terminal server for remote-access services
- Patch servers and application staging servers
- Human machine interface (HMI) servers
- Network monitoring and management (for example, Simple Network Management Protocol server)
- Domain services such as Dynamic Host Configuration Protocol (DHCP), Active Directory, Domain Name System (DNS), Network Time Protocol (NTP), and file and print servers

These applications are critical to plant operations, but they often do not have the same tight convergence or performance requirements (for example, low latency and jitter) as the IACS devices on the network.

Plant productivity depends on the ability of operators to access IACS applications and services necessary to do their job quickly and efficiently. Consistent and reliable access to the servers that support the applications that drive the plant is critical to ensuring the plant stays online and productive.

Technical Overview

Cisco SBA recognizes the importance of the operations and server-room facility and its function in the converged industrial Ethernet network. The design provides a small, yet resilient and scalable, Ethernet LAN foundation that connects the application servers to the users located throughout the rest of the industrial Ethernet network.

Design Goals

This chapter is designed to address four primary operations and server-room needs of manufacturing organizations:

- Provide reliable access for servers and operator workstations
- Provide a an organization with a primary server room for plant systems
- Secure the organization's critical data
- Reduce operational costs

Reliable Access to Organization Resources

Data networks are critical to an organization's ability to operate and compete. Industrial Ethernet networks must be functional for the plant to continue operation. Operator workstations and management and monitoring servers reside in the operations and server room, within the Manufacturing zone, and they need reliable access to the manufacturing devices in the Cell/Area zone and to the enterprise network. As networks become more complex, the risk increases that the operations and server-room systems may lose availability or suffer poor performance due to inadequate design, configuration errors, maintenance and upgrade outages, or hardware and software faults. The design and methods used in this deployment guide were created to minimize these risks.

Primary Server Room for the Plant

As organizations merge Ethernet and IACS networks into industrial Ethernet networks, reliance on the converged network increases. Plant machines or lines are no longer isolated, and operator workstations and monitoring and management servers need an available and secure place to reside within the industrial Ethernet network. Because these systems are critical

to plant floor operations, they should not be placed in the Enterprise zone's data center, and the best solution is a server-room segment within the Manufacturing zone and located at the plant. An example environment has controlled cooling and power, two to three equipment racks for application servers, network connectivity, and a backup system.

Securing the Organization's Critical Data

Frequently, threats to an organization's data may come from within the internal network. This may come in the form of onsite vendors, contaminated employee laptops, or existing servers that are already compromised and may be used as a platform to launch further attacks. With the centralized repository of the manufacturing organization's critical data being the industrial Ethernet network server room, security for the server room is not an optional component. The plant needs to be secured from traffic and threats from the enterprise network, as something that would be a minor disruption in an enterprise network could cause a manufacturing environment to shut down.

The Cisco SBA discrete manufacturing security design illustrates how to cleanly integrate network security capabilities such as VPN, firewall, and intrusion prevention, protecting areas of the network housing plant systems. The architecture provides the flexibility to secure specific portions of the industrial Ethernet network via the DMZ, according to the security policy agreed upon by the organization.

Reduced Operational Costs

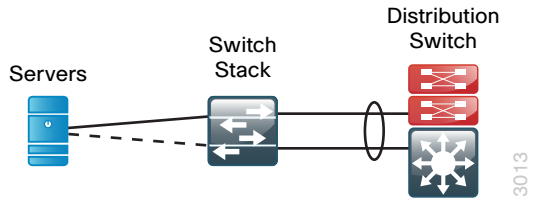
Organizations constantly pursue opportunities to reduce network operational costs while maintaining the network's effectiveness. Operational costs include not only the cost of the physical operation (for example, power and cooling), but also the labor cost required to staff an IT department that monitors and maintains the network. Additionally, network outages and performance issues impose costs that are more difficult to quantify, in the form of loss of productivity and interruption of business continuity. Consolidating industrial Ethernet and enterprise networks allows you to build a single higher-performing network that centralizes IT service and support and can lower the risk of unplanned and lengthy outages that stop production in the plant. The network design provided by this deployment guide offers network resilience in its ability to tolerate failure or outage of portions of the network, and it is a sufficiently robust—yet simple—design that staff should be able to operate, troubleshoot, and return to service in the event of a network outage.

Design Overview of the Server Room

In Cisco SBA, the operations and server room provides basic compute capability for plant operations and is designed to accommodate 24-48 physical servers and workstations. The design uses the Cisco Catalyst 3560-X Series standalone switch and Cisco Catalyst 3750-X Series stackable Ethernet LAN switches, and both switches support 10/100/1000 Ethernet in order to accommodate a wide range of server and workstation Ethernet interface speeds.

The Cisco StackWise Plus feature of Cisco Catalyst 3750-X Series switches provides a resilient, high-speed backplane for the operations and server-room environment and provides the ability to dual-home servers and workstations to the server-room LAN, for increased resiliency. With two switches in the stack and dual-homing to servers and the plant LAN distribution/core-layer switches, your server room is protected from single points of failure. The Catalyst 3750-X Series switches in a stack provide automated control-plane failover in the event that the master switch experiences an issue. The option of dual power supplies and Cisco StackPower with the Catalyst 3750-X Series switches provides more resilience to the operations and server-room design. Cisco Catalyst 3560-X Series does not provide the same level of resilience as Cisco Catalyst 3750-X Series, but it is suitable for single connected servers and workstations running less-critical systems.

Figure 13 - Server-room switch or switch stack with EtherChannel uplinks



In the Cisco SBA design, the server-room switches are connected to the distribution/core layer with an EtherChannel so that two 1-Gigabit Ethernet ports combine to make a single 2-Gigabit Ethernet channel. It is possible to increase the number of distribution/core layer links from the server room up to four or eight, for more bandwidth if needed. If you require very high bandwidth, you can use 10-Gigabit Ethernet links in order to connect the appropriate distribution/core-layer switch ports to 10-Gigabit ports on uplink modules installed in the server-room switches.

Both the server-room and the client LAN-access methods connect devices to the network; the difference between the two methods that changes the switch model is whether LAN access requires Power over Ethernet (PoE).

Although PoE-capable devices are not typical in the server room, using PoE-capable switches offers a benefit worth considering: the minor initial cost savings of a non-PoE switch may not be worth the benefits of using the same switch across multiple modules of your local LAN. Although configurations differ between LAN access-layer switches and server-room switches, the ability to use a single switch type between multiple modules can lower operational costs by allowing for simpler sparing and management, as well as provide a better chance of reuse as the industrial Ethernet network grows.

Deployment Details

This section includes the procedures you need to perform in order to configure your server-room Ethernet LAN connectivity. As you review the deployment procedures, refer to the following table for the IP addressing and VLAN assignments used in the server-room deployment. Your design requirements for IP addressing and VLAN numbering may differ.

Table 4 - VLANs and IP addressing for server-room deployment

VLAN	IP address range	Usage
148	10.13.48.x /24	Server VLAN 1
149	10.13.49.x /24	Server VLAN 2
115	10.13.15.x /25	Management VLAN

Process

Configuring the Server Room

1. Configure the server-room platform
2. Configure switch universal settings
3. Configure switch global settings

For the server-room Ethernet LAN, the following procedures are designed to configure a standalone Cisco Catalyst 3560-X Series server-room switch or a stack of two Cisco Catalyst 3750-X Series switches.

Procedure 1 Configure the server-room platform

When there are multiple Cisco Catalyst 3750-X Series switches configured in a stack, one of the switches controls the operation of the stack and is called the *stack master*.

By default, the 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. This configuration preserves the original stack-master MAC address in order prevent convergence issues.

Step 1: If you are using a Cisco Catalyst 3560-X Series switch, skip to the next step.

If you are using the Cisco Catalyst 3750-X Series switch stack, ensure that the original master MAC address remains the stack MAC address after a failure.

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

Step 2: Create access lists and class maps that differentiate the various types of manufacturing traffic.

```
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
ip access-list extended default-data-acl
 permit ip any any
class-map match-all CIP-Implicit_dscp_55
 match access-group 101
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_43
 match access-group 103
```

```
class-map match-all CIP-Implicit_dscp_any
 match access-group 104
class-map match-all CIP-Other
 match access-group 105
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all voip-data
  match ip dscp ef
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all voip-control
  match ip dscp cs3
```

Step 3: Configure the global quality of service (QoS) settings and create two macros. These macros are used in later procedures and ease consistent deployment of QoS.

```
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4
5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34
35 36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42
44 45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54
56 57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31
43 46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12
13 14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20
21 22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30
32 33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39
40 41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51
52 53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61
62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47
48 55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
```

```
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos

policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
  set ip dscp 55
  class CIP-Implicit_dscp_47
  set ip dscp 47
  class CIP-Implicit_dscp_43
  set ip dscp 43
  class CIP-Implicit_dscp_any
  set ip dscp 31
  class CIP-Other
   set ip dscp 27
  class 1588-PTP-Event
   set ip dscp 59
  class 1588-PTP-General
   set ip dscp 47

policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit

macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@
```

Procedure 2 Configure switch universal settings

This procedure configures system settings that simplify and secure the management of the switch. The values and actual settings used in your deployment depend on your current network configuration.

Table 5 - Common network services used in the deployment examples

Network parameter	Cisco SBA value
Domain name	cisco.local
Active Directory, DNS, DHCP server	10.13.48.10
Cisco Secure ACS server	10.13.48.15
NTP server	10.13.48.17

In this procedure, you configure a local login account and password that provide basic device access authentication in order 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. By default, HTTPS access to the switch uses the enable password for authentication.

Reader Tip

For more information about the protocols used in this procedure, see the "Protocols" section of the "Discrete Manufacturing LAN Overview" chapter.

Step 1: On the server-room switch, configure the device host name. This makes it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure VTP transparent mode.

```
vtp mode transparent
```

Step 3: Enable RPVST+.

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

Step 4: Enable UDLD.

```
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.

```
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 10.13.48.10
```

Step 7: Configure HTTPS and SSH device management protocols, and then specify the **transport preferred none** command on vty lines.

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

Tech Tip

The **transport preferred none** command prevents errant connection attempts from the CLI prompt, and without it, long timeout delays may occur for mistyped commands if the IP name server is unreachable.

Step 8: Enable SNMP in order to allow the network infrastructure devices to be managed by a Network Management System, 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 and you want to increase network security, use an access list to limit the networks that can access your device. In this example, only devices on the 10.13.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.13.48.0 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 router to the next, for hop-by-hop troubleshooting.

Step 10: Configure the local login and password.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 11: If you want to use AAA services for centralized user authentication, use TACACS+ protocol in order to authenticate management logins to infrastructure devices.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.13.48.15
  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: Program network devices to synchronize to a local NTP server in the network, and then configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```
ntp server 10.13.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 3 Configure switch global settings

Configure the server-room switch VLANs according to the values listed in Table 4.

Step 1: On the server-room switch, configure the server and management VLANs.

Step 2:

```
vlan [Server vlan 1]
  name Server_VLAN_1
vlan [Server vlan 2]
  name Server_VLAN_2
vlan [Management vlan]
  name Management
```

Step 3: Configure the switch with an IP address, and then assign an IP default gateway. This allows management via in-band connectivity.

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

Step 4: Configure BPDU guard globally. This protects PortFast-enabled interfaces by disabling the port if another switch is plugged into the port.

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

Reader Tip

For more information about BPDU guard, see the "BPDU Guard" section of the "Discrete Manufacturing LAN Overview" chapter.

Example

```
vlan 148
  name Server_VLAN_1
vlan 149
  name Server_VLAN_2
vlan 115
  name Management
!
interface Vlan 115
  ip address 10.13.15.50 255.255.255.128
  no shutdown
ip default-gateway 10.13.15.1
```

Process

Connecting the Server Room to the Distribution/Core Layer

1. Configure server-room uplink ports
2. Configure server-room access ports
3. Configure distribution/core-layer downlinks

Procedure 1 Configure server-room uplink ports

This procedure details how to connect a server-room switch to the distribution/core layer.

Configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. This sequence 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.

An 802.1Q trunk is used for the connection to the upstream device, which allows the uplink to provide Layer 3 services to all the VLANs defined on the server-room switch.

Step 1: On the server-room switch, set LACP negotiation to active. Then apply the CiscoIEEgress QoS macro that was defined in Procedure 1, "Configure the server-room platform." This configures EtherChannel member interfaces and ensures traffic is prioritized appropriately.

```
interface [interface type] [port 1]
  description Link to Distribution port 1
interface [interface type] [port 2]
  description Link to Distribution port 2
interface range [interface type] [port 1], [interface type]
[port 2]
  switchport
  macro apply CiscoIEEgress
  channel-protocol lacp
  channel-group 1 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 2: Configure the 802.1Q trunk, and then prune the VLANs allowed on the trunk to only the VLANs that are active on the server-room switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in Step 1.

```
interface Port-channel [number]
  description EtherChannel Link to Distribution
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [server vlan 1],
[server vlan 2],[management vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

Step 3: Configure an unused VLAN on the switch-to-switch 802.1Q trunk link from the server room to the distribution/core layer, and then set the native VLAN for the server-room uplink 802.1Q trunk to the VLAN you just created. Using a hard-to-guess, unused VLAN for the native VLAN reduces the possibility of a VLAN-hopping attack.

```
vlan 999
!
interface Port-channel [number]
  switchport trunk native vlan 999
```

Reader Tip

For more information about VLAN-hopping attacks, see the "802.1Q Trunking" section of the "Discrete Manufacturing LAN Overview" chapter.

Example

```
interface GigabitEthernet1/1/1
  description Link to LAN Distribution port 1
interface GigabitEthernet2/1/1
  description Link to LAN Distribution port 2
interface range GigabitEthernet 1/1/1, GigabitEthernet 2/1/1
  channel-protocol lacp
  channel-group 1 mode active
  macro apply CiscoIEEgress
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
interface Port-channel 1
  description EtherChannel Link to LAN Distribution
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 148-149,115
  switchport mode trunk
  logging event link-status
  no shutdown
!
vlan 999
!
interface Port-channel 1
 switchport trunk native vlan 999
```

Procedure 2 Configure server-room access ports

To make configuration easier when you are applying the same configuration 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.

Step 1: On the server-room switch, configure switch interfaces to offer basic server connectivity.

```
interface range [interface type] [port number]-[port number]
  switchport access vlan [server vlan 1]
```

Step 2: Set the switchport to host made. This shortens the time it takes for a port to go into a forwarding state.

```
switchport host
```

Step 3: Apply the CiscoEtherNetIP macro defined in Procedure 1, "Configure the server-room platform." This enables trust for the QoS markings on the traffic from the servers.

```
macro apply CiscoEtherNetIP
```

Tech Tip

It is possible that your server or application may require special configuration such as trunking or port-channeling. Refer to vendor documentation for this information.

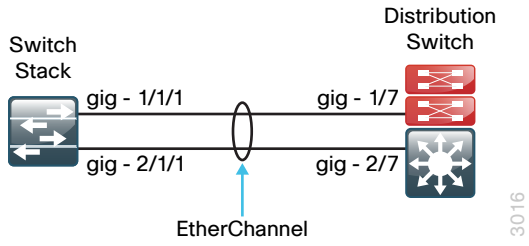
Step 4: Save the running configuration that you have entered as the startup configuration file. When your server-room switch is rebooted or power-cycled, this configuration is used.

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

Procedure 3 Configure distribution/core-layer downlinks

The links to the server-room switch are Layer 2 EtherChannels. Connect the server-room EtherChannel uplinks to separate stack members or interface modules on the distribution/core-layer switch.

Figure 14 - EtherChannel with stack member or switch blade diversity



An 802.1Q trunk is used for the connection between the distribution/core-layer switch and the server-room switch, which allows the uplink to provide Layer 3 services to all the VLANs defined in the server room.

Step 1: On the distribution/core-layer switch, add the server-room VLANs to the VLAN database that the downlink carries.

```
vlan [Server vlan 1]
  name Server_VLAN_1
vlan [Server vlan 2]
  name Server_VLAN_2
```

Step 2: Set LACP negotiation to active and then apply the CiscoIEEgress QoS macro that was defined in Procedure 1, "Configure the distribution/core platform." This configures the EtherChannel member interfaces and ensures traffic is prioritized appropriately.

```
interface [interface type] [port 1]
  description Link to Server Room port 1
interface [interface type] [port 2]
  description Link to Server Room port 2
interface range [interface type] [port 1], [interface type]
[port 2]
  switchport
  macro apply CiscoIEEgress
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 3: If you are using a Cisco Catalyst 3750-X Series switch stack, on the distribution/core-layer switch, configure an 802.1Q trunk, and then prune the VLANs allowed on the trunk to only the VLANs that are active on the server-room switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in Step 2.

```
interface Port-Channel[number]
  description EtherChannel Link to Server Room
    switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [server vlan 1],
[server vlan 2],[mgmt vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

If you are using a Cisco Catalyst 4507R+E switch, on the distribution/core-layer switch, configure an 802.1Q trunk, and then prune the VLANs allowed on the trunk to only the VLANs that are active on the server-room switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel group configured in Step 2.

```
interface Port-Channel[number]
  description EtherChannel Link to Server Room
  macro apply CiscoIEEgress-PC
  switchport trunk allowed vlan [server vlan 1],
[server vlan 2],[mgmt vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

Step 4: Add VLAN-hopping mitigation for the trunk.

```
interface Port-channel [number]
 switchport trunk native vlan 999
```

Step 5: If the VLANs for the server room do not already exist on the distribution/core-layer switch, add a switched virtual interface (SVI) for every server-room VLAN. This enables the VLANs to route to the rest of the network.

If you are using DHCP to assign IP addresses for servers in the server room, use the **ip helper-address** command to allow remote DHCP servers to provide IP addresses for this network. The **helper** command points to the DHCP server address; if you have more than one DHCP server, multiple **helper** commands can be listed on an interface.

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

Example

```
vlan 148
  name Server_VLAN_1
vlan 149
  name Server_VLAN_2
!
interface GigabitEthernet1/23
  description Link to Server Room port 1
interface GigabitEthernet2/23
  description Link to Server Room port 2
interface range GigabitEthernet 1/23, GigabitEthernet 2/23
  channel-protocol lacp
  channel-group 1 mode active
  macro apply CiscoIEEgress
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
interface Port-channel 1
  description EtherChannel Link to Server Room
  macro apply CiscoIEEgress-PC
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 148-149,115
  switchport mode trunk
  logging event link-status
  no shutdown
!
interface Port-channel 1
 switchport trunk native vlan 999
!
interface Vlan 148
  ip address 10.13.48.1 255.255.255.0
  ip pim sparse-mode
  no shutdown
interface Vlan 149
  ip address 10.13.49.1 255.255.255.0
  ip pim sparse-mode
  no shutdown
```

Notes

Appendix A: Product List

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE 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)SE 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)SE 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	

Functional Area	Product Description	Part Numbers	Software
Industrial Ethernet Modular Access Layer Switch	Cisco Catalyst IE 3000 Switch, 8 10/100 + 2 T/SFP	IE-3000-8TC	15.0(2)SE LAN Base license
	Cisco Catalyst IE 3000 Switch, 4 10/100 + 2 T/SFP	IE-3000-4TC	
	Cisco Catalyst IE 3000 Expansion Module, 8 10/100	IEM-3000-8TM=	
	Cisco Catalyst IE 3000 Expansion Module, 8 100FX	IEM-3000-8FM=	
	Cisco Catalyst IE 3000 8 port SFP expansion module	IEM-3000-8SM=	
	Cisco Catalyst IE 3000 4 port SFP expansion module	IEM-3000-4SM=	
Industrial Ethernet Access Layer Switch	Cisco Catalyst IE 16 10/100,2 FE SFP+2 T/SFP, Base with 1588, Comf. Coat	IE-2000-16TC-G-X	15.0(2)SE LAN Base license
	Cisco Catalyst IE 16 10/100,2 FE SFP+2 T/SFP, Base with 1588	IE-2000-16TC-G-E	
	Cisco Catalyst IE 16 10/100,2 FE SFP+2 T/SFP FE, Base	IE-2000-16TC-B	
	Cisco Catalyst IE 8 10/100,2 T/SFP, Base with 1588	IE-2000-8TC-G-E	
	Cisco Catalyst IE 8 10/100,2 T/SFP, Base	IE-2000-8TC-G-B	
	Cisco Catalyst IE 8 10/100,2 FE SFP+2 T/SFP FE, Base	IE-2000-8TC-B	
	Cisco Catalyst IE 4 10/100,2 SFP Gig port, Base	IE-2000-4TS-G-B	
	Cisco Catalyst IE 4 10/100,2 FE SFP, Base	IE-2000-4TS-B	
	Cisco Catalyst IE 4 10/100,2 Gig port, Base	IE-2000-4T-G-B	
	Cisco Catalyst IE 4 10/100,2 FE, Base	IE-2000-4T-B	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) 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)SE 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	

Server Room

Functional Area	Product Description	Part Numbers	Software
Stackable Ethernet Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 ports	WS-C3750X-48T-S	15.0(2)SE IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Ethernet Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 ports	WS-C3560X-48T-S	15.0(2)SE IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 ports	WS-C3560X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Appendix B: Configuration Files

Distribution/Core-Layer Configurations

D4507R

```
version 15.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service compress-config
!
hostname D4507R
!
boot-start-marker
boot-end-marker
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
username admin password 7 04585A150C2E1D1C5A
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
udld enable
!
ip vrf mgmtVrf
!
ip multicast-routing
ip domain-name cisco.local
ip name-server 10.13.48.10
!
vtp mode transparent
!
crypto pki trustpoint CISCO_IDEVID_SUDI
 revocation-check none
 rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDI0
 revocation-check none
!
crypto pki trustpoint TP-self-signed-14461
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-14461
 revocation-check none
 rsakeypair TP-self-signed-14461
!
power redundancy-mode redundant
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
!
redundancy
 mode sso
```

```
!
vlan internal allocation policy ascending
!
vlan 100
 name CZ1-IACS
!
vlan 101
 name CZ1-Workstation
!
vlan 102
 name CZ1-Voice
!
vlan 103
 name CZ2-IACS
!
vlan 104
 name CZ2-Workstation
!
vlan 105
 name CZ2-Voice
!
vlan 106
 name CZ3-IACS
!
vlan 107
 name CZ3-Workstation
!
vlan 108
 name CZ3-Voice
!
vlan 115
 name Management
!
vlan 148
 name Server_VLAN_1
!
vlan 149
 name Server_VLAN_2
!
vlan 999
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any CONTROL-MGMT-QUEUE
  match cos  3
class-map match-any SCAVENGER-QUEUE
  match cos  1
class-map match-any CIP-PTP-General
  match cos  5  6
class-map match-any PRIORITY-QUEUE
  match cos  7
!
policy-map 1P5Q1T
 class PRIORITY-QUEUE
    priority
 class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 40
 class CIP-PTP-General
    bandwidth remaining percent 40
 class SCAVENGER-QUEUE
    bandwidth remaining percent 1
 class class-default
    bandwidth remaining percent 18
    dbl
policy-map 1P5Q1T-PC
 class PRIORITY-QUEUE
    police cir 200000000    conform-action transmit     exceed-
action drop
!
macro name CiscoIEEgress
service-policy output 1P5Q1T
@
macro name CiscoIEEgress-PC
```

```
service-policy output 1P5Q1T-PC
@
!
interface Loopback0
 ip address 10.13.15.254 255.255.255.255
 ip pim sparse-mode
!
interface Loopback1
 ip address 10.13.15.253 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 description EtherChannel Link to Server Room
 switchport
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
 macro description CiscoIEEgress-PC
 service-policy output 1P5Q1T-PC
!
interface Port-channel10
 description EtherChannel link to CZ1-IE2K-1
 switchport
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
 macro description CiscoIEEgress-PC
 service-policy output 1P5Q1T-PC
!
interface Port-channel11
 description EtherChannel link to CZ2-2960S-1
 switchport
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
 macro description CiscoIEEgress-PC
 service-policy output 1P5Q1T-PC
!
interface Port-channel12
 description EtherChannel link to CZ3-3560X-1
 switchport
 switchport trunk native vlan 999
 switchport trunk allowed vlan 106-108,115
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
 macro description CiscoIEEgress-PC
 service-policy output 1P5Q1T-PC
!
interface FastEthernet1
 ip vrf forwarding mgmtVrf
 no ip address
 speed auto
 duplex auto
!
interface GigabitEthernet1/1
 description Link to CZ1-IE2K-1 port 1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 10 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet1/2
```

```
 description Link to CZ2-2960S-1 port 1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 11 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet1/3
 description Link to CZ3-3560X-1 port 1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 106-108,115
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 12 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet1/4
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 1/5 - 1/22 are all configured
! the same as 1/4 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet1/23
 description Link to Server Room port 1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet1/24
 shutdown
!
interface GigabitEthernet2/1
 description Link to CZ1-IE2K-1 port 2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 10 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet2/2
 description Link to CZ2-2960S-1 port 2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 11 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet2/3
 description Link to CZ3-3560X-1 port 2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 106-108,115
```

```
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 12 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet2/4
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 2/5 - 2/22 are all configured
! the same as 2/4 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet2/23
 description Link to Server Room port 2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 service-policy output 1P5Q1T
!
interface GigabitEthernet2/24
 shutdown
!
interface TenGigabitEthernet3/1
 shutdown
!
! ************************************************************
! Interface TenGigabitEthernet 3/1 - 4/4 are all configured
! the same as 3/1 and have been removed for conciseness
! ************************************************************
!
interface Vlan1
 no ip address
!
interface Vlan100
 description CZ1-IACS
 ip address 10.13.0.1 255.255.255.0
 ip pim sparse-mode
!
interface Vlan101
 description CZ1-Workstation
 ip address 10.13.1.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan102
 description CZ1-Voice
 ip address 10.13.2.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan103
 description CZ2-IACS
 ip address 10.13.3.1 255.255.255.0
 ip pim sparse-mode
!
interface Vlan104
 description CZ2-Workstation
 ip address 10.13.4.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan105
 description CZ2-Voice
 ip address 10.13.5.1 255.255.255.0
 ip helper-address 10.13.48.10
```

```
 ip pim sparse-mode
!
interface Vlan106
 description CZ3-IACS
 ip address 10.13.6.1 255.255.255.0
 ip pim sparse-mode
!
interface Vlan107
 description CZ3-Workstation
 ip address 10.13.7.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan108
 description CZ3-Voice
 ip address 10.13.8.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan115
 description Management
 ip address 10.13.15.1 255.255.255.128
 ip pim sparse-mode
!
interface Vlan148
 description Servers 1
 ip address 10.13.48.1 255.255.255.0
 ip pim sparse-mode
!
interface Vlan149
 description Servers 2
 ip address 10.13.49.1 255.255.255.0
 ip pim sparse-mode
!
router eigrp 101
 network 10.13.0.0 0.0.255.255
 passive-interface default
 eigrp router-id 10.13.15.254
 eigrp stub connected summary
 nsf
!
no ip http server
ip http authentication aaa
ip http secure-server
ip pim autorp listener
ip pim send-rp-announce Loopback1 scope 32 group-list 10
ip pim send-rp-discovery Loopback0 scope 32
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
access-list 10 permit 239.1.0.0 0.0.255.255
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.13.48.15
 key 7 0812494D1B1C113C1712
!
line con 0
 stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp update-calendar
ntp server 10.13.48.17
end
```

D3750X

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname D3750X
!
boot-start-marker
boot-end-marker
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
username admin password 7 141443180F0B7B7977
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-12s
switch 2 provision ws-c3750x-12s
switch 3 provision ws-c3750x-12s
stack-mac persistent timer 0
system mtu routing 1500
ip routing
!
ip domain-name cisco.local
ip name-server 10.13.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34 35
36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42 44
45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54 56
57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31 43
46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
```

```
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30 32
33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39 40
41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51 52
53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61 62
63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47 48
55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos
!
crypto pki trustpoint TP-self-signed-2103206656
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2103206656
 revocation-check none
 rsakeypair TP-self-signed-2103206656
!
license boot level ipservices switch 1
license boot level ipservices switch 2
license boot level ipservices switch 3
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 100
 name CZ1-IACS
!
vlan 101
 name CZ1-Workstation
!
vlan 102
 name CZ1-Voice
!
vlan 103
 name CZ2-IACS
!
vlan 104
 name CZ2-Workstation
!
vlan 105
 name CZ2-Voice
!
vlan 106
 name CZ3-IACS
!
vlan 107
 name CZ3-Workstation
!
vlan 108
 name CZ3-Voice
!
vlan 115
 name Management
```

```
!
vlan 999
!
ip ssh source-interface Loopback0
ip ssh version 2
!
macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
!
interface Loopback0
 ip address 10.13.15.254 255.255.255.255
 ip pim sparse-mode
!
interface Loopback1
 ip address 10.13.15.253 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel10
 description EtherChannel link to SR-3750X
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148-149
 switchport mode trunk
!
interface Port-channel10
 description EtherChannel link to CZ1-IE2K-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
!
interface Port-channel11
 description EtherChannel link to CZ2-2960S-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
!
interface Port-channel12
 description EtherChannel link to CZ3-3560X-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 106-108,115
 switchport mode trunk
!
interface FastEthernet0
 no ip address
 no ip route-cache
 shutdown
!
interface GigabitEthernet1/0/1
 description Link to CZ1-IE2K-1 port 1
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 10 mode active
!
interface GigabitEthernet1/0/2
 description Link to CZ2-2960S-1 port 1
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
```

```
 channel-protocol lacp
 channel-group 11 mode active
!
interface GigabitEthernet1/0/3
 description Link to CZ3-3560X-1 port 1
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 12 mode active
!
interface GigabitEthernet1/0/4
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 1/0/5 - 1/0/10 are all configured
! the same as 1/0/4 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet1/0/11
 description Link to SR-3750X port 1
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/0/12
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 1/1/1 - TenGigabitEthernet 2/1/2
! are all configured the same as GigabitEthernet 1/0/12 and
! have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet3/0/1
 description Link to CZ1-IE2K-1 port 2
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 10 mode active
!
interface GigabitEthernet3/0/2
 description Link to CZ2-2960S-1 port 2
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 11 mode active
!
interface GigabitEthernet3/0/3
 description Link to CZ3-3560X-1 port 2
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
```

```
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 12 mode active
!
interface GigabitEthernet3/0/4
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 3/0/5 - 3/0/10 are all configured
! the same as 3/0/4 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet3/0/11
 description Link to SR-3750X port 2
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet3/0/12
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 3/1/1 - TenGigabitEthernet 3/1/2
! are all configured the same as GigabitEthernet 3/0/12 and
! have been removed for conciseness
! ************************************************************
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 description Cell Zone 1 IACS VLAN
 ip address 10.13.0.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan101
 description Cell Zone 1 Workstation VLAN
 ip address 10.13.1.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan102
 description Cell Zone 1 Voice VLAN
 ip address 10.13.2.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan103
 description Cell Zone 2 IACS VLAN
 ip address 10.13.3.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan104
 description Cell Zone 2 Workstation VLAN
 ip address 10.13.4.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan105
 description Cell Zone 2 Voice VLAN
 ip address 10.13.5.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
```

```
!
interface Vlan106
 description Cell Zone 3 IACS VLAN
 ip address 10.13.6.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan107
 description Cell Zone 3 Workstation VLAN
 ip address 10.13.7.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan108
 description Cell Zone 3 Voice VLAN
 ip address 10.13.8.1 255.255.255.0
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
interface Vlan115
 description Management VLAN
 ip address 10.13.15.1 255.255.255.128
 ip helper-address 10.13.48.10
 ip pim sparse-mode
!
router eigrp 101
 network 10.13.0.0 0.0.255.255
 passive-interface default
 eigrp router-id 10.13.15.254
 nsf
!
no ip http server
ip http authentication aaa
ip http secure-server
!
ip pim autorp listener
ip pim send-rp-announce Loopback1 scope 32 group-list 10
ip pim send-rp-discovery Loopback0 scope 32
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
access-list 10 permit 239.1.0.0 0.0.255.255
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.13.48.15
 key 7 04680E051D2458650C00
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.13.48.17
end
```

Access Layer Configurations

CZ1-IE2K-1

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname CZ1-IE2K-1
!
boot-start-marker
boot-end-marker
!
```

```
enable secret 5 $1$r9g5$1SkSAiFWL9xcGECtFSa5o1
!
username admin password 7 15115A1F07257A767B
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
system mtu routing 1500
ip arp inspection vlan 101-102
!
ip dhcp snooping vlan 101-102
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name cisco.local
ip name-server 10.13.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34 35
36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42 44
45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54 56
57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31 43
46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30 32
33 34 35 36
```

```
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39 40
41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51 52
53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61 62
63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47 48
55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos
!
crypto pki trustpoint TP-self-signed-1283359360
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1283359360
 revocation-check none
 rsakeypair TP-self-signed-1283359360
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
port-channel load-balance src-dst-ip
!
alarm profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
vlan internal allocation policy ascending
!
vlan 100
 name CZ1-IACS
!
vlan 101
 name CZ1-Workstation
!
vlan 102
 name CZ1-Voice
!
vlan 115
 name Management
!
vlan 999
!
ip ssh version 2
lldp run
!
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all voip-data
  match ip dscp ef
class-map match-all voip-control
  match ip dscp cs3
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
   set ip dscp 55
 class CIP-Implicit_dscp_47
```

```
   set ip dscp 47
 class CIP-Implicit_dscp_43
   set ip dscp 43
 class CIP-Implicit_dscp_any
   set ip dscp 31
 class CIP-Other
   set ip dscp 27
 class 1588-PTP-Event
   set ip dscp 59
 class 1588-PTP-General
   set ip dscp 47
policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
!
macro name CiscoIEPhone
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 service-policy input Voice-Map
@
macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@
macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
!
interface Port-channel1
 description EtherChannel link to Distribution Layer
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
!
interface FastEthernet1/1
 description Cell/Area Zone - IACS Access Port
 switchport access vlan 100
 switchport mode access
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 macro description CiscoEtherNetIP
 storm-control broadcast level 3.00 1.00
 spanning-tree portfast
 service-policy input CIP-PTP-Traffic
!
interface FastEthernet1/2
 description Cell/Area Zone - Workstation/VoIP Access Port
 switchport access vlan 101
 switchport mode access
 switchport voice vlan 102
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
```

```
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description CiscoIEPhone
 spanning-tree portfast
 service-policy input Voice-Map
 ip verify source
 ip dhcp snooping limit rate 100
!
interface FastEthernet1/3
 shutdown
!
interface FastEthernet1/4
 shutdown
!
interface GigabitEthernet1/1
 description Link to Distribution Layer port 1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface GigabitEthernet1/2
 description Link to Distribution Layer port 2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan115
 ip address 10.13.15.5 255.255.255.128
!
ip default-gateway 10.13.15.1
no ip http server
ip http authentication aaa
ip http secure-server
!
ip access-list extended default-data-acl
 permit ip any any
logging esm config
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
snmp-server community cisco RO
snmp-server community cisco123 RW
tacacs server TACACS-SERVER-1
```

```
 address ipv4 10.13.48.15
 key 7 04680E051D2458650C00
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp server 10.13.48.17
end
```

CZ2-2960S-1

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname CZ2-2960S-1
!
boot-start-marker
boot-end-marker
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
username admin password 7 070C705F4D06485744
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c2960s-24pd-l
ip arp inspection vlan 104-105
!
ip dhcp snooping vlan 104-105
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name cisco.local
ip name-server 10.13.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30 32
33 34 35 36
```

```
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39 40
41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51 52
53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61 62
63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47 48
55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos
!
crypto pki trustpoint TP-self-signed-3554231936
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3554231936
 revocation-check none
 rsakeypair TP-self-signed-3554231936
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 103
 name CZ2-IACS
!
vlan 104
 name CZ2-Workstation
!
vlan 105
 name CZ2-Voice
!
vlan 115
 name Management
!
vlan 999
!
ip ssh version 2
!
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all voip-data
  match ip dscp ef
class-map match-all voip-control
  match ip dscp cs3
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
   set ip dscp 55
 class CIP-Implicit_dscp_47
   set ip dscp 47
 class CIP-Implicit_dscp_43
   set ip dscp 43
 class CIP-Implicit_dscp_any
   set ip dscp 31
 class CIP-Other
```

```
   set ip dscp 27
 class 1588-PTP-Event
   set ip dscp 59
 class 1588-PTP-General
   set ip dscp 47
policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
!
macro name CiscoIEPhone
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 service-policy input Voice-Map
@
macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@
macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
!
interface Port-channel1
 description EtherChannel link to Distribution Layer
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 description Cell/Area Zone - IACS Access Port
 switchport access vlan 103
 switchport mode access
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 macro description CiscoEtherNetIP
 storm-control broadcast level 3.00 1.00
 spanning-tree portfast
 service-policy input CIP-PTP-Traffic
!
interface GigabitEthernet1/0/2
 description Cell/Area Zone - Workstation/VoIP Access Port
 switchport access vlan 104
 switchport mode access
 switchport voice vlan 105
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description CiscoIEPhone
```

```
 spanning-tree portfast
 service-policy input Voice-Map
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet1/0/3
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 1/0/4 - 1/0/24 are all configured
! the same as 1/0/3 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet1/0/25
 description Link to Distribution Layer port 1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/26
 description Link to Distribution Layer port 2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 103-105,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/1
 shutdown
!
interface TenGigabitEthernet1/0/2
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan115
 ip address 10.13.15.6 255.255.255.128
!
ip default-gateway 10.13.15.1
no ip http server
ip http authentication aaa
ip http secure-server
!
ip access-list extended default-data-acl
 permit ip any any
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
```

```
snmp-server community cisco RO
snmp-server community cisco123 RW
tacacs server TACACS-SERVER-1
 address ipv4 10.13.48.15
 key 7 00371605165E1F2D0A38
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp server 10.13.48.17
end
```

CZ3-3560X-1

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname CZ3-3560X-1
!
boot-start-marker
boot-end-marker
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
username admin password 7 070C705F4D06485744
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
system mtu routing 1500
ip arp inspection vlan 107-108
!
ip dhcp snooping vlan 107-108
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name cisco.local
ip name-server 10.13.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5
6 7
```

```
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34 35
36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42 44
45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54 56
57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31 43
46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30 32
33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39 40
41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51 52
53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61 62
63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47 48
55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos
!
crypto pki trustpoint TP-self-signed-1212907008
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1212907008
 revocation-check none
 rsakeypair TP-self-signed-1212907008
!
cts server deadtime 0
no cts server test all enable
cts server test all idle-time 0
cts server test all deadtime 0
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 106
 name CZ3-IACS
!
vlan 107
 name CZ3-Workstation
!
vlan 108
 name CZ3-Voice
!
vlan 115
 name Management
```

```
!
vlan 999
!
ip ssh version 2
!
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all voip-data
  match ip dscp ef
class-map match-all voip-control
  match ip dscp cs3
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
   set ip dscp 55
 class CIP-Implicit_dscp_47
   set ip dscp 47
 class CIP-Implicit_dscp_43
   set ip dscp 43
 class CIP-Implicit_dscp_any
   set ip dscp 31
 class CIP-Other
   set ip dscp 27
 class 1588-PTP-Event
   set ip dscp 59
 class 1588-PTP-General
   set ip dscp 47
policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
!
macro name CiscoIEPhone
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 service-policy input Voice-Map
@
macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@
macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
!
interface Port-channel1
 description EtherChannel link to Distribution Layer
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
```

```
 switchport trunk allowed vlan 106-108,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 description Cell/Area Zone - IACS Access Port
 switchport access vlan 106
 switchport mode access
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 macro description CiscoEtherNetIP
 storm-control broadcast level 3.00 1.00
 spanning-tree portfast
 service-policy input CIP-PTP-Traffic
!
interface GigabitEthernet0/2
 description Cell/Area Zone - Workstation/VoIP Access Port
 switchport access vlan 107
 switchport mode access
 switchport voice vlan 108
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 25 35 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description CiscoIEPhone
 spanning-tree portfast
 service-policy input Voice-Map
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/3
 shutdown
!
! ************************************************************
! Interface GigabitEthernet 0/4 - 0/5 are all configured
! the same as 0/3 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet1/1
 description Link to Distribution Layer port 1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 106-108,115
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface GigabitEthernet1/2
 description Link to Distribution Layer port 2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 106-108,115
```

```
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface TenGigabitEthernet1/1
 shutdown
!
interface TenGigabitEthernet1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan115
 ip address 10.13.15.7 255.255.255.128
!
ip default-gateway 10.13.15.1
no ip http server
ip http authentication aaa
ip http secure-server
!
ip access-list extended default-data-acl
 permit ip any any
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
snmp-server community cisco RO
snmp-server community cisco123 RW
tacacs server TACACS-SERVER-1
 address ipv4 10.13.48.15
 key 7 113A1C0605171F270133
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp server 10.13.48.17
end
```

Server Room Configuration

SR-3750X

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname SR-3750X
!
```

```
boot-start-marker
boot-end-marker
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
username admin password 7 04585A150C2E1D1C5A
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-24
switch 2 provision ws-c3750x-24
stack-mac persistent timer 0
system mtu routing 1500
!
ip domain-name cisco.local
ip name-server 10.13.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp  24 27 31 43 46 47 55 59 to 0
mls qos map dscp-cos  9 11 12 13 14 15 to 0
mls qos map dscp-cos  25 26 28 29 30 to 2
mls qos map dscp-cos  40 41 42 44 45 49 50 51 to 4
mls qos map dscp-cos  52 53 54 56 57 58 60 61 to 4
mls qos map dscp-cos  62 63 to 4
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input bandwidth 40 60
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue input dscp-map queue 1 threshold 3 18 19 20 21
22 23 25 26
mls qos srr-queue input dscp-map queue 1 threshold 3 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34 35
36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42 44
45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54 56
57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31 43
46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12 13
14 15 16 17
mls qos srr-queue output dscp-map queue 2 threshold 3 18 19 20 21
22 23 25 26
```

```
mls qos srr-queue output dscp-map queue 2 threshold 3 28 29 30 32
33 34 35 36
mls qos srr-queue output dscp-map queue 2 threshold 3 37 38 39 40
41 42 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 49 50 51 52
53 54 56 57
mls qos srr-queue output dscp-map queue 2 threshold 3 58 60 61 62
63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47 48
55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
no mls qos rewrite ip dscp
mls qos
!
crypto pki trustpoint TP-self-signed-157229824
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-157229824
 revocation-check none
 rsakeypair TP-self-signed-157229824
!
cts server deadtime 0
no cts server test all enable
cts server test all idle-time 0
cts server test all deadtime 0
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 115
 name Management
!
vlan 148
 name Server_VLAN_1
!
vlan 149
 name Server_VLAN_2
!
vlan 999
!
ip ssh version 2
!
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all voip-data
  match ip dscp ef
class-map match-all voip-control
  match ip dscp cs3
class-map match-all default-data
  match access-group name default-data-acl
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
   set ip dscp 55
 class CIP-Implicit_dscp_47
   set ip dscp 47
 class CIP-Implicit_dscp_43
```

```
   set ip dscp 43
 class CIP-Implicit_dscp_any
   set ip dscp 31
 class CIP-Other
   set ip dscp 27
 class 1588-PTP-Event
   set ip dscp 59
 class 1588-PTP-General
   set ip dscp 47
policy-map Voice-Map
 class voip-data
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class voip-control
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class default-data
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
!
macro name CiscoIEEgress
 mls qos trust cos
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
@
macro name CiscoEtherNetIP
 service-policy input CIP-PTP-Traffic
 priority-queue out
 srr-queue bandwidth share 1 19 40 40
@
!
interface Port-channel1
 description EtherChannel Link to Distribution
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149
 switchport mode trunk
 logging event link-status
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 macro description CiscoEtherNetIP
 spanning-tree portfast
 service-policy input CIP-PTP-Traffic
!
! ************************************************************
! Interface GigabitEthernet 1/0/2 - 1/0/24 are all configured
! the same as 1/0/1 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet1/1/1
 description Link to Distribution port 1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/1/2
 shutdown
```

```
!
interface GigabitEthernet1/1/3
 shutdown
!
interface GigabitEthernet1/1/4
 shutdown
!
interface TenGigabitEthernet1/1/1
 shutdown
!
interface TenGigabitEthernet1/1/2
 shutdown
!
interface GigabitEthernet2/0/1
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 macro description CiscoEtherNetIP
 spanning-tree portfast
 service-policy input CIP-PTP-Traffic
!
! ************************************************************
! Interface GigabitEthernet 2/0/2 - 2/0/24 are all configured
! the same as 2/0/1 and have been removed for conciseness
! ************************************************************
!
interface GigabitEthernet2/1/1
 description Link to Distribution port 2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 19 40 40
```

Notes

```
 macro description CiscoIEEgress
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet2/1/2
 shutdown
!
interface GigabitEthernet2/1/3
 shutdown
!
interface GigabitEthernet2/1/4
 shutdown
!
interface TenGigabitEthernet2/1/1
 shutdown
!
interface TenGigabitEthernet2/1/2
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan115
 ip address 10.13.15.50 255.255.255.128
!
ip default-gateway 10.13.15.1
no ip http server
ip http authentication aaa
ip http secure-server
!
ip access-list extended default-data-acl
 permit ip any any
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
```

```
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
snmp-server community cisco RO
snmp-server community cisco123 RW
tacacs server TACACS-SERVER-1
 address ipv4 10.13.48.15
 key 7 13361211190910012E3D
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp server 10.13.48.17
end
```

Feedback

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

SMART BUSINESS ARCHITECTURE

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.

B-0000168-1 2/13