Networking and Security in Industrial Automation Environments

Executive Summary

Industrial companies are seeking to drive operational improvements into their production systems and assets through convergence and digitization by leveraging the new paradigms in Industrial Internet of Things (IIoT) and Industry 4.0. However, these initiatives require securely connecting production environments via standard networking technologies to allow companies and their key partners access to a rich stream of new data, real-time visibility, and when needed remote access to the systems and assets in the operational environments.

New data and visibility are the key to IIoT and Industry 4.0 initiatives that unlock new business value and transformational use cases. The industrial ecosystem is seeking to continuously improve efficiency, reduce costs, and increase Overall Equipment Effectiveness (OEE) through better access to information from real-time production systems in industrial areas. With a constant flow of data, industrial companies can develop more efficient ways to connect globally with suppliers, employees, and partners and to more effectively meet the needs of their customers. Securely connecting to plant systems and assets for improved access to new data is the key to enabling use cases such as predictive maintenance, real-time quality detection, asset tracking, and safety enhancements.

The Cisco® Industrial Automation solution and relevant product technologies are an essential foundation to securely connect and digitize industrial and production environments to achieve these significantly improved business operation outcomes. The Cisco solution overcomes top customer barriers to digitization and Industry 4.0 including security concerns, inflexible legacy networks, and complexity. The solution provides a proven and validated blueprint for connecting Industrial Automation and Control Systems (IACS) and production assets, improving industrial security, and improving plant data access and operating reliability. Following this best practice blueprint with Cisco market-leading technologies will help decrease deployment time, decrease risk, decrease complexity, and improve overall security and operating uptime.

Figure 1 Industrial Automation Customer Objectives and Challenges
Executive Summary

Figure 2  Why Industrial Automation Solution?

Industrial Automation Reference Architecture

The Industrial Automation Cisco Validated Design (CVD) solution applies network, security, and data management technologies to Industrial Automation and Control System (IACS) plant environments and key production assets that are the core to operational environments. It provides a Cisco validated reference architecture and design and deployment guidance for customers, partners, and system implementers. This solution is comprehensively tested with a wide range of industrial devices (e.g., sensors, actuators, controllers, remote terminal units, etc.), applications, and partners. This solution’s features include high-speed connectivity, scalability, high availability, ease of use, market leading industrial security, open standards, precise time distribution, and enablement of alignment and connection of information technology (IT) and operational technology (OT) environments. The solution is meant to be applied in a range of industrial verticals for secure networking of Industrial Automation systems including manufacturing, mining, oil and gas, and utility companies and for places such as plants, factories, refineries, mines, treatment facilities, substations, and warehouses.

This solution provides a blueprint for the essential security and connectivity foundation required to deploy and implement Industry 4.0 and IIoT concepts and models. This solution is thus the key to digitizing industrial and production environments to achieve significantly improved business operation outcomes.
Cross-Industry Applicability

This Industrial Automation solution encompasses networking, security, and data management applied to a wide range of industrial verticals and applications, providing a range of design and implementation alternatives that may be applicable to several industries. Although the size, vendors, applications, and devices may significantly vary among these facilities, many of the core networking and security concepts are applicable. For example, while high availability is a key requirement across all industrial use cases, oil and gas and utilities may have more stringent availability requirements than a manufacturing facility. Nonetheless, the CVD solution best practice guidance is applicable across many industries and industrial customer environments.
## Executive Summary

<table>
<thead>
<tr>
<th>Business Imperatives</th>
<th>Manufacturing</th>
<th>Utility Substation</th>
<th>Oil and Gas Plant</th>
<th>Mining Production</th>
<th>Waste Water</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximize uptime and quality</strong></td>
<td>Retain and acquire customers</td>
<td>Maximize uptime and quality</td>
<td>Increased mechanization through automated plant</td>
<td>Maximize uptime and quality</td>
<td></td>
</tr>
<tr>
<td><strong>Improve safety, security, and reliability</strong></td>
<td>Improve safety, security, and reliability</td>
<td>Improve safety, security, and reliability</td>
<td>Improve safety, security, and reliability</td>
<td>Improve safety, security, and reliability</td>
<td></td>
</tr>
<tr>
<td><strong>Drive predictive maintenance, machine learning, and Digital Twin applications</strong></td>
<td>Integrate new energy sources and consumption models</td>
<td>Improve decision making and drive machine learning</td>
<td>Optimization of material and equipment flow</td>
<td>Drive predictive maintenance</td>
<td></td>
</tr>
<tr>
<td><strong>Connect factory to partners and suppliers</strong></td>
<td>Modernize the utility grid</td>
<td>Connect Refinery and Pipeline to partners and suppliers</td>
<td>Monitoring of real-time performance</td>
<td>Monitoring of real-time performance</td>
<td></td>
</tr>
<tr>
<td><strong>Retain and acquire customers</strong></td>
<td></td>
<td></td>
<td>Maximized production</td>
<td>Maximized production</td>
<td></td>
</tr>
<tr>
<td><strong>Improve safety, security, and reliability</strong></td>
<td></td>
<td></td>
<td>Increased mechanization through automated plant</td>
<td>Improved safety, security, and reliability</td>
<td></td>
</tr>
<tr>
<td><strong>Drive predictive maintenance, machine learning, and Digital Twin applications</strong></td>
<td></td>
<td></td>
<td>Improved decision making and drive machine learning</td>
<td>Drive predictive maintenance</td>
<td></td>
</tr>
<tr>
<td><strong>Connect factory to partners and suppliers</strong></td>
<td></td>
<td></td>
<td>Connect Refinery and Pipeline to partners and suppliers</td>
<td>Monitoring of real-time performance</td>
<td></td>
</tr>
<tr>
<td><strong>Increased mechanization</strong></td>
<td></td>
<td></td>
<td>Improved safety, security, and reliability</td>
<td>Maximized production</td>
<td></td>
</tr>
<tr>
<td><strong>Integrate new energy sources and consumption models</strong></td>
<td></td>
<td></td>
<td>Optimization of material and equipment flow</td>
<td>Maximized production</td>
<td></td>
</tr>
<tr>
<td><strong>Modernize the utility grid</strong></td>
<td></td>
<td></td>
<td>Monitoring of real-time performance</td>
<td>Monitoring of real-time performance</td>
<td></td>
</tr>
<tr>
<td><strong>Access production assets and data</strong></td>
<td>Access production assets and data</td>
<td>Access production assets and data</td>
<td>Access production assets and data</td>
<td>Access production assets and data</td>
<td></td>
</tr>
<tr>
<td><strong>Security risks</strong></td>
<td>Security risks</td>
<td>Security risks</td>
<td>Security risks</td>
<td>Security risks</td>
<td></td>
</tr>
<tr>
<td><strong>Complex network silos creating downtime, data isolation, and vulnerabilities. Inflexible and high operating costs</strong></td>
<td>Aging infrastructure</td>
<td>Managing and securing silo proprietary applications and networks is costly</td>
<td>Complex network silos creating downtime, data isolation, and vulnerabilities</td>
<td>Complex network silos creating downtime, data isolation, and vulnerabilities</td>
<td></td>
</tr>
<tr>
<td><strong>Expertise to manage data, networks, and security</strong></td>
<td>Expertise to manage data, networks, and security</td>
<td>Expertise to manage data, networks, and security</td>
<td>Expertise to manage data, networks, and security</td>
<td>Expertise to manage data, networks, and security</td>
<td></td>
</tr>
<tr>
<td><strong>Asset reliability</strong></td>
<td>Asset reliability</td>
<td>Asset reliability</td>
<td>Asset reliability</td>
<td>Asset reliability</td>
<td></td>
</tr>
<tr>
<td><strong>People and asset optimization</strong></td>
<td>People and asset optimization</td>
<td>People and asset optimization</td>
<td>People and asset optimization</td>
<td>People and asset optimization</td>
<td></td>
</tr>
<tr>
<td><strong>Security risks</strong></td>
<td>Security risks</td>
<td>Security risks</td>
<td>Security risks</td>
<td>Security risks</td>
<td></td>
</tr>
<tr>
<td><strong>Employee safety</strong></td>
<td>Employee safety</td>
<td>Employee safety</td>
<td>Employee safety</td>
<td>Employee safety</td>
<td></td>
</tr>
<tr>
<td><strong>Complex network silos creating downtime, data isolation, and vulnerabilities</strong></td>
<td>Complex network silos creating downtime, data isolation, and vulnerabilities</td>
<td>Complex network silos creating downtime, data isolation, and vulnerabilities</td>
<td>Complex network silos creating downtime, data isolation, and vulnerabilities</td>
<td>Complex network silos creating downtime, data isolation, and vulnerabilities</td>
<td></td>
</tr>
<tr>
<td><strong>Inflexible networks and high operating costs</strong></td>
<td></td>
<td></td>
<td>Rising costs of maintenance, equipment, and supplies</td>
<td>Rising costs of maintenance, equipment, and supplies</td>
<td></td>
</tr>
<tr>
<td><strong>Expertise to manage data, networks, and security</strong></td>
<td></td>
<td></td>
<td>Dealing with leakage issues, especially in drought-impacted countries</td>
<td>Dealing with leakage issues, especially in drought-impacted countries</td>
<td></td>
</tr>
<tr>
<td><strong>Asset reliability</strong></td>
<td></td>
<td></td>
<td>Managing facilities within geographic areas with fewer personnel</td>
<td>Managing facilities within geographic areas with fewer personnel</td>
<td></td>
</tr>
<tr>
<td><strong>People and asset optimization</strong></td>
<td></td>
<td></td>
<td>Remaining compliant with changing regulations</td>
<td>Remaining compliant with changing regulations</td>
<td></td>
</tr>
<tr>
<td><strong>Security risks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Employee safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Complex network silos creating downtime, data isolation, and vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Inflexible networks and high operating costs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Expertise to manage data, networks, and security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Asset reliability</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>People and asset optimization</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security risks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Employee safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Complex network silos creating downtime, data isolation, and vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rising costs of maintenance, equipment, and supplies</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dealing with leakage issues, especially in drought-impacted countries</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Managing facilities within geographic areas with fewer personnel</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Remaining compliant with changing regulations</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Executive Summary

### Table 1 Cross-Industry Applicability—Part 2 of 2

<table>
<thead>
<tr>
<th>Cisco Industrial Automation Solution Features</th>
<th>Manufacturing</th>
<th>Utility Substation</th>
<th>Oil and Gas Plant</th>
<th>Mining Production</th>
<th>Waste Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>High availability</td>
<td>High availability</td>
<td>High availability</td>
<td>High availability</td>
<td>High availability</td>
<td>High availability</td>
</tr>
<tr>
<td>One solution that is interoperable across all major industrial control system protocols</td>
<td>One solution that is interoperable across all major industrial control system protocols</td>
<td>One solution that is interoperable across all major industrial control system protocols</td>
<td>One solution that is interoperable across all major industrial control system protocols</td>
<td>One solution that is interoperable across all major industrial control system protocols</td>
<td>One solution that is interoperable across all major industrial control system protocols</td>
</tr>
<tr>
<td>End-to-end connectivity for data visibility (not physically segmented)</td>
<td>End-to-end connectivity for data visibility (not physically segmented)</td>
<td>End-to-end connectivity for data visibility (not physically segmented)</td>
<td>End-to-end connectivity for data visibility (not physically segmented)</td>
<td>End-to-end connectivity for data visibility (not physically segmented)</td>
<td>End-to-end connectivity for data visibility (not physically segmented)</td>
</tr>
<tr>
<td>Integrated security at all levels (that works for OT and IT)</td>
<td>Integrated security at all levels (that works for OT and IT)</td>
<td>Integrated security at all levels (that works for OT and IT)</td>
<td>Integrated security at all levels (that works for OT and IT)</td>
<td>Integrated security at all levels (that works for OT and IT)</td>
<td>Integrated security at all levels (that works for OT and IT)</td>
</tr>
<tr>
<td>Real-time, deterministic</td>
<td>Real-time, deterministic</td>
<td>Real-time, deterministic</td>
<td>Real-time, deterministic</td>
<td>Real-time, deterministic</td>
<td>Real-time, deterministic</td>
</tr>
<tr>
<td>Industrial best practice designed</td>
<td>Industrial best practice designed</td>
<td>Industrial best practice designed</td>
<td>Industrial best practice designed</td>
<td>Industrial best practice designed</td>
<td>Industrial best practice designed</td>
</tr>
<tr>
<td>Intent-based ease of use</td>
<td>Intent-based ease of use</td>
<td>Intent-based ease of use</td>
<td>Intent-based ease of use</td>
<td>Intent-based ease of use</td>
<td>Intent-based ease of use</td>
</tr>
<tr>
<td>Flexibility (modularity)</td>
<td>Flexibility (modularity)</td>
<td>Flexibility (modularity)</td>
<td>Flexibility (modularity)</td>
<td>Flexibility (modularity)</td>
<td>Flexibility (modularity)</td>
</tr>
</tbody>
</table>

### Customer Benefits

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Manufacturing</th>
<th>Utility Substation</th>
<th>Oil and Gas Plant</th>
<th>Mining Production</th>
<th>Waste Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliable plant operations—higher uptime and OEE from improved data visibility</td>
<td>Increased operational reliability</td>
<td>Improve reliability and manage risks</td>
<td>OEE and availability</td>
<td>Secure utility information management</td>
<td></td>
</tr>
<tr>
<td>Lower costs and scrap through improved real-time process visibility</td>
<td>Real-Time data visibility</td>
<td>Reduce waste and processing</td>
<td>Increased production</td>
<td>Reduced risk from security attacks</td>
<td></td>
</tr>
<tr>
<td>Lower costs from reduced OpEx—Easy to configure, upgrade, replace, and maintain</td>
<td>Reduced risk from security attacks</td>
<td>Increased operational reliability</td>
<td>Safety and environmental compliance</td>
<td>Remote monitoring</td>
<td></td>
</tr>
<tr>
<td>Secure plant operation</td>
<td>Reliable network for time-sensitive and mission-critical communications</td>
<td>Shorten turnaround times</td>
<td>Reduced OpEx—Easy to configure, upgrade, replace, and maintain</td>
<td>High availability</td>
<td></td>
</tr>
<tr>
<td>Less downtime</td>
<td>High availability</td>
<td>Minimize fines and penalties</td>
<td>Wireless to wireline to securely connect machines and people for agility and safety</td>
<td>Reduced OpEx—Easy to configure, upgrade, replace, and maintain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real-time visibility</td>
<td>Improve worker safety and environmental compliance</td>
<td>Improved safety and productivity of staff</td>
<td>Safety and environmental compliance</td>
<td></td>
</tr>
</tbody>
</table>
Executive Summary

Evolving Plant Environment

Over the past decade or so, the pace of change in the Industrial Automation space has clearly accelerated, driven largely by technology improvements epitomized by terms such as Industrial Internet of Things, Fog/Edge computing, Smart Factories, and Industry 4.0—the 4th revolution in industrial capabilities and digitization. This section examines some of these trends and how this solution is aligned to enable them.

Industrial Internet of Things (IIoT)

The Industrial Internet of Things is based on the idea that the growth of connected devices is more and more driven not by computers and mobile devices used by humans, but by things used in all forms of automation and in the control of the industrial ecosystem. The industrial ecosystem is turning away from the use of proprietary networking technologies, sometime called fieldbus technologies, to the use of open, standard networking such as Ethernet, WiFi, IP, etc. This focus on open networking standards is a foundational aspect—the devices or “things” that make up the industrial ecosystem are capable of communicating on converged, open networks, which significantly improves the accessibility of data and information. This IIoT therefore enables Digital Transformation and the revolution of the industrial ecosystem referred to as Industrie 4.0. This solution, by driving converged, open networks into these industrial ecosystems establishes the IIoT for customers who adopt it.

Industry 4.0

Industry 4.0 is based on the idea that manufacturing (and also utilities, mining, and oil and gas) is going through a fourth industrial revolution. It can be seen as the summation of industrial and computing trends. At the heart is the concept that physical devices, machines, and processes can be tightly controlled and operated significantly better by combing them with cyber-systems, IIoT, cloud computing, artificial intelligence, machine learning, and other relevant technologies.

Industry 4.0 outlines four key design principles:

- Interconnection—The ability of machines, devices, sensors, and people to connect and communicate with each other via the Internet of Things (IoT) or the Internet of People (IoP).
- Information transparency—The transparency afforded by Industry 4.0 technology provides operators with vast amounts of useful information needed to make appropriate decisions. Interconnectivity allows operators to collect immense amounts of data and information from all points in the manufacturing process, thus aiding functionality and identifying key areas that can benefit from innovation and improvement.
- Technical assistance—First, the ability of assistance systems to support humans by aggregating and visualizing information comprehensively for making informed decisions and solving urgent problems on short notice. Second, the ability of cyber physical systems to physically support humans by conducting a range of tasks that are unpleasant, too exhausting, or unsafe for their human co-workers.
- Decentralized decisions—The ability of cyber physical systems to make decisions on their own and to perform their tasks as autonomously as possible. Only in the case of exceptions, interferences, or conflicting goals are tasks delegated to a higher level.

The Cisco Industrial Automation solution is a foundational aspect of an Industry 4.0 approach, focusing heavily on the interconnection and cybersecurity of industrial environments, but also providing information transparency through data management capabilities, technical assistance through remote connectivity and collaboration capabilities, as well as decentralized decisions with the fog/edge computing capabilities.

Cisco Industrial Automation Solution Features

This Industrial Automation solution applies the best information technology (IT) capabilities and expertise tuned and aligned with operation technology (OT) requirements and applications and delivers for industrial environments:

- High Availability for all key industrial communication and services
- Real-time, deterministic application support with low network latency and jitter for the most challenging applications, such as motion control
Networking and Security in Industrial Automation Environments

Executive Summary

- Deployable in a range of industrial environmental conditions with Industrial-grade as well as commercial-off-the-shelf (COTS) IT equipment
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s) deployments
- Intent-based manageability and ease-of-use to facilitate deployment and maintenance especially by OT personnel with limited IT capabilities and knowledge
- Compatible with industrial vendors, including Rockwell Automation, Schneider Electric, Siemens, Mitsubishi Electric, Emerson, Honeywell, Omron, and SEL
- Reliance on open standards to ensure vendor choice and protection from proprietary constraints
- Distribution of Precise Time across the site to support motion applications and Schedule of Events data collection
- Converged network to support communication from sensor to cloud enabling many Industry 4.0 use cases
- IT-preferred security architecture integrating OT context and applicable and validated for Industrial applications (achieves best practices for both OT and IT environments)

Solution Benefits for Industrial Environments

Benefits of securely connecting industrial automation systems via deploying this solution and the relevant Cisco technologies include:

- Reduce risk in the production environment through industry-leading security
- Improve operational equipment effectiveness (OEE) and asset utilization through increased production availability and increased control system and asset visibility
- Reduce product defects through early indication of quality impacting events or conditions
- Faster deployment of new lines or line modifications or new plants
- Faster troubleshooting of equipment (with reduction in connectivity or security-related downtime)

What’s New for Industrial Environments in this CVD?

This solution leverages and extends existing documentation and testing, as indicated in the executive summary. This version relies on that body of work and incorporates new products and technologies to further enhance the offer. Solution enhancements include:

- **Industrial Automation**—Introduction of one validated, best practice solution architecture that enables multiple industry verticals and interoperability across multiple industrial control system and device vendors and protocols
- **Introduction of Cisco Software-Defined Access (SDA) Ready platforms**—The Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 Rugged Series switches and Cisco Catalyst 9300 and Cisco Catalyst 9500 Series switches
- **High-availability**—Additional lossless resiliency capabilities with enhanced support for Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) protocols
- **IT Security to Cell/Area Zone**—Additional security capabilities for device and traffic visibility, segmentation, and anomaly detection (including leverage of TrustSec, Identity Services, and enhanced segmentation in industrial environments)
- **Site-wide Precision Time distribution**—Support for site-wide precise time to enable challenging IACS applications (e.g., Motion Control) and data/event collection with precise timestamps (e.g., Sequence of Events)
Note on SDA-Ready Platforms—The Cisco Catalyst 9300 switch was introduced and validated as the distribution switch for the Cell/Area Zone. The Cisco Catalyst 9300 platform currently supports Software-Defined Access, which provides automated end-to-end segmentation to separate user, device, and application traffic without redesigning the network. SDA automates user access policy so organizations can make sure the right policies are established for any user or device with any application across the network. Ease of management and intent-driven networking with policy will be valuable additions for the industrial plant environments. However, SDA is not yet ready for deployment to support industrial plant environments. The new platforms are being positioned in the architecture to prepare for when SDA is able to support industrial plant requirements and protocols.

Intended Audience

This CVD solution is intended for anyone deploying IACS systems. The solution provides industrial automation network and security design and implementation guidance for vendors, partners, system implementers, customers, and service providers involved in designing, deploying, or operating production systems. This design and implementation guide provides a comprehensive explanation of the Cisco recommended networking and security for IACS. It includes information about the system architecture, possible deployment models, and guidelines for implementation and configuration. This guide also recommends best practices when deploying the validated reference architecture.

Industrial Automation Architecture Considerations

The section provides foundational concepts, building blocks, and considerations for Industrial Automation environments.

Plant Logical Framework

The 20th century saw a significant increase in the output of industrial processes and verticals, from utilities to process and discrete manufacturing. These developments were largely driven through automation and control technology advancements including the invention of the programmable logic controllers (PLCs), industrial robots, computerized-numeric control machines (machine tools), and the like; these paired with software-based applications, such as SCADA, Manufacturing Execution System (MES), and Historian and Asset Management systems launched IACS.

To understand the security and network systems requirements of an IACS, this DIG uses a logical framework to describe the basic functions and composition of an industrial system. The Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) is a common and well-understood model in the industry that segments devices and equipment into hierarchical functions. Based on this segmentation of IACS technology, the International Society of Automation ISA-99 Committee for Industrial and Control Systems Security and IEC 62443 Industrial Cybersecurity framework have identified the levels and logical framework shown in Figure 3. Each zone and the related levels are then subsequently described in detail in the section “Industrial Automation and Control System Reference Model” in Chapter 2 of the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:
Networking and Security in Industrial Automation Environments

Industrial Automation Architecture Considerations

This model identifies levels of operations and defines each level. In this CVD, levels refer to this concept of levels of operations. The Open Systems Interconnection (OSI) reference model, which defines layers of network communications, is also commonly referred to when discussing network architectures. The OSI model refers to layers of network communication functions. In this CVD, unless specified, layers refer to layers of the OSI model.

Safety Zone—Safety in the Industrial Automation Control System

The need for safety is imperative in industrial environments. For example in a manufacturing environment, a robot can cause a fatal impact to personnel if proper safety procedures are not followed. Indeed, even when such procedures are followed, the robot can cause harm if it is under malicious control. Another example is Substation Automation, where the need for safety is crucial in such a high-voltage environment. As with robots in Manufacturing, a malicious actor could easily impact safety by simply engaging relays that were expected to provide isolation.

Safety in the IACS is so important that not only are safety networks isolated from (and overlaid on) the rest of the IACS, they typically have color-coded hardware and are subject to more stringent standards. In addition, Personal Protection Equipment (PPE) and physical barriers are required to promote safety. Industrial automation allows safety devices to coexist and interoperate with standard IACS devices on the same physical infrastructure, which reduces cost and improves operational efficiency.

Cell Area/Zones—Access and Control

The Cell/Area Zone is a functional area within a plant facility and many plants have multiple Cell/Area Zones. Larger plants might have “Zones” designated for fairly broad processes that have smaller subsets of “Cell Areas” within them where the process is broken down into ever smaller subsets. For example, in an automotive assembly plant, a “Zone” might be a Paint Shop—where unfinished chassis arrive from the Stamping Plant, are painted, and then proceed on to the rest of assembly. In this case, a “Cell” within that Zone might be a Cell for priming that feeds another Cell for base color and yet another cell for top coat.
Networking and Security in Industrial Automation Environments

Industrial Automation Architecture Considerations

Because most networks in this area carry both non-critical traffic (for example, Historian) as well as time critical, deterministic traffic (for control loops), managed switching with strict quality of service (QoS) requirements is necessary. All switches, routers, firewalls, and so on are strictly maintained. However, unmanaged switches do exist in the machine networks (but still not routers or firewalls), but these are only possible because of the highly controlled nature of the traffic. These unmanaged switches are preferred because of their boot time speed and ease of replacement, versus a fully-managed switch equipped with troubleshooting and monitoring capabilities.

This zone has essentially three levels of activity occurring, as described in the following subsections.

Level 0—Process

Level 0 consists of a wide variety of sensors and actuators involved in the basic industrial process. These devices perform the basic functions of the IACS, such as driving a motor, measuring variables, setting an output, and performing key functions such as painting, welding, bending, and so on. These functions can be very simple (temperature gauge) to highly complex (a moving robot).

These devices take direction from and communicate status to the control devices in Level 1 of the logical model. In addition, other IACS devices or applications may need to directly access Level 0 devices to perform maintenance or resolve problems on the devices. The main attributes of Level 0 devices are:

- Drive the real-time, deterministic communication requirements
- Measure the process variables and control process outputs
- Exist in challenging physical environments that drive topology constraints
- Vary according to the size of the IACS network from a small (10s) to a large (1000s) number of devices
- Once designed and installed, are not replaced all together until the plant line is overhauled or replaced, which is typically five or more years

Level 1—Basic Control

Level 1 consists of controllers that direct and manipulate the manufacturing process, primarily interfacing with the Level 0 devices (for example, I/O, sensors and actuators). In discrete environments, the controller is typically a programmable logic controller (PLC), whereas in process environments, the controller is referred to as a distributed control system (DCS). For the purposes of this solution architecture, “controllers” refers to multidiscipline controllers used across industries.

IACS controllers run industry-specific operating systems that are programmed and configured from engineering workstations. IACS controllers are modular computers that consist of some or all of the following:

- A controller that computes all the data and executes programs loaded onto it
- I/O or network modules that communicate with Level 0 devices, Level 2 human-machine interfaces (HMIs), or other Level 1 controllers
- Integrated or separate power modules that deliver power to the rest of the controller and potentially other devices

IACS controllers are the intelligence of the IACS, making the basic decisions based on feedback from the devices found at Level 0. Controllers act alone or in conjunction with other controllers to manage the devices and thereby the industrial process. Controllers also communicate with other functions in the IACS (for example, Historian, asset manager, and manufacturing execution system) in Levels 2 and 3. The controller performs as a director function in the Industrial zone, translating high-level parameters (for example, recipes) into executable orders, consolidating the I/O traffic from devices, and passing the I/O data on to the upper-level plant floor functions.

Thus, controllers produce IACS network traffic in three directions from a level perspective:

- Downward to the devices in Level 0 that they control and manage
- Peer-to-peer to other controllers to manage the IACS for a Cell/Area Zone
Networking and Security in Industrial Automation Environments

Industrial Automation Architecture Considerations

- Upward to HMs and information management systems in Levels 2 and 3

Level 2—Area Supervisory Control

Level 2 represents the applications and functions associated with the Cell/Area Zone runtime supervision and operation, which include:

- Operator interfaces or HMs
- Alarms or alerting systems
- Control room workstations

Depending on the size or structure of a plant, these functions may exist at the site level (Level 3). These applications communicate with the controllers in Level 1 and interface or share data with the site level (Level 3) or enterprise (Levels 4 to 5) systems and applications through the demilitarized zone (DMZ). These applications can be implemented on dedicated IACS vendor operator interface terminals or on standard computing equipment and operating systems such as Microsoft Windows. These applications are more likely to communicate with standard Ethernet and IP networking protocols and are typically implemented and maintained by the industrial organization.

Industrial Zone

The Industrial zone comprises the Cell/Area zones (Levels 0 to 2) and site-level (Level 3) activities. The Industrial zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant floor IACS operations are in this zone. To preserve smooth plant operations and functioning of the IACS applications and IACS network in alignment with standards such as IEC 62443, this zone requires clear logical segmentation and protection from Levels 4 and 5.

Level 3—Site Operations and Control

Level 3, the site level, represents the highest level of the IACS. This space is generally “carpeted space”—meaning it has HVAC with typical 19” rack-mounted equipment in hot/cold aisles utilizing commercial grade equipment.

As the name implies, this is where applications related to operating the site reside, where operating the site means the applications and services that are directly driving production. For example, what is generally not included at this level are the more Enterprise-centric applications such as Engineering Resource Planning (ERP) systems or Manufacturing Execution Systems (MES), as those applications tend to be more business management applications and therefore more closely aligned and integrated with Enterprise applications. Examples of services at this level would be Historians, control applications, network and IACS management software, and network security services. Control applications will vary greatly on the specifics of the plant. An example from an automotive assembly plant would be for a Paint Coordination application that might be directly controlling chassis coming from the Stamping Plant fed to Robotic Paint Controllers in the Paint zone. The Level 1 controllers (the Robotic Controller in this example) would often be ruggedized, require determinism for their control loops, and be at or near the actual operations. In contrast, the Paint Coordination applications at the Site level are not true control loop applications and can reside in carpeted space.

The systems and applications that exist at this level manage plantwide IACS functions. Levels 0 through 3 are considered critical to site operations. The applications and functions that exist at this level include the following:

- Level 3 IACS network
- Reporting (for example: cycle times, quality index, predictive maintenance)
- Plant historian
- Detailed production scheduling
- Site-level operations management
- Asset and material management
Networking and Security in Industrial Automation Environments

Industrial Automation Architecture Considerations

- Control room workstations
- Patch launch server
- File server
- Other domain services, for example Active Directory (AD), DHCP, Domain Name System (DNS), Windows Internet Naming Service (WINS), Network Time Protocol (NTP), Precision Time Protocol Grandmaster Clock, and so on
- Terminal server for remote access support
- Staging area
- Administration and control applications

The Level 3 IACS network may communicate with Level 1 controllers and Level 0 devices, function as a staging area for changes into the Industrial zone, and share data with the enterprise (Levels 4 and 5) systems and applications through the DMZ. These applications are primarily based on standard computing equipment and operating systems (Unix-based or Microsoft Windows). For this reason, these systems are more likely to communicate with standard Ethernet and IP networking protocols.

Additionally, because these systems tend to be more aligned with standard IT technologies, they may also be implemented and supported by personnel with IT skill sets.

Enterprise Zone

Level 4—Site Business Planning and Logistics

Level 4 is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. These functions and systems include wired and wireless access to enterprise network services such as the following:

- Access to the Internet and email (hosted in data centers)
- Non-critical plant systems such as manufacturing execution systems and overall plant reporting such as inventory, performance, and so on
- Access to enterprise applications such as SAP and Oracle (hosted in data centers)

Although important, these services are not viewed as critical to the IACS and thus the plant floor operations. Because of the more open nature of the systems and applications within the enterprise network, this level is often viewed as a source of threats and disruptions to the IACS network.

The users and systems in Level 4 often require summarized data and information from the lower levels of the IACS network. The network traffic and patterns here are typical of a branch or campus network found in general enterprises where approximately 90 percent of the network traffic goes to the Internet or to data center applications.

This level is typically under the management and control of the IT organization.

Level 5—Enterprise

Level 5 is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level. Often the external partner or guest access systems exist here, although it is not uncommon to find them in lower levels (Level 3) of the framework to gain flexibility that may be difficult to achieve at the enterprise level. However, this approach may lead to significant security risks if not implemented within IT security policy and standards.
The IACS must communicate with the enterprise applications to exchange manufacturing and resource data. Direct access to the IACS is typically not required. One exception to this would be remote access for management of the IACS by employees or partners such as system integrators and machine builders. Access to data and the IACS network must be managed and controlled through the DMZ to maintain the security, availability, and stability of the IACS.

The services, systems, and applications at this level are directly managed and operated by the IT organization.

**Industrial DMZ**

Although not part of Purdue reference model, the industrial automation solution includes a DMZ between the Industrial and Enterprise zones. The industrial DMZ is deployed within plant environments to separate the enterprise networks and the operational domain of the plant environment. Downtime in the IACS network can be costly and have a severe impact on revenue, so the operational zone cannot be impacted by any outside influences. Network access is not permitted directly between the enterprise and the plant, however, data and services are required to be shared between the zones, thus the industrial DMZ provides architecture for the secure transport of data. Typical services deployed in the DMZ include remote access servers and mirrored services. Further details on the design recommendations for the industrial DMZ can be found later in this guide.

As with IT network DMZs, the industrial DMZ is there to primarily be a buffer between the plant floor and the Enterprise or the Internet—placing the most vulnerable services, such as email, web, and DNS servers, in this isolated network. The industrial DMZ not only isolates the factory from the outside world, but also from its own Enterprise networks. The primary reason this additional isolation is recommended is that, unlike Enterprise services, the plant floor contains the most critical services of the company—the services that produce the very product the company sells. Often applications on the plant floor are antiquated, running on vulnerable operating systems such as Windows 95. The industrial DMZ provides another level of security for these vulnerable systems.

Another key use of the industrial DMZ is for remote access, aiding troubleshooting of production equipment affecting the company product and therefore revenue. The risk of external access compounded with antiquated equipment underscores the need for some additional security measures. The details as to how the industrial DMZ is used for such services are described in later sections.

**Figure 5   Industrial Plant Reference Architecture with IDMZ**
IACS Requirements and Considerations

Operational Technology Application Requirements

OT applications at their core are focused on maintaining stability, continuity, and integrity of industrial processes. At the core is a loop of sensors, controllers, and actuators that must be maintained to properly operate the industrial processes. Additionally, a number of other applications need to gather information to display status, maintain history, and optimize the industrial process operations. From this standpoint, this solution outlines how to achieve a set of key requirements to support the OT applications, including:

- High availability as applications often have to run 24x7x365
- Focus on local, real-time communication between IACS devices requiring low latency and jitter in the communication to maintain the control loop integrity
- Ability to access diagnostic and telemetry information from IACS devices for IoT-based applications
- Challenge to update or change devices, software, or update configurations as the processes often run for extended periods of time
- Deployable in a range of industrial environmental conditions with industrial-grade as well as COTS IT equipment when applicable
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s) deployments
- Access to precise time for challenging applications such as Motion Control and Sequence of Events
- Simple and easy to use to management tools to facilitate deployment and maintenance, especially by OT personnel with limited IT capabilities and knowledge
- Use of open standards to ensure vendor choice and protection from proprietary constraints

Ruggedization and Environmental Requirements

Typical enterprise network devices reside in controlled environments, which is a key differentiator of the IACS from typical enterprise applications. The IACS end devices and network infrastructure are located in harsh environments that require compliance to environmental specifications such as IEC 529 (ingress protection) or National Electrical Manufacturers Association (NEMA) specifications. The IACS end devices and network infrastructure may be located in physically disparate locations and in non-controlled or even harsh environmental conditions such as temperature, humidity, vibration, noise, explosiveness, or electronic interference.

Due to these environmental considerations the IACS devices and network infrastructure must support and withstand these harsh conditions. Also DIN rail compliant form factor is ideal for industrial environments when compared to enterprise which typically reside in 19-inch rack mounts.

Performance in the Industrial Automation Control System

Performance is an important consideration for design of the network. Networking engineers in general have dealt with both latency and jitter for many years, especially in VoIP networks. However, in industrial automation networks, especially as the networking gets closer to the lower Purdue levels (ANSI/ISA 951/Purdue2 Level 0-1, machines, relays), the requirements for both latency and jitter become orders of magnitude more stringent than VoIP networks. Industrial automation network equipment is very demanding and some of these devices have limited software and processing capabilities, which makes them susceptible to network-related disruptions or extraneous communication. In addition, a very quickly changing manufacturing process (for example, a paper mill) or complex automation (for example, a multi-axis robot) demand very high levels of determinism—predictable inter-packet delay in the IACS. A lack of determinism in a network can fail and shut down an industrial process causing downtime which impacts the business. To support the level of determinism needed for industrial automation networks, the following must be considered:

- Marking the applications that need real-time traffic with high priority
Networking and Security in Industrial Automation Environments

Industrial Automation Architecture Considerations

- Creating a QoS policy that guarantees an appropriate bandwidth for the high priority traffic
- Planning an appropriate bandwidth on the network links

Availability is the most important aspect of IACS networks. This highlights another key difference with other non-industrial networking; while most IT networks have become more and more “business critical” over the years, they are generally not at the core of the business, but rather part of a service organization. In contrast, OT networking is business critical in that it is part of what the company actually does; when critical parts of the OT network go down, production stops and revenue is impacted. Note that some parts of the IACS network are more critical than others and therefore have higher availability requirements. Such criticality is ultimately translated into availability or Service Level Agreement (SLA) requirements, much of which can be seen in various parts of this CVD, but most notably in sections describing various ways of increasing availability such as sections describing resiliency protocols.

To achieve availability:

- No single point of failure for IACS network infrastructure. For example: redundant links, switches, Layer 3 devices, and firewalls.
- Implement network resiliency and convergence protocols which meet the IACS application requirements.
- Quick and easy zero-touch replacement of network devices in industrial environments.

Security

The traditional approach of security deployed in Industrial automation is “Security by obscurity”, which is to have a very closed air gap environment and implement proprietary protocols with no public access. The need for physical security can easily be seen in not only the examples above, but in real world examples such as Stuxnet (https://en.wikipedia.org/wiki/Stuxnet). Stuxnet demonstrated that “security by obscurity” and even “air-gapping” are insufficient security measures (more on those topics later). In addition to the Stuxnet example, the need for physical security can be seen with more generic “man-in-the-middle” attacks or simple “network taps”, where physical devices are inserted into the network. This intersection of physical and cybersecurity is generally a component of all Industrial Automation networks. The proprietary protocols were seen as being difficult to compromise and security incidents were more likely to be accidental. However, over the course of the last few years the industrial ecosystem has moved away from the use of proprietary network technologies to the use of open, standard networking such as Ethernet, WiFi, IP, and so on.

This approach of adding obscurity as a way of securing the networks does not meet the requirements of the current trends in industrial automation because:

- Proliferation of many devices in the plant floor-First, plant networks are increasingly using COTS technology products to perform operational tasks, replacing devices that were built from the ground up specifically for the process control environment. Second, many sensors are added to the plant floor as part of Big Data and Analytics, primarily to derive the data from the machines which can be used to enhance the productivity of the plant floor and also as a means to perform preventive maintenance on the equipment. These new devices support standard protocols and also may need access to certain resources such as cloud and internet.

- Convergence of IT and OT-Organizationally, IT and OT teams and tools, which were historically separate, have begun to converge, leading to more traditionally IT-centric solutions being introduced to support operational activities. As the borders between traditionally separate OT and IT domains blur, they must align strategies and work more closely together to ensure end-to-end security.

Security Characteristics

With these trends in the manufacturer networks, the following fundamental principles must be adopted by the plant network operator to ensure secure systems:

- Visibility of all devices in the plant network-Traditionally, enterprise devices such as laptops, mobile phones, printers, and scanners were identified by the enterprise management systems when these devices accessed the network. This visibility must be extended to all devices on the plant floor.
Network Architecture Considerations

- Segmentation and zoning of the network—Segmentation is a process of bounding the reachability of a device and zoning is defining a layer where all the members in that zone will have identical security functions. Providing zones in a network provides an organized way of managing access within and across the zone. Segmenting the devices further reduces the risk of spread of an infection when a device gets subjected to malware.

- Identification and restricted data flow—All the devices in the plant floor—enterprise (IT-managed) and operations (OT-managed)—must be identified, authenticated, and authorized and the network must enforce a policy when the users and IACS assets attach to the network.

- Network anomalies—Any unusual behavior in network activity must be detected and examined to determine if the change is intended or due to a malfunction of the device. Detecting network anomalies as soon as possible gives plant operations the means to remediate an abnormality in the network sooner, thereby reducing possible downtimes.

- Malware detection and mitigation—The unusual behavior displayed by an infected device must be detected immediately and the security tools should allow a remediation action to the infected device.

- Traditional firewalls are not typically built for industrial environments. There is a need for an industrial firewall which can perform deep packet inspection on industrial protocols to identify anomalies in IACS traffic flow.

- Secure infrastructure hardening of the networking assets in the plant floor.

- Adhering to the security standards—In the 1990s, the Purdue Reference Model and ISA 95 created a strong emphasis on architecture using segmented levels between various parts of the control system. This was further developed in ISA99 and IEC 62443, which brought focus to risk assessment and process. The security risk assessment will identify which PMSs are defined as critical control systems, non-critical control systems, and non-control systems.

Information Technology and Operational Technology Convergence

Historically, production environments and the IACS in them have been the sole responsibility of the operational organizations within enterprises. Enterprise applications and networks have been the sole responsibility of IT organizations. But as OT has started adopting standard networking, there has been a need to not only interconnect these environments, but to converge organizational capabilities and drive collaboration between vendors and suppliers.

Decisions impacting IACS networks are typically driven by plant managers and control engineers, rather than the IT department. Additionally, the IACS vendor and support supply chain are different than those typically used by the IT department. That being said, the IT departments of manufacturers are increasingly engaging with plant managers and control engineers to leverage the knowledge and expertise in standard networking technologies for the benefit of plant operations.
Cross-Industry Industrial Networking Requirements

Table 2 summarizes cross-industry industrial network requirements, challenges, and Industrial Automation Solution features to help customers achieve various business outcomes.
Table 2  Cross-Industry Industrial Networking Requirements—Part 1 of 2

<table>
<thead>
<tr>
<th>Industries</th>
<th>Cross Industry Industrial Network Requirements</th>
<th>Challenges</th>
<th>Industrial Automation Solution Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>High availability for all key communication and services</td>
<td>Solutions that work without downtime across all multiple control system vendors 24 x 7 operations  More than 99.999% (&quot;five 9s&quot;) of uptime expected Harsh environments No single point of failure High cost of downtime Expert resources not onsite to fix or debug</td>
<td>Proven to work with highest reliability with all leading control systems Rugged, high MTBF network infrastructure Maintains communication despite incidents with support with resilient topologies and protocols Redundant network services Simple device replacement Prioritization of IACS communication Protect communication resources from attack Enable rapid fault isolation and repair Securely enable remote access and remote management</td>
</tr>
<tr>
<td>Utilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub Station</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oil and Gas Plant</td>
<td>End-to-end connectivity to support communication from sensor to cloud—converged</td>
<td>Production environments air-gapped Islands of devices within production environments Need to replicate cell or machine implementations Multiple applications with varying priority Need for data from currently air-gapped systems</td>
<td>Securely access any IACS device or application for optimization Granular QoS to prioritize critical traffic Integrate replicated machines or cells deployments via various Layer 2 NAT Integrate plant networks into enterprise with the industrial DMZ model for secure data flow from edge to analytics</td>
</tr>
<tr>
<td>Mining</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Waste Water</td>
<td>Interoperability and reliance on open standards to ensure vendor choice and protection from proprietary constraints</td>
<td>Lots of proprietary protocols Often 100s or 1000s of device and system suppliers to be integrated Assets utilized for years or decades Multiple supplier strategies are commonplace</td>
<td>Based on modern, open networking standards such as IEEE, Ethernet, IP, Wi-Fi and IETF Proven to work with various industrial protocols (e.g. EtherNet/IP, PROFINET, Modbus, IEC 61850, CC-Link IE, DNP3, etc.) Backward compatibility required for network innovations</td>
</tr>
<tr>
<td>Water</td>
<td>Real-time, deterministic application support with low network latency and jitter for the most challenging applications, such as motion control</td>
<td>Precise schedule of events need to be auditable and traceable High-speed coordination and control requiring low latency and jitter networks Need to collect more and more data from every device</td>
<td>Precise, network-based time synchronization support High-speed network infrastructure Sophisticated QoS capability Converged network to support multiple application types</td>
</tr>
</tbody>
</table>
# Industrial Automation Architecture Considerations

<table>
<thead>
<tr>
<th>Industries</th>
<th>Cross Industry Industrial Network Requirements</th>
<th>Challenges</th>
<th>Industrial Automation Solution Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td><strong>Industrial designed</strong> for harsh environmental conditions</td>
<td>Broad range of harsh, environmental conditions including intrinsically safe Size is a expensive commodity Need to collect more and more data from every device</td>
<td>Purpose built for harsh industrial environments with the flexibility to also support and operate in intrinsically safe environments Precise, network-based time synchronization support High-speed network infrastructure Sophisticated QoS capability Converged network to support multiple application types</td>
</tr>
<tr>
<td>Utilities Sub Station</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oil and Gas Plant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mining Waster Water</td>
<td><strong>Security</strong> Stop threats and protect industrial operations Infrastructure</td>
<td>Insecure networking devices threaten overall plant Unpatched, legacy systems Lack of segmentation OT security skills Lack of visibility Limited remote Access Lack of threat monitoring for OT systems</td>
<td>Cisco networking HW and SW inherently secure and (secure root of trust and many other best practice capabilities) Ability to discover and classify assets in OT environments Ability to understand OT device behavior and identify Threats Ability to set up and enforce security policy in granular way (e.g., for contractor, remote vendor, which devices talk to which devices,) Active monitoring Network segmentation—from basic to advanced</td>
</tr>
<tr>
<td>Manageability</td>
<td>and ease of use to facilitate deployment and maintenance, especially by OT personnel with limited IT capabilities and knowledge</td>
<td>Lack of networking and security expertise Fast response to outages Limited capability of IACS devices Different toolsets used by IT and OT Upgrades very limited Assets used for extended time (years/decades)</td>
<td>Network supports industrial protocols for visibility and config by IACS applications Easy to replace network infrastructure Tools designed for OT and integrates with IT tools IT tools for scalable network and security management Templates to deploy key configurations Support plug n play for ease of use and fast repair and install</td>
</tr>
</tbody>
</table>
Industry Standards and Regulations

Standards and guidelines are an essential foundation, but they do not prescribe how to secure and design specific systems. As all systems are different, standards and guidelines should be leveraged as a best practice framework and specifically tailored to business needs. In this section, a few of the industry standards are briefly described and limited to those that are both generally applicable and generally applied.

ISA-95/PERA (Purdue)
ISA-95 and PERA provide a general architecture for all types of IACS, providing not only common nomenclature but also common building blocks. More details can be found at:

- ISA-95 web site
  https://isa-95.com/
- PERA web site
  http://www.pera.net/

IEC 62443/ISA-99
The IEC 62443 series builds on established standards for the security of general purpose IT systems (for example, the ISO/IEC 27000 series), identifying and addressing the important differences present in an industrial control system (ICS). Many of these differences are based on the reality that cybersecurity risks within an ICS may have Health, Safety, or Environment (HSE) implications and that the response should be integrated with other existing risk management practices addressing these risks.

NIST Cybersecurity Framework
The National Institute of Standards and Technology (NIST) Cybersecurity Framework (https://www.nist.gov/cyberframework) is a Best Practices guideline, not a requirements standard, the genesis of which came from the 2014 changes to the NIST National Institute of Standards and Technology Act, which was amended to add “…on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure.”

NIST 800 Series
The NIST 800 Series, as it is commonly called, is a set of documents from NIST covering U.S. government security policies, procedures, and guidelines. Although NIST is a U.S. government unit (under the Commerce Department), these guidelines are referenced and indeed mandated by not only the U.S. but many governments and corporations around the world—even those not directly involved in the public sector. In particular to this CVD and the associated CVDs, the subset called NIST SP 800-82 “Guide to Industrial Control Systems Security” is of particular importance as it is specifically targeted at the IACS space. The purpose of this document is to provide guidance for securing ICS, including SCADA systems, DCS, and other systems performing control functions. The document provides a notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. Additionally, it presents an ICS-tailored security control overlay, based on NIST SP 800-53 Rev. 4 [22], to provide a customization of controls as they apply to the unique characteristics of the ICS domain.

NERC CIP
NERC CIP, or more properly the “North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)”, as the name implies, is utility specific in origin, however it is widely referenced and adopted outside of the utility space. Also as its name implies, it targets “Critical Infrastructure Protection”, which is a widely used term and the subject of many standards, guidelines, and best practices (see https://en.wikipedia.org/wiki/Critical_infrastructure_protection for more details). NERC CIP in particular is used in this CVD and the associated CVDs primarily because it was developed around the particulars of the IACS infrastructure (and is therefore more highly relevant to the subject and hand as well utilizing much of the same terminology).
IEEE 1588 Precise Time Protocol (PTP)

Defined in IEEE1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, it was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead. PTP facilitates services which require extremely precise time accuracy and stability like peak-hour billing, virtual power generators, outage monitoring and management, etc.

PTP was originally developed in 2002. It was enhanced in 2008 (IEEE 1588-2008) and is referred to as PTPv2. This version establishes the basic concept and algorithms for distribution of precise time. These basics have been adopted into "profiles" that are specific definitions for distribution of time designed for particular use cases. The following PTP Profiles are:

- Default Profile—This profile was defined by the IEEE 1588 working group. It has been adopted in many industrial applications, including the ODVA, Inc.'s Common Industrial Profile (CIP) as CIP Sync services. This solution supports the default profile in the Sitewide Precise Time Distribution feature. As well, the Rockwell Automation and Cisco Converged Plantwide Ethernet (CPwE) solution supports the default profile in the Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture (https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html).

- Power Profile—This profile was defined by the International Electrotechnical Commission (IEC) standard 62439. The power profile is used in the IEC 61850 standard for communication protocol for substation automation. This profile is supported in the Cisco Substation Automation Local Area Network and Security CVD (https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG.html).

- Telecom Profile—The International Telecommunication Union’s Telecommunications Standards (ITU-T) group has established a set of PTP profiles for the telecoms industries. A variety of Cisco products support these profiles, but are not commonly used in Industrial Automation. This profile is not supported in this solution.

- IEEE 802.1 AS profile—The IEEE created the Timing and Synchronization for Time-Sensitive Applications at this profile as part of the Audio-Visual Bridging (AVB) set of technical standards. This profile is being enhanced for the industrial ecosystem driven Time-Sensitive Networks set of technical standards under the IEEE 802.1AS-Rev working group. Some Cisco products support 802.1AS for AVB and TSN applications. This solution does not support 802.1AS at this time.

Industrial Automation Network Model and IACS Reference Architecture

The typical enterprise campus network design is ideal for providing resilient, highly scalable, and secure connectivity for all network assets. The campus model is a proven hierarchal design that consists of three main layers: core, distribution, and access. The DMZ layer is added to provide a security interface outside of the operational plant domain. The following section maps the Enterprise campus model to the IACS reference model.

Aligning the Cisco Enterprise Networking Model for the Industrial Plant

DMZ and Industrial DMZ–Level 3.5

The DMZ in the campus model typically provides an interface and restricts access into the Enterprises network assets and services from the internet. The Industrial DMZ is deployed within our plant environments to separate the enterprise networks and the operational domain of the plant environment. Downtime in the IACS network can be costly and have a severe impact on revenue, therefore the operational zone cannot be impacted by any outside influences, as availability of the IACS assets and processes are paramount. Therefore network access is not permitted directly between the enterprise and the plant. However data and services are required to be shared between the operational domain and the
enterprise, therefore a secure architecture for the industrial DMZ to provide secure traversal of data between the zones is required. Typical services deployed in the DMZ include Remote access servers and Mirrored services. Further details on the design recommendations for the industrial DMZ can be found later in this guide.

**Figure 7  Industrial DMZ Functional Model**

![Industrial DMZ Functional Model]

**Core Network**

The core is designed to be highly reliable and stable to aggregate all the elements in the operational plant, typically Layer 3 devices, with high speed connectivity, redundant links, and redundant hardware. Within the context of the plant architecture it aggregates all of the Cell/Area Zones and provides access to the industrial DMZ and centralized services.

For industrial automation, services required across the plant include: Production control, Historians, domain controllers, and networking security platforms such as Cisco Identity Services Engine (ISE) and Cisco Stealthwatch. The core will align with plant operations and control zone which resides at Level 3 of the Purdue model.

**Summary**

- Provides reliable connectivity between distribution layers for large sites focusing on scale and availability
- Enables site-wide Redundancy
- Non-disrupting in-service upgrades
The distribution layer in its simplest form provides policy-based connectivity and demarcation between the access layer and the core layer. In the Purdue model, it is part of the Cell/Area Zone to provide aggregation and policy control and act as a demarcation point between the Cell/Area Zone and the rest of the IACS network.

Summary
- Layer 3 connectivity to the core layer and Layer 2 into the access
- Aggregates access layers and provides connectivity services
- Connectivity and policy services within the access-distribution network
- Distribution, policy control, and isolation/demarcation points between the Cell/Area Zones and the rest of the network
Collapsed Core Distribution Network

In small-to-medium plants, it is possible to collapse the core into the distribution switches as shown in Figure 9. However, for large plants, in which a large number of Cell/Area Zones exist, this level of hierarchical segmentation is not recommended and a traditional three tier layer is deployed.

Figure 9  Collapsed Core/Distribution

Access Network

The access layer provides the intelligent demarcation between the network infrastructure and the devices that leverage that infrastructure. As such, it provides a security, QoS, and policy trust boundary. When looking at the overall IACS network design, the access switch provides the majority of these access layer services and is a key element in enabling multiple IACS network services.

The Cell/Area Zone can be considered an access layer network that is specialized and optimized for IACS networks.

Summary

- Provides endpoints (PCs, controllers, I/O devices, drives, cameras, etc.) and users access to the network
- Enforces security, segmentation, QoS, and policy trust enforcement
- Labels packets to enforce segmentation
- Comprised of rapid convergent ring topologies or parallel access network topologies
Networking and Security in Industrial Automation Environments

Industrial Automation Network Model and IACS Reference Architecture

- Potential multicast-rich local traffic flows
- Provides Network Address Translation options

Access Network Topologies for the Industrial Plant Environments

Traditional enterprise IT networks are modeled predominantly on redundant star topologies as they tend to have better performance and resiliency, however within the IACS networks there are a number of factors that define the layout of the access network. The physical layout of the plant, cost of cabling, and desired availability are three important factors in plants. For example, ring or linear topologies are more cost effective for long production lines; the cost of cabling these long production lines in a redundant star topology is prohibitive and if availability is required a ring topology map be preferred. Newer technologies, such as PRP and HSR, can provide improved ring resiliency and availability for the IACS plant. HSR can provide lossless redundancy over a ring topology and PRP provides lossless redundancy over two diverse, parallel LANs (LAN-A and LAN-B), which could be two separate rings.

The following are key considerations in determining the topology in an IACS environment:

- Physical Layout—Physical layout of the process facility or the production line influences the networking topology. Installation of cabling can be expensive in industrial environments and is significantly higher than that of the enterprise. Star topologies may be cost prohibitive in long production lines; if real-time communication and availability requirements permit, ring network topology can reduce cost.

- Availability—Availability is a key performance metric that contributes to a plant OEE. The design of the network should enforce maximum uptime. Deploying resilient network topologies allows the network to continue to function after a loss of a link or switch failure. Although some of these events may still lead to downtime of the industrial automation and control systems, a resilient network topology may reduce that chance and should improve the recovery time.

- Real-time communications—The requirement for real-time communications dictates that IACS applications are able to reliably communicate over the network with a level of predictability. Multiple factors, including bandwidth and network hops, can cause latency, jitter, and unpredictable performance. Dedicated star network topologies are better equipped to provide reliable communications, but would have higher cabling costs.

Cell/Area Zone Linear Topology

Linear topologies are a chain of switches connected in a serial fashion. This design has the following characteristics:

- Potential bottlenecks (between the distribution and adjacent Layer 2 switch)
- Ease of implementation
- Reduced cabling costs
- Lack of resiliency
- Higher degree of flexibility for a factory floor layout
Cell/Area Zone Redundant Star Topology

Figure 11 shows a redundant star architecture. There are only two hops in the path between devices and there is redundancy to provide fast convergence. The network has an element of predictability because of the consistent number of hops in the path. The following are key characteristics of this network topology:

- Predictable path with two hops between any access Layer 2 switch
- Redundant links and resiliency in case of multiple link failures
- Faster predictable convergence than rings (other than lossless ring resiliency technologies)
- Most expensive cabling design
Cell/Area Zone Ring Topologies

The ring topology provides resiliency in that there is always a network path available even with a single link failure. It is a progression of the linear topology, with the last switch in the chain being connected back to the distribution switch to form a ring. The ring shares dual paths around the ring and can reduce bottlenecks and oversubscription. With newer technologies described in the Cell/Area Zone design section, the resiliency can be hitless in a ring deployment. Key considerations of the ring topology include:

- Simplicity, which reduces cabling costs
- Resiliency from the loss of one network connection
- Hitless or lossless technologies can be deployed with High-Availability Seamless Redundancy (HSR)
Table 3 summarizes the IACS network topology option advantages and disadvantages for the access network.
Converging the enterprise model with the IACS applications and Purdue model, we have the high-level reference architecture in Figure 13. This scheme maps core, distribution, and access layers, site operations and control, and the Cell/Area Zone. This is the wired network reference architecture only.

Table 3  Network Access Topologies—Advantages and Disadvantage

<table>
<thead>
<tr>
<th>Type</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant star</td>
<td>Resiliency from multiple connection failures</td>
<td>Additional wiring (and relevant costs) required to connect Layer 2 access switches directly to a Layer 3 distribution switch</td>
</tr>
</tbody>
</table>
<pre><code>      | Faster convergence to connection loss                                                        | Additional configuration complexity (for example, Spanning Tree with multiple blocks) |
      | Consistent number of hops (typically two in a flat design) provides predictable and consistent performance and real-time characteristics |                                                                                |
      | Fewer bottlenecks in the design reduces chances of segment over-subscription             |                                                                                |
</code></pre>
<p>| Ring         | Resiliency from loss of one network connection                                               | Additional configuration complexity (for example, Spanning Tree with a single block) |
| Less cabling complexity in certain plant floor layouts                                      | Longer convergence times                                                      |
| Multiple paths reduces potential for over-subscription and bottlenecks                     | Variable number of hops makes designing predictable performance more complex  |
| Linear/Star  | Easy to design, configure, and implement                                                    | Loss of network service in case of connection failure (no resiliency)         |
| Least amount of cabling (and associated cost)                                                | Creates bottlenecks on the links closest to Layer 3 device, and varying number of hops make it more difficult to produce reliable performance. |</p>
Multiservice Traffic (Non-Operational Applications)

Multiple services can be deployed in plants to support plant operations communications. The services are not part of the operational systems and applications running within the IACS infrastructure. These services typically include physical security badge access, video surveillance, and business enabling applications such as email, telephony, and voice systems. Segmentation of the multi-service applications from the IACS system is a common requirement. Regulatory demands, security concerns, risk management, and confidence of the business to maintain multi-service traffic on the same infrastructure as the IACS process and assets will drive the multi-service architecture.

There are two models that may be considered based on risk acceptance. Generally, a separate physical infrastructure for the non-operational applications and services is acceptable. This in essence is an extended enterprise where the non-operational assets move into non-carpeted space. Figure 14 illustrates a connection from the enterprise into the industrial plant and therefore extends the enterprise network. Hardened industrial switches are used in areas where more traditional enterprise switches cannot be deployed. Assets such as phones or video cameras may also require hardening. The other option could be to deploy services on the same physical infrastructure in Level 3 and extend the services through the industrial DMZ from the enterprise. A separate switch network could be deployed off of the Level 3 core or distribution switches, which could keep the services off of the process networks. Additional consideration must be given to mixed Enterprise/IACS QoS model and bandwidth utilization to help ensure IACS traffic is prioritized and maintains determinism.
Utility Substation Architecture

Utility substation communication architectures have much in common with other industries. Industrial Automation and utilities both have process networks, DMZ, operations and control, ruggedization, and timing requirements. However this CVD is focused on the implementation and design at the IACS process network layer within the Cell/Area Zone in industrial plants. Electronic Security Perimeter (ESP) in substations is very different. From a functional block perspective, Figure 15 aligns the two architectures of an industrial automation plant and a utility substation.
The immediately observed difference is that the level 3 operations within the utilities substation architectures are centralized and off-site, whereas in the manufacturing and processing facility this would normally be on-site where the IACS process is running. The centralized substation operations layer has a control center which monitors multiple substations across geographically separate locations over a wide area network (WAN) in what is distributed automation. An industry that has a similar architecture is oil and gas for the transport and distribution of the product along the length of the pipeline. Pipeline stations are distributed along the length of a pipeline and the process is managed centrally at a control center (note that larger pipeline stations and utility substations could have localized control for specific IACS within the facility.)

- Critical Infrastructure Protection—A DMZ is seen on location in both the industrial plant architecture and the utilities architecture. Within the utilities this DMZ is the Critical Infrastructure and Protection Zone. Although slightly different in that the plant has this above the site level operations layer and the utilities substation has this at the station edge below the operations layer, the function remains the same. The DMZ protects the process and automation Industrial Zone in the plant and the CIP protects the ESP in the utilities substation, providing segmentation and separation between the zones as well as controlled access into the ESP. Services within the CIP aligned include Remote Access, Physical security logging, and AAA.

- Corporate SubStation (CorpSS)—Enterprise and operational support services such as voice, web access, and email are housed in the CorpSS Zone within the utilities substation. The design for this zone follows a similar ethos to that of the Multiservice Zone in the industrial plant. It is an extension of the enterprise, delivered over a WAN, and segmented from the ESP Process zone. Within an industrial plant these multiservices and enterprise services would also be segmented from the industrial IACS network. Logical versus physical segmentation for the deployment of multiservices is discussed in this CVD for the industrial plant.

- ESP Zone—The ESP zone is the zone where critical utility monitoring and controlling infrastructure resides. Devices like remote terminal units (RTU), Intelligent Electronic Devices (IED), PLC, relays, etc. all reside within the ESP zone. It is akin to the level 0–2 within the Purdue model. This ESP Zone contains the Station and Process buses. The Station Bus connects the entire substation and provides connectivity between central management and individual bays. The Station Bus connects IEDs within a bay, it connects bays to each other, and bays with the gateway router. The process bus connects the primary measurement and control equipment and I/O to the IEDs. Typically limited to a bay, however busbar protection and differential protection traffic might span multiple bays.

Figure 16 from IEC 61850 illustrates the architecture for the ESP and the process and station buses.
At the process layer on the surface there are similar design considerations. Both architectures require ruggedization, secure segmentation, Layer 2 networking, multicast support, real-time network performance, and high availability to preserve the integrity and performance of the IACS process. However, it is key to understand the traffic types defined within 61850 as this drives the differentiation in design at the process layer between a substation implementation and an industrial plant (the following are the traffic class definitions as taken from IEC-61850-90-4 Ed1). 61850 utilizes GOOSE and Sample value traffic within a substation architecture. GOOSE allows IEDs to exchange data “horizontally” in a bay or between bays. It is used for tasks such as interlocking, measurements, and tripping of circuit breakers. Based on Layer 2 Multicast traffic, GOOSE usually flows over the station bus but can extend to the process bus and even the WAN. Sampled Values is mainly used to transmit analogue values (current and voltage) from the sensors to the IEDs. This traffic flows normally on the process bus but can also flow over the station bus. This traffic is also Layer 2 multicast. MMS traffic allows an MMS client such as the SCADA, an OPC server, or a gateway to access “vertically” all IED objects. This is regular Layer 3 IP unicast traffic.

With the dominance of no IP header, Ethertype multicast for GOOSE, and SV traffic, the design has to be carefully planned. The process bus generally sets a limit of six devices within a process bus due to the high rate of SV traffic. Filtering of traffic is manually created with very scoped VLAN design and MAC access lists to restrict bandwidth. This manual definition from planning to implementation is more complex and needs to consider a well defined VLAN and VLAN trunking design to permit cross station traffic flow of GOOSE and SV because nothing is routed. Not having an IP header in the traffic flow restricts the use of Netflow to baseline traffic in the ESP with GOOSE and SV traffic, however the MMS traffic and other IP-based traffic would be visible and could still be used to identify anomalies in the substation as documented in this DIG. The security architecture would be potentially different as the segmentation scheme is primarily bandwidth derived to restrict or permit multicast traffic across the station with scoped VLANs and Layer 2 multicast access lists. The value of Trustsec and a centralized security implementation (as defined for the industrial plant) for MMS flows needs to be assessed.

Table 4 summarizes the key design consideration for the Cell/Area Zone versus ESP in the areas of performance, availability, multicast, traffic management, and security. These are the areas of design and validation documented in this CVD. Availability and redundancy use similar redundancy protocols. Therefore, with the differences in design the only validation in this CVD specific to substation utility ESP is HSR and PRP in the area of redundancy. With the differences
explained previously and referenced in Table 4, the specific substation design guide will provide design guidance for the ESP zone.

Table 4  Key Design Considerations for Cell/Area Zone versus ESP

<table>
<thead>
<tr>
<th>Features and Considerations</th>
<th>Cell Area Zone</th>
<th>ESP Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>IACS protocols</td>
<td>CIP, PROFINET, MODBUS, CC-LINK IE</td>
<td>SCADA Modbus and DNP3 61850 GOOSE, SV, MMS</td>
</tr>
<tr>
<td>Segmentation</td>
<td>VLAN, IP ACLs, and Trustsec</td>
<td>VLAN, MAC, and IP ACL</td>
</tr>
<tr>
<td>Multicast management</td>
<td>IP IGMP</td>
<td>Scoped VLANs, MAC ACL to restrict propagation and restrict bandwidth</td>
</tr>
<tr>
<td>Timing</td>
<td>NTP, PTP default Profile</td>
<td>PTP Power profile</td>
</tr>
<tr>
<td>Redundancy</td>
<td>REP, HSR, PRP (less PRP requires dual infrastructure)</td>
<td>HSR, PRP, and HSR</td>
</tr>
<tr>
<td>Netflow</td>
<td>Yes generally provides full visibility across the plant with IP-based IACS traffic (PROFINET is the exception)</td>
<td>Only IP-based flows (MMS)</td>
</tr>
</tbody>
</table>

Industrial Networking and Security Design for the Cell/Area Zone

Design Overview and Deliverables

This section describes the industrial automation networking and security architecture for services, applications, equipment, and devices found in industrial plant environments. The industrial wired network solution design has a large amount of commonalities across various industries and the objective is to promote re-use where possible. The design could be referenced for a large-scale auto manufacturer, a pharmaceutical producer, a mine, oil and gas processing facility, or refinery.

At a high level, key deliverables in this DIG include providing Cell/Area Zone network and security design and laying the foundation for multiple IACS applications that will reside on this framework. The validation focuses on the Cell/Area Zone networks in these plants with new resiliency protocol support, advanced security providing visibility, segmentation, and anomaly detection, and the introduction of the Cisco next generation Industrial Ethernet switches, the Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 in addition to other Cisco Industrial Ethernet switching products such as Cisco IE 2000, Cisco IE 4000, and Cisco IE 5000. Key functions and new platforms included in this phase of the Industrial Automation CVD include:

- **SDA-Ready Platforms**—Introduction and validation of the Cisco Catalyst 9300 switch as the distribution switch for the Cell/Area Zone. The Cisco Catalyst 9300 platform is the next generation platform that supports SDA today. SDA is the industry’s first intent–based networking solution for the enterprise built on the principles of the Cisco Digital Network Architecture (DNA). SDA provides automated end-to-end segmentation to separate user, device, and application traffic without redesigning the network. SDA automates user access policy so organizations can make sure the right policies are established for any user or device with any application across the network. Ease of management and intent–driven networking with policy will be valuable additions for the industrial plant environments. However SDA is not yet ready for deployment to support industrial plant requirements and protocols. The new platforms are being positioned in the architecture to prepare for when SDA is able to support industrial plant requirements and protocols. The architecture is promoting SDA switch ready.
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

- **Next Generation Industrial Ethernet Switching**—The Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 are Cisco next generation Industrial Ethernet switches. These switches are inserted into the Cell/Area Zone for Industrial Automation. As part of the SDA readiness the Cisco IE 3400 switch will be the industrial Ethernet switching platform that will support the SDA Fabric edge switch functionality. The Cisco IE 3400 and Cisco Catalyst 9300 switches will provide a foundation to move towards SDA in the wired infrastructure. This will provide a platform to enable SDA features as they become available. Today these platforms will be deployed as non-SDA enabled switches, performing traditional network switching functions.

- **Lossless Resiliency Protocols**—New lossless resiliency protocols and technologies that can be considered for deployment across industries with the introduction of Parallel Redundancy Protocol (PRP), High-Availability Seamless Redundancy (HSR), and the HSR/PRP combined box. Industrial automation applications can have very strict availability requirements that must be adhered to and the network resiliency design and network topologies are critical in helping adhere to these requirements. Cisco Industrial Ethernet platforms Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 support lossless redundancy protocols HSR and PRP. These aid in keeping the network highly available in supporting the industrial applications within the Cell/Area Zone.

- **Network Visibility and OT Management**—Visibility and Identification of network devices and IACS assets in Cell/Area Zone(s) with the Cisco Industrial Network Director (IND). A problem within industrial plant environments is not having visibility into what is connected in these environments. It becomes very difficult to manage and secure the infrastructure to apply security policies without visibility. A key component to implementing security and part of an ongoing risk assessment is to understand what is connected. The Cisco IND provides operations-centric network management for industrial Ethernet networks. The system supports industrial automation protocols such as ODVA, Inc. Common Industrial Protocol (CIP), PROFINET, OPC-UA, Modbus, BACnet, etc. to discover automation devices such as PLC, IO, HMI, and Drives and delivers an integrated topology map of automation and networking assets to provide a common framework for operations and plant IT personnel to manage and maintain the industrial network. This information can be presented to our security applications such as Cisco ISE and Cisco Stealthwatch to provide context to assets and help with security policies.

- **TrustSec and Enhanced Segmentation**—A key component for security implementations and detailed in IEC 62443–3–3 is segmentation of assets into group-based policies. What assets and users need to communicate within a Cell/Area Zone and external to the Cell/Area Zone across an industrial plant needs to be defined. IND provides the visibility of the connected assets to Cisco ISE. Cisco ISE creates and administers the policy defined by the security and OT teams across a Cisco infrastructure. This version of Industrial Automation provides design guidance and validation for assets discovery, policy definition, and application across a Cisco managed infrastructure for an industrial plant which can be deployed across industries.

- **Security using NetFlow and Stealthwatch for Anomaly Detection**—This version of industrial Automation has design guidance for implementing Stealthwatch and enabling NetFlow to provide anomaly detection within the Industrial zone of a plant for multiple industries. Further visibility into the traffic traversing the plant infrastructure can aid with troubleshooting and highlight abnormal behaviors such as detection of malware that is sprawling across a plant. With the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000, NetFlow can be enabled on these devices that can provide data flow metrics to Stealthwatch. Stealthwatch takes the flow data from the network and has many inbuilt machine learning algorithms that can assist an IT security professional in detecting possible malware propagation in the network.
Cell/Area Zone Design and Recommendations

The Industrial zone contains the Site Operations (Level 3) and the Cell/Area Zone (Levels 0-2). The Cell/Area Zone comprises all of the systems, devices, controllers, and applications to keep the plant floor production or processes running. It is extremely important to preserve smooth plant floor operations and functions, therefore security, segmentation, and availability best practices are key components of the design.

The Cell/Area Zone is the key functional zone where IACS devices and controllers are executing the real-time control of an industrial process. This network connects sensors, actuators, drives, controllers, and any other IACS devices that need to communicate in real-time (I/O communication. It is essentially the major building block within the Industrial Automation architecture.
Industrial Characteristics and Design Considerations

The Cell/Area Zone is an access network, but has very different requirements than a traditional IT access layer network. There are key requirements and industrial characteristics that the networking platforms must align with and support. Environmental conditions such as temperature, humidity, and invasive materials require different physical attributes from a networking platform. In addition, continuous availability is critical to ensure the uptime of the industrial process to minimize impact to revenue. Finally, industrial networks also differ from IT in that they need IACS protocol support to integrate with IACS systems.

The following highlights the key design considerations for the Cell/Area Zone, which will directly impact the platform selection, network topology, security implementation, and overall design:

- Industrial Characteristics—Environmental conditions, plant layout, and cabling costs all impact the platform choices and network topology in the design. Industrial plants and processing facilities generally require physically hardened platforms in the Cell/Area Zone. Mines, oil and gas refineries, and plant environments are subject to harsh physical conditions that an IT networking platform cannot withstand. Hardened platforms are equipped for extended temperature ranges, shock and vibration, and invasive materials.

- Interoperability and Interconnectivity—Within the Industrial Zone, Ethernet provides the best technology to interconnect IACS devices and protocols. IACS vendors are adopting the OSI model with Ethernet as the standard to provide communication for a mixture of IACS devices, controllers, and management servers over the network. However, the network must be engineered to support the IACS implementations with an emphasis on real-time communications, availability, and segmentation.

- Real-Time Communications, Determinism, and Performance—Packet delay and jitter within an IACS network can have significant impact to the underlying industrial process. Depending on the industrial application, a delay or variance and lack of determinism in the network can shut down an industrial process and impact its overall efficiency. Achieving predictable, reliable packet delivery is a fundamental requirement for a successful network design in the
Cell/Area Zone. A design will need to factor the number of network hops, bandwidth requirements, and network QoS and prioritization to provide a greater degree of determinism and performance for the real-time applications and functions. Precision Time Protocol can also help with the deterministic nature of the network and applications.

- Availability—A key metric within industrial automation is overall equipment effectiveness (OEE). Availability of the critical IACS communications is a key factor that contributes to the OEE score. Network topologies and resiliency design choices, such as QoS and segmentation, are critical in helping maintain availability of IACS applications, reducing the impact of a failure or security breach.

- Security—When discussing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain. The Purdue Model of Control Hierarchy, International Society of Automation 95 (ISA95) and IEC 62443, NIST 800-82, and NERC CIP for utility substations are examples of such architectures. Key security requirements in the Cell/Area Zone include device and IACS asset visibility, secure access to the network, segmentation, group-based security policy, and Layer 2 hardening (control plane and data plane) to protect the infrastructure.

- Management—Plant infrastructures are becoming more advanced and connected than ever before. Within the Cell/Area Zone there are two personas and skillsets taking on responsibility of the network infrastructure, namely IT and OT staff. OT teams require an easy-to-use, lightweight, and intelligent platform that presents network information in the context of automation equipment. Key functions at this layer will include plug-and-play, easy switch replacement, and ease of use to maintain the network infrastructure.

- Traffic types—The IACS traffic within the Cell/Area Zone is predominantly local and stays within the same Layer 2 domain. Cyclical I/O data communicated on very short intervals (milliseconds) from devices to controllers and workstations or HMIs occurs all on the same LAN or VLAN. Layer 2 multicast is also used in IACS networks.

Cell/Area Zone Components

Cisco has an extensive range of Industrial Ethernet switches. Within the Cell/Area Zone at the access layer, environmental conditions as described earlier are usually a key factor in selecting a hardened, DIN-mountable access switch, such as a Cisco IE 4000 or Cisco IE 3200. The Layer 3 distribution switch may have less stringent requirements, allowing for models such as the Cisco Catalyst 3850 and Cisco Catalyst 9300. The distribution switch is typically located in a controlled, carpeted space, however if industrial protocols are still required, the Cisco IE 5000 or Cisco IE 4010 could be deployed at this layer.
Levels 0, 1, and 2 components; for example, devices, controllers, and HMs

Layer 2 access switches

Layer 3 distribution switches

Table 5 provides guidance on choosing switches based on multiple factors which are critical in industrial environments.

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Industrial Ethernet (IE)</th>
<th>Typical Non-Industrial Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor/Mounting Options</td>
<td>Din Rail, Panel, and Rack Mount</td>
<td>Rack Mount</td>
</tr>
<tr>
<td>Interface Options</td>
<td>Port density 6-28 ports</td>
<td>High port density</td>
</tr>
<tr>
<td>PoE Density/Max Power</td>
<td>Port density 6-28 ports</td>
<td>High port density</td>
</tr>
<tr>
<td>Power Supply Options</td>
<td>DC input voltage range = 10 to 300*</td>
<td>DC input voltage range = 36 to 72</td>
</tr>
<tr>
<td>Environment Design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fanless (no moving part) versus Fans</td>
<td>Fanless</td>
<td>Fans</td>
</tr>
<tr>
<td>Operating Temperature Range</td>
<td>-30c to +60c (+85c type test)*</td>
<td>-5c to +45c</td>
</tr>
<tr>
<td>Ingress Protection (IP) Rating</td>
<td>IP30 (models up to IP67)</td>
<td>IP XX (Not Specified, IP20 or less)</td>
</tr>
<tr>
<td>Industry Certifications</td>
<td>Hardened for vibration, shock, surge, and noise immunity*</td>
<td>Enterprise-class certifications</td>
</tr>
<tr>
<td>“Swap Drive”—Removable Flash</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Dying Gasp—Upon loss of input power</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 5  Industrial Automation Switching Considerations (continued)

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Industrial Ethernet (IE)</th>
<th>Typical Non-Industrial Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Ports</td>
<td>Yes (Inputs on most models and Output on all models)</td>
<td>No</td>
</tr>
<tr>
<td>Deterministic Ethernet</td>
<td>Yes—Supported on Cisco IE 4000 and Cisco IE 5000 (under development)</td>
<td>No</td>
</tr>
<tr>
<td>IEEE 802.1 TSN</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IEEE 1588 PTP</td>
<td>IEEE 1588, Inc. Power Profile level of accuracy (50ns per hop)</td>
<td>No</td>
</tr>
<tr>
<td>IEEE C37.238-2011 (Power Profile)</td>
<td>Option for GPS and IRIG-B on Cisco IE 5000, including Grandmaster with Stratum 3E on-board oscillator</td>
<td>No</td>
</tr>
</tbody>
</table>

Switching Platform, Industrial Security Appliance, and Industrial Compute Portfolio for the Cell/Area Zone

There has been an evolution of switching platforms since the previous industrial automation architectures and validated designs such as Ethernet to the Factory, CPWE, and Connected Refinery/Processing plant were released. Newer features and hardware capabilities have been added to increase performance, security, and capabilities of the Industrial Automation architecture. The following highlights some of these capabilities that are extremely relevant in this phase of the architecture and also features which show future benefit:

- NetFlow export enabled on industrial switches provides network visibility into the traffic within the Cell/Area Zone. Consuming NetFlow in Cisco Stealthwatch provides anomaly detection to help secure the network. NetFlow is available on the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 switches.

- Cisco TrustSec-enabled industrial switches provide scalable segmentation across the industrial automation architecture.

- Network resiliency protocols, such as PRP and HSR, improve availability by providing lossless failover. Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 support PRP and HSR deployments.

- Inserting the Cisco Catalyst 3400 (SDA-capable) and Cisco Catalyst 9300 switches into the architecture provides SDA platform readiness and a potential path to intent-based services.

**Figure 20** provide an extensive industrial switching portfolio for the industrial automation plant environments. Multiple platforms are available to accommodate various feature requirements. Cisco IND is the management platform to support the industrial switches in the industrial plant environments.
Figure 20   Cisco IoT Industrial Switching Portfolio

Table 6   Cisco IoT Industrial Switching Portfolio

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco IE 2000 access</th>
<th>Cisco IE 4000 access/distrib</th>
<th>Cisco IE 4010 access/distrib</th>
<th>Cisco IE 5000 access/distrib</th>
<th>Cisco IE 3200 access</th>
<th>Cisco IE 3300 access/distrib</th>
<th>Cisco IE 3400 access/distrib</th>
<th>Cisco Catalyst 9300</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 inch</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Dinrail</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>TrustSec</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>HW Ready</td>
<td>Yes</td>
</tr>
<tr>
<td>dot1X</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Netflow</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>Yes</td>
</tr>
<tr>
<td>REP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HSR (HSR-SA N, HSR-PRP)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>HW Ready</td>
<td>No</td>
</tr>
<tr>
<td>PRP (Red box)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>HW Ready</td>
<td>No</td>
</tr>
<tr>
<td>PROFINET</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>No</td>
</tr>
<tr>
<td>MRP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>No</td>
</tr>
<tr>
<td>IND support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 6  Cisco IoT Industrial Switching Portfolio (continued)

<table>
<thead>
<tr>
<th>SDA Extended Node</th>
<th>Cisco IE 2000 access</th>
<th>Cisco IE 4000 access/dist</th>
<th>Cisco IE 4010 access/dist</th>
<th>Cisco IE 5000 access/dist</th>
<th>Cisco IE 3200 access</th>
<th>Cisco IE 3300 access/dist</th>
<th>Cisco IE 3400 access/dist</th>
<th>Cisco Catalyst 9300</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SDA fabric edge node</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>HW Ready</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco DNA support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 7 provides a view of the hardware and software components validated in this version of Industrial Automation CVD.

Note: Table 6 shows software features and capabilities supported at the time of this CVD release (Jan 25, 2019). Refer to the product data sheet for the latest feature support: https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html

Cell/Area Zone IP Addressing

The IACS devices have to be assigned with IP addresses to communicate with other IACS devices and also with Level 3 site operations. The IP address to the IACS device can be assigned statically or by using DHCP service. This section describes the factors that need to be considered while choosing between static assignment or by DHCP service.
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

Static IP Addressing

Generally, IACS devices are not moved around the Cell/Area Zone when wired to a port. There is a requirement for ease of use and ease of replacement. The default method used most often is for the operations team to statically assign an IP address to the IACS device. Manual DIP switches or dials for addressing IACS devices are still deployed on plant floors which require static configuration by an operator. For an IACS device in the Cell/Area Zone, the time it takes for a device to come back after the boot process is of vital importance. As a result, if an IACS device is using DHCP, then the time it takes to assign IP address increases the amount of time needed for the device to come up and this behavior impacts the performance of the IACS device. However, as the size of the IP address increases, it becomes difficult to manage the IP address table.

Assigning IP Addresses Using DHCP

Assigning IP addresses to IACS devices using DHCP is an alternative method to static assignment. This method resolves the problems pertaining to static assignment, management of IP addresses and changing IP address of the IACS devices because DHCP protocol is an automatic process that allows for an IP address to be assigned from a pool. When a device needs to be replaced or moved to a different location and if DHCP service is enabled, then the IACS device always gets an IP address from the DHCP pool.

Considerations for DHCP Service

Assigning IP addresses to IACS devices has several advantages, such as when devices move to a different cell enabled with a different VLAN then there is no need to re-provision a different IP address to the IACS device because DHCP assigns IP addresses automatically when a device asks for it. However, for IACS applications that need quick up time after a device is re-booted, moved, or replaced then this additional delay may not meet the stringent requirement.

To solve the problem of managing IP addresses and also not add additional delay due to DHCP, Industrial Automation recommends using DHCP with persistence enabled on industrial switches deployed in the Cell/Area Zone. DHCP persistence assigns an IP address to a port. This feature allows the same IP address to be provisioned so that upon replacement of an asset, the same IP address is provisioned. In the static nature of IACS this helps with ease of use and replacement.

Cell/Area Zone Traffic Patterns and Considerations

Within the IACS networks, there are two traffic types—real-time traffic flows and non real-time traffic flows:

- Real-time traffic flows are typically between IACS devices and controllers or between two controllers. This traffic is extremely chatty and driven by cyclical I/O data being communicated on very short intervals between devices and controllers on the same VLAN. The only exception is with interlocking controllers where traffic for real-time data transfer would be between VLANs through one Layer 3 switch hop. Some IACS protocols only support Layer 2/Ethernet for real-time traffic (PROFINET). This, combined with requiring determinism and predictability, lends itself to keeping the majority of this traffic for real-time at Layer 2.

- Non-real-time traffic is not as critical to the IACS communications and does not have the same constraints or network requirements as the real-time traffic. It is typically informational in nature and would flow between workstation or server in Level 3 operations and devices in Levels 0–2. This traffic is IP/TCP or IP/UDP and is routable.

Multicast traffic is an important consideration of a Cell/Area IACS network because it is used by some of the key IACS communication protocols. It is usually non-routable and so stays within the Cell/Area Zone.
As shown in Figure 21, Figure 22, Table 8, and Table 9, which describe CIP and PROFINET traffic flows, the majority of real-time traffic is local and non-real-time management and informational traffic is routed to the operations and control Level 3.

### Table 8 CIP Typical Traffic Flows

<table>
<thead>
<tr>
<th>Reference Number in Figure 21</th>
<th>From</th>
<th>To</th>
<th>Description</th>
<th>Protocol</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
</table>
| 1a, b, c                      | Producer (for example, VFD Drive) | Consumer (for example, controller) | A producer (for example, VFD Drive, or controller) communicates data via CIP Implicit I/O (UDP multicast) traffic to multiple consumers  
  a—Represents device to controller IO  
  b—Represents controller–controller I/O  
  c—Represents controller reporting real-time status to HMI | EtherNet/IP | UDP | 2222 |
| 2                             | Producer                    | Consumer                  | Producers can communicate data via CIP I/O as UDP unicast traffic to a consumer. | EtherNet/IP | UDP | 2222 |
| 3                             | Consumer                    | Producer                  | Consumer (for example, controller or HMI) responds with output data or a heartbeat via CIP I/O (UDP unicast) traffic to the producer. | EtherNet/IP | UDP | 2222 |
Figure 21  CIP Cell/Area Zone Traffic Flows
Figure 22  PROFINET Cell/Area Zone Traffic Flows

Table 9  Typical PROFINET Data Flows

<table>
<thead>
<tr>
<th>Traffic Number in Figure 22</th>
<th>Description</th>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Supervisor uses PN-DCP or LLDP to discover all devices on LAN and for configuring IP address and device name</td>
<td>TIA Portal</td>
<td>All PROFINET devices</td>
<td>PN-DCP/LLDP</td>
<td>RT/NRT</td>
</tr>
<tr>
<td>2</td>
<td>Alarms</td>
<td>Device</td>
<td>PLC</td>
<td>PROFINET</td>
<td>RT</td>
</tr>
<tr>
<td>3</td>
<td>Process data</td>
<td>PLC</td>
<td>Device</td>
<td>PROFINET</td>
<td>RT</td>
</tr>
<tr>
<td>4</td>
<td>Process data</td>
<td>Device</td>
<td>PLC</td>
<td>PROFINET</td>
<td>RT</td>
</tr>
<tr>
<td>5</td>
<td>Configuration pushed from supervisor</td>
<td>TIA</td>
<td>PLC</td>
<td>TCP/IP</td>
<td>NRT</td>
</tr>
<tr>
<td>6</td>
<td>Process information or to accept action from HMI</td>
<td>PLC</td>
<td>HMI</td>
<td>TCP/IP</td>
<td>NRT</td>
</tr>
<tr>
<td>7</td>
<td>Controller to controller communication</td>
<td>PLC</td>
<td>PLC</td>
<td>PROFINET</td>
<td>RT</td>
</tr>
<tr>
<td>8</td>
<td>Mail message to warn or to inform status</td>
<td>HMI/PLC</td>
<td>Mail server</td>
<td>SMTP</td>
<td>Ethernet</td>
</tr>
<tr>
<td>9</td>
<td>All network infrastructure (for example, switches and routers) and many Ethernet devices can send SNMP messages</td>
<td>Device</td>
<td>Network manager</td>
<td>SNMP</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>
Cell/Area Zone Performance and QoS Design

QoS provides classification, prioritization, and preferential forwarding treatment to various traffic flows within the Cell/Area Zone. Dedicated bandwidth and predictable jitter and latency are required by some IACS applications (real-time). QoS can help provide this in the Cell/Area Zone; IACS real-time traffic flows with the highest performance requirements will be given precedence over all traffic types. This prioritization helps to contribute to network performance, assurance, and predictability which is required to ensure ACS application uptime and efficiency and ultimately contribute to OEE.

Traffic types not involving IACS devices also exist within the Cell/Area Zone. In reference to the description of traffic flows in the Cell/Area Zone, Level 3 traffic originating from workstations and servers occurs, such as SNMP and HTTP traffic. An industrial customer may choose to deploy operational support services such as voice or video in the industrial zone on a shared network infrastructure, however this should be evaluated as part of the risk assessment and aligned with a QoS model defined for a converged architecture. In contrast, operational support services can be physically separated from the IACS devices and applications with independent network infrastructures.

Real-time performance and characteristics of the IACS applications should be well understood when designing to provide predictability and consistency in networking performance. As previously stated, the IACS applications and performance are paramount to ensuring uptime, efficiency, and ultimately OEE. A variety of IACS traffic could be deployed within the Cell/Area Zone which have very different network requirements for latency, jitter, and packet loss. Any unpredictability in the network performance causing too much latency or jitter as well as packet loss could cause IACS system errors or a shutdown of equipment. The following tables reference a defined set of requirements for various types of informational and time-critical I/O traffic classes.

IACS Application Real-Time Requirements—Cisco

<table>
<thead>
<tr>
<th>Requirement Class</th>
<th>Typical Cycle Time</th>
<th>Typical RPI</th>
<th>Connection Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information/Process (e.g., HMI)</td>
<td>&lt; 1 s</td>
<td>100 – 250 ms</td>
<td>Product dependent</td>
</tr>
<tr>
<td>Time critical processes (e.g., I/O)</td>
<td>30 – 50 ms</td>
<td>20 ms</td>
<td>4 intervals of RPI, but =100 ms</td>
</tr>
<tr>
<td>Safety</td>
<td>10 – 30 ms</td>
<td>10 ms</td>
<td>24 – 1000 ms</td>
</tr>
<tr>
<td>Motion</td>
<td>500 μs – 5ms</td>
<td>50 μs – 1 ms</td>
<td>4 intervals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement Class</th>
<th>Typical Cycle Time</th>
<th>Typical RPI</th>
<th>Communication Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information/Process</td>
<td>&lt; 1 s</td>
<td>100 – 250 ms</td>
<td>Non-Real Time (NRT)</td>
</tr>
<tr>
<td>Process/Discrete</td>
<td>30 – 50 ms</td>
<td>20 ms</td>
<td>Real Time (RT)</td>
</tr>
</tbody>
</table>

Table 10 and Table 11 highlight the differing network characteristics between the various IACS applications that could be deployed in the Cell/Area Zone. The key IACS performance requirements are machine/process cycle times and the Request Packet Interval (RPI), which if not met can cause a connection timeout or shutdown of the equipment/process. These are usually defined as:

- Machine/process cycle times—The processing time in which industrial automation system application makes decisions
- I/O update time—The processing time at which input/outputs are sent/received
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

Table 10 and Table 11 also show the network would need to provide higher network performance for time critical versus informational traffic and even higher performance for motion and safety applications or systems. The QoS design for Industrial Automation followed the guidelines and standards outlined by ODVA, Inc. for a QoS Model with Common Industrial Protocol (CIP) and Precision Timing Protocol (PTP) traffic. These are built on the following premises:

- Prioritization for IACS traffic over non-IACS traffic in the Cell/Area Zone if deployed on a shared infrastructure
- IACS real-time traffic over IACS non-real-time traffic in the Cell/Area Zone
- Within real-time services further differentiation may be required to support higher performance applications such as Safety and Motion.
- QoS deployed plant wide in a consistent manner. Network devices across the plant need to adhere to the same policy.

Table 12  ODVA, Inc. QoS Model for CIP and PTP Traffic

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>CIP Priority</th>
<th>DSCP Layer</th>
<th>CoS Layer 2</th>
<th>CIP Traffic Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event (IEEE 1588)</td>
<td>N/A</td>
<td>59</td>
<td>7</td>
<td>PTP event messages, used by CIP Sync</td>
</tr>
<tr>
<td>PTP General (IEEE 1588)</td>
<td>N/A</td>
<td>47</td>
<td>5</td>
<td>PTP management messages, used by CIP Sync</td>
</tr>
<tr>
<td>CIP class 0 / 1 Urgent</td>
<td>55</td>
<td>6</td>
<td></td>
<td>CIP Motion</td>
</tr>
<tr>
<td></td>
<td>Scheduled</td>
<td>47</td>
<td>5</td>
<td>Safety I/O</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>43</td>
<td>5</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>31</td>
<td>3</td>
<td>No recommendations at present</td>
</tr>
<tr>
<td>CIP UCMM CIP class 3</td>
<td>All</td>
<td>27</td>
<td>3</td>
<td>CIP messaging</td>
</tr>
</tbody>
</table>

Cisco QoS uses a toolset to provide the priority and preferential treatment for the IACS traffic. The key tools used across the platforms for this version of Industrial Automation are:

- Classification and Marking—Classifying or marking the traffic as it enters the network to establish a trust boundary that is used by subsequent QoS tools, such as scheduling. Class maps and policy maps are the mechanism to provide the network classification.
- Policing and Markdown—Policing tools, known as Policers, determine whether packets are conforming to administratively-defined traffic rates and take action accordingly. Such action could include marking, remarking, or dropping a packet.
- Scheduling (Queuing and Dropping)—Scheduling tools determine how a frame or packet exits a device. Whenever packets enter a device faster than they can exit it, such as with speed mismatches, then a point of congestion or bottleneck can occur. Devices have buffers that allow for scheduling higher priority packets to exit sooner, which is commonly called queueing.

Note: Policing and Markdown is not used in the QoS design for IACS traffic as we do not want to impact control traffic.

Classify and mark all traffic at the access point to the network. Devices that are capable of marking the traffic may be connected to the access switches with trusted ports. Devices not capable of marking their network traffic would need to be classified and marked at the access switch and these network ports would be untrusted. The general guidance is to not trust the CoS/DSCP markings entering the access switch and have the access switch classify and mark all the traffic entering the network. This provides a level of assurance and correct classification at the network edge.
Once classified and in the network, the uplink and outbound ports on the network switches can be trusted and configured to schedule traffic according to the QoS profile. Figure 23 highlights the trusted versus untrusted description.

Table 13  QoS Classification/Markings and Queue Details

<table>
<thead>
<tr>
<th></th>
<th>PTP Event</th>
<th>CIP Urgent</th>
<th>PTP Mang., CIP Scheduled, CIP High</th>
<th>Network Control</th>
<th>Voice Data</th>
<th>CIP Low, CIP Class 3</th>
<th>Voice Control</th>
<th>Best Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>59</td>
<td>55</td>
<td>47, 43, 48</td>
<td>46</td>
<td>31, 27</td>
<td>24</td>
<td>4, 2, 1, 0</td>
<td></td>
</tr>
<tr>
<td>CoS</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>5, 3</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Traffic Type</td>
<td>PTP Event</td>
<td>CIP Motion</td>
<td>PTP Mang., Safety I/O, I/O</td>
<td>STP, etc.</td>
<td>SIP, etc.</td>
<td>CIP Explicit Messages</td>
<td>SIP</td>
<td>All the rest</td>
</tr>
<tr>
<td>CoS-to-Ingress Queue map</td>
<td>Queue 2</td>
<td>Queue 1</td>
<td>Queue 3</td>
<td>Queue 4</td>
<td>Queue 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress Queue Threshold</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CoS-to-Egress Queue map</td>
<td>Queue 1</td>
<td>Queue 3</td>
<td>Queue 4</td>
<td>Queue 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egress Queue Threshold</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ingress and egress queues on all the switches in the Cell/Area Zone including the distribution switches are serviced using the shared round robin mechanism. The classified traffic is mapped to specific ingress and egress queues to provide preferential treatment and avoid packet loss to real-time traffic. Bandwidth can be assigned to the queues to ensure and guarantee that a level of service is maintained during times of network congestion, thus keeping to the availability and assurance required for certain applications. Within the ODVA, Inc. model, a priority queue is assigned to the most critical traffic in the QoS design, which ensures strict prioritization of this queue.

Table 14 and Table 15 shows the QoS settings for the switches in the design that have been tested as part of Industrial Automation. These settings are taken from the ODVA, Inc.QoS recommended settings for CIP traffic.

**Table 14  Ingress Queue Details**

<table>
<thead>
<tr>
<th>Ingress Queue</th>
<th>Queue#</th>
<th>CoS-to-Queue Map</th>
<th>Traffic Type</th>
<th>Queue Weight</th>
<th>Queue (Buffer) Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRR Shared</td>
<td>1</td>
<td>0,1,2</td>
<td>All the rest</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>Priority</td>
<td>2</td>
<td>3, 4, 5, 6, 7</td>
<td>PTP,CIP,Network Control, Voice, Video</td>
<td>60%</td>
<td>60%</td>
</tr>
</tbody>
</table>
Configuration details and an in-depth description of the scheduling mechanisms for all the switches can be found in *Quality of Service*, page 191. The switches evaluated in this round of testing included the Cisco IE 2000, Cisco IE 4000, Cisco IE 3200, Cisco IE 3400, and the Cisco Catalyst 9300 and Cisco Catalyst 3850.

**Multicast Management in the Cell/Area Zone and ESP**

Networking switches within the Cell/Area Zone should facilitate the support of multicast as it is used by some of the IACS protocols. In general, the multicast traffic at Cell/Area Zone does not go beyond Level 2. Mechanisms are used in some of the protocols to prevent passing routed boundaries, such as keeping the TTL at 1 within the IP packet. Within the context of a Layer 2 multicast network, Internet Group Management Protocol (IGMP) snooping is used to manage and control the multicast traffic. Figure 24 highlights the components and functions within the Cell/Area Zone for supporting IACS traffic deployed with multicast.

**Figure 24  Cell/Zone Multicast**

<table>
<thead>
<tr>
<th>Egress</th>
<th>Queue #</th>
<th>CoS-to-Queue</th>
<th>Traffic Type</th>
<th>Queue</th>
<th>Queue Size for Gb</th>
<th>Queue Size for 10/100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>1</td>
<td>7</td>
<td>PTP Event</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>SRR Shared</td>
<td>2</td>
<td>0, 1, 2, 4</td>
<td>All the rest</td>
<td>19</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>SRR Shared</td>
<td>3</td>
<td>5, 6</td>
<td>PTP Management, CIP Implicit I/O, Network Control &amp; Voice data</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>SRR Shared</td>
<td>4</td>
<td>3</td>
<td>CIP Explicit Messages</td>
<td>40</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

- IGMP Snooping—With IGMP snooping in the Layer 2 switches, the switch is able to restrict switching of multicast packets out to only those ports that require it.
- IGMP Querier—Keeps track of the multicast group membership. A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
- Multicast router (Mrouter) port—The port facing the IGMP querier or where the multicast and query traffic will be received. A snooping switch should forward IGMP membership reports only to those ports to where multicast routers are attached or where IGMP queries are to be sent (querier).

Recommendations for Deploying Multicast in the Cell/Area Zone

- Enable IGMP snooping and querier on all the industrial Ethernet switches as well as the distribution switch/router. Do not change any of the IGMP snooping default settings.
- Configure the IGMP querier on the distribution switch or central to the Cell/Area Zone topology. When multiple IGMP queriers are on a VLAN, the IGMP protocol calls for the querier with the lowest IP address to take over the querier function. Therefore, the distribution switch should have the lowest IP address in the subnet.

Availability

Availability of the industrial automation process affects the business directly and is therefore a critical component. Ensuring the uptime of the IACS applications requires a robust, resilient network. This section provides network design to support availability for IACS applications with platform protocol and path redundancy.

Within the QoS and performance section, RPI and cycle time were key metrics that the network needed to be able to support. The cycle time is the critical requirement for network availability. The network needs to recover within the cycle time to prevent any IACS application timeouts which could cause a shutdown of the process. If the network can recover from a failure within the cycle time, then theoretically the IACS application should continue to operate. With this in mind Table 16 provides a view of target network convergence times for the IACS.

Table 16 Industrial Automation Network Convergence Targets

<table>
<thead>
<tr>
<th>Requirement Class</th>
<th>Target Cycle Time</th>
<th>Target RPI</th>
<th>Target Network Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information/Process (e.g. HMI)</td>
<td>&lt; 1 s</td>
<td>100 - 250 ms</td>
<td>&lt; 1 sec</td>
</tr>
<tr>
<td>Time critical processes (e.g., I/O)</td>
<td>30 - 50 ms</td>
<td>20 ms</td>
<td>&lt; 100 ms</td>
</tr>
<tr>
<td>Safety</td>
<td>10 - 30 ms</td>
<td>10 ms</td>
<td>&lt; 24 ms</td>
</tr>
<tr>
<td>Motion</td>
<td>500 μs - 5ms</td>
<td>50 μs - 1 ms</td>
<td>&lt; 1ms</td>
</tr>
</tbody>
</table>

Media Considerations

Media plays a large part in contributing to the convergence times for failures in the network. Copper Ethernet links contribute to larger convergence times than fiber and take longer to detect the failure without any supplementary keepalive mechanism. This is reflected in some of the convergence tests that were conducted.

The specific Cisco Catalyst 9300 platform aggregating the rings was the Cisco Catalyst 9300-48P. At the time of testing this platform only supported copper downlinks. A 1/10 Gbps uplink module was evaluated to provide fiber media convergence numbers. Copper downlinks were also evaluated in certain scenarios.

Distribution Switch Resiliency

This section describes the resiliency options validated for industrial automation at the distribution switch in the Cell/Area Zone boundary.

- Cisco StackWise-480
- Hot Standby Redundancy Protocol
The Cisco Catalyst 3850 and Cisco Catalyst 9300 support StackWise-480 configurations to provide platform resiliency at the distribution layer. A switch stack can have up to eight stacking-capable switches connected through their StackWise-480 ports. The stack members work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

A switch stack always has one active switch and one standby switch. The active switch will provide control of the management plane for the stack. If the active switch becomes unavailable, the standby switch assumes the role of the active switch and keeps the stack operational. In this version of Industrial Automation the switch stacks were validated with two switches to provide the Cell/Area Zone distribution switch resiliency.


Hot Standby Redundancy Protocol

Hot Standby Redundancy Protocol (HSRP) is an alternative to StackWise-480 for the distribution switch. HSRP provides high availability through redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router sends packets; the standby router takes over the routing duties when an active router fails or when preset conditions are met. For the CVD, two Layer 3-enabled switches were deployed for HSRP scenarios, one active and one standby.

Path Redundancy

Network path redundancy provides alternative paths through a network under equipment or link failure. Within the Cell/Area Zone, this network redundancy is provided on all uplinks from the edge switching platforms using a star or a ring topology. A resiliency protocol needs to be deployed to prevent loops within the redundant links; loops are created in Layer 2 networks when there are multiple active paths to the same destination. REP, MRP, PRP, and HSR can prevent frames from looping within a ring topology and EtherChannel or Flex Links within a star topology.
Redundancy for star topologies—EtherChannel or Flex Links

Redundancy for ring topologies—MRP, PRP, REP and HSR

Redundant Star Topology

**EtherChannel**
EtherChannel groups multiple physical Ethernet links into a single logical link between two switches. Traffic traversing the logical link between two switches is load balanced over the physical links. If a physical link fails within the EtherChannel, then the traffic is redistributed across the other available links in the EtherChannel. Although not strictly a resiliency protocol, the EtherChannel can be deployed to provide resiliency when there are multiple links between the same two switches. In industrial automation this is configured as an option for redundant star configurations when connecting between an access switch (for example, Cisco IE 4000) and the distribution switches running StackWise.

**Flex Links**
Flex Links are a pair of a Layer 2 interfaces (switch ports or port channels), where one interface is configured to act as a backup to the other. This feature provides an alternative solution to the Spanning Tree Protocol (STP) and is deployed between an access switch and a distribution switch. The active link is used to forward and receive frames and the standby link does not forward or receive frames, but is in the up/up state. When a failure is detected on the active link, the standby link moves to active and all MAC addresses and multicast entries move to the standby link. On restoration of the failed link it will again become the standby link.
Note: The Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 switches do not support Flex links in the software used for this CVD.

**Redundant Star Design and Validation**

The following figures detail the various scenarios covered for the industrial automation and the convergence times.

Cisco Catalyst 9300 and Cisco Catalyst 3850 switches were evaluated with the Cisco IE 3200/Cisco IE 3400 and Cisco IE 4000 switches in a redundant star configuration with EtherChannel. Only EtherChannel was evaluated for Cisco IE 3200/Cisco IE 3400. **Figure 28** highlights the validation scenario.
Table 17 and Table 18 provide details of the convergence results for multiple types of failures. Link disruptions refer to a single link failure in the ring. Switch failures refer to a primary distribution switch failure where the backup switch would assume the active role. Multiple link and switch failures were conducted where the maximum and average convergence times were recorded. Simulated traffic and real IACS devices were used during validation. The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.

Table 17  Star Topology with Cisco Catalyst 9300

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence Cisco IE 3200/Cisco IE 3400 Fiber</th>
<th>Convergence Cisco IE 3200/Cisco IE 3400 Copper</th>
<th>Convergence Cisco IE 4000 Copper</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L2 Multicast</td>
<td>Max 90 Average 69 Max 320 Average 95 Max 94 Average 53</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>L2 Unicast</td>
<td>Max 90 Average 69 Max 320 Average 95 Max 94 Average 53</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>L3 Unicast</td>
<td>Max 90 Average 69 Max 320 Average 95 Max 94 Average 53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>L2 Multicast</td>
<td>Max 238 Average 48 Max 733 Average 170 Max 102 Average 44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>L2 Unicast</td>
<td>Max 106 Average 41 Max 152 Average 60 Max 102 Average 44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>L3 Unicast</td>
<td>Max 106 Average 48 Max 152 Average 64 Max 102 Average 44</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

Result Considerations

The convergence for link failures using the Cisco Catalyst 9300 copper downlinks with Cisco IE 3200/Cisco IE 3400 were much higher than with the Cisco IE 4000.

Fiber testing for the Cisco IE 3200/Cisco IE 3400 was much improved in these scenarios with both the Cisco Catalyst 3850 and Cisco Catalyst 9300 as the distribution switch.

- With Cisco Catalyst 9300 as the distribution switch, Cisco IE 3200/Cisco IE 3400 is not recommended with copper media for IACS applications with outliers that may cause connection timeouts.

- With the Cisco Catalyst 9300 the distribution switch failure may cause higher convergence time for Layer 2 multicast traffic (238ms) and cause connection timeouts for IACS applications that use multicast. The applications can be tuned to accommodate or potentially not use multicast for the application.

Ring Resiliency Protocols

REP

REP is a Cisco proprietary protocol that provides an alternative to STP to control network loops, handle link failures, and improve convergence time. REP runs a single redundancy instance per segment or physical ring. One REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment and each segment port can have only one external neighbor.

Each end of a network segment terminates at a neighboring Cisco IE access switch or distribution switch. The port where the segment terminates is called the edge port. Figure 29 illustrates a typical REP segment deployed in Industrial Automation.

---

Table 18  Star Topology with Cisco Catalyst 3850

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence Cisco IE 3x00 Fiber</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Max</td>
</tr>
<tr>
<td>Link</td>
<td>Layer 2 Multicast</td>
<td>248</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>128</td>
</tr>
<tr>
<td>Switch</td>
<td>Layer 2 Multicast</td>
<td>228</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>226</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>226</td>
</tr>
</tbody>
</table>
Loop prevention in the ring is maintained with one port in the segment being in a blocked state, also known as the alternate port. If a failure in the segment is detected, then the alternate port will move to a forwarding state allowing traffic to traverse the alternate path avoiding the network failure.

**REP Basic Operation and Failover**

Any REP-enabled node can trigger a failure notification within a segment. Link failures do not rely on there being a ring master node to update all other nodes of the failure, as is the case with STP. REP nodes maintain neighbor adjacencies with a link status layer which sends hello packets to be acknowledged. Segment failures in the ring are discovered through loss of signal or loss of connectivity (no response to the hellos). When a node detects a failure it will send link failure notifications to its REP peers. To maintain fast convergence in industrial environments, Cisco REP uses a fast failure notification, propagating the notifications through the use of a reserved multicast address. The notification is forwarded so that each node in the segment is notified immediately. This will move the alternate port to a forwarding state and cause flushing of the MAC address tables of all switches on the segment.
Figure 30  REP Blocking Port Removed Under Failure
Upon restoration of the failure the point of failure will become the new alternate port which avoids disruption of the ring. If a known desired state is required after failure is required then preemption can be configured to position the blocked port to a specific location in the ring, however this preemption event would trigger a disruption of the ring.

**REP Topologies Design and Recommendations**

**Table 19 REP Ring with Cisco IE 5000 in Distribution**

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max</td>
<td>Average</td>
</tr>
<tr>
<td>Link</td>
<td>Layer 2 Multicast</td>
<td>246</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>320</td>
</tr>
<tr>
<td>Switch</td>
<td>Layer 2 Multicast</td>
<td>138</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>1014</td>
</tr>
</tbody>
</table>

**Result Considerations**

- Convergence was validated for Layer 2 traffic within a VLAN and Layer 3 traffic between VLANs in the same ring.
- Link disruptions refer to a single link failure in the ring. Switch failures refer to primary distribution switch failure.
- Simulated traffic and real IACS devices were used during validation.
- The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.
REP ring was a 10 nodes ring with the following IE switches:
- Cisco IE 5000
- Cisco IE 4000
- Cisco IE 3400
- Cisco IE 3200
- Cisco IE 2000

**REP Ring with Cisco Catalyst 3850/Cisco Catalyst 9300 in Distribution**

Recommendations for this topology:
- It is recommended to use fiber links since it provides faster convergence than copper links.
- When using StackWise for distribution with a REP ring it is a good practice to locate the alternate port in between access switches to achieve higher Layer 3 convergence in case of primary stack member power failure.

**Figure 32  REP Ring with Cisco Catalyst 9300/Cisco Catalyst 3850 in Distribution**

Table 20 and Table 21 summarize convergence results during validation.

### Table 20  REP Ring with Cisco Catalyst 3850 in Distribution

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence mixed ring (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Max</td>
</tr>
</tbody>
</table>
Result Considerations

- Convergence was validated for Layer 2 traffic within a VLAN and Layer 3 traffic between VLANs in the same ring.
- Link disruptions refer to a single link failure in the ring. Switch failures refer to distribution switch failure.
- Validation with Cisco Catalyst 9300 platform was done in a Cisco IE 4000 only ring, a mixed platform ring with the following IE switches:
  - Cisco IE 4000
  - Cisco IE 3400
  - Cisco IE 3200
  - Cisco IE 2000
- Ring topology had 10 IE switches and two Stack members.
- Cisco IE 3200/Cisco IE 3400 ring topology testing was completed with four Cisco IE 3200/Cisco IE 3400 switches and the two node stack at the distribution.
- Simulated traffic and real IACS devices were used during validation. The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.

The Cisco Catalyst 9300 distribution StackWise configuration with Cisco IE 4000 and Cisco IE 3200/Cisco IE 3400 should be considered as the best choice for REP deployments for IACS environments, though considerations should be given to the outlier Max results for convergence which could cause a connection timeout for IACS applications.

### Table 20 REP Ring with Cisco Catalyst 3850 in Distribution

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Link Layer 2 Multicast</th>
<th>Link Layer 2 Unicast</th>
<th>Link Layer 3 Unicast</th>
<th>Switch Layer 2 Multicast</th>
<th>Switch Layer 2 Unicast</th>
<th>Switch Layer 3 Unicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>Layer 2 Multicast</td>
<td>500</td>
<td>119</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>550</td>
<td>90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>548</td>
<td>92</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Layer 2 Multicast</td>
<td>278</td>
<td>95</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>290</td>
<td>99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>384</td>
<td>120</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 21 REP Ring with Cisco Catalyst 9300 in Distribution

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence mixed ring (ms)</th>
<th>Convergence Cisco IE 4000 ring (ms)</th>
<th>Convergence Cisco IE 3x00 ring (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Max</td>
<td>Average</td>
<td>Max</td>
</tr>
<tr>
<td>Link</td>
<td>Layer 2 Multicast</td>
<td>388</td>
<td>85</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>172</td>
<td>42</td>
<td>166</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>176</td>
<td>45</td>
<td>178</td>
</tr>
<tr>
<td>Switch</td>
<td>Layer 2 Multicast</td>
<td>472</td>
<td>80</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>102</td>
<td>44</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>102</td>
<td>60</td>
<td>168</td>
</tr>
</tbody>
</table>
Parallel Redundancy Protocol (Rings or Non-Rings)

PRP is defined in the International Standard IEC 62439-3 and is deployed in utility substations but could be deployed in manufacturing and plant-based environments that require lossless redundancy for their IACS applications. PRP supports PTP, however PRP utilizes two independent LANs which may be more expensive to implement than HSR, which is ring based.

PRP is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks. PRP provides redundancy by connecting to two independent parallel networks (LAN-A and LAN-B) with two separate interfaces at the access or bridging switch. The device connecting to the two independent networks is known as the Dual Attached Node (DAN). This DAN will now have redundant paths to all other DANs in the network.

The DAN sends two packets simultaneously through its two network interfaces to the destination node. A redundancy control trailer (RCT), which includes a sequence number, is added to each frame to help the destination node distinguish between duplicate packets. When the destination DAN receives the first packet successfully, it removes the RCT and consumes the packet and the second packet is discarded. If a failure occurs in one of the paths then the packet will be received on the other network and lossless redundancy is achieved. Lossless redundancy will not be achieved in the unlikely event that both LAN-A and LAN-B have failures at the exact same time. Redundant power is also recommended.

Figure 33 PRP Overview
A Redundancy Box (RedBox) is deployed when an end node does not support two network interfaces and PRP redundancy. The RedBox provides the DAN functionality for devices connecting to it. This is the role of the Cisco IE 4000 or Cisco IE 4010 and Cisco IE 5000 in a PRP redundancy deployment. The node behind a RedBox appears for other nodes like a DAN and is known as a Virtual DAN (VDAN).

The last node in a non-redundant node that only connects to a single network. This node would connect to either LAN-A or LAN-B and is known as a Single Attached Node (SAN).

PRP is not concerned with the topology of the independent networks, however the networks should be of a similar configuration so that packet delay is consistent between the two. Therefore, LAN-A and LAN-B can use ring based or star topologies for the deployments as long as both LAN-A and LAN-B use the same topology.

**PRP Mixed Traffic and Supervisory Frames**

Traffic egressing the RedBox PRP channel group can be mixed, that is, destined to either SANs (connected only on either LAN-A or LAN-B) or DANs. To avoid duplication of packets for SANs, the switch learns source MAC addresses from received supervision frames for DAN entries and source MAC addresses from non-PRP (regular traffic) frames for SAN entries and maintains these addresses in the node table. When forwarding packets out the PRP channel to the SAN MAC addresses, the switch looks up the entry and determines which LAN to send to rather than duplicating the packet.

A RedBox with VDANs needs to send supervisory frames on behalf of those VDANs. For traffic coming in on all other ports and going out PRP channel ports, the switch learns source MAC addresses, adds them to the VDAN table, and starts sending supervisory frames for these addresses. Learned VDAN entries are subject to aging.

**PTP over PRP**

Precision Time Protocol (PTP) can operate over Parallel Redundancy Protocol (PRP) on Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 switches. PRP provides high availability through redundancy for PTP. For a description of PTP and its implementation for this phase of industrial automation, see the PTP design for PRP.


**PRP Summary**

- Lossless Redundancy over two parallel networks (LAN A and LAN B)
- LAN A and B switches do not have to understand PRP protocol and can support any topology.
- High Cost due to need for independent LAN A and LAN B
- Standard IEC 62439–3 Clause 4
- RedBox switches connect PRP LANs to rest of network.
- PRP-capable end devices have one connection to LAN A and one to LAN B.
- Supported on Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, and 8/16 port Cisco IE 2000U
Recommendations for this topology:

- It is recommended to use fiber links since they provide faster convergence than copper links.
- Link bandwidth impacts the latency and the number of nodes that could be part of the HSR and PRP networks.
- GOOSE and Sample Values were classified and transmitted in priority queue on the egress interface.
- Configure unique VLANs for each IED to avoid multicast flooding.
- Enable storm control on the access/IED facing interfaces.

Table 22  Star Topology

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Latency</th>
<th>Packet Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Average (ns)</td>
<td>Max (ns)</td>
</tr>
</tbody>
</table>

Figure 34  Dual Redundant Star Topology Using PRP
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

Table 22  Star Topology

<table>
<thead>
<tr>
<th>Link</th>
<th>GOOSE (300byte)</th>
<th>40066</th>
<th>41900</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Values (128byte)</td>
<td>31556</td>
<td>63680</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>IP (1mix)</td>
<td>43140</td>
<td>109480</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>GOOSE (300byte)</td>
<td>40471</td>
<td>41140</td>
<td>0</td>
</tr>
<tr>
<td>Sample Values (128byte)</td>
<td>32077</td>
<td>61660</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

High Availability Seamless Redundancy (HSR)

HSR is defined in International Standard IEC 62439-3-2016 clause 5. HSR has been seen primarily in utility IEC 61850 substation architectures, however, its lossless redundancy features make it a viable option for other plant-based environments where IACS applications require better ring convergence than REP. HSR is similar to PRP but is designed to work in a ring topology. Instead of two parallel independent networks of any topology (LAN-A and LAN-B), HSR defines a ring with traffic in opposite directions. Port-A sends traffic counter clockwise in the ring and Port-B sends traffic clockwise in the ring. The duplicated packet mechanism provides lossless redundancy under a single failure within the ring.

The HSR packet format is also different from PRP. To allow the switch to determine and discard duplicate packets, additional protocol-specific information is sent with the data frame. For PRP this is part of the RCT, whereas for HSR this is sent as part of the header. Both the RCT and HSR header contain a sequence number, which is the primary data used to determine if the received frame is the first instance or a duplicate instance.

The non-switching nodes with two interfaces attached to the HSR ring are referred to as Doubly Attached Nodes implementing HSR (DANHs). Similar to PRP, SANs are attached to the HSR ring through a RedBox. The RedBox acts as a DANH for all traffic for which it is the source or the destination. The switch implements RedBox functionality using Gigabit Ethernet port connections to the HSR ring.

Figure 35 shows an example of an HSR ring as described in IEC 62439-3. In this example, the RedBoxes are Cisco IE 4000 switches. The Cisco IE 4000 or Cisco IE 4010 and Cisco IE 5000 switches are the only switches that will support an HSR deployment.
Devices that do not support HSR out of the box (for example, laptops and printers) cannot be attached to the HSR ring directly because all HSR capable devices must be able to process the HSR header on packets received from the ring and add the HSR header to all packets sent into the ring. These nodes are attached to the HSR ring through a RedBox. As shown in Figure 35, the RedBox has two ports on the DANH side. Non-HSR SAN devices are attached to the upstream switch ports. The RedBox generates the supervision frames on behalf of these devices so that they are seen as DANH devices on the ring. Because the RedBox emulates these as DANH, they are called Virtual Doubly Attached Nodes (VDAN).

**HSR Loop Avoidance**

To avoid loops and use network bandwidth effectively, the RedBox does not transmit frames that are already transmitted in the same direction. When a node injects a packet into the ring, the packet is handled as follows to avoid loops:

- **Unicast packet with destination inside the ring**—When the unicast packet reaches the destination node, the packet is consumed by the respective node and is not forwarded.

- **Unicast packet with destination not inside the ring**—Because this packet does not have a destination node in the ring, it is forwarded by every node in the ring until it reaches the originating node. Because every node has a record of the packet it sent, along with the direction in which it was sent, the originating node detects that packet has completed the loop and drops the packet. This is illustrated in Figure 35 at the originating node.

- **Multicast packet**—A multicast packet is forwarded by each node because there can be more than one consumer of this packet. For this reason, a multicast packet always reaches the originating node. However, every node will check whether it has already forwarded the received packet through its outgoing interface. Once the packet reaches the originating node, the originating node determines that it already forwarded this packet and drops the packet instead of forwarding it again.
HSR RedBox Modes of Operation

An HSR RedBox can operate in one of the following modes that define how HSR handles packets in different scenarios:

- **HSR–SAN**—This is the most basic mode. In this mode, the RedBox connects SAN devices to an HSR Ring. No other PRP or HSR network is involved in this configuration. In this mode, the traffic on the upstream switch port does not have HSR/PRP tags and the RedBox represents the SAN device as a VDAN in the ring.

- **HSR–PRP**—This configuration is used to bridge HSR and PRP networks. The RedBox extracts the data from the PRP frame and generates the HSR frame using this data and it performs the reverse operation for packets in the opposite direction. This is more prevalent in utility substations deploying IEC 61850, but again could be an option if lossless redundancy for plants is required where two rings are being bridged.

Figure 36  HSR and HSR-PRP Overview


**HSR Summary**

- Lossless redundancy over a ring topology
- All nodes in the ring **must** have special hardware to support HSR and all nodes in the ring must support HSR.
- Useful for networks that require faster convergence than REP as it provides lossless redundancy
- IEC 62439–3 Clause 5 standard
- Supported on Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 only
- Bandwidth available in ring is reduced by up to half due to duplicate packets
- In a typical implementation, the receiving node removes both packets from the HSR Ring.
**HSR Topologies Design and Recommendations**

**Cisco Catalyst 9300/Cisco Catalyst 3850 StackWise REP and HSR with Cisco IE 4000 Switches**

This topology uses StackWise for distribution redundancy. It uses REP for connectivity between the access ring and the distribution as shown in Figure 37. HSR is implemented in the access ring topology. REP is used between the links which directly connect the IE access and Cisco Catalyst 9300 distribution switches. REP edge ports are configured on the access switch uplinks as shown in Figure 37. A disruption in this topology has zero downtime for traffic in the ring. A failure in the REP ring will have an impact on Layer 3 traffic according to REP convergence times. This topology without REP will result in network loops.

*Figure 37  Cisco Catalyst 9300/Cisco Catalyst 3850 StackWise REP and HSR with Cisco IE 4000 Switches*

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>Layer 2 Multicast</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>0</td>
</tr>
</tbody>
</table>

*Table 23 summarizes convergence results during validation.*
HSR-PRP Redbox for Multilevel Rings
HSR-PRP, also known as Dual Redbox, is used to connect PRP and HSR networks together. It is commonly deployed in utility substations, hence the testing results show GOOSE and Sampled Values but are applicable to other IP protocols. The following topology shows an HSR ring connected to a PRP network through two Red Boxes, one for each LAN. In this example, the IP frame originates in the PRP network and GOOSE and Sample Value frames originate and end in the HSR ring. A disruption in this topology has zero downtime for corresponding traffic and ensures that the latency for different traffic streams meet the expected requirements.

Table 23 HSR Ring with Cisco Catalyst 3850 (continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Layer 2 Multicast</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Layer 2 Unicast</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Unicast</td>
<td>780</td>
<td>405</td>
</tr>
</tbody>
</table>

Recommendations for this topology:
- Link bandwidth impacts the latency and the number of nodes that could be part of the HSR and PRP networks.
- HSR–PRP feature is supported only on Cisco IE 4000.
- GOOSE and Sample Values were classified and transmitted in priority queue on the egress interface.
Configure unique VLANs for each IED to avoid multicast flooding.

Enable storm control on the access facing interfaces.

**Table 24  HSR–PRP Redbox Ring**

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Latency</th>
<th>Packet Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Average (ns)</td>
<td>Max (ns)</td>
</tr>
<tr>
<td>Switch</td>
<td>GOOSE (300 byte)</td>
<td>31467</td>
<td>58940</td>
</tr>
<tr>
<td></td>
<td>Sample Values (128 byte)</td>
<td>21170</td>
<td>64400</td>
</tr>
<tr>
<td></td>
<td>IP (Imix)</td>
<td>65321</td>
<td>208900</td>
</tr>
<tr>
<td>Link</td>
<td>GOOSE (300 byte)</td>
<td>37528</td>
<td>60780</td>
</tr>
<tr>
<td></td>
<td>Sample Values (128 byte)</td>
<td>26671</td>
<td>63460</td>
</tr>
<tr>
<td></td>
<td>IP (Imix)</td>
<td>68430</td>
<td>189820</td>
</tr>
</tbody>
</table>

Result considerations:

- Convergence and Latency was validated for Layer 2 GOOSE, Sample Values, and IP traffic with unique VLANs for each type in the same ring.

- Link disruptions refer to a link failure in the active forwarding path. Switch failures refer to primary switch failure in the active forwarding path.

- The HSR ring had eight Cisco IE 4000 switches.

- PRP network had three and four Cisco IE 4010 switches as part of two different PRP LANs running RSTP for loop avoidance.

- Cisco IE 4010 and Cisco IE 5000 switches were configured as PRP Redundant nodes.

- The tests were carried out using GigabitEthernet links in the network.

**Media Redundancy Protocol (MRP)–PROFINET Deployments**

The media redundancy protocol (MRP) is a data network protocol standardized by the International Electrotechnical Commission (IEC) as IEC 62439–2. The MRP allows rings of Ethernet switches to overcome a single failure with recovery time much faster than achievable with traditional STP.

Roles—Cisco Industrial Ethernet switches support the following two roles:

- Media Redundancy Manager (MRM)

- Media Redundancy Client (MRC)

In a ring topology, only one switch or industrial automation System device can act as an MRM; all other devices will act as an MRC. The purpose of an MRM is to keep the ring loop free and provide redundancy when failure happens. The MRM does this by sending a control packet from one ring port and receiving them on its other ring port in both directions. If it receives the control packets then the ring is in an error-free state.

There are three port states used within MRP:
During normal operation, the network operates in the closed state. In this state, one MRM one ring port remains in a blocked port status and the other port is in the forwarding status. All MRCs will be in forwarding status as well. Loops are avoided because of the blocked port on the MRM.

**Figure 39  MRP Normal Mode of Operations**

When a network link or device fails, the ring transitions to the open status. When there is a failure as detailed in Figure 40, the MRM will not receive the control frame and assume a failure in the ring. The MRM will move its previously blocked port to the forwarding state so that both ports are forwarding.
**MRP Summary**

**Advantages include:**
- Fast convergence—MRP can provide convergence times of 200ms.
- Link integrity—MRP does not use an end-to-end polling function between edge ports to verify link integrity. It implements local link failure detection.
- Co-existence with Resilient Ethernet Protocol (REP)—MRP does not interact with REP but can coexist on the same switch. This allows the network architect to create advanced interoperable rings.
- Device level ring support—Because MRP is an inherent resiliency protocol for PROFINET Cisco Industrial Ethernet switch can form a ring with industrial automation systems devices, such as, PLC, Remote I/O.

**Disadvantages include:**
- License requirement for Manager node.
- Does not support multi-ring topologies.
- No hardware level redundancy for Manager (MRM).
- Slower convergence than Cisco REP.
MRP was validated with the Cisco IE 2000, Cisco IE 4000, Cisco IE 4010, and the Cisco IE 5000 switches. The following are the results from validation. Figure 40 was used as the test topology to validate the convergence for MRP. A PROFINET application was set up with the following parameters:

- PLC would monitor the status of the connection to the I/O station.
- If the I/O station does not respond within 100 msec, then an error is flagged and if an IO station responds within 100 msec, then there the error is not flagged.
- The goal of convergence test in MRP with PROFINET is to create a failure—link and switch and observe that the convergence happens within 100 msec.

Table 25  MRP Ring with PROFINET

<table>
<thead>
<tr>
<th>Disruption Type</th>
<th>Traffic Type</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>PLC-IO</td>
<td>&lt; 100 msec</td>
</tr>
<tr>
<td>Switch</td>
<td>PLC-IO</td>
<td>&lt; 100 msec</td>
</tr>
</tbody>
</table>

Result considerations:
- A link disruption refers to a link failure in the forwarding path and switch failures refer to a switch failure in the forwarding path.
- Tests were carried out with fiber cable used in all the switches.

Resiliency Summary and Comparison

Table 26 provides high-level guidance on resiliency protocols based on performance and interoperability. Note the maximum number of nodes is generally a recommendation, rather than an absolute limit.

Table 26  Resiliency Protocols Comparison

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Topology</th>
<th>Number of Nodes</th>
<th>Typical Convergence</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSTP/MSTP</td>
<td>Any</td>
<td>Max hops 255</td>
<td>50 ms - 6 seconds</td>
<td>Provides widest interoperability but poorest convergence and troubleshooting</td>
</tr>
<tr>
<td>MRP</td>
<td>Ring</td>
<td>50</td>
<td>200 - 500 ms</td>
<td>Siemens is big proponent. Interoperable with switches that support Standard IEC 62439-2. Common in PROFINET environment.</td>
</tr>
<tr>
<td>REP</td>
<td>Ring</td>
<td>50</td>
<td>50 - 250 ms</td>
<td>Cisco proprietary. Very easy setup and troubleshooting.</td>
</tr>
<tr>
<td>PRP</td>
<td>Any</td>
<td>Unlimited</td>
<td>0 ms</td>
<td>Duplicate LANs required.(expensive) Standard IEC 62439-3 Clause 4</td>
</tr>
<tr>
<td>HSR</td>
<td>Ring</td>
<td>50</td>
<td>0 ms</td>
<td>Requires all nodes in Ring support HSR. Standard IEC 62439-3 Clause 5</td>
</tr>
</tbody>
</table>

Note: RSTP and MSTP were not verified in this CVD and are only added for informational purposes.
Platform specifics and distribution switch redundancy mechanisms do factor into the equation and should also be considered. These can be found in the relevant sections in this DIG under each of the resiliency protocols for the Industrial Automation DIG validation. The number of nodes validated are also detailed.

Cell/Area Zone Management

Ethernet networks are an integral part of modern automation and control environments and operations personnel are growing increasingly dependent on network monitoring to reduce unplanned downtime. Therefore, OT control engineers are taking on more of a role for basic network management functions. The control engineers require visibility and access to the network when issues arise so network management must address the following key considerations:

- The management network should have a separate out-of-band infrastructure, as mentioned in Network Hardening—A Component of System Integrity, page 81. At a minimum it should have its own logical network so as to provide network connectivity to the Cell/Area Zone networking devices even when the in-band data plane network is impacted. The out-of-band network segments hosts console servers, network management stations, authentication, authorization, and accounting (AAA) servers, analysis and correlation tools, FTP, syslog servers, network compliance management, and any other management and control services. An out-of-band management network should be deployed using the following best practices:
  - Provide network isolation
  - Enforce access control
  - Prevent data traffic from transiting the management network
  - Enforce secure use of network management traffic (SSH, Simple Network Management Protocol Version 3 [SNMPv3])
  - Provide visibility of events, faults, and performance of the network to the operators in the control center using syslog and SNMP
  - If an out-of-band network is not viable, then a dedicated VLAN should be used for the management network.

- Within the Cell/Area Zone, the tools provided to help assist with the management of the network must provide an OT view that is familiar to a control engineer. It should look and feel like a component or extension of the IACS system rather than an IT network management tool.

- The network should be easy to deploy, configure, and monitor. Network components should be easy to replace or install for the OT experienced controls engineer. Zero or near-zero touch replacement of network switches in the Cell/Area Zone is a prime example of this.

Cisco has tools to address the requirements of the OT controls engineer in this space: Cisco IND and the IoT Device Manager (IoT-DM). Figure 41 highlights the network management support model for the Industrial Automation architecture. IoT-DM and IND are highlighted as the tools to support the Cell/Area Zone. Cisco DNA Center (DNA-C) is positioned as the tool to assist with network management at the operations layer where an IT-based team would provide network management functions in support of the industrial plant.
Cisco Industrial Network Director

The Cisco IND provides operations-centric network management for industrial Ethernet networks. The system supports industrial automation protocols such as CIP, PROFINET, OPC-UA, Modbus, BACnet, and so on to discover automation devices such as PLC, I/O, HMI, and Drives and delivers an integrated topology map of automation and networking assets; this provides a common framework for operations and plant IT personnel to manage and maintain the industrial network.

The system uses the full capabilities of the Cisco IE product portfolio to make the network accessible to non-IT operations personnel. The simple user interface streamlines network monitoring and delivers rapid troubleshooting of common network problems found in industrial environments. For more information see: https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf

At a high level the following features address the management requirements detailed earlier for the Cell/Area Zone:

- **Plug-and-play server for zero-touch switch commissioning**—The Cisco IND provides a plug-and-play server for the zero touch provisioning and replacement of industrial Ethernet devices. Pre-provisioned configuration and software for automated network commissioning help to ensure a consistent network design and security policy. A controls engineer now has an easy way to replace faulty network equipment such as the network switch. The engineer can swap the hardware when the switch fails and replace back into the network with the automated configuration and software image replacement using Cisco Plug and Play.

- **Automated Discovery of Industrial and network Assets**—Cisco IND not only discovers the networking topology but it can discover automation devices with Common Industrial Protocol (CIP), PROFINET, Modbus, OPC Unified Architecture (OPC-UA), BACnet, Siemens S7, and other industrial communication protocols. The user interface can provide visibility of connectivity between automation and networking assets on a dynamic topology map.

- **Network Management**—Building on top of the plug-and-play support of the industrial networking switches, Cisco IND can provide continuous monitoring of switch health and traffic statistics and switch configuration backup. GUI-driven actions let non–IT operations personnel securely add automation devices to existing network infrastructure. Cisco IND can provide detailed audit trails to track and adds moves or changes in the network.

- **Ease of Troubleshooting**—When there is unplanned downtime or networking issues the management platform needs to pinpoint issues and recover quickly. Cisco IND can visualize and provide alerts to networking events with contextualized industrial asset visibility.

- **Network Operations intent driven security**—Cisco IND is a key component to providing visibility and context to assets connected within the Cell/Area Zone. Industrial Network Director integrates with Cisco ISE and Stealthwatch, so security IT architects in alignment with OT engineers can define security policies based on the identity and location of industrial assets.
Role Based Access Control—Cisco IND is ideal for environments where different types of users need different levels of information and access. The ability to create multiple users and lock down their access to specific areas of the Cisco IND user interface ensures that only authorized personnel are able to perform more sensitive operations.

Rich APIs for rapid integration with industrial applications—Cisco IND includes a comprehensive RESTful API allowing it to easily integrate with existing industrial asset management tools, automation applications, and control systems. An intuitive API Tool is included with Cisco IND to help system integrators and developers rapidly learn and adopt the API.

Cisco IND Deployment Options and Considerations

Cisco IND can be installed on a server in the industrial zone with tightly restricted access to other areas of the network. It is recommended to use only secure protocols (such as HTTPS and SSH) when possible to protect critical data. If required, Cisco IND is lightweight enough to be installed on a ruggedized laptop that resides within a zone on a plant floor, as long as it meets the system requirements. Figure 42 highlights the position in the architecture for Cisco IND. The example shows a server in the Industrial zone and a secure, ruggedized laptop in the Cell/Area Zone (the laptop connectivity is not shown, but could be through secure onboarding through a wired or wireless access).

The Cisco IND application requires Layer 3 connectivity to all of the network assets and automation clients that it is tasked with discovering and monitoring. This means that all devices that need to be discovered and monitored should have an IP address assigned that is routable and able to reach the Cisco IND server.
If there is a firewall located between the Windows server hosting Cisco IND and the monitored devices, the firewall must be configured to allow the following protocols and ports through both inbound and outbound: TCP ports 5432, 8088, 8443, 443, 80, 21, and 50000-50050.

In order to use the Cisco Active Advisor integration, the client computer which is accessing the Cisco IND web interface also needs to have Internet access to be able to upload network inventory data.

Note: Depending on technical and business requirements, direct access to the Internet for Cisco Smart Licensing may not be available. In this situation, Cisco Software Manager Satellite can be positioned in the IDMZ between the IND server and the Cisco cloud to facilitate license management on premise.

Cisco IND Supported Platforms
- Cisco IE 1000
- Cisco IE 2000
- Cisco IE 3200
- Cisco IE 3300
- Cisco IE 3400
- Cisco IE 4000
- Cisco IE 4010
- Cisco IE 5000

Cisco IND Supported Industrial Protocols
- CIP
- PROFINET I&M
- Siemens S7
- Modbus/TCP
- BACnet/IP
- OPC-UA
Cisco IND System Requirements

**Figure 43  Cisco IND System Requirements**

<table>
<thead>
<tr>
<th>Minimum System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Operating System (OS) 64-bit version</strong></td>
</tr>
<tr>
<td>• Windows 7 Enterprise or Professional with Service Pack 2</td>
</tr>
<tr>
<td>• Windows 10</td>
</tr>
<tr>
<td>• Windows 2012 R2 Server</td>
</tr>
<tr>
<td>• Windows 2016 Server (64-bit version)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU</th>
<th>Quad-core 1.8 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Browser Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Browser</strong></td>
</tr>
<tr>
<td>• Chrome: Version 50.0.2661.102 or later</td>
</tr>
<tr>
<td>• Firefox: Version 46.01 or later</td>
</tr>
</tbody>
</table>

Cisco IoT Device Manager

The Device Manager is in the switch memory to manage individual and standalone switches. This web interface provides a user-friendly web device manager for easy out-of-the-box configuration and simplified operational manageability. You can access Device Manager from anywhere in your network through a web browser. The Device manager can be used to supplement the features and functions of the Cisco IND. The device manager eliminates the need for complex terminal emulation programs to configure the switch through a CLI. Modifications to switch configurations can be made and then backed up to Cisco IND.

Cell/Area Zone Security

Digital transformation initiatives in the plant are changing the dimension of traditional OT. Newer networking technologies and COTS hardware and software are replacing legacy products and newer business initiatives are forging a movement towards IT/OT convergence. Technology itself cannot address the entire security realm; people and process must play a critical part in addressing the cybersecurity threat. This is key when addressing OT security. The IT teams need to have a thorough understanding of the business requirements and processes that apply within the industrial environment and assist with implementation. This is extremely relevant in the Cell/Area Zone where traditional IT skillsets are limited and the IT/OT teams need to move away from the traditional siloed approach to network management and work together. A 2015 Gartner study found security can be enhanced if IT security teams are shared, seconded, or combined with OT staff to plan a holistic security strategy.

Security in the Cell/zone needs to be viewed as a component of an overall end-to-end security architecture within the plant. Any security capability needs to span the breadth of the plant and must encompass existing processes and strategy linked to an overall compliance effort while supporting the safety, 24/7 availability, and high OEE requirements of the plant.

This section addresses network hardening for the Cell/Area Zone and basic segmentation and restricted data flow techniques with VLAN segmentation. The evolution of this baseline security features to a more robust, scalable security architecture is addressed in OT Intent-based Security for Industrial Automation Use Cases, page 103, which focuses on asset visibility with Cisco IND, segmentation using TrustSec with Cisco ISE, and flow-based anomaly detection with Cisco Stealthwatch.
Restricted Data Flow Segmentation and Zoning

Segmentation is a key component to creating zones of trust to help protect IACS networks and processes. IEC 62443 details restricted data flow recommendations to segment the control system into zones and conduits to limit the unnecessary flow of data between process networks or services. Intentional or accidental cross-pollination of traffic between untrusted entities must be restricted. The Industrial Automation solution provides basic logical isolation guidance for segmenting the Cell/Area Zone traffic. Some plants may segment the networks into totally physically separate networks based on risk. For example, plants may provide a physically separate dedicated network for non-operational multiservice type applications such as voice services within the plant.

Within typical plant networks zones are defined as Cell/Area (Level 0–2), Industrial Operations and Control (Level 3), IDMZ and the Enterprise (Level 5). For Cell/Area Zone, further segmentation will apply to grouped IACS assets that need to communicate with each other, generally per cell or area. VLAN segmentation is the traditional approach that has been adopted to creating segmentation across the Cell/Area Zone. The VLAN will be defined for a group of devices that need to communicate with each other within the Layer 2 domain/subnet and a boundary device such as a Layer 3 router, switch, or firewall will allow or deny communications outside of the VLAN to provide inter-cell/area communication such as controller-to-controller communication or controller-to-IACS applications. The boundary device can apply access control between the VLANs or Cell/Area and other areas of the plant using traditional ACLs or firewall rules manually configured on the device deployed at the boundary. Within Cisco’s Industrial Automation the Layer 3 distribution switch can provide this functionality and becoming a policy enforcement point for the Cell/Area Zone.

Figure 44  Cell/Area Zone Layer 3 Distribution Boundary Device

The VLAN segmentation and ACLs has been the traditional way to provide restricted dataflow within IACS networks. While manageable for smaller plants, maintaining access policies can be cumbersome and difficult for larger plants. As more devices are added to a network, ACLs start to become large at policy enforcement points and are implemented at various places in the network, making it a distributed application of policy across an industrial plant. Continually updating ACLs poses a higher risk of misconfiguration and is generally not scalable. OT Intent-based Security for Industrial Automation Use Cases, page 103 details the use cases and evolution to a Cisco TrustSec architecture that helps enhance
security for industrial automation networks.

Network Hardening—A Component of System Integrity

System hardening, within the realms of cybersecurity, can be defined as reducing the attack surface or vulnerability of a system and making it more resilient to attack through hardening measures. Hardening activities include disabling unnecessary services and applications, providing least privilege user access to systems, and adding additional security features such as anti-malware, anti-virus, and endpoint security. General system hardening practices apply to networks as well. Network hardening will deploy least privilege access control, disabling or removing unused services, logging, and enabling secure protocols. These hardening features and functions need to be configured across the three functional planes within a networking system. These three functional planes are the Management Plane, the Control Plane and the Data Plane.

- Management Plane—The management plane provides access to the networking devices and consists of functions that provide management of the networking system. The management plane is used to access, configure, and manage a device, as well as monitor its operations and the network on which it is deployed. This includes interactive management sessions that use SSH, as well as statistics gathering with SNMP or NetFlow. When you consider the security of a network device, it is critical that the management plane be protected. If a security incident undermines the functions of the management plane, it may be impossible for you to recover or stabilize the network. Where possible an out-of-band network for network management should be deployed. This keeps network management traffic separated from IACS traffic, which has the advantage of keeping the device reachability independent of any issues that may be occurring in the IACS network. If an out-of-band network is not possible, a logically separated network using a dedicated network management VLAN should be utilized.

- Control Plane—The control plane of a network device processes the traffic that is paramount to maintain the functionality of the network infrastructure. The control plane consists of applications and protocols between network devices, which includes the routing protocols and Layer 2 protocols such as REP. It is important that events in the management and data planes do not adversely affect the control plane. Should a data plane event such as a DoS attack impact the control plane, the entire network could become unstable. It should also be stated that control plane traffic needs to be understood and protected so that abnormalities do not affect the performance of the network devices’ CPUs, thus making the networking device unstable and therefore creating/contributing to network-wide instability.

- Data Plane—The data plane forwards data throughout a networking system traversing the networking devices. This would be the IACS data traffic between controllers, I/O, HMI, and any other devices plugged into the network. The data plane contains the logical group of “customer” application traffic generated by hosts, clients, servers, and applications that are sourced from and destined to other similar devices supported by the network. Within the context of security, and because the data plane represents the highest traffic rates, it is critical that the data plane be secured to prevent exception packets from punting to the CPU and impacting the control and management planes.

The following provides best practices for network hardening.

Management Plane

- Dedicated out-of-band network should be deployed throughout the plant including the IDMZ.
- Least Privilege Access and AAA—The AAA framework, which is critical in order to secure interactive access to network devices, provides a highly configurable environment that can be tailored based on the needs of the network.
- Configure Infrastructure Access Control Lists—Devised to prevent unauthorized direct communication to network devices, infrastructure access control lists (iACLs) to prevent access to the network devices.
- Configure Secure Networking Protocols for access to the networking equipment such as SSH in place of telnet, SNMP v3.
- Network System Logging should be enabled throughout the architecture.
- All network device configuration should be backed up after initial installation, setup, and following modifications.
Control Plane
- Control Plane Protection or Policing—Most routers and switches can protect the CPU from DoS-style attacks through functionality equivalent to Control Plane protection or policing.

Switches
- Within switched networks, it is important to protect the overall switched network from instability. Mechanisms are deployed in these types of networks to protect the integrity of the Layer 2 switched domains. For example, Spanning Tree Protocol (STP) can be used within these switched domains to help maintain a loop free topology in a redundant Layer 2 infrastructure. Within Layer 2 networks, root devices exist that help provide information about the stability of the network. Guard mechanisms need to be configured so that these root devices are not changed. Bridge Protocol Data Units (BPDU) Guard and Root Guard are examples that should be configured to help protect the Layer 2 domain and prevent Spanning Tree instability.

Router/Routing Protection/Layer 3 Switches
- Neighbor Authentication—When configured, neighbor authentication occurs whenever routing updates are exchanged between neighbor routers. This authentication ensures that a router receives reliable routing information from a trusted device.
- Routing Peer Definition—The same dynamic peer discovery mechanisms that facilitate deployment and setup of routers can potentially be used to insert bogus routers into the routing infrastructure. Disabling such dynamic mechanisms by statically configuring a list of trusted neighbors with known IP addresses prevents this problem. This can be used in conjunction with other routing security features such as neighbor authentication and route filtering.
- Control Plane Policing/Protection—This option should be configured to help protect routing sessions by preventing the establishment of unauthorized sessions, thus reducing the chances for session reset attacks.

Data Plane
- Shutdown any unused ports—Place any ports not being used into a shutdown state. For the purpose of a switch, add the switchport VLAN command with an unused VLAN (not VLAN 1) so that if a port is accidentally activated, it will not affect any deployed VLANs.
- Port security limits the number of MACs on a particular interface. This helps to prevent threats such as MAC attacks. Port security should be enabled on switch access ports.
- DHCP Snooping—If servers or workstations in the architecture are using Dynamic Host Configuration Protocol (DHCP), then DHCP snooping and Dynamic ARP Inspection (DAI) should be considered.
- Traffic Storm Control—A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature can be used to prevent disruptions on Ethernet interfaces by a broadcast, multicast, or unknown unicast traffic storm. Storm control can be configured on the switch.

VLAN Best Practices
- Disable all unused ports and put them in an unused VLAN. Any enabled open port provides an access medium into the network.
- Do not use VLAN 1 for anything. VLAN 1 is the default VLAN and is enabled on all ports by default; therefore, it is a security best practice to configure all the ports on all switches to be associated with VLANs other than VLAN 1.
- To assist with preventing VLAN hopping attacks, whereby an end station can spoof as a switch, configure all user-facing ports as non-trunking. This prevents the port from going into trunking mode unless explicitly configured. Force tagging for the native VLAN on trunks and drop untagged frames to assist with preventing VLAN hopping.
- Explicitly configure trunking on infrastructure ports. For ports connecting switches, trunking is used to extend VLANs throughout the network. Explicitly configure only the VLANs required to be extended to other switches.

Note: DHCP snooping or Dynamic Advance Resolution Protocol (ARP) inspection utilizes IP Device Tracking. Certain industrial environments are susceptible to issues when IP device tracking is enabled. Follow the design best practices for IP device tracking as detailed in OT Intent-based Security for Industrial Automation Use Cases, page 103.
Industrial Networking and Security Design for the Cell/Area Zone

OT Intent-Based Networking Security

Industrial plant networks are not immune to malware propagation as compared to Enterprise networks. For example, the PLC blaster worm (Ralf Spenneberg, n.d.) demonstrated in a lab how a vulnerability in a PLC can be exploited by a worm and once the PLC is infected with a worm it can discover other vulnerable devices (PLCs) in the network and replicate itself on those discovered targets. Even though this attack is demonstrated in a lab, not in a production environment, it shows how malware can attack IACS devices if there are not adequate security protections such as asset visibility, traffic segmentation, malware detection and remediation of infected devices, and OT intent-based control mechanisms deployed in a plant floor.

To prevent malware such as PLC blaster from attacking the industrial plant, the following must be considered:

- Gain visibility of all IACS devices present on a plant floor. Knowing what is present and active in a network will be vitally important to designing a policy which controls who should communicate with whom. For example, if a PLC attached to a network is visible, then a security policy can be designed from that PLC to the rest of the network.

- Restrict the communication of flows going in the plant floor. Restricting the communication of flows reduces the reach of a particular device. If an infected PLC is able to communicate only to devices that it should communicate with and not allowed to go across, then the size of infection can be bound to a smaller value.

- Detecting malware spared in a network—The behavior of PLC blaster worm, first, is to scan the network and discover other vulnerable devices present in the network. The key defense strategy is to discover that a scan is happening in the network, the device doing the scans, and plan for an immediate remediate action.

- Allowing a remote expert to perform advanced analysis on an IACS device—When an IACS device is down or needs advanced troubleshooting, then in some situations a remote expert may need to access the device and do further analysis. The operations team is the best team to determine which IACS device has to be allowed to reach the remote expert and also when that access should be terminated.

Note: Cisco and Rockwell Automation jointly designed and validated OT Intent-Based Network Security for EtherNet/IP based devices. See the CPwE Network CVD listed in Previous and Related Documentation, page 313 for more information.

This section describes the following:

- IACS plant security reference architecture
- System components overview
- Cell/Area Zone
- Design considerations for deploying network security in Cell/Area Zone

Plantwide Security Reference Architecture

Figure 45 provides a plantwide view of security and suggested areas of responsibility for deploying security. This highlights collaboration between control system engineers, IT network engineers, and IT security architects.
The CPwE CVD defined personae for the security architecture. The following provides details aligned with the figures above.

- **Control System Engineers (highlighted in tan)**—IACS asset hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network monitoring and change management, network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, and IACS application authentication, authorization, and accounting (AAA).

- **Control System Engineers in collaboration with IT Network (highlighted in blue)**—Computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), network monitoring and inspection, and wired and wireless LAN access policies.

- **IT Security Architects in collaboration with Control Systems Engineers (highlighted in purple)**—Identity and Mobility Services (wired and wireless), network monitoring with anomaly detection, Active Directory (AD), Remote Access Servers, plant firewalls, and Industrial Demilitarized Zone (IDMZ) design best practices.

Standardization plays an important role in helping to provide an overall security strategy to align people process and technology. A security risk assessment is a key step and will help define which systems are critical control, non-critical control, and non-operational to assist with defining an overall security architecture while still meeting business and safety requirements. Risk assessment guidelines are provided in IEC 62443–3–2. Once the risk has been assessed, foundational security requirements as defined in IEC 62443–3–3 can provide guidance in securing the industrial control system. The DIG for the Industrial Automation program aligns with these foundational requirements:

- **FR1 Identification and Authentication Control**—Identify and authenticate all users (humans, software processes, and devices) before allowing them to access to the control system.

- **FR2 Use Control**—Enforce the assigned privileges of an authenticated user to perform the requested action on the IACS and monitor the use of these privileges.

- **FR3 System Integrity**—Ensure the integrity of the IACS to prevent unauthorized manipulation.
Networking and Security in Industrial Automation Environments

Industrial Networking and Security Design for the Cell/Area Zone

- FR4 Data Confidentiality—Ensure the confidentiality of information on the communications network and in storage. This may include methods such as segmentation, protecting against unauthorized access, and data encryption.
- FR5 Restricted Dataflow—Use segmentation and zones to provide isolation for each environment and conduits to limit the unnecessary flow of data between zones and architectural tiers.
- FR6 Timely Response to Events—Manage, monitor, log, and control the security of the infrastructure to identify, defend, and prevent any security threats or breaches including management audit, logging, and threat detection.
- FR7 Resources Availability—Ensure the availability of the control system against the degradation or denial of essential services.

System Components Overview

The following Cisco security components assist in helping secure the Cell/Area Zone for the Industrial Automation CVD.

Industrial Network Director

Cisco IND is a network management product for OT. Cisco IND provides operations teams with an easily-integrated system delivering increased operator and technician productivity through streamlined network monitoring and rapid troubleshooting. Cisco IND is part of a comprehensive IoT solution from Cisco:

- Easy-to-adopt network management system purpose-built for industrial applications that leverages the full capabilities of the Cisco Industrial Ethernet product family to make the network accessible to non-IT operations personnel.
- Creates a dynamic, integrated topology of automation and networking assets using discovery via industrial protocols (CIP, PROFINET) to provide a common framework for OT and IT personnel to monitor and troubleshoot the network and quickly recover from unplanned downtime. This CIP and PROFINET discovery also allows Cisco IND to display details of the connected industrial devices (such as PLCs, I/O, Drives, HMI etc.).
- Rich APIs allow for easy integration of network information into existing industrial asset management systems and allow customers and system integrators to build dashboards customized to meet specific monitoring and accounting needs.

Although IND is targeted as a network management tool for OT personnel, the asset visibility function is utilized in the Industrial Automation security architecture. This asset visibility using the discovery function is a key component to provide context to a security profile and policy that can be applied to the Cell/Area Zone through Cisco ISE. This enriched context from Cisco IND is pushed to Cisco ISE using Cisco Platform Exchange Grid (pxGrid). For more information see: https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf

Cisco Identity Services Engine

Cisco ISE brings awareness of all the devices that are accessing the network. It permits an IT security professional to create consistent security policies across the breadth of the entire network. Cisco ISE becomes the policy engine for users and assets that require access to the network. ISE shares user, device, and network details through pxGRID with partner platforms so that the other platforms can enhance their security policy. ISE can also take in information from other platforms through pxGRID to enhance security visibility and context. An example in this phase of Industrial Automation is with IND sharing devices discovered and pushing into ISE to enrich ISE with device context. Cisco ISE can reduce risks and contain threats by dynamically controlling network access. For more information about Cisco ISE see the Cisco ISE Overview: https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html#~stickynav=1

Stealthwatch

Cisco Stealthwatch improves threat defense with network visibility and security analytics. Cisco Stealthwatch collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic
on the extended network, so they can quickly and effectively respond to threats. Stealthwatch leverages NetFlow, IPFIX, and other types of flow data from existing infrastructure such as routers, switches, firewalls, proxy servers, endpoints, and other network infrastructure devices. The data is collected and analyzed to provide a complete picture of network activity.

With in-depth insight into everything going on across the network, you can quickly baseline your environment's normal behavior, no matter what your organization's size or type. This knowledge makes it easier to identify something suspicious.

Use cases for deploying in industrial plants include:

- Continuously monitor the extended network
- Detect threats in real-time
- Speed incident response and forensics
- Simplify network segmentation
- Meet regulatory compliance requirements
- Improve network performance and capacity planning


Cell/Area Zone Security Design Considerations

The Industrial Zone comprises the Cell/Area Zone(s) (Levels 0 to 2) and Site Operations (Level 3) activities. The Industrial Zone is important because all the IACS applications, assets, and controllers critical to monitoring and controlling the plant-wide industrial operations are in this zone. To preserve smooth industrial operations and functioning of the IACS applications and IACS network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the enterprise operations.

The Cell/Area Zone is a functional zone where the IACS assets interact with each other. The industrial network is a critical factor for the Cell/Area Zone because all the IACS assets must communicate to ensure that requirements for industrial operations are met. A plant-wide architecture may have one or multiple Cell/Area Zones. Each Cell/Area Zone can have the same or different network topologies. There could be different network topologies present throughout the entire plant-wide architecture. For the purpose of this Industrial Automation CVD, a ring topology (depicted in Figure 46) was chosen for design, testing, and validation because the ring topology design provides resiliency.
Figure 46 has the following components deployed at the following positions:

- **ISE** is deployed in distributed design—The policy service node (PSN) is deployed at Level 3–Site Operations and the ISE Primary Administration Node (PAN) and the primary Management Node (MnT) are deployed in the enterprise zone.
- **IND** is deployed in Level 3–Site Operations.
- **Stealthwatch**—Flow collector (FC) and the Stelathwatch Management Console (SMC) are deployed in the Level 3–Site operations.

The next section covers the design considerations that must be considered by OT control system engineers and IT security architects when deploying Industrial Automation Network Security solutions. The design considerations are important to understand how segmentation works and also the different approaches and why we chose an approach for this design.

**IACS Traffic Flows in a Network**

Horizontal communication among peer-to-peer IACS devices in a network is called East-West communication. Figure 47 depicts East-West communication in a plant-wide architecture. In plant floor operation peer-to-peer communication happens between devices that have interlocking feature enabled between them. An interlock is a feature that makes the state of two mechanisms usually dependent on each other. For example, when several process conditions have to be met before a piece of equipment is allowed to start, and when these processes are located in different Cell/Area Zones, then peer-to-peer communication must happen among these processes for starting a piece of equipment.
Allowing a server or any other device in Level-3 Site Operation, IDMZ or Enterprise Zone to communicate with an IACS asset in the Cell/Area Zone is called North-South communication. In Figure 48, the Engineering Workstation (EWS) is accessing a controller in the Cell/Area Zone and this communication flow is defined as North-South communication.
Cell/Area Zone Segmentation

IT security architects in conjunction with a control system engineer should design an access policy that specifies the East-West and North-South communication flows that must be allowed in an IACS network. In an IACS network, having an open policy that allows every IACS asset to communicate with every IACS asset is convenient, but that approach increases the risk of cyber threat propagation. On the other hand, implementing a restrictive policy that does not allow any inter Cell/Area Zone communication is also counter-productive because certain IACS assets need to access other IACS assets that exist in different Cell/Area Zones. Since the exact requirements of a particular scenario are based on the current IACS application requirements, specifying a policy that would work for all the deployments is not possible. Hence in this Industrial Automation Network Security CVD, an access policy example is shown that can be customized for use in different environments.

Assumptions about the access policy for an IACS network:

- All the traffic within the Cell/Area Zone is implicitly permitted because it is assumed that a Cell/Area Zone is formed because a group of IACS assets need to communicate with each other, so no enforcement is applied to any IES in the Cell/Area Zone.

- All the traffic between any two different Cell/Area Zones will be enforced. As an example, in Figure 49 Controller_A in one Cell/Area Zone is allowed to access Controller_C in another Cell/Area Zone, but Controller_B is not allowed to access Controller_C.

The next few subsections describe the general idea of segmentation, the different types of segmentation, and the pros and cons of choosing a segmentation technique.

**Figure 49  Example of Enforcement in East-West Traffic Flow**
Segmentation Using Layer 3 Access Control List (ACL)

When an IACS asset is not configured with MAC authentication bypass (MAB) and is unable to get a downloadable access control list (dACL) from ISE, use a static ACL on the distribution switch which is connecting different Cell/Area Zones. In Figure 50, ACL is applied on the distribution switch connecting the two Cell/Area Zones. In Figure 50, the ACL must allow communication between 10.20.25.10 and 10.20.8.10 so that Controller-A is able to establish communication with Controller-B.

![Segmentation Using Layer 3 ACL](image)

The above method has similar disadvantages in managing the ACL as the dACL. Whenever the controller IP address changes or is moved to a different location, then the ACL needs to be updated. The old entries need to be purged and the new entries added. This process can be burdensome and may lead to an IT security architect making mistakes.

Segmentation Using Downloadable Access Control Lists (dACLs)

Segmentation is the practice of zoning the IACS network to create smaller domains of trust to help protect the IACS network from known and unknown risks in the network. This section describes the first approach to segmentation by using Downloadable Access Control Lists (dACLs). See Figure 51, which describes how a dACL is provisioned on a device when an IACS asset gets attached to the network. In Figure 51, there are two Cell/Area Zones connected via a distribution switch. There are two controllers: Controller-A (10.20.25.10) in Cell/Area Zone -1 and Controller-B (10.20.8.10) in Cell/Area Zone -2.
The Controller connects to an access port on the IES which in turn sends an 802.1X MAB authentication request to the Cisco ISE.

The Cisco ISE, upon receiving the request, processes the request using the configured authentication and authorization policy and sends the authorization result as a dACL to the distribution layer switch.

The dACL installed on the IES to which Controller-A is attached determines the destination IP addresses with which this controller can communicate. If a control needs to be imposed, then add an entry in the dACL.

The dACL must have Access Control Entries (ACEs) specifying which IP address is allowed to communicate with which IP address. In Figure 51, if CONTROLLER-A with IP address of 10.20.25.10 is permitted to communicate with CONTROLLER-B with IP address of 10.20.8.10, then the ACE must have a permit statement with 10.20.25.10 to 10.20.8.10.

The above method works in controlling access to a Cell/Area Zone and also between the Cell/Area Zones. However, this method has the following disadvantages:

- Assume communication is allowed between CONTROLLER_A and CONTROLLER_B. If CONTROLLER_B moved to a new location with a different IP address, then the dACL needs to be updated.
- If a CONTROLLER_A is allowed to communicate with a particular server in the Industrial Zone and if the IP address of the server changes, then the dACL needs to be updated again.
- If there is a large dACL, then it could impact the performance of the distribution switch.

Cell/Area Zone Segmentation using TrustSec Technology

Cisco TrustSec technology assigns SGTs to IACS assets, networking devices, and users when they attach to a network. By using these tags, an IT security architect can define an access policy and enforce that policy on any networking device.
Cisco TrustSec is defined in three phases: classification, propagation, and enforcement. When the users and IACS assets connect to a network, the network assigns them a specific SGT in a process called classification. Classification can be based on the results of the authentication and authorization policies and SGT is an end result of that process. For example, an IACS asset can be classified and assigned a specific tag if the IACS asset is a controller, I/O, HMI, or Windows workstation. Depending on the IACS asset type, a separate tag can be assigned to the IACS asset. Figure 52 shows how a controller is assigned an SGT value of 5. The process of SGT assignment is similar to how a dACL is pushed to the Cisco distribution switch when an IACS asset is attached to the IES. The only difference is that instead of a dACL, an SGT value is assigned. As shown in Figure 52, when Controller-A attaches to the IES, the IES goes through the 802.1X authentication and authorization with ISE and the result is a tag assignment to the IACS asset.

Apart from using Cisco TrustSec, customers can also use the methods described in the previous sections to segment the network, such as static ACLs and dACLs. However, the above two methods are difficult to manage, which can introduce errors during the deployment. Static ACLs need to be constantly managed, for example removing older entries and adding newer entries. Also, if the static ACL size becomes very large, then this can cause performance impact to the distribution switch. The second method using dACLs works well when the policy enforcement is done in the north-south communication flow—restricting communication from the Cell/Area Zone to any Zone above it. To restrict communication for the inter-Cell/Area Zone, dACL has the same limitation as static ACLs, namely the need to update the IP addresses whenever an IACS asset IP address changes.

The next phase of TrustSec is propagation in which the SGT tag is made of the Ethernet frame and sent from one switch or router to another device. The SGT tag that is assigned to the IACS asset must propagate along with every packet generated by the IACS asset. Figure 53 shows how an SGT inserted frame is propagated in the network. In Figure 53, the Controller-A has IP address of 10.20.25.10 and is assigned an SGT value of 5. When an Ethernet frame is generated by Controller-A, the IES inserts the SGT value of 5 along with the IP address and sends it to the next switch. The incoming switch, if configured with SGT in-line tagging, propagates the same frame to the next switch and this information travels in hop-by-hop fashion to the destination.
The previous phase describes a scenario for propagation using a method called in-line tagging. However, in certain network topologies there could be a situation where a switch in the path from the source to the destination does not support in-line tagging. When that scenario happens, the non-SGT capable switch would ignore the SGT in the frame and would send a normal Ethernet frame on the out-going interface. In other words, for in-line tagging feature to work, all the switches in the path must support this feature or the technology would not be applicable.

To circumvent that problem, Cisco TrustSec also supports a different mechanism to transport SGT frames over a path when a non-SGT capable IES (e.g., Cisco IE 2000) is present by using an exchange protocol called SGT Exchange Protocol (SXP). SXP is used to securely share SGT-to-IP address mapping. Figure 54 shows how to exchange SGT binding over SXP tunnel. In Figure 54, Controller-A is establishing communication with Controller-B using an SGT tag value of 5. As you can see there is a non-SGT device in the path and this switch would ignore the SGT enabled frame coming from the distribution switch. For SGT information to be sent to Switch-B, an SXP tunnel is required between Switch-A and Switch-B. This tunnel would carry the binding information, which is 10.20.25.10 mapped to SGT 5.
The third stage of Cisco TrustSec is policy enforcement. The enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router, or switch. The enforcement device takes the source SGT and looks it up against the destination SGT to determine if the traffic should be allowed or denied. The advantage of Cisco TrustSec is that any switch, router, or firewall between the source and the destination can impose the policy, but the key requirement is that the enforcement point must be able to map the destination IP address to the tag value. This process is further explained in Figure 55. In this scenario Controller_A has been given SGT value of 5 and Controller_B, which is of similar device type, is also given an SGT value of 5. The I/O device is given a different tag value because it is of a different device type. Now, in this scenario Controller_A is allowed to establish communication with Controller_C. However, the I/O device is not allowed to establish communication with Controller_C. The access policy can be described in Table 27.

Table 27 Access Policy Example

<table>
<thead>
<tr>
<th></th>
<th>SGT 5</th>
<th>SGT 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGT 5</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SGT 6</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The next step is to determine where to apply the policy. As shown in Figure 55, the enforcement can be at switches A, B, C, or D. However, as previously indicated, for a switch to enforce a policy it must be able to derive the destination IP address to the tag value. For example, at point A there are two flows occurring: 1) 10.20.25.10, 5 ---- 10.20.8.10, 5 and 2) 10.20.25.12,6 --- 10.20.8.10,5. If the access policy at point A is imposed, then the switch would be only able to understand the source tag, but it has no knowledge of the destination IP address to tag mapping. Switch A would see that the destination IP address is 10.20.8.10, but it does not know that 10.20.8.10 is mapped to tag value of 5, which should be allowed. The same behavior would be seen if the policy is applied at the point B. If the policy is applied at point C or D it would work because both C, which is Layer 2 adjacent to D, and Switch D, which is directly attached to Controller C, would be able to enforce the policy correctly because it would be able to derive the association between the destination IP and the associated SGT value.
Even though applying access policy at the point which is closest to the IACS asset is the preferred choice, in some situations a policy needs to be applied at a different point. Whenever away from the IACS asset, the knowledge of the mapping between the SGT value and the IP address is lost. To circumvent that problem establish SXP tunnels to the IES that has IACS assets attached to it. The details of using SXP for deriving the mapping information are covered below.

**Figure 55  Access Policy Enforcement Example**

**TrustSec Network Policy Enforcement**

The IT security architect must next decide where in the design the access policy should be enforced. Policy enforcement occurs at the distribution switch and there are pros and cons associated with each design choice. For example, consider the case where the policy is enforced on an IES located in the Cell/Area Zone. As stated in the previous section, the basic assumption is that every IACS asset in the Cell/Area Zone must be able to access every other IACS asset. The second assumption is that policies are enforced on East-West communication going across the Cell/Area Zones. For example, two Cell/Area Zones, Cell/Area Zone-1 and Cell/Area Zone-2, and a PAC and I/O are both in the Cell/Area Zones. From a Cell/Area Zone-1 intra-zone policy perspective, every PAC and I/O in Cell/Area Zone-1 must be able to access one another. The inter-Cell/Area Zone security access policy is to block the communication between I/O in Cell/Area Zone-1 to PAC in Cell/Area Zone-2. This security access policy is shown in Table 28.

**Table 28  Network Policy Matrix Example**

<table>
<thead>
<tr>
<th>PAC-Cell/Area-1</th>
<th>I/O-Cell/Area-1</th>
<th>PAC-Cell/Area-2</th>
<th>I/O-Cell/Area-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAC-Cell/Area-1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>I/O-Cell/Area-1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PAC-Cell/Area-2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>I/O-Cell/Area-2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
When designing a security policy using TrustSec, associate each IACS asset with a tag. If a PAC tag of 10 and I/O tag of 20 are assigned, designing the same matrix and restricting communication between 10 and 20, then two policy tables are needed: 1) Intra_Cell/Area Zone and 2) Inter_Cell/Area Zone.

**Table 29 Intra_Cell/Area Zone Access Policy Enforcement Example**

<table>
<thead>
<tr>
<th></th>
<th>10</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>20</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Table 30 Inter_Cell/Area Zone Access Policy Enforcement**

<table>
<thead>
<tr>
<th></th>
<th>10</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>20</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

As seen above, the Cell/Area Zone IES needs to have two tables implemented and that is not possible with the current design. The current TrustSec policy enforcement supports only a single matrix. To ensure both objectives are achieved, implement the security access policy on the distribution switch and do not have any enforcement on the Cell/Area Zone IES. By doing so, the Table 29 and Table 30 policy requirements have been met because when no policy is imposed on the Cell/Area Zone IES, then all the IACS assets on the Cell/Area Zone IES can communicate with each other. When Figure 55 is implemented on the distribution switch, then the inter-Cell/Area Zone or East-West communication can be restricted. Figure 56 shows the inter-Cell/Area Zone security access policy enforcement point. If the industrial security access policy requires intra-Cell/Area Zone access control, this CVD recommends IACS application security such as ODVA, Inc. CIP Security.

**Figure 56 Enforcement Point in Industrial Automation Network Security**
Scalable Group Tag Exchange Protocol Considerations

Scalable Group Tag Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint’s SGT along with the IP address from one SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically and the SGT can be used as a classifier in network policies.

SXP uses TCP as its transport protocol to set up an SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them acts as both speaker and listener.

Connections can be initiated by either peer, but mapping information is always propagated from a speaker to a listener.

As shown in the previous section, the enforcement is moved to the distribution switch, so the distribution switch needs to derive the destination IP address to SGT. This is because the Ethernet frame has only the source SGT information and to enforce the policy the distribution switch needs to learn the SGT binding associated with the destination IP address. To help the distribution switch to derive the destination tag, SXP tunnels are needed from the access layer IES to the distribution.

In the current design, SXP tunnels are established from the access layer IES to the Cisco ISE and the distribution switch also has an SXP tunnel to the Cisco ISE. This way the IP-SGT binding information is sent to the Cisco ISE and the distribution switch learns the IP-SGT binding information from the Cisco ISE. Figure 57 depicts the design.

Figure 57  SXP Design in Industrial Automation Network Security CVD
NetFlow

The Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, Cisco Catalyst 3850, and Cisco Catalyst 9300 support full Flexible NetFlow. NetFlow is an embedded instrumentation within Cisco software to characterize network operation. It provides visibility into the data flows through a switch or router. Enabling NetFlow provides a trace of every data conversation in the network without the need for any SPAN ports.

**Figure 58  NetFlow Example**

---

Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine if the packet is unique or similar to other packets. Traditionally, an IP Flow is based on a set of 5 and up to 7 IP packet attributes.

IP packet attributes used by NetFlow:

- IP source address
- IP destination address
- Source port
- Destination port
- Layer 3 protocol type
- Class of Service
- Router or switch interface
All packets with the same source/destination IP address, source/destination ports, protocol interface, and class of service are grouped into a flow and then packets and bytes are tallied and stored in the NetFlow Cache. The Cache can then be exported to a system such as Cisco Stealthwatch where deeper analysis of the networking data can be used to identify threats or Malware. For more information see: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-2_5_e/configuration_guide/b_1525

NetFlow Data Collection

A flow is a unidirectional connection between a source and a destination. To describe a full exchange between two devices, two independent unidirectional flows are needed. For example, when data is flowing between client and server, then there are two flows occurring: from client to server and from server to client. NetFlow is a protocol that creates flow records for the packets flowing through the switches and the routers in a network between the end devices and exports the flow records to a Flow Collector. The data collected by the Flow Collector is used for different applications to provide further analysis. Initially, NetFlow was used for providing traffic statistics in a network, but later it started gaining traction as a network security tool. In Industrial Automation Network Security CVD, NetFlow is primarily used for providing security analysis, such as malware detection, network anomalies, and so on. There are many advantages in deploying NetFlow:

- NetFlow can be used for both ingress and egress packets.
- Each networking device in a network can be independently enabled with NetFlow.
- NetFlow does not see a separate management network to collect the traffic.

In a normal flow the 5-tuples information (source IP, destination IP, source port, destination port, and protocol) information is recorded as shown in Figure 59.

**Figure 59  NetFlow Data Collection**

With the latest releases of NetFlow, the switch/router can gather additional information such as ToS, source MAC address, destination MAC address, interface input, interface output, and so on. For IND and ISE integration, collecting the MAC address of the device is very critical. If IND does not gather the MAC address, then the device is not imported into ISE. The following configuration shows the information collected at the IES in the Cell/Area Zone:

```
flow record Cisco Stealthwatch_Record
description NetFlow record format to send to Cisco Stealthwatch match datalink mac source address input match datalink mac destination address input match ipv4 tos
```
match ipv4 protocol
match ipv4 source address match ipv4 destination address match transport source-port
match transport destination-port collect transport tcp flags collect interface input
collect interface output collect counter bytes long collect counter packets long
collect timestamp sysuptime first collect timestamp sysuptime last

Configuration of flow records can be done by using IND, which is discussed in more detail in Cisco Industrial Network Director, page 201. The next important consideration is on managing flows. As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch flow collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets are received for the flow) or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download and the standard CIP/IO connections). There are timers to determine whether a flow is inactive or a flow is long lived.

After the flow time out the NetFlow record information is sent to the flow collector and deleted on the switch. Since the NetFlow implementation is done mainly to detect security-based incidents rather than traffic analysis, This CVD recommends leaving the default value in the switch, which is 30 seconds for inactive timeout and 60 seconds for active time out.

The next consideration is on enabling NetFlow in the network. Since in this CVD NetFlow is enabled for security perspective, the recommendation is to enable NetFlow monitoring on all the interfaces in the Industrial Automation network.

Stealthwatch Deployment Considerations

The Stealthwatch system has two different components, both of which are installed on different systems:

- Flow Collectors
- Stealthwatch Management Console

The Flow Collector collects the NetFlow data from the networking devices, analyzes the data gathered, creates a profile of normal network activity, and generates an alert for any behavior that falls outside of the normal profile. Based on the network flow traffic, there could be one or multiple Flow Collectors in a network. The Stealthwatch Management Console (SMC) provides a single point for the IT security architect to get a contextual view of the entire network traffic.

Note: For example, if there is a single Flow Collector and a single SMC, then there are two virtual or hardware appliances and each appliance has its own IP address and its own device credentials.

The SMC client allows an IT security architect to access the SMC graphical user interface by using a web browser. SMC enables the following:

- Centralized management, configuration, and reporting for up to 25 Flow Collectors
- Graphical Charts for visualizing traffic
- Drill down analysis for troubleshooting
- Consolidated and customizable reports:
  - Trend analysis
  - Performance monitoring
  - Immediate notification of security breaches

Some important considerations when deploying a Stealthwatch system include:
Stealthwatch is available as both hardware (physical appliances) and virtual appliances. To install hardware and software appliances, refer to the Stealthwatch guide:

The resources allocation for the Stealthwatch Flow Collector are dependent on the number of flows per second expected on the network and the number of exporters (networking devices that are enabled with NetFlow) and the number of hosts attached to the each networking device. The scalability requirements for the Flow Collector are available at:

The Data Storage requirements must be taken into consideration, which are again dependent on the number of flows in the network. The sizing table for Data Storage is available at:

A specific set of ports needs to be open to the Stealthwatch solution in both the inbound and outbound directions. For example, HTTPS needs to be open inbound so that a client can access the Stealthwatch solution for managing the appliances. Similarly, certain ports such as DNS, NTP, and external log sources should be open in the outbound direction so that the Stealthwatch solution can reach those services. For the complete list of ports that are recommended to be open, refer to:

Cisco ISE Deployment Considerations

Deploying Cisco ISE in a large network requires an IT security architect to consider several factors such as scalability and high-availability of the Cisco ISE deployment. This design guide covers in depth many factors related to deploying a large-scale Cisco ISE deployment model. The design considerations listed in the CVD are very much related to the current CVD effort. We encourage the reader to read the CPwE DIG to develop a good understanding of large-scale solution deployments. Some of the key recommendations given in the design guide are shown here as a quick reference.

In the distributed installation, the Cisco ISE system is divided into three discrete nodes (personas)—Administration, Policy Service, and Monitoring—which are described as follows:

- Policy Administration Node (PAN) allows the Enterprise IT team to perform all administrative operations on the distributed Cisco ISE system. The PAN (located in the Enterprise Zone) handles all system configurations that are related to functionality such as authentication and authorization policies. A distributed Cisco ISE deployment can have one or a maximum of two nodes with the Administration persona that can take on the primary or secondary role for high availability.

- Policy Service Node (PSN) provides client authentication, authorization, provisioning, profiling, and posturing services. The PSN (located within the Industrial and the Enterprise Zone) evaluates the policies and provides network access to devices based on the result of the policy evaluation. At least one node in a distributed setup should assume the Policy Service persona and usually more than one PSN exists in a large distributed deployment.

- Monitoring Node (MnT) functions as the log collector and stores log messages and statistics from all the Administration and Policy Service Nodes in a network. The MnT (located in the Enterprise Zone) aggregates and correlates the data in meaningful reports for the Enterprise IT and operational technology (OT) personnel. A distributed Cisco ISE system can have at least one or a maximum of two nodes with the Monitoring persona that can take on primary or secondary roles for high availability.

For optimal performance and resiliency, this CVD provides these recommendations for the Industrial Automation Identity and Mobility Services architecture:

- Administration and Policy Service personas should be configured on different Cisco ISE nodes.
Monitoring and Policy Service personas should not be enabled on the same Cisco ISE node. The Monitoring node should be dedicated solely to monitoring for optimum performance.

A PSN should be placed in the Industrial Zone (Levels 0-3) to provide services for clients in the Industrial Zone. If the Enterprise and Industrial Zones become isolated, any existing clients will still be able to securely access the network. For best practices, see Previous and Related Documentation, page 313 for links to the Industrial Automation IDMZ CVD DIG.

A PSN should also be present in the Enterprise Zone to authenticate corporate mobile users who connect to the corporate network through the IDMZ in a secure data tunnel. This scenario is covered in detail later in the document.

Based on the recommendations above, a typical distributed Cisco ISE deployment in the Industrial Automation architecture consists of the following nodes (hardware appliances or VM) as shown in Figure 60.

- One Primary Administration/Secondary Monitoring node
- One Secondary Administration/Primary Monitoring node
- One or several PSN in the Enterprise Zone
- One or several PSN in the Industrial Zone

Note: The number of PSN in the Enterprise and Industrial Zones may depend on the company size, the number of active clients, redundancy requirements, and geographical distribution (for example, one PSN per each plant).
IPDT Considerations

IP Device Tracking (IPDT) is a feature that allows an IES or any other switch or router to keep track of connected hosts attached to it. The IPDT feature must be enabled for several security features such as dot1x, MAB, Web-Auth, auth-proxy, and so on. The IPDT feature keeps mappings between IP addresses and MAC addresses. To do the tracking, the IES when enabled with IPDT feature sends an ARP probe with default interval of 30 seconds. The probes are implemented as per RFC5227 where the source IP address is set to 0.0.0.0. If the IPDT feature is enabled with a default source IP address of 0.0.0.0, then there could be conflict between the IES and an IACS asset that is also doing device tracking (the Duplicate IP address 0.0.0.0) problem is explained in: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/8021x/116529-problemsolution-product-00.html).

The recommended option is to modify the standard IP address used with the IPDT feature prior to the implementation of IPDT. The following command can be used in an IES:

ip device tracking probe auto-source fallback 169.254.26.64 0.0.0.0 override

This command uses the source of the probe to SVI if present and falls back to 169.254.26.64, which is a link-local IP address. The rational for using a link-local IP address as a fallback is based on the assumption that any device attached to the switch does not have a link-local IP address. The link-local IP address is used only to route packets within a local segment and if a router receives a link-local IP address then it does not forward the packet. The IT security architect must verify if there is any link-local IP address present in the network before enabling the command.

Note: IP Device Tracking (IPDT), which operates in accordance with RFC 5227, must be enabled on the IES to implement RADIUS downloadable ACL, NetFlow, and SGT. IPDT uses ARP probes to determine the IP addresses of hosts on different ports; this behavior may disrupt IACS assets devices and applications.

IPDT should only be enabled in the following situations on IES ports with 802.1X authentication:

- Maintenance ports and/or designated non-IACS equipment ports
- IACS ports with MAC Authentication Bypass if DACL is required by the security policy, with proper IPDT workaround applied and tested with IACS assets devices and applications

By default, IPDT should not be enabled on ports connected to IACS assets devices and applications if DACL functionality is not required. For more information and IPDT workarounds see: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html

OT Intent-based Security for Industrial Automation Use Cases

This section describes the implementation of the Network Security use cases documented in this Industrial Automation Network Security CVD DIG. The objective is to provide more details about each of the following use cases and also how different components, such as IES, ISE, IND, and Stealthwatch work together to support these use cases. This section describes the following use cases:

- Visibility and Identification of Network Devices and IACS Assets in the Cell/Area Zone
- Security Group Policy Assignment of IACS Assets in Industrial Zone
- Network Detection of Network Devices and IACS Assets
- Malware Detection of Flows in Cell/Area Zone and Level-3 Operations
- OT Managed Remote User (Employee or Partner) Accessing from (Enterprise or Internet) to a Network Device or an IACS Asset
Visibility and Identification of Network Devices and IACS Assets in the Cell/Area Zone

The purpose of this use case is to show how an OT control system engineer and IT security architect can work together to gain visibility of the network devices and IACS assets in the Cell/Area Zone. To segment traffic flows going across in East-West or North-South direction it is important that the IT security architect gain visibility of the current network topology in the plant-wide network. The visibility must be granular enough that the IT security architect can know the type of the IACS asset-Controller, I/O, drive, HMI, and others. Figure 61 illustrates the high-level steps to perform this use case.

Figure 61  Visibility and Identification of Network Devices and IACS Assets in the Cell/Area Zone

1. An OT control system engineer defines the IACS Asset Discovery profiles for IACS assets and the networking devices in IND. Refer to Creating Asset Discovery Profile, page 228.

2. OT control system engineer scans the IACS assets and the networking devices and verifies that the IACS assets and networking devices are grouped in Asset Inventory section of IND. Refer to Asset Inventory, page 229.

3. The IT security architect configures the pxGrid between IND and ISE. Refer to Configuring pxGrid between Cisco ISE and IND, page 232.

4. IT security architect configures profiling policies in ISE to profile the IACS assets based on the attributes provided by IND. Refer to Profiling in Cisco ISE, page 236.

5. ISE is able to identify Level_1_Controller in a Cell/Area Zone. Refer to Level_1_controller Policy, page 238.

6. ISE is able to identify Level_0_IO in a Cell/Area Zone. Refer to Level_0_IO_policy, page 239.

7. ISE is able to identify Level_3 in a Cell/Area Zone. Refer to Level_3_policy, page 241.
Cell/Area Zone Segmentation of IACS

This use case describes in detail about how to achieve segmentation of different traffic flows in a Cell/Area Zone. To understand traffic flows, refer to IACS Traffic Flows in a Network, page 87. The idea behind segmentation is defined in Cell/Area Zone Segmentation, page 89. Figure 62 provides the steps that an IT security architect needs to perform to achieve segmentation of different traffic flows.

**Figure 62  Segmentation of Traffic Flows in Cell/Area Zone**

1. The IT security architect must configure port-based authentication on all the IES. Refer to Configuring Port-based Authentication, page 251.

2. The IT security architect must configure TrustSec SGTs for different IACS assets - Level_1_Controller, Level_0_IO, and Level_3 in ISE. Refer to Configuring SGT Components, page 246.


4. The IT security architect must configure SXP tunnels from IES and the distribution switch to ISE. Refer to Configuring SXP Tunnel on an IES, page 252.

5. The IT security architect must configure the TrustSec Policy Matrix on ISE. Refer to Configuring TrustSec Access Policy Matrix, page 246.

6. The IT security architect must configure the enforcement on the Cisco Catalyst 3850 distribution switch. Refer to Configuring Distribution Switch—Cisco Catalyst 3850, page 254.
Flow Based Anomaly Detection

Network Detection of Network Devices and IACS Assets

This use case describes how an IT security architect can use Stealthwatch along with NetFlow enabled on IES and Cisco Catalyst 3850 to monitor the network flows in the plant-wide network. To detect traffic flows occurring in a plant-wide network, it is important that NetFlow is enabled on all the networking devices to capture the traffic flows that are sent to FlowCollector. Stealthwatch management console (SMC) retrieves the flow data from the FlowCollector and runs pre-built algorithms to display the network flows and also detect and warn if there is any malicious or abnormal behavior occurring in the network. In this CVD, three flows are shown to demonstrate the capability of Stealthwatch using NetFlow:

- Traffic between IACS assets in a Cell/Area Zone (Intra-Cell/Area Zone).
- Traffic between Level_3 IACS assets across the Cell/Area Zone (East-West or Inter-Cell/Area Zone traffic).
- Traffic between the EWS and a Level_3 IACS asset (North-South) traffic.

Figure 63  Network Flow Detection in Plant-wide Network

The following steps must be performed by the IT security architect to detect the above-mentioned flows:

1. IT security architect must enable NetFlow on all the IES and the Cisco Catalyst 3850 switches. Refer to Configuring NetFlow on IES, page 252.

2. IT security architect must use Host group feature in Stealthwatch to focus on certain flows if needed. A host group is essentially a virtual container of multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology. By grouping hosts into host groups, you can control how the Stealthwatch Flow Collectors monitor and respond to the behavior of those hosts as a group, rather than individually. To configure host group see: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf
Note: Although Cisco Catalyst 6800 and Cisco Catalyst 4500X core switches support NetFlow, the Industrial Automation CVD was only tested and validated with NetFlow enabled on the Cisco IE 4000 and Cisco Catalyst 3850. This CVD recommends that NetFlow be enabled throughout the plant-wide architecture.

Malware Detection of Flows in Cell/Area Zone and Level-3 Operations

This section discusses how Stealthwatch using NetFlow data collected by the FlowCollector detects malware flows happening in a plant-wide network. When malware is spreading in the network, it becomes very difficult to pinpoint where the malware propagation is occurring. An IT security architect needs to identify the source of the problem and then develop a remediation plan to address the problem. Stealthwatch has many inbuilt machine learning algorithms that can assist an IT security professional in detecting possible malware propagation in the network. Stealthwatch can detect any abnormal behavior occurring in the network and can also provide the IP address of the device that is causing the propagation. This information greatly simplifies the detection process.

Without Stealthwatch implemented in the network, the normal operation done by the IT security architect is to perform a number of steps that may involve many time-consuming operations, such as shutting down parts of the network, going through logs of many devices, checking the DNS log, and enabling debugs on many other devices to isolate the problem. All these steps not only take time to isolate, but also increase the risk of other vulnerable devices becoming infected. When active malware is detected, then quickly formulating a remediation plan is essential in building a defense against malware.

The malware behavior is to immediately scan the network to identify any other vulnerable devices in the plant-wide network. In this CVD, two traffic flows related to malware are discussed:

- An infected laptop attached to an IES. Figure 64 shows an example of how a scan can be performed by an infected laptop.

**Figure 64  Scan by an Infected Laptop**

- An infected laptop attached to a Layer-3 site operations center.
In both the cases, the infected laptop attempts to scan the entire IP address range to identify the next possible targets and attempt to infect them. Stealthwatch would immediately detect a possible infiltration by generating an alarm under High Concern Index. Any alarm that comes under High Concern Index must be immediately taken into consideration. Figure 65 shows how an alarm is displayed in the Stealthwatch Management Console. In Figure 65, the host 10.20.25.221 is attempting to do a scan for the 10.17.10.0/24 network.

Figure 65  Alarm Displayed in Stealthwatch Management Console


Figure 66 shows the scenario where an infected laptop is connected to Cell/Area Zone or Level_3 operations and is being detected by the Stealthwatch. The steps involved are:

1. The IES in the Cell/Area Zone or the distribution switch in Level_3 operations is enabled with NetFlow. Refer to Configuring NetFlow on IES, page 252.

2. The Stealthwatch Management Console reports an alarm indicating that there is a malicious activity occurring in the network.

3. IT security architect responds to the alarm by planning the next stage of remediation that can involve doing further investigation, restricting the access of the IACS asset, and so on.
OT Managed Remote Access to Plant Floor

This use case describes how a remote user employee or partner can access a networking device or an IACS asset from either internet or Enterprise Zone. The Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide (for best practices, see Previous and Related Documentation, page 313 for links to the Industrial Automation IDMZ CVD) provides design considerations and implementation details for providing remote access. The high-level steps for the remote access solution in that CVD as described in Figure 67 are:

1. A remote VPN gateway (ASA firewall) is enabled with VPN group that authenticates a remote user and authorizes a service, which in this case is to access a remote desktop gateway in the IDMZ.

2. The remote user, either employee or partner, uses a remote access VPN client (Cisco AnyConnect) to connect to the remote VPN gateway (ASA Firewall) and establishes a VPN session.

3. From the remote VPN gateway a connection is established to the remote desktop gateway in the IDMZ.

4. From the remote desktop gateway, a connection is established to the Terminal Server with FactoryTalk applications in the Level_3 - Site Operations.
This use case builds on the previous Securely Traversing IACS Data Across the Industrial Demilitarized Zone CVD and expands the remote user use case by providing the means for an OT control system engineer to influence the remote access. In the previous CVD, when a remote user needs access an OT control system engineer opens a request to IT security architect to enable remote access for IACS assets. The remote user than accesses the desired IACS asset. However, when the remote user no longer needs access to the IACS asset, then the OT control system engineer must open another case for removing access for a partner or an employee who no longer needs access. This process works, but when access is not removed in time then there could be a situation where a remote user has access to a networking device or IACS asset for longer than desired. Also, having this access open for a longer duration can open a window where a hacker can exploit this access to gain access to the networking device or IACS asset.

ISE-IND integration via pxGrid provides a way for an OT control system engineer to express operational intent to ISE using IND tool. The OT control system engineer expresses the intent by modifying the group of the networking device or IACS asset to a different group. In this CVD, a separate group called Remote_Access was defined to enable this feature. When an OT control system engineer changes the group of the IACS asset to the Remote_Access group, then remote access is enabled for that IACS asset and when the IACS asset is moved back to the original group, then the remote access to the IACS asset is revoked. The operation that needs to be done is to modify the group information of the IACS asset. Figure 68 shows the group information of an asset.
In this Industrial Automation CVD, the remote access use case is demonstrated by creating a separate group called Remote. A device that needs Remote_Access needs to be moved to this group called Remote. When such an action is performed the following events are triggered:

1. The IND sends a new device attribute “Remote” to ISE, which ISE reads as “assetGroup”. Refer to Remote_Access, page 241.

2. ISE classifies this device as Remote_Access and since there is a new classification, ISE issues Change of Authorization to the IACS asset. This triggers a new authentication/authorization, which results in a new SGT assignment “Remote_Access”. Refer to Remote_Access, page 241.

3. The Cisco Catalyst 3850 distribution switch downloads the new Secure Group Access Control (SGACL) from the ISE to allow access to Remote_Access. Refer to Configuring TrustSec Access Policy Matrix, page 246 and Enforcement, page 254. The traffic would flow from the FactoryTalk Application Server to the IACS asset.

4. Once the access to the IACS asset has been completed, the OT control system engineer moves the IACS asset back to the original group.

5. The IND communicates the new group information to ISE, which derives this information using assetTag. ISE would profile this as normal IACS asset. Refer to Level_1_controller Policy, page 238.

6. The Cisco Catalyst 3850 distribution switch has an existing policy that denies communication from Remote_Desktop to Level_1_Controller, so the communication from Remote_Desktop to Remote_Access is blocked.

Note: When a new SGT is assigned to an IACS asset there will be a temporary loss of connectivity for few seconds before applications can communicate with the IACS asset.

Device Onboarding

This section discusses the different scenarios related to managing an IACS asset as it is attached to the network. The scenarios described here are the following:

- A new IACS asset attached to the IES
An onboarded IACS asset is moved to a different port in the IES
- An onboarded IACS asset goes offline and comes back
- Replacement of a failed IACS asset

Onboarding a New IACS Asset

Onboarding a new IACS asset successfully means the following in this CVD:
- The IACS asset is scanned successfully by the IND.
- ISE learns about the IACS asset information from IND using pxGrid probe.
- The IACS asset has successfully completed port-based authentication and authorization to ISE and receives an appropriate SGT value.
- The IACS asset initiates traffic flows both intra-Cell/Area Zone and inter-Cell/Area Zone.
- The distribution switch (Cisco Catalyst 3850) is able to download the policy matrix from ISE and then enforce the traffic flows generated by the IACS asset.
- Steathwatch Management Console (SMC) is able to detect the traffic flows initiated by the IACS asset.
- SMC is able to generate an alarm if there is any malicious behavior generated by the IACS asset.

When all of the above activities are completed, then this solution assumes that the IACS asset is onboarded successfully in the network. When all the activities are completed, an IT security architect has accomplished the following objectives:
- Visibility of the IACS asset-Device type, Location (where it is connected), IP address, MAC address
- Segmentation of the IACS asset-Enforce the traffic matrix and control access to the IACS asset and also restrict the traffic flows initiated by the IACS asset.
- Network flow detection-Gain full visibility of the traffic flows generated by the IACS asset-where it is talking and who is talking to this IACS asset.
- Malware detection-Protect the IACS asset or other devices in the network from an infected device. The IT security architect would gain an understanding of the source of the infection and can develop and execute an immediate remediation plan.

In the above sequence, it is important to understand which part of the tasks are automated and where there is a dependency on the engineer in deploying the solution. The following tasks are performed when a new IACS asset attaches to the network:
- Scanning of the IACS asset by the IND-This is the only process where there is a dependency on the OT control system engineer to scan the IACS assets attached in the network. This process needs an OT control system engineer to press the scan button to learn about the IACS asset along with its attributes. Refer to Creating Asset Discovery Profile, page 228.
- Profiling of the IACS asset by the ISE-The profiling policies are expected to be configured on ISE (refer to the Profiling Policies in Cisco ISE, page 238) and when an IACS asset needs to be authenticated and authorized, ISE matches the policies and applies the appropriate authorization profile (refer to Authorization Policies, page 248). There is no manual intervention needed and this process happens as per the design. However, if ISE did not learn about the IACS asset from the IND and the IACS asset came online before that event, then ISE can only apply a default policy to the IACS asset.
- Whenever an OT control system engineer initiates a scan of the IACS asset, then the IND and ISE would gain visibility of the device. When ISE learns about more information it profiles the IACS asset and when the profiling policy matches the authorization policies, then ISE issues Change of Authorization (CoA) to the IACS asset. This process triggers a new instance of authentication/authorization to the ISE and this process enables an IACS asset in getting the correct SGT value.
NetFlow is enabled on all the ports where an IACS asset can get attached. So, whenever a new IACS asset is attached the traffic flow is automatically captured in SMC. There is no need for manual intervention by either OT control system engineer or by IT security architect.

SMC also monitors if there is any malicious behavior happening in the network by enabling several machine learning algorithms on the data collected from the network using NetFlow. This process also happens automatically and there is no manual intervention needed.

Figure 69 shows a detailed process flow diagram for onboarding a new IACS asset.

Figure 69  Process Flow Diagram for On-boarding a New IACS Asset
An Onboarded IACS Asset Moves to a Different Port in an IES

This section discusses the behavior of the network when an IACS asset is moved to a different port in the IES. The scenario described here is for a situation where an IACS asset is currently on-boarded, authenticated, authorized, and has an SGT tag assignment done and, in that state, it is moved to a different port in the IES. The assumption is that the new port has an identical configuration to the previous one. In this scenario, the following steps will happen:

- The port-based authentication (refer to Configuring Port-based Authentication, page 251) will authenticate any device attached to it. So, the IACS asset needs to re-authenticate to the ISE.
- ISE sees that the new device is already profiled and it matches the IP Address and MAC address, so it authorizes the IACS asset and issues the same SGT value as in the previous case.
- The IACS device will have the same access as it had in the previous case.

An Onboarded IACS Asset Goes Offline and Comes Back

This section describes a situation where an onboarded IACS asset goes offline and comes back to the network. The underlying assumptions are similar to the previous section. The IACS asset before going offline was assigned a SGT and was communicating to other devices based on the access that the particular device was assigned. Now in that situation, the IACS asset has become offline and the reasons could be a failure of the asset, longer maintenance work, and so on. Once the device comes back the following are the sequence of the events:

1. If the IACS asset is present in the endpoint data store, then the authentication and authorization will happen in normal fashion. By default, the IACS assets are saved permanently in the PSN data base. So even if the IACS asset comes back after a longer duration, the IACS asset can retain its older privileges.
2. If the IACS asset is purged from the endpoint data store, then the ISE will not be able to profile the IACS asset and the default policy would be applied.
3. When the condition 2 happens where an IACS asset is removed from the ISE, then the OT control system engineer needs to re-scan the device (refer to Creating Asset Discovery Profile, page 228) and then ISE will be able to learn the device, profile it, issue CoA, and then push the IACS asset the original SGT value.

Replacement of a Failed IACS Asset

This section describes the workflow items that need to be performed by OT control system engineer to replace a failed IACS asset.

1. The new IACS asset needs to be connected to the same port where the previous IACS asset was connected.
2. The OT control system engineer needs to re-scan the IACS asset using IND. The scan process will take a few minutes and depends on how many IACS assets are being scanned. The time taken to discover the IACS assets is linearly dependent on the number of IACS devices in the Access Discovery Profile.
3. Once the discovery is completed by IND, the information is sent immediately to ISE which re-profiles the device, issues CoA, and assigns SGT to the IACS asset.
4. Once the IACS asset is assigned the SGT, then the access of the new IACS asset would be same as the old one.
5. Only the OT control system engineer is required for the whole process, the rest of the infrastructure is automatic and the only process that needs to be done by the OT control system engineer is to re-scan the device.

Industrial Zone—Site Operations and Control Reference

The main focus of Industrial Automation from a validation perspective was the validation within the Cell/Area Zone of Cisco IE switches and the Cisco Catalyst 9300 at the distribution layer as the new platforms.
Note: The following sections provide design guidance and a reference architecture only for the Level 3 Site Operations and Control. High level design is provided only as this layer was not specifically validated in Industrial Automation or updated from previously validated CVDs. However the services such as ISE, IND, and Stealthwatch were deployed at this layer for security and network management services to support the Cell/Area Zone validation.

The Industrial Zone reference architecture in Figure 67 highlights the services (not all) deployed at the operations and control Level 3 within Industrial Automation. Key additions for the architecture are the addition of the Cisco Catalyst products at the core and distribution layer.

This level represents the functions required within Level 3 of the Purdue model and aligns with the core/distribution of the Enterprise networking model. The Industrial Site Operations and Control provides the Industrial applications and servers such as Historians, asset management, plant floor visualization, monitoring, and reporting. These applications would run on a plant or industrial data center. Network management and security services are deployed at this level including IND, ISE, and Stealthwatch, which are described in OT Intent-Based Networking Security, page 83. This level provides the networking functions to route traffic between the Cell/Area Zones and the applications within the Site Operations and Control. The Core and distribution would run Layer 3 routing protocols to support plantwide connectivity and provide the following key functions:

- Interconnecting the various Cell/Area IACS networks
- Interconnecting the Level 3 Site Manufacturing Systems
- Providing network management and security services to the Level 0 to 3 systems and devices
- Interface to the Plant Industrial DMZ

Figure 70  Site Operations and Control
Industrial Site Operations and Control Characteristics

The majority of industrial plant facilities have a very different physical environment at this layer of the architecture compared to the Cell/Area Zone Level 2 and below. The networking characteristics are less intensive with respect to realtime performance for the industrial protocols and equipment is physically situated in an environmentally controlled area, cabinet or room.

The following highlight the key design considerations for Site Operations and Control which directly impact platform selection, network topology, security implementation, and overall design:

- Industrial Characteristics—Environmental conditions, plant layout, and cabling costs all impact the platform choices and network topology in the design. Detailed earlier, the Cell/Area Zone in Industrial plants and processing facilities generally require physically hardened platforms. The general location and management strategy changes at Level 3. The networking platforms and servers housing the applications to support the plant are usually housed in environmentally controlled areas rather than the plant floor. This changes the dynamic of the platform choice which aligns with that of the traditional IT platforms such as the Cisco Catalyst 9500/Cisco Catalyst 9300/Cisco Catalyst 9200 products and Cisco non-hardened UCS platforms housing the IACS, security, and network management applications.

- Interoperability and Interconnectivity—Within the Industrial Zone one of the key requirements required at this level is to provide internetworking for inter Cell/Area Zone and plant wide communications. Layer 3 is required to connect the various cell area zones with Site Operations and Control and provide a path from the IDMZ. Core and distribution layer switches will provide this routing and align with any performance or QoS requirements that may be required for inter Cell/Area Zone traffic.

- Real-time communications, Determinism, and Performance—Packet delay and jitter within an IACS network can have significant impact on the underlying industrial process, however at Level 3 Site Operations and Control this requirement is very different to that of the Cell/Area Zone. Critical I/O real time traffic is generally restricted to the Cell/Area Zone. Inter-locking PLC type traffic may traverse between the Cell/Area Zone so QoS models should be configured at this layer to facilitate prioritization of this traffic. The general performance criteria is less sensitive to packet delay, latency, and jitter as the majority traffic flows between the Site operations level 3 and the Cell/Area Zones are generally non-real time from an industrial application perspective.

- Availability—A key metric within industrial automation is overall equipment effectiveness (OEE). Availability is still a critical requirement of the network at this Level 3. Although the applications at this layer may be more resilient to network outages than the Cell/Area Zone, it is still important that they are available to maintain operations within the Cell/Area Zone. Resilient networking protocols and QoS need to be addressed to support the traffic traversing the Layer 3 boundaries.

- Security—Security, safety, and availability are tightly aligned within an industrial security framework. When discussing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain.

- Recommended models would be the Purdue Model of Control Hierarchy, International Society of Automation 95 (ISA95) and IEC 62443, NIST 800-82 and NERC CIP for utility substations. Key security features are configures and provided at this Level 3 to support the Cell/Area Zone including device and IACS asset visibility, secure access to the network, segmentation and grouping of assets. Network hardening (control plane and data plane) are configured to protect the infrastructure.

- Management—Within the Industrial Zone and Site Operations and Control layer there needs to be a consistent management strategy. Where the Cell/Area Zone was operationally focused with a mixture of OT and IT personae, the operations and control level 3 has security and IT platforms which drive a higher IT skillset. Network management and security needs a combination of Security architects, IT personnel, and OT controls engineers to work in unison across a common network management framework.

- Traffic types—The traffic flows at this level in Site Operations and Control will predominantly support IACS applications such as Historians, asset management, IACS alarms and reporting, and network and security management applications (ISE, NetFlow, IND discovery). Multicast traffic seen supporting the IACS applications in the cell area zone does not leave the Cell/Area Zone so is not seen at this level.
Site Operations and Control Level 3 Components

The model above depicts a medium to large plant model which utilizes a classic enterprise networking model concept. There is a core, distribution within the Level 3 Domain which provides the plant-wide networking through regular routing protocols such as EIGRP or OSPF. The core provides connectivity into the “plant Data center” where the Cisco UCS would house the industrial applications and the network management and security functions for the industrial facility (Level 3 and below). These core switches would provide connectivity for communications to/from the Industrial DMZ.

Within the Industrial Data enter a Cisco Catalyst 3850 or Cisco Catalyst 9300 provides the connectivity for the servers deployed in the data center. A Cisco UCS is deployed to provide the physical hardware for the virtually hosted applications. The Cisco Catalyst3850 switch highlighted previously in the Cell/Area Zone components provided connectivity for the Industrial Data center in this phase, but the Cisco Catalyst 9200 and Cisco Catalyst 9300 could be positioned for the Industrial Data center switching. However, any data center design needs to consider the performance requirements of the applications hosted and the network requirements to support these applications.

Cisco Site Operations and Control Hosted Applications

Cisco Security Platforms

- Cisco Identity Services Engine–ISE as previously described would sit within the industrial data center. The ISE Policy services node sits at this layer. It provides asset authentication, authorization, provisioning, profiling, and posturing services. The PSN (located within the Industrial and the Enterprise Zone) evaluates the policies and provides network access to devices based on the result of the policy evaluation.

- Cisco Stealthwatch–Stealthwatch is hosted in the industrial data center. It improves threat defense with network visibility and security analytics. Cisco Stealthwatch collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection.

Network Management

Cisco Industrial Network Director (IND)–Cisco IND can be hosted in the industrial data center. It will manage and communicate with assets and networking equipment in the Cell/Area Zones. Cisco IND provides visibility into the IACS assets attached to the network. IND supports industrial automation protocols such as CIP, PROFINET, OPC-UA, Modbus, BACnet, etc. to discover automation devices such as PLC, IO, HMI, and Drives and delivers an integrated topology map of automation and networking assets to provide a common framework for operations and plant IT personnel to manage and maintain the industrial network.

Cisco DNA Center was not validated in this phase of Industrial Automation, however it can be positioned as the management platform for the Cisco Catalyst products. This aligns with the tool being more IT intuitive at this level where a more IT aware knowledge base would be required working in conjunction with control engineers and the industrial requirements.

Time Synchronization

Time synchronization is critical for event and data analysis with correlation across the entire industrial infrastructure. This though is not always the case where Islands of time may be maintained per Cell/Area Zone. Network Timing Protocol (NTP) or Precision Time Protocol (PTP) must be enabled on all infrastructure components to ensure consistent timing is maintained and event correlation can be provided plantwide. This should be enabled at Level 3 across the entire industrial zone into the Cell/Area Zones.

Common Network-based Services

- DNS–Within the plant environment a dedicated DNS server is usually deployed for applications within the Industrial Zone.

- DHCP–DHCP services could be deployed across the Industrial Zone, however within the wired Industrial IACS devices the IP addressing is usually statically defined. See Cell/Area Zone IP Addressing, page 42.
Domain Controller/Directory Services—Dedicated to the Industrial Zone again, but could be synchronized with the Enterprise via the IDMZ architecture. The CPwE IDMZ CVD has details about the replicated services between the Enterprise and the Industrial Zone for EtherNet/IP environments.

High Level Network Design

Critical I/O real time traffic is generally restricted to the Cell/Area Zone. Inter-locking PLC type traffic may traverse between the Cell/Area Zone, so QoS models should be configured at this layer to facilitate prioritization of this traffic. The general performance criteria is less sensitive to packet delay, latency, and jitter as the majority traffic flows between the Site operations Level 3 and the Cell/Area Zones are generally non–real time from an industrial application perspective. Layer 3 is configured at this layer and the Layer 3 network convergence times will need to be factored into supporting the traffic flows, but it is generally acknowledged that this will suffice.

High Availability

The following looks at core routing and Layer 3 switch resiliency. Layer 3 routing starts at the Level 3 from the Distribution switches aggregating the Cell/Area Zones. The Level 3 Site Operations and Control traffic is very different from a performance perspective looking at the Cell/Area Zone and the Industrial Zone traffic flows previously described. Table 31 highlights Information/process times for typical traffic between the Cell/Area Zone and the Level 3 Site Operations and Control layer. Cycle times are in the second range, but this is product dependent so understanding the performance metrics of the applications must still be considered and factored into the network availability design.

Table 31: IACS Application Requirements Example

<table>
<thead>
<tr>
<th>Requirement Class</th>
<th>Typical Cycle Time</th>
<th>Typical RPI</th>
<th>Connection Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information/Process (e.g. HMI)</td>
<td>&lt; 1 s</td>
<td>100 – 250 ms</td>
<td>Product dependent</td>
</tr>
<tr>
<td>Time critical processes (e.g. I/O)</td>
<td>30 – 50 ms</td>
<td>20 ms</td>
<td>4 intervals of RPI, but =100 ms</td>
</tr>
<tr>
<td>Safety</td>
<td>10 – 30 ms</td>
<td>10 ms</td>
<td>24 – 1000 ms</td>
</tr>
<tr>
<td>Motion</td>
<td>500 μs – 5 ms</td>
<td>50 μs – 1 ms</td>
<td>4 intervals</td>
</tr>
</tbody>
</table>

The following provides high-level design guidance and recommendations with regard to availability for the Site Operations and Control Networking:

- Layer 3 routing between the core and the distribution switches (Large Plant deployments)
- Redundant Core/distribution routers with Active/Standby or Virtual switch redundancy features and functions. This includes Stacking or HSRP for the Cisco Catalyst 9300 at the distribution, HSRP at the distribution for the Cisco IE 5000, and StackWise Virtual for the Cisco Catalyst 9500 in the Core.
- Layer 3 routing between the IDMZ and the core/distribution routers
- Redundant Links throughout the architecture
- Configuration Backups of all networking devices (Cisco IND for the Cisco IE switches)
- Network Hardening best practices to protect the Management, Control, and Data planes of the network infrastructure
- Segment IACS applications with similar dedicated functions or separating critical from non–critical applications into their own VLAN. An example would be to keep security and network management on a different VLAN to the industrial applications supporting the Cell/Area Zone. This promotes security and availability if hosts are infected so that the Layer 3 boundary devices can be deployed to protect devices outside of the infected VLAN.
- Layer 2 Redundant star topologies described in the Cell/Area Zone deployed for the server switch connectivity
Networking and Security in Industrial Automation Environments

Industrial Zone—Site Operations and Control Reference

- Dual NIC connectivity from the servers to the redundant switches. Dual NIC technologies from the Virtual servers.
- Server, Virtual Server, or application redundancy where required
- IDMZ to prevent unauthorized access from the enterprise into the Industrial zone and to stop IACS traffic from leaving the Industrial Zone

Management

Generally there is a shift in the support model at the Level 3 for the network infrastructure. Generally, at Level 3 and above there is more of an IT awareness in the support staff. Security applications being deployed require a higher IT skillset. This does not detract from the fact that the network still needs to be intuitive and easy to support. The following are guidelines and high-level design recommendations to help support the management of the network infrastructure:

- Carry through the recommendation of a separate out-of-band management network where possible; at a minimum provide its own dedicated management VLAN.
- Logging is a cornerstone of a sound security and network management strategy. The network infrastructure needs to be configured with logging capabilities and reporting functions to a centralized security management system. Syslogs, along with SNMPv3, should be enabled to report any events or incidents discovered at the endpoints.
- Although not validated, Cisco DNA Center or Cisco Prime Infrastructure can manage the Cisco Catalyst products positioned at this layer. You can manage the Cisco Catalyst 9000 series switches using the Cisco IOS software Command-Line Interface (CLI), using Cisco Prime® Infrastructure 3.1.7 DP13, Cisco DNA Center, onboard Cisco IOS XE Software Web User Interface (WebUI), Simple Network Management Protocol (SNMP), or Netconf/YANG.
- UCS Server Management recommendations are outside the scope of this document. The management of the physical and virtual servers in the industrial data center are specific to platform choice, storage architecture, and Virtualization vendor.

Security

Segmentation

- Within the industrial data center, segment IACS applications with similar dedicated functions or separating critical from non-critical applications into their own VLAN.
- Policy enforcement using Cisco IND, Cisco ISE, and TrustSec as per the Cell/Area Zone use case for advanced segmentation. Policy enforcement and segmentation are administered at the Distribution switch in Industrial Automation.
- For deployments where TrustSec is not deployed, access control lists should be used to provide the security policies for the domain.
- Visibility with NetFlow and Stealthwatch—The Cisco Catalyst 9000 series support NetFlow. Enabling NetFlow on all the NetFlow capable switches in Level 3, Core, Distribution, and the industrial data center and exporting to Stealthwatch will provide a plantwide view of application and network traffic. This can be used to help provide a baseline traffic profile and used to help identify anomalies in the network data flows.

Network Hardening

Secure the Control Plane, Management Plane, and Data Plane following the premise and guidance outlined in Network Hardening—A Component of System Integrity, page 81.

Server Hardening Practices and Endpoint Security

The following are examples of server hardening practices:
Networking and Security in Industrial Automation Environments

Site-wide Precise Time—Design Considerations

- Patching and Upgrading Operating Systems-To reduce vulnerability to attacks, systems should be patched to the latest vendor-recommended software and firmware levels. Patches should be tested before implementation. A plan for implementation of patches should be considered.
- Removing or disabling unnecessary services, applications, and network protocols
- OS User Authentication, least privilege access
- Host-based IDS and vulnerability scanning and endpoint security. When implementing, consider the impact of the security systems on application performance.
- Secure Networking protocols—SFTP (Secure File Transport Protocol), SCP (Secure CoPy) and SSH (Secure Shell), and SNMPv3 (Simple Network Management Protocol version 3)
- Backup or redundant databases
- Redundant servers and networking to support the availability of the applications

Site-wide Precise Time—Design Considerations

This section describes site-wide precise time based on IEEE 1588-2008 Precision Time Protocol version 2 (PTPv2). The section starts with the business value of precise time, describes other timing concepts, outlines the basic PTP architecture, and provides design considerations and recommendations to deploy site-wide precise time.

Note: Readers should review the relevant sections that introduce precision time standards and profiles, such as:
- Time Synchronization, page 117
- PTP over PRP, page 184
  - Configuring PTP over PRP, page 187
  - Troubleshooting PTP over PRP, page 187
- Cisco IE 5000 as PTP Grandmaster, page 189
  - Configuring PTP Grandmaster, page 190
  - Troubleshooting PTP Grandmaster, page 190

Introduction

Why Precise Time

The Industrial Automation solution is an important foundation for industrial companies driving IoT and Industrie 4.0 initiatives. By securely connecting IACS systems, devices, and applications, the solution enables access to rich amounts of data to drive IoT applications such as Predictive Maintenance, Digital Twin, and Big-Data analytics. That data is significantly more valuable when it is understood precisely when the data is produced. These IoT analytic applications can then derive better results (e.g., causality) based on consistent and precise time awareness.

Additionally, the key IACS applications that this solution was designed to support increasingly require precise time to perform their operations. PTP provides a common (i.e., network-based) precise time that applications can use to act and analyze sensed information from a range of devices. IACS standards and protocols are beginning to adopt PTP to support a range of functions, such as Sequence of Events and Motion Control applications. Examples of that include the ODVA, Inc.’s Common Industrial Protocols Sync function (CIP-Sync), OPC Foundations Unified Architecture, and IEC’s 61850 for Substation Automation.
Industry control systems typically have the time precision requirements shown in Table 32.¹

<table>
<thead>
<tr>
<th>Applications</th>
<th>Accuracy</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical substations</td>
<td>10 μs</td>
<td>Absolute time</td>
</tr>
<tr>
<td>Electrical grids</td>
<td>1 μs</td>
<td>Absolute time</td>
</tr>
<tr>
<td>Motion control</td>
<td>500 μs – 5 ms</td>
<td>Four intervals</td>
</tr>
<tr>
<td>Drive</td>
<td>1 μs</td>
<td>Relative time</td>
</tr>
<tr>
<td>IO</td>
<td>30 - 50 ms</td>
<td>Four intervals of RPI</td>
</tr>
<tr>
<td>Safety</td>
<td>10 – 30 ms</td>
<td>Four intervals of RPI</td>
</tr>
</tbody>
</table>

NTP, IRIG-B, and PTP are three typical time synchronization protocols developed to meet the above requirements, as shown in Table 33.²

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Media</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>Ethernet</td>
<td>50 - 100 ms</td>
</tr>
<tr>
<td>IRIG-B</td>
<td>Coaxial</td>
<td>1 - 10 ms</td>
</tr>
<tr>
<td>PTP</td>
<td>Ethernet</td>
<td>20 - 100 ns</td>
</tr>
</tbody>
</table>

Due to customer and application requirements for more time-aware applications and data, this solution now supports the site-wide distribution of precise time as a feature.

Other Timing Technologies

Synchronizing devices and applications in a network is not a new problem and has been addressed in several ways. Many IT applications, with lower precision requirements, use the Network Time Protocol (NTP). For industrial applications, either GPS was used for specific devices or IRIG was used to distribute time in an overlay network. IRIG is based on deploying an overlay network, which adds significant costs. Now, PTP has solved the problem of distributing precise time on converged, open, standard networks. Before PTP, achieving high precision required proprietary communication standards and overlay networks (e.g., IRIG-B). Here is a brief summary of timing technologies:

- **Global Positioning System (GPS)**—Precise time and geo-location are achieved with devices that receive satellite-based signals. Other similar services are being developed by Russia (GLONASS), China (BeiDou), and Europe (Galileo).

- **Inter-range instrumentation group time codes (IRIG)**—Before PTP, this was the most prevalent means of distributing precise time across a network based on non-Ethernet, single-function technology.

- **Network Time Protocol (NTP)**—An open standard protocol (current version IETF RFC 5905) to distribute time commonly found in IT systems.

- **Synchronous Ethernet (SnycE)**—An ITU-based method to distribute precise time over Ethernet commonly used in the telecommunications industry.

This solution is focused on distributing precise time via PTP across a site-wide network. In this architecture, GPS (or similar systems) or IRIG can be used to establish alignment with Coordinated Universal Time (UTC).

Networking and Security in Industrial Automation Environments

Site-wide Precise Time—Design Considerations

PTP Architecture Overview

The PTP (IEEE 1588v2) standard provides a series of mechanisms and algorithms to distribute time accurately while compensating for latency and jitter as the time is communicated over the network. The protocol operates in a hierarchical manner, establishing master-slave relationships among devices where slaves will synchronize their clocks with a master clock. The IACS devices and IES maintain time synchronization by sending and receiving PTP event messages containing information that allows them to correct time differences between master and slaves.

The process that builds the clock hierarchy, determining what devices will be assigned as master or slave, is done by using the Best Master Clock Algorithm (BMCA). When a PTP-capable clock joins the network, it will listen to PTP messages called PTP announce messages. These messages contain information such as time source, clock quality, and priority numbers. The BMCA runs continuously and uses the announce messages information to make these assignments and adjustments as necessary. The BMCA establishes the “grandmaster” clock and, depending on the configuration and capability of the network infrastructure, builds a hierarchy of master and slave clocks which are used to distribute time.

Components

PTP identifies the following key roles to perform time distribution:

- Grandmaster Clock (GM)
- Ordinary Clock (OC)
- Transparent Clock (TC)
- Boundary Clock (BC)

Grandmaster Clock (GMC)

The grandmaster clock is the primary source of time in the PTP domain. The GMC is chosen by the BMCA algorithm. GMCs should have high quality oscillators and be synchronized to UTC, for example from a GPS receiver.

- For the site-wide distribution of precise time, we recommend customers to acquire specific “grandmaster” devices, multiple for resiliency, and operate them as part of the manufacturing/site-wide application level of the network architecture.

  Or:

- Establish two Cisco IE 5000 aggregation switches as GMCs with appropriate access to GPS (or similar satellite-based time) or IRIG connectivity to align with UTC.

Ordinary Clock (OC)

An ordinary clock is a device that has a single PTP port. It functions as an end-node in the PTP topology. Any clock can be selected by the BMCA as a master or slave within the PTP domain depending on the presence of other clocks. Ordinary clocks are the most common clock type in a PTP system because they are used as end nodes in the system. Typical examples of ordinary clocks in an IACS application are a Programmable Automation Controller (PAC) or an I/O device.

Boundary Clock (BC)

A Boundary Clock (BC) is a multi-PTP port device (e.g., IE switches). The BCs, along with Transparent Clocks, distribute time through the network. When not chosen as the Grandmaster, a boundary clock’s port on which the Grandmaster can be reached becomes a “slave” port. As a slave clock, the BC synchronizes its internal clock to the master. The boundary clock then becomes a master to IACS and network devices connected to the other ports. Other clocks connected to these ports will become slaves to the BC and synchronize to the BC’s internal clock. A BC relieves the GM from having to respond to every OC clock’s PTP messages, which is an important scaling consideration.
BCs can also be configured to infinitely persist time-properties received from the GMC, which is beneficial when the GM is unavailable, either due to device outages or connectivity loss. In this situation, the BC maintains consistent time distribution services helping maintain the availability of any IACS relying upon those services. In this case, customers should also consider network devices that are designed to provide consistent quality time over extended periods, for example have Temperature Compensated Crystal Oscillators (a.k.a. TCXO) or Oven-controlled Crystal Oscillator (OCXO, e.g., Cisco IE 5000s are Stratum 3E). BCs can also be used to distribute PTP into different VLANs.

BC clocks also tend to take longer to start up and re-configure when the GM clock timing configurations change, require more configuration, and tend to introduce more drift as the depth of BCs increases.

**Transparent Clock (TC)**

Transparent Clocks (TC) are another means by which network infrastructure devices distribute time. TCs measure and account for the delay in a time-interval field in network timing packets, making the switches temporarily transparent to the other master and slave nodes on the network. TCs compensate for latency across the network by inserting delay corrections into the PTP packets. TCs do not become nodes in the PTP hierarchy and are therefore neither master or slave clocks. TCs sit in-line between the master and slave clocks and provide time correction between these devices.

There are two types of transparent clocks defined in the PTPv2 specification:

- End-to-end (E2E) transparent clocks compensate for latency across a network by measuring how long the devices in the network take to process and forward the PTP packets. These measurements are added to the correction field in the PTP packets. This mechanism works on both brownfield, where some network infrastructure devices do not support PTP and greenfield, where all network infrastructure devices support PTP scenarios.

- Peer-to-peer (P2P) transparent distributes the delay measurement across the network which suggests all devices must be PTP compliant. P2P TCs are not compatible with E2E TCs. P2P is specified as part of the Utility profile and used in the Substation use cases. P2P TCs are not used in CI Sync applications.

TC clocks also tend to more quickly start up and re-configure when the GM clock timing configurations change, require little configuration, and tend to maintain more precise time as they scale.

This site-wide precise time distribution design recommends TCs using E2E for access-level switches.

**Resiliency**

As mentioned earlier, Precise Time is becoming a critical network-based function for Industrial Automation and Control applications and the associated IoT applications accessing them. Therefore, it is critical that the precise timing function is available and consistent for production operations. This section reviews resiliency considerations for PTP.

**Grandmaster Clock**

A functioning grandmaster is a requirement for consistent delivery of precise time in a network. The BMCA ensures that a grandmaster is chosen and, if connectivity or service is lost, another is chosen quickly, within a second or two. This solution recommends redundant third-party grandmaster devices in the manufacturing zone of the network to provide consistent time. Additionally, the solution recommends setting priorities in the network infrastructure to ensure a certain order of grandmaster “failover” in the case that connectivity or service is lost to the specific GM devices. Our recommendation is to establish the following GM priority for the BMCA:

1. Third-party grandmasters
2. Core switches
3. Aggregation switches
4. Controller devices with GM capability
Networking and Security in Industrial Automation Environments

Site-wide Precise Time–Design Considerations

In combination with the time-property persist setting, this ensures a single grandmaster is available as long as some network connectivity is available and that as network connectivity and/or third-party GM services are restored, that the PTP services are available and consistent, avoiding disruption to IACS systems that rely upon it. See Site-wide PTP Design Considerations, page 125 for more details.

Network Infrastructure

Much of this Industrial Automation solution has been dedicated to describing network resiliency in the core, aggregation, and access layers. In particular the use of Layer 2 resiliency protocols such as Etherchannel and ring protocols (e.g., Resilient Ethernet Protocol—REP, Spanning Tree, MRP, DLR, PRP, and HSR) as well as network resiliency features such as virtual switching, switch stacking, and HSRP for Layer 3 functions.

Unfortunately, PTP is not supported on all of these protocols and features. PTP is currently not supported on Etherchannel links, HSR, MRP, virtual switch bundles, stacked switches, or Layer 3 links. This solution recommends establishing separate, single-path Layer 2 connections between the GMCs in the manufacturing zone and over the core switches to the aggregation switches. Although there may be single-points of failure of connectivity to the manufacturing zone GMCs, the priority and BMCA configuration ensure quality devices are ready to take over GM functions quickly until connectivity and service are re-established.

In this way, PTP services can be site-wide distributed over resilient network infrastructure and topologies that provide highly-resilient network and precise time services. The solution does recommend distributing precise time in Spanning Tree or REP managed ring/multipath Cell/Area zone topologies. The Substation Automation solution, applying the Power profile, makes use of PTP over PRP topologies.

Additionally, to support site-wide PTP, we recommend that customers maintain resilient aggregation and core networking services based on HSRP between matched switches.

Components

The components used to test site-wide precision time distribution are shown in Table 34.

<table>
<thead>
<tr>
<th>Product Role</th>
<th>Product</th>
<th>Software Version</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Cisco IE 4000</td>
<td>15.2(7)E0s</td>
<td>Unit Under Test (UUT)–Boundary and Transparent Clock E2E</td>
</tr>
<tr>
<td>Access</td>
<td>Cisco IE 3000</td>
<td>15.2(7)E0s</td>
<td>UUT–Transparent Clock E2E</td>
</tr>
<tr>
<td>Access</td>
<td>Cisco IE 3400</td>
<td>16.11.1a(ED)</td>
<td>UUT–Transparent Clock E2E</td>
</tr>
<tr>
<td>Distribution</td>
<td>Cisco IE 5000</td>
<td>15.2(7)E0s</td>
<td>UUT–Boundary Clock</td>
</tr>
<tr>
<td>Core Switch</td>
<td>Cisco Catalyst 9300</td>
<td>16.9.2</td>
<td>UUT–Boundary Clock</td>
</tr>
<tr>
<td>Grandmaster clock</td>
<td>MeinBerg LANTime</td>
<td>6.24.021</td>
<td>Third-party GPS–based GM</td>
</tr>
<tr>
<td>PTP Analysis Tool</td>
<td>Calnex Paragon-X</td>
<td>27.10.40</td>
<td>PTP protocol/performance analyzer</td>
</tr>
</tbody>
</table>

Architecture Summary

The above sections outlined the key components in a PTP architecture. For site-wide distribution of precise time, this document suggests the following:

- Specialized third-party GMCs are installed in the manufacturing zone. For resiliency reasons, two GMCs are recommended. Each GMC should support and be connected to external antennae to receive GPS (or similar services) to align the clock with UTC.
Site-wide Precise Time—Design Considerations

- Cisco IE 5000s can perform as GMCs in certain scenarios, especially smaller networks with collapsed core/aggregation switching.
- Use core and aggregation switches that support PTP, specifically default profile and configured to be Boundary Clocks within the PTP hierarchy. These devices can then distribute PTP into multiple Cell/Area Zones within the site or production facility.
- Access switches can be configured to be E2E TCs to distribute time to an IACS VLAN.

**Note:** This design only supports distribution of time into one VLAN over a set of access switches supporting a Cell/Area Zone.

*Figure 71* depicts the site-wide precise time architecture.

**Figure 71** Site-wide Precise Time Architecture

---

**Site-wide PTP Design Considerations**

Refer to the following for additional information:

- IEEE 1588 Precise Time Protocol (PTP), page 21
- Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture
- Substation Automation Local Area Network and Security Cisco Validated Design
Best Master Clock Algorithm

This is the process that builds the PTP clock hierarchy, determining what devices will be assigned as master or slave, is done by using the Best Master Clock Algorithm (BMCA). In essence, it works in a similar manner to Spanning Tree Protocol. The GM is somewhat like a root switch and all master/slave settings are established based on that. When a PTP network is operational, all devices are started and synchronized. Moving the GM due to connectivity or device availability issues should not disrupt the level of synchronization if the network infrastructure has good oscillators to hold consistent time and the time meta-data does not change. The master/slave ports may change depending on the location of the GM, but the synchronization stays stable. This effect is measured and reported in the Performance, page 303.

When a PTP-capable clock joins the network, it will listen to PTP messages called PTP announce messages. These messages will contain information such as time source, clock quality, and priority numbers. Customers should ensure PTP devices that join the network are configured with appropriate priority settings to avoid unwanted devices becoming GM and potentially impacting the PTP operations. The BMCA runs continuously and uses the announce message information to make these assignments and adjustments as necessary. We recommend the following structure for site-wide precise time:

Grandmaster (GM) Tier

The grandmaster tier contains the designated grandmasters for the PTP domain. For site-wide precision time distribution it is recommended to select a third-party device to be the primary grandmaster and redundant for resiliency. This device should have an accurate and reliable clock and ideally be synchronized to UTC using a reference clock. The primary grandmaster should be protected from faults such as power failures to improve stability of the PTP domain. It is also recommended to designate a secondary grandmaster which should use the same PTP timescale and UTC offset to minimize impact to IACS applications when the secondary grandmaster becomes the grandmaster. However, failing over from a primary grandmaster to a secondary grandmaster and vice versa may cause disruptions to time synchronization.

For smaller production facilities, a Cisco IE 5000 switch can also act as grandmaster as they are designed to receive GPS or IRIG timing signals.

The specified grandmaster device(s) should have the BMCA priority1 value set low so that they win the BMCA election. The priority2 value should be used to differentiate between the primary and secondary grandmasters with the primary having the lowest priority2 value.

Infrastructure Tier

The network infrastructure tier consists of core, aggregation, and access switches. The infrastructure should have the priority1 value set so first the core switches become GM if the GM devices are unreachable. Subsequently the aggregation switches should become GM if the core switches are unreachable. In addition, the `ptp time-property persist infinite` command should be applied to all switches configured as boundary clocks to preserve the time properties when the redundant GMC comes out of standby to prevent slave clocks from detecting a variance in the time values.

It is recommended to provide power protection to the infrastructure tier to improve overall IACS application reliability. Engineers should consider installing the infrastructure in separate enclosures (if appropriate) with dedicated power supplies and backup batteries.

Controller Tier

The controller tier is designed to reduce time synchronization issues when the network is down, such as when the control panel is powered on as IACS devices take different amounts of time to start up. Some IACS devices like Programmable Automation Controllers (PAC) feature battery backed real-time clocks and will continue to keep time when the power is disconnected. These IACS devices should have their priority1 value set so they become grandmaster until connectivity to the network is restored. This reduces the chance of a device without a real-time clock becoming grandmaster and setting an arbitrary time, like January 1 1970 00:00:00. Some IACS devices such as FactoryTalk Historian ME modules may fault if they detect an IACS application time that is significantly earlier than the time logged for existing data points.
Device Tier

The device tier contains all other PTP-aware IACS devices. Most of these IACS devices exclude battery backed real-time clocks and will revert to some known epoch on startup, such as January 1 1970 00:00:00. Therefore, they should not be relied on as a grandmaster clock. Their priority1 and priority2 values should be set so they will not become the grandmaster. The device tier is likely to contain most of the IACS devices in the plant-wide IACS architecture. The overhead of configuring the system can be reduced by using the default priority1 and priority2 value of 128 for the IACS devices in the device tier.

Table 35 shows an example of the priority settings that establish the above recommendations.

### Table 35 Priority Settings

<table>
<thead>
<tr>
<th>Role</th>
<th>Priority 1</th>
<th>Priority 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>GM1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GM2 (backup)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Core Switch BC</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>Core Switch BC (backup)</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Aggregation Switch BC</td>
<td>100</td>
<td>101</td>
</tr>
<tr>
<td>Aggregation Switch BC (backup)</td>
<td>100</td>
<td>102</td>
</tr>
<tr>
<td>Access Switch BC</td>
<td>110</td>
<td>111</td>
</tr>
<tr>
<td>Access Switch BC (backup)</td>
<td>110</td>
<td>112</td>
</tr>
<tr>
<td>Ordinary Clocks–PLC (Time module)</td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>Ordinary Clocks–IACS</td>
<td>128</td>
<td>128</td>
</tr>
</tbody>
</table>

Grandmaster Configuration

These recommendations are for devices intended to perform the GMC function:

- Third-party GM device PTP message update interval should align with IES and PLC and be compliant with customer PLC performance requirements.
- IES GNSS is supported only on Cisco IE 5000 switches with SKUs that have Version ID (VID) v05 or higher, GNSS is available as a timing source for PTP default and power profiles only.
- If IES PTP grandmaster clock loses the antenna signal, the clock quality will degrade, resulting in a GM switchover.
- GNSS receiver comes up in self-survey mode and attempts to lock on to a minimum of four different satellites to obtain a 3-D fix on its current position. It computes nearly 2000 different positions for these satellites, which takes about 35 minutes. The timing signal obtained during self-survey mode can be off by 20 seconds; therefore, Cisco IOS collects PPS only during OD mode.
- The participating grandmaster clock, switches, and slave devices should be in the same domain.

Network Infrastructure–PTP Port Settings

As PTP is a critical network function, it should be handled with high priority and appropriately marked with in the QoS fields of the VLAN tag. Therefore we recommend that each PTP capable network infrastructure be configured as tagged packets by entering the `global vlan dot1q tag native` command.
Table 36 shows the port-based PTP setting recommendations for network infrastructure in PTP default profile and in either BC or TC mode.

### Table 36  Port-based PTP Setting Recommendations

<table>
<thead>
<tr>
<th>PTP Port Interface Characteristic</th>
<th>What it does</th>
<th>When to use</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announce interval</td>
<td>Establishes frequency of the BMCA runs</td>
<td>If the BMCA algorithm needs to run more or less frequently.</td>
<td>1 (2 seconds, default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Should be consistent across the domain.</td>
<td></td>
</tr>
<tr>
<td>Announce timeout</td>
<td>Time Interval to declare announce msg timeout</td>
<td>Specifies the time for announcing timeout messages as a factor of 2.</td>
<td>3 (8 seconds, default)</td>
</tr>
<tr>
<td>delay-req interval</td>
<td>Interval to send delay-Req when ports is in Master state (device is slave)</td>
<td>Setting communicated to slaves (e.g., end devices with OC clock). This can improve startup synchronization time if device does not over-sample at startup. Increased number of delay requests can cause performance issues for TC clocks.</td>
<td>0 (1pps)</td>
</tr>
<tr>
<td>Sync interval</td>
<td>Changes frequency of Sync msgs transmits</td>
<td>The BC or GMC sends Sync msgs 1 per second. More frequent Syncs converge faster, but increase CPU utilization on OCs and BCs. Less frequent Syncs converge slower, but lower CPU utilization.</td>
<td>0 (1 second, default)</td>
</tr>
<tr>
<td>Sync limit</td>
<td>Max offset until attempt to resync</td>
<td>Is only in effect when switch is in BC mode and applicable on slave port. When the slave port drifts beyond this limit, the switch BC will resync likely disrupting PTP services and applications relying on it. As slave port can change, recommend setting on all ports.</td>
<td>10,000 ns</td>
</tr>
<tr>
<td>vlan</td>
<td>PTP VLAN on Trunk port</td>
<td>For BCs, change the 802.1Q tagged VLAN for PTP messages. Needs to be the same VLAN tag on both ends of Ethernet link.</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

### Boundary Clock Configuration

#### Synchronization Algorithm

The boundary clock mode has three different transfer functions that change how the boundary clock adjusts for packet delay variation (PDV) as shown in **Table 37**. PDV is a measure of the difference in the one-way end-to-end delay of packets in a network flow and is a more precise description of what is commonly referred to network “jitter”.

### Table 37  Boundary Clock Transfer Functions

<table>
<thead>
<tr>
<th>Transfer Function</th>
<th>PDV Filtering</th>
<th>Time Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (Linear)</td>
<td>Low</td>
<td>Average</td>
</tr>
<tr>
<td>Feedforward</td>
<td>None</td>
<td>Fast</td>
</tr>
<tr>
<td>Adaptive</td>
<td>High</td>
<td>Slow</td>
</tr>
</tbody>
</table>
This solution recommends use of the feedforward transfer function for production environments. Because the feedforward transfer does not filter PDV, it should only be implemented in networks where all of the network infrastructure supports PTP in hardware.

The adaptive filter can be used in applications with high PDV such as 802.11 wireless LANs. It can also be used in applications where the network consists of non-PTP aware switches and high PDV.

**Note:** The adaptive filter does not meet the time performance requirements specified in ITU-T G.8261.

**PTP VLAN**
A switch in PTP BC mode has the ability to process PTP traffic from different VLANs. This is a key means by which PTP becomes a site-wide service, although it is a Layer 2 protocol. BCs are used to distribute a consistent PTP across the network to various VLANs and Cell/Area Zones.

- Establish a PTP site-VLAN to distribute PTP from GM and across core and aggregation switches set in BC mode.
- Set the PTP VLAN on a trunk port. On trunk ports between the core and aggregation switches, this should be the PTP site-VLAN. On trunk ports to Cell/Area Zone (i.e., access switches), the VLAN is the IACS VLAN that needs PTP services.
- In BC mode, only PTP packets in port-associated PTP VLAN will be processed, PTP packets from other VLANs will be dropped.
- Before configuring the PTP VLAN on an trunk interface, the PTP VLAN must be created and allowed on the trunk port.
- When VLAN is disabled on the grandmaster clock, the PTP interface must be configured as an access port.
- Currently Cisco Catalyst 9300 platform PTP is supported only on VLAN-based SVI interfaces, not over Layer 3 links. Therefore additional Layer 2 links must be established to distribute PTP.

**Summary of Configuration Recommendations**

- **Grandmaster Tier**
  - Select a specific device to be a reliable grandmaster for the IACS applications. Connect it in the manufacturing zone directly to the core switches.
  - Select a PTP domain to be used consistently throughout the site.
  - Protect the grandmaster from faults such as power disruptions to increase stability of IACS applications.
  - Synchronize the grandmaster to UTC via GPS or similar technology.

- **Infrastructure Tier**
  - Configure the PTP Domain to be consistent throughout the site.
  - Ensure consistent PTP VLAN configuration on all links where PTP is communicated.
  - Use switches in PTP boundary clock mode to propagate time between VLANs and across core and aggregation switches.
  - On BC clock, use the feedforward transfer function and the sync limit (e.g., 10,000) to improve synchronization across IACS applications.
  - On BC clock switches, use the `ptp time-property persist infinite` command to help ride through the loss of the grandmaster.
  - Configure the switches to send PTP as tagged packets. Enter the `global vlan dot1q tag native` command.
Networking and Security in Industrial Automation Environments

Edge Compute with the Cisco IC3000 Industrial Compute Gateway

- Use switches in PTP E2E TC mode to propagate time on a ring or linear topology.
- Isolate and provide battery backed power to the switches to reduce Layer 2 and PTP topology changes.
- Do not send PTP traffic over EtherChannels, virtual switches, stacked switches, or Layer 3 links.

Controller Tier
- Configure IACS devices with real-time clocks, such as PACs, to become the grandmaster if the network is down.

Device Tier
- Use the default priority1 and 2 values (i.e., 128) to simplify configuration.

Cross-Industry Applicability

This Industrial Automation solution encompasses networking, security, and data management applied to a wide range of industrial verticals and applications, providing a range of design and implementation alternatives that may be applicable to several industries. Although the size, vendors, applications, and devices may significantly vary among these facilities, many of the core networking and security concepts are applicable. For example, while high availability is a key requirement across all industrial use cases, oil and gas and utilities may have more stringent availability requirements than a manufacturing facility. Nonetheless, the CVD solution best practice guidance is applicable across many industries and industrial customer environments.

Table 38  Cross-Industry Applicability

<table>
<thead>
<tr>
<th>Business Imperatives</th>
<th>Manufacturing</th>
<th>Utility Substation</th>
<th>Oil and Gas Plant</th>
<th>Mining Production</th>
<th>Waste Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximize uptime and quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve safety, security, and reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive predictive maintenance, machine learning, and Digital Twin applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect factory to partners and suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retain and acquire customers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve safety, security, and reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrate new energy sources and consumption models</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modernize the utility grid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximize uptime and quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve safety, security, and reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve decision making and drive machine learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect Refinery and Pipeline to partners and suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased mechanization through automated plant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve safety, security, and reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimization of material and equipment flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve anticipation of failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring of real-time performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Edge Compute with the Cisco IC3000 Industrial Compute Gateway

In the Internet of Things (IoT) space, devices at the edge require network connectivity to unleash value in the data these devices capture over time. Traditional networking infrastructure can provide this connectivity. Depending on the environment, more hardened industrial switching and routing hardware is required. Cisco offers a number of such devices that are fan-less, can withstand hot/harsh environments, and be deployed outside traditional networking.
cabinets. Devices such as Cisco Industrial Ethernet (IEx000) switches, Cisco Integrated Services Routers (IR8x9), and Cisco IC3000 Industrial Compute Gateways all provide hardened casings while performing different functions depending on the topology and the means of connectivity.

With network connectivity established, the very first question a networking engineer must answer is how to communicate with the edge devices above the Layer 3 network layer. Often what is required here is a compute device (such as an industrial PC) placed near the devices to communicate at the application/protocol level and extract the data from the devices. For this reason, Cisco introduced IOx. A compute environment exists within these devices and allows for the deployment of applications in the form of containers to extract device data.

Cisco IOx combines IoT application execution at the edge, secure connectivity with Cisco IOS, and powerful services for rapid, reliable integration with IoT sensors and the cloud, reducing for the need for external standalone compute deployments requiring additional management, space, and power. The advent of edge computing platforms offers many opportunities with Cisco IOx paving the way for innovative applications to emerge and demonstrate the wide-ranging capabilities of IoT.

Overview

Cisco IC3000 Industrial Compute Gateway extends data intelligence to the edge of the IoT network to seamlessly bridge the intent-based network and IoT data fabric in a complete end-to-end solution for applications such as intelligent roadways, smart factories, and so on.

- The IC 3000 is a device that can managed at scale using the Cisco IoT Field Networking Director product. See the data sheet at: https://www.cisco.com/c/en/us/products/cloud-systems-management/iot-field-network-director/index.html

Other related documentation includes:

- Cisco IOx DevNet https://developer.cisco.com/site/iox/
- MTconnect is the communication standard http://www.mtconnect.org/

The section is provided to guide the reader through the process of deploying an edge application on the Cisco IC 3000 with a Linux Containers (IOx Packaged/OVA/Docker) based app. To demonstrate the use of Cisco IOx, the open source MTConnect agent is described as a sample application.

The process will rely on the Cisco IoT Field Networking Director (FND) to deploy, manage, and monitor the application running on the IC3000. To demonstrate the capability of an MTConnect agent, two applications will be deployed on the IC 3000:

- The agent itself, which is an application that talks to an MTConnect-capable machine and makes the data visible to applications that need it via a REST interface.
- A machine simulator, which feeds data into the agent in the absence of real machine data for demonstration purposes.
As the IC 3000 is a compute device, not a networking device, it is ready to run IOx out of the box without any additional configuration beyond what is needed for the application itself. Once deployed, it will be immediately ready to receive applications deployed on top of IOx environment at scale using the Cisco FND.

Use Cases/Services/Deployment Models

This section addresses the following technology use cases:

- Edge Compute using Cisco IC 3000 with Cisco IOx and MTConnect agent as sample application.
- Application life cycle management at scale using Cisco FND and for individual devices using the IOx built-in Local Manager.

System Overview

By integrating the converged platform to the machine, downtime can be reduced and the Overall Equipment Effectiveness (OEE) can be improved. Figure 72 shows a typical customer deployment (on the left) versus Cisco’s offering (on the right). This network represents a sample zone with machines connected to a Cisco IC 3000 which, in turn, is connected to the data center where an application such as OEE resides.

Digitally connecting machines provides manufacturers with a way to capture critical data on machine utilization. This is one of the most important metrics to gauge how productive an operation is. Cisco Edge Compute devices provide the necessary tools to integrate, capture, and share machine data with upstream applications.

System Components

When Cisco IC 3000 is deployed with an application like MTConnect, it communicates to various machines pulling streaming data. Since it is not a networking device, it needs to connect to a switch like the Cisco IE 2000 or Cisco IE 4000. The switches are managed by the Cisco Industrial Network Director and the IC 3000s are managed with Cisco FND. as shown in Figure 73.
System Functional Considerations

As the IC 3000 is an industrial PC capable of having four physical interfaces in addition to the management Ethernet interface, it is potentially possible to have applications use one or more of the physical interfaces for data traffic or even have multiple applications share the same physical interface if they will communicate on the same subnet. For MTConnect application, two versions of the app have been tested:

- The first uses a single interface eth0 to communicate to the outside world (both machine side and enterprise side) using a single IP address.
- The second version has two interfaces, et0 and eth1. Each interface can be assigned to a physical interface, where each interface will be a different subnet. This is critical in situations where machines traffic isolation is necessary. The application will then communicate with the machine over one subnet using one physical interface and to the enterprise using a second subnet over a second physical interface.

The choice of design depends on the requirements for the specific deployment.

Note: While MTConnect is used here as a sample app for the deployment steps, any IOx Packaged or Docker applications can be ported over to IOx and the deployment steps would be the same.

System Implementation

This section includes the following major topics:

- Install Field Network Director, page 134
- IC3000 Bring Up and Application Install, page 135
Install Field Network Director

Cisco FND software can be installed one component at a time in an existing Linux OS. But a simpler way to install the software is to deploy the fully inclusive OVA file Cisco provides on CCO, using VMware ESXi 5.5/6.0 environment. You must download FND version 4.5.1-5 or higher for proper support of IC3000 code.


Once deployed, you can log in to the server at https://ip using the default credentials for the UI (root/root123). When asked to change the password, create a new password and login using the new password.

At this point the software is ready to create device configurations for the devices that will be managed by the server. The process is done using an csv file with the serial numbers of the IC3000 devices that will be added. An example of such a file with one IC3000 is:

eid,deviceType,lat,lng,IOxUserName,IOxUserPassword
IC3000-2C2F-K9+FCH2302Y003,IC3000,10,10,system,Cisco123

The contents of the file are:

- **eid**—PID VID + Serial number off the IC3000 label
- **deviceType**—IC3000
- **lat,lng**—Represents the geo coordinates where the device is located.
- **IOxUserName**—Creates a user name which will be used to access the devices IOx.
- **IOxUserPassword**—Assigns a password to the IOxUser defined for the device (minimum eight characters).

**Note:** The user ID and password will be used by FND to access the IOx on the device, but the user can also use these credentials to login in the Local Manager interface for the device. It is important to make sure the password defined is at least eight characters and has capital and special characters.

Next upload this csv file in FND under Devices->Add devices->Upload and ensure the UI reports success after uploading. At this point an IC3000 with any of the serial numbers that were imported will be able to communicate with this FND and download a configuration for the group of devices it belongs to or the default configuration. A configuration captures a number of items for a device such as heartbeat frequency, but mainly it tells the device which physical interfaces are to be enabled and the NTP server it will use to synchronize its clock going forward. This last step is very critical as it is the only means to set the clock of an IC3000 running in production mode with FND. Figure 74 is an example of such a configuration which enables two of the four physical interfaces and adds one NTP server as preferred.
IC3000 Bring Up and Application Install

IC3000 Boot Up and FND Connectivity

The boot up process described below is referred to as Production Mode, in which the IC3000 is managed by FND. If the device is brought up without FND, it is called developer mode. Refer to Troubleshooting, page 140 for more info on developer mode.

Each IC3000 needs to have its management interface connected to a DHCP-capable network device. This is because DHCP will provide critical pieces of information for this management interface in addition to the IP address. Currently the IP address of this interface must be assigned through DHCP and not statically. If a specific IP address needs to be assigned, then it is possible to use the host and client-identifier statements under the DHCP pool in IOS to force a specific address for a specific IC3000. Below is an example of IOS DHCP pool configurations to allow an IC3000 to register with FND where its serial number has been imported. The critical statements below are option 43 which specifies the IP address and port of the FND server (192.168.0.175:9125).

Note: It is no longer necessary to use option 42 to provide a ntp server IP as FND will provide it as shown above. If option 42 is provided, it will be ignored.

```
ip dhcp pool IC3KNET
    network 192.168.0.0 255.255.255.0
    default-router 192.168.0.50
    dns-server 192.168.0.15 8.8.8.8 1.1.1.1
    option 43 ascii 5A;K4;B2;I192.168.0.175;J9125
```

Once an IC3000 device is rebooted with this DHCP config, it will register with FND server and it should show up under the list of Up devices and its color will be green (see Figure 75). Also, the physical interfaces on this IC3000 which are being enabled by the downloaded configuration should also turn green to indicate they are active when connected to another device (a switch for example). The IC3000 is now ready to have IOx applications installed.
IC3000 Firmware Upgrade

If the IC3000 software version is Factory Default (1.0.1), you need to upgrade to version 1.1.1 to gain access to the latest features and fixes. The upgrade is done on all FND connected IC3000s at once that belong to same group. The upgrade steps are:

1. Make sure the ADMIN -> Provisioning Settings -> IoT-FND URL point to the FND server by IP or by name if reachable by DNS.
2. In CONFIG -> Firmware Update -> Images, select IC3000 from left panel and upload new image.
3. In CONFIG -> Firmware Update -> Groups, make sure that all IC3000s to upgrade belong to the same group, click Upload Image, and select the IC3000 image to upload to all devices.
4. In CONFIG -> Firmware Update, select the Group in the previous step and click Install Image. This step will install the image downloaded. Note that an upgrade could take 15 min if it requires a firmware upgrade and not just an IOx upgrade.

Note: If the upgrade fails for some reason, a device reset might be necessary (see IC3000 Reset, page 141).

Application Install and Configuration

The following steps install the MTConnect Agent application on one or many IC3000 devices at once. Unlike app installation via the Local Manager, the steps below install, activate, and start an app automatically with no further user intervention.

1. From the APPS tab in FND, select Import Apps to first add the app in the FND catalog. Here you are given an option to Import an app as an IOx SDK Packaged container, as an OVA, or from a Docker registry. The steps below assume an application tar file packaged with IOx SDK.
2. Browse for the app file on the local machine and click Upload to store the app on FND.
3. From APPS tab in FND, choose app and click Install.
4. Select one or more devices, then click Add Selected Devices to install list.
5. Click Next> to configure the app.
6. It is possible to customize a number of features on this screen, but we will only check the networking to make sure we are using int1(bridge) interface in Dynamic mode. Once selected, click REASSIGN NETWORKS to apply the change.
7. If asked to Configure VCPUs, select a value from 1–4 and click REASSIGN VCPU to confirm.
Networking and Security in Industrial Automation Environments

Edge Compute with the Cisco IC3000 Industrial Compute Gateway

8. Click **Done Let's Go** to complete the install.

9. Repeat the same process for the Simulator app if needed.

**Note:** While the deployed device configuration to IC3000 activated two interfaces, both MTConnect agent app and the simulator app require only one interface for operation. A version of the MTConnect agent app also exists which uses two interfaces if the deployment requires machine and enterprise segment separation.

**Application Uninstall**

To uninstall an application on one or many IC3000 devices at once:

1. From the **Apps** tab in FND, choose the application to uninstall and click **Uninstall**.

2. Select one or more devices, then click **Add Selected Devices** to the uninstall list.

3. Click **Done Let's Go** to complete the uninstall.

**MTConnect Agent Application Access and Configuration**

THE MTConnect agent application being deployed here is built on the open source version 1.4 of the agent published by: http://www.mtconnect.org/

The application comes pre-configured with a number of agents. Once installed and started, four of those agents automatically come up running. Each agent listens on a specific port (mapped to one machine) and provides a REST interface to northbound applications on another port. There are two ways to configure the agents running in a single MTConnect application:

- The first method is to use the application built in Web UI.
- The second method is to SSH directly to the application.

The IP address information of the app can be found in FND by choosing the device, then the **Apps** tab where all applications deployed on the device will be listed with their status and IP address information.

Each configured agent requires two critical files to operate:

- The first is the agent.cfg file, which includes IP addresses, port numbers, etc.,
- The second is a machine specific xml file that provides the agent with the schema of the data that will be arriving from the machine on this specific configured port.

Below is an example of an agent.cfg file with some inline comments.

```
# name of the machine xml file to be used for this agent. Found in same directory
Devices = ./VMC-3Axis.xml
AllowPut = true
# this is the northbound port to be used by upstream applications
# needing access to the data from this agent via REST API.
# Port = 5001
ReconnectInterval = 1000
BufferSize = 17
SchemaVersion = 1.3

Adapters {
    VMC-3Axis {
        # IP address of the machine/adapter where data is coming to the agent from (can be DNS)
        Host = gos.iotspdev.local
        # Port on the machine/adapter IP for access to streaming data
        Port = 7878
    }
}
```
Networking and Security in Industrial Automation Environments

Edge Compute with the Cisco IC3000 Industrial Compute Gateway

```xml

Files {
    schemas {
        Path = /home/root/schemas
        Location = /schemas/
    }
    styles {
        Path = /home/root/styles
        Location = /styles/
    }
    Favicon {
        Path = /home/root/styles/favicon.ico
        Location = /favicon.ico
    }
}

StreamsStyle {
    Location = /styles/Streams.xsl
}

# Logger Configuration
logger_config
{
    logging_level = info
    # location of log file, currently set to same dir as the agent.cfg
    output = file /home/root/data/appdata/agent1/agent.log
}
```

The machine xml file is unique to that machine since it provides the agent with all the data to expect from this machine. The data usually arrives directly from a machine if it has a built-in adapter or from an adapter that sits between the machine and MTConnect application providing the translation. A sample xml file is provided in Sample Machine XML File, page 143.

Managing Agents using Web UI

The MTConnect application built in Web UI can be accessed at the URL http://IP:5010/mtconnect.shtml, where IP is the IP address of the application itself. Figure 76 is an example of the UI of a running MTConnect app. The user can select one or more agents and click **Start** or **Stop**. The **Import File** and **Export File** options allow for copying the cfg or xml file from the agent to the local machine for editing and vice versa. The **View Agent Log** option shows the current log of the running agent and the **View Adapter** option provides a quick view of the machine and port number with which this agent is communicating.
Managing Agents using SSH

The MTConnect application supports SSH and the user can login using the credentials root/Cisco123. As can be seen from the log below, the dir agent1 represents one of the four agents running and the files in that dir can be changed as needed.

```
user@linux:~$ ssh root@192.168.0.136
root@192.168.0.136's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general information about administrating Alpine systems. See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

ic3k:~# ls /home/root/data/appdata/agent1/
VMC-3Axis.xml  agent.cfg      agent.log
ic3k:~#
```

Scale Validation

This section provides some scale results performed on an IC3000 showing an MTConnect Agent application running on a device using all of its memory and CPU resources for the purpose of this testing. Testing was done with traffic simulation under controlled environment to be able to scale the number of tags per second and the number of agents within the app (which would translate to number of machines) a single device can handle traffic from.

IC3000 test conditions:

- Image: Version: 1.0.1, Platform ID: IC3000-2C2F-K9, HW ID: FCH2302Y003 (1.4 MTConnect)
- MTConnect agent container is provisioned with max CPU resources available: 9000 CPU and 6000 MB RAM.
All agents were added to EFM in streaming mode.

Each agent used in test has four devices (machines). Each device has 71 data items, so 284 data items per agent.

Table 39  Two Agents: Total Eight Machines

<table>
<thead>
<tr>
<th>tags/sec/machine</th>
<th>total tags/sec</th>
<th>mem (mb)</th>
<th>cpu used</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>112</td>
<td>838</td>
<td>35%</td>
</tr>
<tr>
<td>30</td>
<td>240</td>
<td>1037</td>
<td>37%</td>
</tr>
<tr>
<td>43</td>
<td>344</td>
<td>1057</td>
<td>39%</td>
</tr>
<tr>
<td>62</td>
<td>500</td>
<td>1062</td>
<td>41%</td>
</tr>
<tr>
<td>125</td>
<td>1024</td>
<td>1057</td>
<td>45%</td>
</tr>
</tbody>
</table>

Table 40  Three Agents: Total 12 Machines

<table>
<thead>
<tr>
<th>tags/sec/machine</th>
<th>total tags/sec</th>
<th>mem (mb)</th>
<th>cpu used</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>168</td>
<td>840</td>
<td>35%</td>
</tr>
<tr>
<td>30</td>
<td>360</td>
<td>1152</td>
<td>39%</td>
</tr>
<tr>
<td>43</td>
<td>516</td>
<td>1170</td>
<td>41%</td>
</tr>
<tr>
<td>60</td>
<td>720</td>
<td>1176</td>
<td>44%</td>
</tr>
<tr>
<td>105</td>
<td>1260</td>
<td>1172</td>
<td>50%</td>
</tr>
</tbody>
</table>

Table 41  Five Agents: Total 20 Machines

<table>
<thead>
<tr>
<th>tags/sec/machine</th>
<th>total tags/sec</th>
<th>mem (mb)</th>
<th>cpu used</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>275</td>
<td>857</td>
<td>40%</td>
</tr>
<tr>
<td>30</td>
<td>600</td>
<td>1382</td>
<td>41%</td>
</tr>
<tr>
<td>43</td>
<td>870</td>
<td>1388</td>
<td>45%</td>
</tr>
<tr>
<td>62</td>
<td>1240</td>
<td>1404</td>
<td>51%</td>
</tr>
<tr>
<td>100</td>
<td>2000</td>
<td>1401</td>
<td>59%</td>
</tr>
</tbody>
</table>

Table 42  10 Agents: Total 40 Machines

<table>
<thead>
<tr>
<th>tags/sec/machine</th>
<th>total tags/sec</th>
<th>mem (mb)</th>
<th>cpu used</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>550</td>
<td>1891</td>
<td>40%</td>
</tr>
<tr>
<td>30</td>
<td>1200</td>
<td>1957</td>
<td>47%</td>
</tr>
<tr>
<td>40</td>
<td>1600</td>
<td>1957</td>
<td>55%</td>
</tr>
<tr>
<td>55</td>
<td>2200</td>
<td>1973</td>
<td>64%</td>
</tr>
<tr>
<td>74</td>
<td>2960</td>
<td>1971</td>
<td>74%</td>
</tr>
</tbody>
</table>

Troubleshooting

This section goes over basic troubleshooting to follow to find the root cause of various issues.
IC3000Reset

The reset button to the left of the management port is a multi-function button. Its behavior depends on the amount of time in seconds the button is held down. It is important to follow the guidelines below as the button will not have any effect if pressed outside these guidelines.

- **10-15 seconds:**
  Reboot—A normal reboot of the device equivalent to power cycle.

- **30-35 seconds:**
  Config-reset—Erases all the user config, including apps, and reboots the device. The device will reboot with the last software image that was running.

- **60-65 seconds:**
  Factory-reset—Erases everything and boots up with the factory default image (1.0.1).

IC3000 IOx Troubleshooting

There are three ways to troubleshoot and collect logs from an IC300:

- Using the FND Field Device Page with the various tabs and Upload Logs mechanism.

![Figure 77 FND Field Device Page](image)

- Using System Troubleshoot Page of the Ox Local Manager via https://IP:8443, where IP is management IP address. It is important to know that the **Device Config** tab below with all its settings is valid only when the device is in Developer Mode. In this mode the user can use this tab to configure the IC3000 interfaces, DNS, and NTP and perform software upgrade.

![Figure 78 System Troubleshoot Page](image)

- Using the CLI via a serial cable connected to the console port of the IC300; no login is required.
  - Show version to verify software and device serial number:

```
ic3k> show version
Version: 1.1.1
```
Verify IC3000 to NTP server connectivity and clock synchronization:

```
ic3k> show clock
Mon Aug 19 20:20:15 UTC 2019
```

```
ic3k> show ntp association
  remote refid st t when poll reach delay offset jitter
  127.127.1.0 .LOCL. 14 1 51 64 1 0.000 0.000 0.000
  10.81.254.202 .GNSS. 1 u 40 64 1 0.501 -0.050 0.625
```

```
ind assid status conf reach auth condition last_event cnt
  ------------------------------------------------------------
  1 38631  9014   yes   yes  none    reject   reachable  1
  2 38632  961a   yes   yes  none  sys.peer    sys.peer  1
  * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

```
ic3k> show ntp status
Clock is synchronized, stratum 2, reference is 10.81.254.202
nominal freq is 100.0000HZ, precision is 2**21
reference time is E1057F8C.4F5A814C (20:05:32.309000 Mon Aug 19 2019)
clock offset is -0.942843 msec, root delay is 0.478 msec
root dispersion is 938.569 msec, peer dispersion is 437.529 msec
```

NTP Servers received from DHCP:
10.81.254.202

Verify the status of IC3000 and its connectivity to FND. The **bold** values reflect key values to look for, including that the device is running, is in production mode, and is registered and connected to the proper FND.

```
ic3k> show ida status
IDA Version: 2.0.1
Status: Running
Operation Mode: Production
FND Host: 192.168.0.175:9121
FND Connection Status: Connected
Periodic Metrics Interval: 300
Heartbeat Interval: 60
Is Registered: True
HTTP Server Status: N/A (Stopped)
Remote Device Management: N/A
```

Show iox summary or detail which provides data about the guest OS IOx status.

```
ic3k> show iox summary
IOx Infrastructure Summary:
---------------------------
eid: IC3000-2C2F-K9+FCH2302Y003
pfm: IC3000-2C2F-K9
s/n: FCH2302Y003
images: Lnx: 0.10.360., IOx: 1.8.0:r/1.8.0.0:74512d0
boot: 2019-08-09 19:03:34
time: 2019-08-19 20:21:33
load: 20:21:33 up 10 days, 1:17, 0 users, load average: 0.90, 0.56, 0.38
memory: ok, used: 6964/7798 (89%)
disk: ok, used: /:487865/543588 (89%), /software:34598976/87462892 (39%)
process: warning, running: 4/5, failed: sshd
networking: ok
logs: warning, errors: caf (1059)
apps: warning, Alleantia (D) MTCConnect14 (D) MTCsim (D) Win12USB (R) centos7 (D) ubuntu18 (D)

142
Sample Machine XML File

```xml
<?xml version="1.0" encoding="UTF-8"?>
<MTConnectDevices xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn:mtconnect.org:MTConnectDevices:1.1"
    xsi:schemaLocation="urn:mtconnect.org:MTConnectDevices:1.1 http://www.mtconnect.org/schemas/MTConnectDevices_1.1.xsd">
    <Header creationTime="2010-03-04T18:44:40+00:00" sender="localhost" instanceId="1267728234"
        bufferSize="131072" version="1.1"/>
    <Devices>
        <Device id="dev" iso841Class="6" name="VMC-3Axis" sampleInterval="10" uuid="000">
            <Description manufacturer="SystemInsights"/>
            <DataItems>
                <DataItem category="EVENT" id="avail" type="AVAILABILITY"/>
            </DataItems>
            <Components>
                <Axes id="ax" name="Axes">
                    <Rotary id="c1" name="C">
                        <DataItems>
                            <DataItem category="SAMPLE" id="c2" name="Sspeed" nativeUnits="REVOLUTION/MINUTE" subType="ACTUAL" type="SPINDLE_SPEED" units="REVOLUTION/MINUTE">
                                <Source>spindle_speed</Source>
                            </DataItem>
                            <DataItem category="SAMPLE" id="c3" name="Sovr" nativeUnits="PERCENT" subType="OVERRIDE" type="SPINDLE_SPEED" units="PERCENT">
                                <Source>SspeedOvr</Source>
                            </DataItem>
                            <DataItem category="EVENT" id="cm" name="Cmode" type="ROTARY_MODE">
                                <Constraints>
                                    <Value>SPINDLE</Value>
                                </Constraints>
                            </DataItem>
                            <DataItem category="CONDITION" id="Cloadc" type="LOAD"/>
                            <DataItem category="CONDITION" id="Csystem" type="SYSTEM"/>
                            <DataItem category="SAMPLE" id="c13" name="Cload" nativeUnits="PERCENT" type="LOAD" units="PERCENT"/>
                        </DataItems>
                    </Rotary>
                    <Linear id="x1" name="X">
                        <DataItems>
                            <DataItem category="SAMPLE" id="x2" name="Xact" nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION" units="MILLIMETER"/>
                            <DataItem category="SAMPLE" id="x3" name="Xcom" nativeUnits="MILLIMETER" subType="COMMANDED" type="POSITION" units="MILLIMETER"/>
                            <DataItem category="SAMPLE" id="n3" name="Xload" nativeUnits="PERCENT" type="LOAD" units="PERCENT"/>
                            <DataItem category="CONDITION" id="Xloadc" type="LOAD"/>
                            <DataItem category="CONDITION" id="Xsystem" type="SYSTEM"/>
                        </DataItems>
                    </Linear>
                    <Linear id="y1" name="Y">
                        <DataItems>
                        </DataItems>
                    </Linear>
                </Axes>
            </Components>
        </Device>
    </Devices>
</MTConnectDevices>
```
Industrial DMZ Reference

The following sections provide design guidance for the IDMZ. Design overview and guidance is provided only as this layer was not specifically validated in this Industrial Automation CVD, though the traffic required to pass through the IDMZ such as ISE and Remote access were part of the testing. The CPwE IDMZ is at the following link: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

The Industrial Zone contains all IACS network and automation equipment that is critical to controlling and monitoring plant-wide operations. Industrial security standards including IEC-62443 recommend strict separation between the Industrial zone (levels 0-3) and the Enterprise/business domain and above (Levels 4-5). This segmentation and strict policy helps to provide a secure industrial infrastructure and availability of the Industrial processes. Data though is still required to be shared between the two entities such as MES or ERP data and security networking services may be required to be managed and applied throughout the enterprise and industrial zones. A zone and infrastructure is required between the Trusted industrial zone and the untrusted Enterprise zone. The IDMZ commonly referred to as Level 3.5 provides a point of access and control for the access and exchange of data between these two entities.
The IDMZ architecture provides termination points for the Enterprise and the Industrial domain and then has various servers, applications, and security policies to broker and police communications between the two domains.

The following are key guidelines and concepts for the IDMZ:

- As a best practice no direct communications should occur between the Enterprise and the Industrial Zone although in some instances this may not be possible with Enterprise systems being utilized in the Industrial Zone (ISE deployments).
- The IDMZ needs to provide secure communications between the Enterprise and the Industrial Zone using mirrored or replicated servers and applications in the IDMZ.
- The IDMZ provides for remote access services from the external networks into the Industrial Zone.
- The IDMZ must provide a security barrier to prevent unauthorized communications into the Industrial Zone and, therefore create security policies to explicitly allow authorized communications (ISE between Enterprise and Industrial Zone).
- This applies to Industrial traffic leaking into the enterprise too; no IACS traffic will pass directly through the IDMZ (Controller, I/O traffic).

**Figure 79  Industrial DMZ Reference**

The reference design above provides a view into the components and architecture. The Redundant Firewalls are deployed to inspect and control as it enters or exits the IDMZ. Cisco Catalyst servers are deployed within the IDMZ to provide network access for UCS servers hosting the application mirrors and IDMZ services. The firewalls will run Layer 3 to both the enterprise Zone and the IDMZ. **Figure 79** re-iterates the concepts of traffic flow through a DMZ related to an industrial facility.

**IDMZ Industrial Characteristics and Design Considerations**

The majority of industrial plant facilities have a very different physical environment at this layer of the architecture compared to the Cell/Area Zone Level 2 and below. The networking characteristics are less intensive with respect to realtime performance and equipment is physically situated in an environmentally controlled area, cabinet or room.

The following highlight the key design considerations for the IDMZ which impact platform selection, network topology, security implementation, and overall design:
Industrial Characteristics—Environmental conditions, plant layout, and cabling costs all impact the platform choices and network topology in the design. The general location and management strategy changes at Level 3 and Level 3.5 even more so. The networking platforms and servers housing the applications to support the plant are usually housed in environmentally controlled areas rather than the plant floor. The IDMZ would typically be led from a management perspective by security architects and IT professionals with considerations and requirements taken from OT as to the types of traffic required to traverse between the Enterprise and the Industrial Zones. This changes the dynamic of the platform choice which aligns with that of the traditional IT platforms. These platforms include IT based Next Generation Firewalls such as the ASA and the Cisco Firepower Threat Defense (FTD) firewalls, Cisco Catalyst 9300/Cisco Catalyst 9200 products and Cisco non-hardened UCS platforms housing the patch management, Remote access, and mirror servers.

Interoperability and Interconnectivity—The IDMZ is the one and only communications interface between the Industrial Zone and the Enterprise Zone. The IDMZ allows interconnectivity but will strictly control and restrict the traffic flow as well as security functions such as remote access and IACS application mirrored services. Layer 3 is required to be enabled between the IDMZ and the enterprise and the IDMZ and the Industrial Zone.

Real-time communications, Determinism, and Performance—Packet delay and jitter within an IACS network can have significant impact on the underlying industrial process, however at the IDMZ this requirement is very different to that of the Cell/Area Zone. The general performance criteria is less sensitive to packet delay, latency, and jitter as the majority traffic flows between the Enterprise and the Industrial Zone through the IDMZ are non-real time from an industrial application perspective, and at best are near real-time.

Availability—A key metric within industrial automation is overall equipment effectiveness (OEE). Availability is still a critical requirement of the network at the IDMZ. However, if the IDMZ were to fail, the operations and processes running in the Industrial Zone and more critically the Cell/Area Zone must continue to function. Therefore, there is no dependency on the processes related to the production environment in the Industrial Zone with the applications or systems in the Enterprise Zone. Industrial Automation promotes resiliency and availability in the IDMZ with redundant servers, firewalls, Ethernet links, etc, though in smaller plant environments this may not be applied.

Security—Security, safety, and availability are tightly aligned within an industrial security framework. When discussing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain. Recommended models would be the Purdue Model of Control Hierarchy, International Society of Automation 95 (ISA95) and IEC 62443, NIST 800-82 and NERC CIP for utility substations. The IDMZ is the key security segmentation layer between the Enterprise and the Industrial Zones. Security concepts and features are designed and implemented to provide an interface into the Industrial Zone for the business domain to support production visibility, interfaces for IACS application functions, as well as support networking and security services provided by the enterprise into the Industrial Zone. Functional sub-zones within the IDMZ are configured to segment access to IACS data and network services (for example, IT, Operations and Trusted Partner zones). The nature of firewalls at this layer provides functionality to provide enhanced security measures with the Next Generation firewalls such as Intrusion Prevention and Detection (IPS/IDS) malware detection, content security for data traversing or entering the IDMZ, and Controlled VPN termination for remote access.

Management—Within the Industrial Zone and Site Operations and Control layer there needs to be a consistent management strategy. This collaboration needs to extend into supporting the design and best practices for the IDMZ too. Where the Cell/Area Zone was operationally focused with a mixture of OT and IT personae, and the operations and control level zone was led by IT and OT personae with assistance from security architects, the IDMZ management and design will be led by IT security architects in collaboration with OT and IT engineers.

IDMZ Firewalls

Cisco ASA with FirePOWER Services brings distinctive threat-focused next-generation security services to the Cisco ASA 5500-X Series Next-Generation Firewalls. It provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks (Figure 80). Cisco ASA is the world’s most widely deployed, enterprise-class stateful firewall. Cisco ASA with FirePOWER Services features these comprehensive capabilities:
Networking and Security in Industrial Automation Environments

Industrial DMZ Reference

- Site-to-site and remote access VPN and advanced clustering provide highly secure, high-performance access and high availability to help ensure business continuity.

- Granular Application Visibility and Control (AVC) supports more than 4,000 application-layer and risk-based controls that can launch tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.

- The industry-leading Cisco ASA with FirePOWER next-generation IPS (NGIPS) provides highly effective threat prevention and full contextual awareness of users, infrastructure, applications, and content to detect multivector threats and automate defense response.

- Reputation- and category-based URL filtering offer comprehensive alerting and control over suspicious web traffic and enforce policies on hundreds of millions of URLs in more than 80 categories.

- AMP provides industry-leading breach detection effectiveness, sandboxing, a low total cost of ownership, and superior protection value that helps you discover, understand, and stop malware and emerging threats missed by other security layers.

Figure 80  Cisco Collective Security


IDMZ Data and Information Exchange

At a high level the following are the types of services that would be hosted in the IDMZ to help facilitate secure passing of IACS data and communications between the industrial zone and the Enterprise zone. The promotion of no direct access permitted between the Enterprise Zone and the Industrial zone highlights the requirement for the deployment of servers or services deployed in the IDMZ to broker communications or act as a landing pad for services between the two zones.

- IACS replicated or Mirrored Data Services—As explained previously, the differing security methodologies and requirements between the enterprise and industrial zone promote the use of a DMZ, though to provide greater business agility and business intelligence data needs to be shared between the industrial zone and the enterprise zone. The DMZ will deploy servers, applications, or services to securely replicate or mirror data from the industrial zone to the enterprise zone. Depending on the IACS vendor these servers or technologies to replicate the data may be different, but the principles and functions of operation remain the same.
Secure File Transfer Services—Updates to security patches or software installation files for installation onto assets in the industrial domain are examples of files that need to be brought securely from the enterprise zone into the Industrial zone. In order to achieve this in a secure fashion and keep the premise of no direct communication, a secure file server and patch management server are deployed to provide a landing pad in the IDMZ. Files would be downloaded to the IDMZ and then could be passed to the Industrial file server situated in the Industrial zone.

Remote Access Services—Secure remote access can provide an authorized user a real-time view of a process or industrial assets in the industrial zone. A remote access server such as a windows Remote desktop gateway can be deployed in the IDMZ. Remote Users would access this server and then remote access to authorized assets in the Industrial Zone.

Security Policy Exceptions—Within Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide there were some use cases where direct access was permitted between the enterprise and the industrial zone. Specific ports and guidance for deployment are highlighted in this DIG. This though is a risk acceptance that each customer should consider. Some risk may be acceptable based on lower cost of implementation and support or better performance of the application deployed.

IDMZ Data Flows Overview

Security Policy Exceptions—Within Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide there were some use cases where direct access was permitted between the enterprise and the industrial zone. Specific ports and guidance for deployment is highlighted in this design guide (see link below). This though is a risk acceptance that each customer should consider. Some risk may be acceptable based on lower cost of implementation and support or better performance of the application deployed. The ISE deployment though is bound by the implementation of synchronization. An ISE Policy Service Node (PSN) must synchronize with the Policy Admin Node. In the model today, this Admin node is in the Enterprise and there is not a proxy or mirrored service function for this service. Therefore, ISE will pass directly through the firewalls at the IDMZ. The following provides a high-level view of data flows traversing between the Industrial Zone and the Enterprise Zone.

The following use cases were validated in the Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide. Detailed design guidance and implementation are given in this document: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

- Remote Access
- IACS Applications (Historians)
- Secure File Transfer
- Active Directory Services
- Certificate Services
- Network Time Protocol (NTP)
- Identity Services
- WLAN Personnel Access

High Availability

Availability is still a critical requirement of the network at the IDMZ. However, if the IDMZ was to fail the operations and processes running in the Industrial Zone and more critically the Cell Area zone must continue to function. Therefore, there is no dependency on the processes related to the production environment in the Industrial Zone with the applications or systems in the Enterprise Zone. The design guidance for availability is as follows.
Networking and Security in Industrial Automation Environments

Availability

Firewall Resiliency

- Deploy Redundant Firewalls and configure Active/Standby failover mode with a single security context.
- Use Stateful Failover configuration with a dedicated interface each of the failover link and the stateful Failover link.
- Encrypt failover communication with a failover key.
- EtherChannels on the active and standby units to connect to redundant switches
- Configure Layer 3 Routing to communicate between the Enterprise Zones.

IDMZ Network Availability

- Layer 3 routing between the IDMZ and the core/distribution routers and the IDMZ and the enterprise
- Redundant Links throughout the architecture
- Configuration Backups of all networking devices and firewalls
- Network Hardening best practices to protect the Management, Control, and Data planes of the network infrastructure
- Dual Layer 2 switches deployed for the server switch connectivity
- Dual NIC connectivity from the physical servers to the redundant switches. Dual NIC technologies from the Virtual servers.
- Server, Virtual Server, or application redundancy where required

Security

- IDMZ VLAN segmentation—VLAN segmentation, as explained earlier, is a common component in the security framework to assist with isolating services in the IACS level 3 servers. This should be implemented in the IDMZ architecture too. In creating several VLANs within the IDMZ and DSS environment, the servers can be isolated so that, if compromised, the servers within the VLAN container can be restricted from impacting other servers within the IDMZ.
- Policy enforcement using the Cisco Next Generations Firewall
- Visibility with NetFlow and Stealthwatch—The Cisco Catalyst 9000 series supports NetFlow. Enabling NetFlow on all the NetFlow capable switches in IDMZ in alignment with the level 3, Core, Distribution, and the Industrial Data center and exporting to Stealthwatch will provide a plantwide view of application and network traffic. This can be used to help provide a baseline traffic profile and used to help identify anomalies in the network data flows.
- Enhanced NGN features:
  - IPS/IDS can be deployed at the IP NGN firewalls for any traffic traversing the IDMZ.
  - Anomaly malware detection can be deployed to inspect any files traversing the firewall.


Availability

This section describes the resiliency options validated for Industrial Automation at the Distribution switch and the Cell/Area Zone.
Availability

Distribution Switch Resiliency

Cisco StackWise—480

The Cisco Catalyst 3850 and Cisco Catalyst 9300 support StackWise-480 configurations to provide platform resiliency at the distribution layer. A switch stack can have up to eight stacking-capable switches connected through their StackWise-480 ports. The stack members work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

A switch stack always has one active switch and one standby switch. The active switch will provide control of the management plane for the stack. If the active switch becomes unavailable, the standby switch assumes the role of the active switch and continues to the keep the stack operational. In this version of Industrial Automation the switch stacks were validated with two switches to provide the Cell/Area Zone distribution switch resiliency.

The active switch has the saved and running configuration file for the switch stack. The standby switch automatically receives the synchronized running configuration file. Stack members receive synchronized copies when the running configuration file is saved into the startup configuration file. If the active switch becomes unavailable, the standby switch takes over with the current running configuration.

Configuring Cisco StackWise

**Stack Member Priority**

A higher priority value for a stack member increases the probability of it being elected active switch and retaining its stack member number. The priority value can be 1 to 15. The default priority value is 1. You can display the stack member priority value by using the `show switch EXEC` command.

```
P5-9300-2#show switch
Switch/Stack Mac Address : 00bc.60ad.a500 - Local Mac Address
Mac persistency wait time: Indefinite

<table>
<thead>
<tr>
<th>Role</th>
<th>Mac Address</th>
<th>Priority</th>
<th>Version</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>*1</td>
<td>Active</td>
<td>00bc.60ad.a500</td>
<td>15</td>
<td>V01</td>
</tr>
<tr>
<td>2</td>
<td>Standby</td>
<td>00bc.60ad.9b80</td>
<td>1</td>
<td>V01</td>
</tr>
</tbody>
</table>
```

We recommend assigning the highest priority value to the switch that you prefer to be the active switch. This ensures that the switch is reelected as the active switch if a reelection occurs.

To change the priority value for a stack member, use the following command:

```
switch stack-member-number priority new priority-value
```

For example:

```
switch 1 priority 15
```

The new priority value takes effect immediately but does not affect the current active switch. The new priority value helps determine which stack member is elected as the new active switch when the current active switch or the switch stack resets.

**Stack MAC Address Persistence**

A switch stack is identified in the network by its bridge ID and, if it is operating as a Layer 3 device, its router MAC address. The bridge ID and router MAC address are determined by the MAC address of the active switch. If the active switch changes, the MAC address of the new active switch determines the new bridge ID and router MAC address. The default behavior could cause traffic disruption due to the new MAC address being learned in the network. To avoid this situation, configure stack MAC persistency so that the stack MAC address never changes to the new active switch MAC address.
To configure use the following command:

```
stack-mac persistent timer 0
```
Stack Member Renumbering

The stack member number (1 to 9) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the `show switch EXEC` command:

```
P5-9300-2#show switch
Switch/Stack Mac Address : 00bc.60ad.a500 - Local Mac Address
Mac persistency wait time: Indefinite
<table>
<thead>
<tr>
<th>H/W</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Mac Address</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>*1</td>
<td>Active</td>
</tr>
<tr>
<td>2</td>
<td>Standby</td>
</tr>
</tbody>
</table>
```

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack.

It is possible to manually change the stack member number by configuring:

```
switch current-stack-member-number renumber new-stack-member-number
```

The new number goes into effect after that stack member resets (or after you use the `reload slot stack-member-number privileged EXEC` command) and only if that number is not already assigned to any other members in the stack.

For more information on the Cisco Catalyst 3850 StackWise–480 configuration, see:

- For Cisco Catalyst 3850
  https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg_chapter_010.html#reference_5415C09868764F0A05F88897F108139

- For Cisco Catalyst 9300
Networking and Security in Industrial Automation Environments

Troubleshooting Cisco StackWise

The following `show` commands provide information about the stack.

### Table 43 Commands for Displaying Stack Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `show switch` and `show switch detail` | Displays summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode. These commands show the following information about the configuration:  
  - Switch or Stack MAC Address  
  - MAC persistence setting (should be Indefinite)  
  - The switch numbers, MAC addresses, priority values, and current states  
  - The status of the stack ports on each switch, as well as the neighbor to which each port is connected |
| `show switchstack-member-number` | Displays information about a specific member. |
| `show switch detail` | Displays detailed information about the stack. |
| `show switch neighbors` | Displays the stack neighbors. |
| `show switch stack-ports[summary]` | Displays port information for the stack. Use the `summary` keyword to display the stack cable length, the stack link status, and the loopback status. |
| `show redundancy` | Displays the redundant system and the current processor information. The redundant system information includes the system uptime, standby failures, switchover reason, hardware, and configured and operating redundancy mode. The current processor information displayed includes the active location, the software state, the uptime in the current state, and so on. |
| `show redundancy state` | Displays all the redundancy states of the active and standby switches. |

Hot Standby Router Protocol

The `standby ip interface configuration` command activates Hot Standby Router Protocol (HSRP) on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. You must configure at least one Layer 3 port on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use. It is recommended to configure the lowest IP in the network as standby IP to guarantee that the master router will become the Internet Group Management Protocol (IGMP) snooping querier.

In the recommended implementation, HSRP is configured in a Switch Virtual Interface (SVI). To configure HSRP, assign a virtual IP and group number to the interface. The following is an example of HSRP configuration in master peer:

```
interface Vlan10
ip address 10.17.10.2 255.255.255.0
standby 1 ip 10.17.10.1
```

The following is an example of the standby peer:

```
interface Vlan10
ip address 10.17.10.3 255.255.255.0
standby 1 ip 10.17.10.1
```
Availability

Note that virtual IP is the same while physical IP varies per peer.

Configuring HSRP Priority

Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router again after recovering from a failure. If priorities are equal, the current active router does not change. The highest number (1 to 255) represents the highest priority (most likely to become the active router).

When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

To configure priority in the desired active peer, add this line to the interface configuration (since default priority is 100, the configured number should be higher):

```
standby 1 priority 254
```

Configuring Preemption

When the local router has a higher priority than the active router, it assumes control as the active router. As an option a delay can be configured, which will cause the local router to postpone taking over the active role for the number of seconds shown:

```
standby 1 preempt delay minimum 30
```

HSRP Timers

HSRP uses two timers: hello interval and hold time. Hello interval defines the frequency that hello packets are sent to the other peer. Hold time indicates the amount of time to wait before marking the peer as down. The hold time should be three or more times greater than the hello interval. The values used in the following example were used during validation to provide faster convergence than the default values. To configure those timers:

```
standby 1 timers msec 200 msec 750
```

Troubleshooting HSRP

The commands `show standby` and `show standby brief` provide configuration and current status details:

```
IE5K-3#show standby
Vlan10 - Group 1
State is Active
7 state changes, last state change 2w1d
Virtual IP address is 10.17.10.1
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 200 msec, hold time 750 msec
Next hello sent in 0.144 secs
Preemption enabled
Active router is local
Standby router is 10.17.10.3, priority 170 (expires in 0.736 sec)
Priority 200 (configured 200)
Group name is "hsrp-Vl10-1" (default)
IE5K-3#
IE5K-3#sh standby brief
|
Interface Grp Pri P State Active Standby Virtual IP
Vl10 1 200 P Active local 10.17.10.3 10.17.10.1
```
### Availability

If HSRP does not recognize its HSRP peers, verify physical layer connectivity and configuration.

### Internet Group Management Protocol Considerations

IGMP snooping should be configured to route multicast traffic only to those hosts that request traffic from the specific multicast group. IGMP snooping is configured by default in Cisco Industrial Ethernet (IE) switches, but IGMP snooping querier should be configured in the distribution switches (Cisco IE 5000s) using the following command:

```bash
ip igmp snooping querier
```

IGMP selects the querier with the lowest IP in the network, hence the importance of configuring the HSRP IP to be the lowest in the network.

### Cell/Area Zone Resiliency

**EtherChannel**

To configure an EtherChannel using Link Aggregation Control Protocol (LACP) in active mode between the access and distribution switches, configure a port-channel interface on each switch and then configure the links as members of the port-channel.

*Figure 81 Example of EtherChannel in the Cell/Area Zone*
The **channel-group** command binds the physical port and the logical interface. The following is an example of ether channel configuration:

```plaintext
interface Port-channel2
interface GigabitEthernet1/0/3
channel-group 2 mode active
interface GigabitEthernet2/0/3
channel-group 2 mode active
```

The mode active refers to the LACP negotiation state; in this mode the port is able to start negotiation with other ports sending LACP packets.

After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, **spanning-tree** commands or commands to configure a Layer 2 EtherChannel as a trunk.

### Troubleshooting EtherChannels

The **show** commands in **Table 44** provide information about the EtherChannel.

**Table 44 Commands Providing Information about EtherChannel.**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show etherchannel</code> `[channel-group-number]{detail</td>
<td>port</td>
</tr>
<tr>
<td><code>show lacp</code> <code>[channel-group-number]</code> `{counters</td>
<td>internal</td>
</tr>
</tbody>
</table>

### Configure EtherChannels Using Device Manager

This section assumes that the Cisco IE switch has been installed and configured with IP Address for management. For more details on setting up a Cisco IE switch, refer to the corresponding installation guides.

1. Log in to the switch using Device Manager credentials.
2. Go to the Configuration menu.
3. Select **Interface**->**Logical** as shown in Figure 82.
4. Fill out port channel details and associate interfaces as shown in Figure 83.
5. Click **Save & Apply to Device**.

**Resilient Ethernet Protocol (REP)**

Resilient Ethernet Protocol (REP) is a resiliency protocol used on cell area rings as shown in **Figure 84** or as an open segment to connect an HSR ring to the distribution as shown in **Figure 85**. When used on a ring, the edge ports reside on the same logical switch in the distribution. When used as an open segment, the edge ports are located on separate switches. Refer to **Table 45** for edge port location used with different Distributed Layer Resiliency protocols.

**Table 45  Edge Port Location on REP Segment**

<table>
<thead>
<tr>
<th>Topology</th>
<th>Distribution Layer Resiliency Protocol</th>
<th>Edge Port Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>REP Ring</td>
<td>Cisco StackWise</td>
<td>Edge ports should be located on the Stack switch, with each edge port on different stack member.</td>
</tr>
<tr>
<td>REP Ring</td>
<td>HSRP</td>
<td>Both edge ports should be located on the primary HSRP distribution switch.</td>
</tr>
<tr>
<td>HSR Ring</td>
<td>Cisco StackWise or HSRP</td>
<td>Each edge ports should be located on access switches connected to the distribution, with only one edge per access switch</td>
</tr>
</tbody>
</table>
REP Guidelines

- REP ports must be Layer 2 trunk ports.
Availability

- REP and Spanning Tree Protocol (STP) cannot run on the same segment or interface.
- Begin by configuring one port at the end of the segment and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.
- A device can have no more than two ports that belong to the same segment.
- Each segment port can have only one external neighbor.
- REP ports follow these rules:
  - If only one port on a device is configured in a segment, the port should be an edge port.
  - If two ports on a device belong to the same segment, both ports must be edge ports or both ports must be regular segment ports.
  - If two ports on a device belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

Configure Administrative VLAN

To avoid the delay introduced by relaying messages that are related to link-failures or VLAN-blocking notifications during VLAN load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network and not just to the REP segment. You can control the flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- Only one administrative VLAN can exist on a switch and on a segment. However, the software does not enforce this.
- If you do not configure an administrative VLAN, the default is VLAN 1.
- If you want to configure REP on an interface, ensure that the REP administrative VLAN is part of the Trunk encapsulation list.

Configuration Commands:

```
vlan <vlanID>
name REP_Admin_VLAN
rep admin vlan <vlanID>
```

Enable REP on Interfaces

For the REP operation, you must enable REP on each interface (that will be part of the segment) and identify the segment ID. This task is required and must be done before other REP configuration. You must also configure a primary and secondary edge port on each segment. All other steps are optional.

**Edge Ports**

To configure a port as an edge port, use the following command in interface configuration mode:

```
rep segment ID edge (primary)
```

The primary keyword is optional and allows for manual selection of the primary edge. If the primary keyword is used, the other edge port becomes the secondary edge port (no keyword required). To configure the secondary edge port, omit the primary keyword:

```
rep segment ID edge
```
Availability

Non-Edge Ports
To configure a port as a member of the REP segment, use the following command in interface configuration mode:

```
rep segment ID
```

Preemption
Preemption is done either manually with the `rep preempt segment <ID>` command or automatically if you configure `rep preempt delay seconds` under the primary edge port.

When a segment recovers after a link failure, one of the two ports adjacent to the failure comes up as the ALT port. Then, after preemption, the location of the ALT ports become the primary edge port unless additional configuration is done for load balancing and alternate port.

Example of automatic preemption:
```
interface GigabitEthernet1/1
rep segment 30 edge primary
rep preempt delay 30
```

Example of manual preemption:
```
rep preempt segment 30
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

Proceeding with Manual Preemption

Selecting an Alternate Port
It is possible to select an alternate port other than the edge port by configuring the load balancing feature on the primary edge port and specifying the alternate port using the port ID or the neighbor offset number using the following command:

```
rep block port id vlan vlan-list
```

Port ID
To identify the port ID of a port in the segment, for the port enter the command:

```
show interface rep detail interface
```

Neighbor Offset Number
The neighbor offset number of a port in the segment identifies the downstream neighbor port of an edge port. The neighbor offset number range is -256 to 256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers indicate the secondary edge port (offset number -1) and its downstream neighbors.

Example
The following example uses the neighbor offset number, in this case the alternate port is 7 ports downstream:

```
interface TenGigabitEthernet1/1/1
rep segment 11 edge primary
rep block port 7 vlan all
```

For more information, refer to Cisco Industrial Ethernet 4000, 4010, and 5000 Switch Software Configuration Guide:
Availability

Note: When using Cisco StackWise for distribution with a REP ring, it is a good practice to locate the alternate port in between access switches to achieve higher Layer 3 convergence in case of primary stack member power failure.

Troubleshooting REP

Enter this command in order to see the status of a REP adjacency:

```
show int gi1/7 rep
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Seg-id</th>
<th>Type</th>
<th>LinkOp</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet1/7</td>
<td>10</td>
<td>Primary</td>
<td>Edge</td>
<td>TWO_WAY</td>
</tr>
</tbody>
</table>

Use the `show rep topology` command on any router on the segment to see the current topology:

```
W2025-IE4K-RING#sh rep topology
REP Segment 10
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
W2024-IE4K-RING                  Gi1/1      Pri  Alt
W2023-IE4K-RING                  Gi1/1           Open
W2022-IE4K-RING                  Gi1/2           Open
W2022-IE4K-RING                  Gi1/1           Open
W2021-IE4K-RING                  Gi1/1           Open
W2021-IE4K-RING                  Gi1/2           Open
W2026-IE4K-RING                  Gi1/2           Open
W2026-IE4K-RING                  Gi1/1           Open
W2025-IE4K-RING                  Gi1/1           Open
W2024-IE4K-RING                  Gi1/2           Open
W2025-IE4K-RING                  Gi1/2      Sec  Open
```

Configure REP Using Device Manager

This section assumes that the Cisco IE switch has been installed and configured with IP Address for management access. For more details on setting up Cisco IE switch, refer corresponding Installation Guides.

1. Log in to the switch using Device Manager credentials.

2. Go to the Configuration menu.

3. Select **Layer 2 -> REP**.

4. Select the Admin VLAN for the entire domain (all segments).

5. Click a row for an interface to bring up the Edit Rep Interface window and then click **Enable** to enable REP on the interface. REP is disabled by default. When enabled, the interface is a regular segment port unless it is configured as an edge port.
6. Enter the **Segment ID**.

7. Select the **REP Port Type**:

   - Edge—A secondary edge port that participates in VLAN load balancing.
   - Edge no-neighbor—A secondary edge port that is connected to a non-REP switch.
   - Preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing.
   - Edge no-neighbor preferred—A secondary edge port that is connected to a non-REP switch and is the preferred port for VLAN load balancing.
   - Edge no-neighbor primary—A secondary edge port that always participates in VLAN load balancing in this REP segment and is connected to a non-REP switch.
   - Edge no-neighbor primary preferred—An edge port that always participates in VLAN load balancing in this REP segment, is connected to a non-REP switch, and is the preferred port for VLAN load balancing.
   - Edge preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing.
   - Edge primary—An edge port that always participates in VLAN load balancing in this REP segment.
   - Edge primary preferred—An edge port that always participates in VLAN load balancing in this REP segment and is the preferred port for VLAN load balancing.
   - None—This port is not part of the REP segment. This is the default.
   - Transit—A non-edge port in the REP segment.

8. (Optional) Designate a physical interface to receive segment topology change notices (STCNs).

9. (Optional) Identify one or more segments to receive STCNs. Enable to enable sending STCNs to STP networks.

10. Click **Update & Apply to Device**.
Before configuring HSR, check if HSR is enabled; newer versions have it enabled by default.

```
show version | inc Feature
Feature Mode : 0x25 Enabled: HSR (Disabled: MRP TSN)
```

If HSR is enabled, skip this step; otherwise, use the following command to enable:

```
license right-to-use activate hsr
```

For the change to take effect, the switch must be reloaded. Confirm the reload when prompted and wait for the switch to reload and boot. Verify that the HSR feature is activated.

Ensure that the member interfaces of a HSR ring are not participating in any redundancy protocols such as FlexLinks, EtherChannel, or REP before configuring a HSR ring.

Configuring HSR

Follow these steps to configure HSR:

1. Shut down the ports before configuring the HSR ring:
   ```
   interface range GigabitEthernet1/1-2
   shutdown
   ```

2. Configure switch port and VLANs as desired:
   ```
   switchport mode trunk
   switchport trunk allowed vlan 10,20,900 switchport trunk native vlan 900
   ```
3. Disable Precision Time Protocol (PTP), which is not supported on HSR interfaces:
   
   no ptp enable

4. Create the HSR ring interface and assign the ports to the HSR ring. This command should be issued in the interface configuration. The two interfaces will be bundled in a HSR interface:
   
   hsr-ring 1

5. Turn on the HSR interface:
   
   no shutdown

6. Make sure the enable DualUplinkEnhancement feature is not disabled. This feature is required to support the connectivity to a dual router (HSRP in this case) on the distribution layer.
   
   show run | include fpgamode-DualUplinkEnhancement

7. If the output shows no hsr-ring 1 fpgamode-DualUplinkEnhancement, issue the following command:
   
   hsr-ring 1 fpgamode-DualUplinkEnhancement

8. Follow these optional steps to configure CDP and LLDP to provide information about HSR ring nodes:
   
   - Enable LLDP globally:
     
     lldp run
   
   - Enable LLDP on the ports to be assigned to the HSR ring:
     
     interface range GigabitEthernet1/1-2
     lldp transmit
     lldp receive
   
   - Enable CDP on the ports to be assigned to the HSR ring:
     
     interface range GigabitEthernet1/1-2
     cdp enable

9. Follow these optional steps to enable HSR alarms:
   
   - Enable the HSR alarm facility:
     
     alarm facility hsr enable
   
   - Enable SNMP notification for HSR alarms:
     
     alarm facility hsr notifies
   
   - Associate HSR alarms with the Major Relay:
     
     alarm facility hsr relay major

**HSR with REP Best Practices**

- If REP preemption is required, it is recommended to do manual preemption to avoid an unplanned downtime. REP preemption could cause a multicast tree re-convergence that affects nodes attached to the REP segment.

- For REP segment, the edge port in the Cisco IE 4000 connected directly to HSRP slave should be primary so it gets blocked by default in preemption.

- Enable bridge protocol data unit (BPDU) filtering in ports connecting to end devices and distribution on the Cisco IE 4000 participating in HSR ring to avoid ports getting into a blocked state after topology changes.
Avoid using access ports on the distribution switch for VLANs being used in the ring to avoid a HSRP split brain scenario. If connecting devices directly to the distribution switches, use a different VLAN.

Troubleshooting HSR

The `show` commands in Table 46 can be used to troubleshoot HSR.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show hsr ring { 1</td>
<td>2 } [ detail ]`</td>
</tr>
<tr>
<td><code>show hsr statistics</code></td>
<td>Displays statistics for HSR components. To clear HSR statistics information, enter the command <code>clear hsr statistics</code>.</td>
</tr>
<tr>
<td><code>show hsr node-table</code></td>
<td>Displays all MAC addresses accessible to the switch using the HSR interface, including other nodes in the ring as well as devices attached to other nodes.</td>
</tr>
<tr>
<td><code>show hsr vdan-table</code></td>
<td>Displays the HSR Virtual Doubly Attached Node (VDAN) table, which contains devices directly connected to the switch for which the switch acts as proxy. This table is also known as the Proxy node table.</td>
</tr>
<tr>
<td><code>show cdp neighbors</code> and <code>show lldp neighbors</code></td>
<td>Displays neighbor information for the switch, which is useful when troubleshooting connectivity issues.</td>
</tr>
<tr>
<td>`show alarm settings</td>
<td>begin hsr`</td>
</tr>
</tbody>
</table>

Example of HSR Ring Detail:

```
IE4000-1# sh hsr ring 2 detail
HSR-ring: HS2
----------
Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled Redbox Mode = hsr-san
Ports in the ring:
1) Port: Gi1/3
   Logical slot/port = 1/3 Port state = Inuse ' Port is up
   Protocol = Enabled
2) Port: Gi1/4
   Logical slot/port = 1/4 Port state = Inuse ' Port is up
   Protocol = Enabled

Ring Parameters:
Redbox MacAddr: f454.3365.8a84
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 2000 ms
Pause Time: 25 ms
fpgamode-DualUplinkEnhancement: Enabled
```
### HSR Events

You can view currently active alarms using the `show facility alarm status` command. The following example shows alarm status for minor and major HSR alarms:

```
show facility-alarm status
Source Severity Description Relay Time
Switch MINOR 34 HSR ring is partially down MAJ Oct 24 2017 10:16:10
-------
show facility-alarm status
Source Severity Description Relay Time
Switch MAJOR 33 HSR ring is down MAJ Oct 24 2017 10:17:07
```

### Configure HSR Using Device Manager

This section assumes that the Cisco IE switch has been installed and configured with an IP Address for remote access. For more details on setting up a Cisco IE switch, refer to the corresponding installation guides.

1. Log in to the switch using Device Manager credentials.

<table>
<thead>
<tr>
<th>Event Number</th>
<th>Event Description</th>
<th>System Log (Level)</th>
<th>Alert/Alarm Log</th>
<th>Alarm LED and Output Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ring goes from UP to DOWN state.</td>
<td>2</td>
<td>2</td>
<td>Major Alarm/Assert</td>
</tr>
<tr>
<td>2</td>
<td>Ring goes from DOWN to UP state.</td>
<td>6</td>
<td>6</td>
<td>De-assert</td>
</tr>
<tr>
<td>3</td>
<td>One ring port goes DOWN and the other ring port and the ring itself are UP.</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Both ring ports are UP again.</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
2. After a successful login, the Dashboard for the switch loads.

3. Enable the HSR feature on the Cisco IE switch using the options highlighted in Figure 90.
4. Configure HSR Ring and its related parameters on the Cisco IE switch using the options highlighted in Figure 91.

Figure 90   Enable HSR Feature

Figure 91   HSR Ring Parameters
HSR–PRP RedBox (Dual RedBox)

A Redundancy Box (RedBox) is deployed when an end node does not support two network interfaces and PRP redundancy. The RedBox provides the DAN functionality for devices connecting to it. This is the role of the Cisco IE 4000 or Cisco IE 4010 and Cisco IE 5000 in a PRP redundancy deployment. The node behind a RedBox appears for other nodes like a DAN and is known as a Virtual DAN (VDAN).

HSR–PRP RedBox, also known as Dual RedBox, is used to connect PRP and HSR networks together. The HSR–PRP feature is supported only on the Cisco IE 4000.

A typical deployment of the HSR–PRP feature is to use two switches to connect to two different LANs, namely LAN-A and LAN-B of a PRP network and HSR network. Traffic flows between the PRP and HSR networks through RedBoxes. RedBoxes do not forward duplicate frames in the same direction to avoid loops. RedBoxes convert PRP frames to HSR frames and vice versa.

Figure 92 shows an HSR ring connected to a PRP network through two RedBoxes, one for each LAN. In this example, the source frame originates in the PRP network and reaches the destination in the HSR network. RedBoxes are configured to support PRP traffic on the interlink ports and HSR traffic on the ring ports.

Figure 92  HSR–PRP RedBox
Follow these steps to configure HSR-PRP mode on the switch. Enabling HSR-PRP mode creates an HSR ring and a PRP channel.

Before You Begin

- Enabling HSR-PRP mode will disable all ports other than two HSR ports and one PRP port and all port settings for these disabled ports will return to default values. A warning message is displayed to notify you that interface configurations will be removed. Before enabling or disabling HSR-PRP mode, check for cables connected to the switch and verify the ports' status.

- HSR-PRP RedBox mode uses ports Gi1/3 and Gi1/4 as HSR ring 2 interfaces and Gi1/1 (for RedBox A) or Gi1/2 (for RedBox B) as PRP channel 1 interfaces. These port assignments are fixed and cannot be changed. Therefore, HSR-PRP Dual RedBox mode is supported only on HSR ring 2.

- PRP uplink interfaces can be configured as access, trunk, or routed interfaces.

- PRP Dual Attached Nodes and RedBoxes add a 6-byte PRP trailer to the packet. To ensure that all packets can flow through the PRP network, increase the maximum transmission unit (MTU) size for switches within the PRP LAN-A and LAN-B network to 1506 as follows:

  ```
  system mtu 1506
  system mtu jumbo 1506
  ```

  When an intelligent electronic device (IED) sends VLAN 0 tagged packets, it is recommended to configure the IED facing interface and the uplink interfaces as trunk port allowing VLAN 1 along with other required VLANs:

  ```
  interface gigabitEthernet 1/5
  switchport mode trunk
  switchport trunk
  allowed vlan 1
  ```

Recommended Best Practices

- Disable PTP on interfaces where PTP is not necessary.

- Enable storm control for broadcast, multicast traffic on access facing interfaces:

  ```
  interface GigabitEthernet1/5
  storm-control broadcast level pps 1k
  storm-control multicast level pps 5k
  storm-control action shutdown
  storm-control action trap
  ```

- Configure different VLANs for different IEDs so as to avoid flooding of multicast, broadcast messages to other devices.

Configuring HSR-PRP RedBox

1. Activate HSR feature mode:

   ```
   license right-to-use activate hsr
   ```

   Note: Reload the switch for the change to take effect. Confirm the reload when prompted and wait for the switch to reload and boot.

2. Verify that the HSR feature is activated:

   ```
   show version inc Feature
   Feature Mode: 0x25 Enabled: HSR (Disabled: MRP TSN)
   ```

3. Enter global configuration mode:
Availability

```plaintext
configure terminal

4. Enable HSR-PRP mode and select LAN A or LAN B and the PRP Net ID:

   hsr-prp-mode enable prp-lan-a 1

   Note: PRP LAN: prp-lan-a-RedBox Interlink is connected to lan-A. prp-lan-b-RedBox Interlink is connected to
   lan-B.

5. Enter yes to confirm enabling HSR-PRP mode. To disable HSR-PRP RedBox mode, use the command:

   no hsr-prp-mode enable

6. Enter interface configuration mode and disable PTP on the ports to be assigned to the HSR ring:

   interface range gigabitEthernet 1/3-4
   no ptp enable

   Note: The PTP feature over HSR ring is currently not supported.

7. Shut down the ports before configuring the HSR ring:

   shutdown

8. Create the HSR ring interface:

   interface HSR-ring2
   switchport mode trunk

9. Assign HSR ring to the physical interfaces:

   interface range gigabitEthernet 1/3-4
   hsr-ring 2
   no shutdown

10. Create the PRP LAN interface. Repeat the step on the second HSR-PRP RedBox.

    interface PRP-channel1
    switchport mode trunk

11. Assign PRP channel to the physical interface. Follow the guidelines for identifying the switch role and the
    corresponding interface.

    interface range gigabitEthernet 1/1
    prp-channel-group 1
    no shutdown
```
12. Refer to Configuring HSR, page 165 to configure HSR ring on other switches that are part of the HSR ring.

13. Refer to PRP RedBox Configuration, page 179 to configure PRP on required switches that are part of the PRP network.

Troubleshooting HSR-PRP RedBox

Use the following commands to verify and troubleshoot HSR-PRP Redbox:

```
show prp channel detail
PRP-channel listing:
---------------------
PRP-channel: PR1
-------------
Layer type = L2
Ports: 1      Maxports = 2
Port state = prp-channel is Inuse
Protocol = Disabled
Ports in the group:
  1) Port: Gi1/1
     Logical slot/port = 1/1   Port state = Inuse
     Protocol = Disabled

show hsr ring detail
HSR-ring listing:
---------------------
HSR-ring: HS2
-------------
Layer type = L2
Operation Mode = mode-H
Ports: 2      Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled  Redbox Mode = hsr-prp-lan-a  PathId = 1
Ports in the ring:
  1) Port: Gi1/3
     Logical slot/port = 1/3   Port state = Inuse
     Protocol = Enabled
  2) Port: Gi1/4
     Logical slot/port = 1/4   Port state = Inuse
     Protocol = Enabled

Ring Parameters:
Redbox MacAddr: 84b8.02dd.c604
Node Forget Time: 60000 ms
```

Table 48  HSR-PRP RedBox Cisco IE 4000 Interface Mapping

<table>
<thead>
<tr>
<th>SKU</th>
<th>HSR Mode</th>
<th>Port Type</th>
<th>Interface Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE4000</td>
<td>HSR-PRP</td>
<td>PRP-LAN-A (RedBox A)</td>
<td>PRP channel interface—Gi1/1 (Port 3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HSR ring interfaces—Gi1/3 (Port 1), Gi1/4 (Port 2) Gi 1/2 is unused.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRP-LAN-B (RedBox B)</td>
<td>PRP channel interface—Gi1/2 (Port 3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HSR ring interfaces—Gi1/3 (Port 1), Gi1/4 (Port 2) Gi 1/1 is unused.</td>
</tr>
</tbody>
</table>
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CPI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 1600 ms
Pause Time: 25 ms
fpgamode-DualUplinkEnhancement: Enabled

**show hsr statistics egressPacketStatistics**

HSR ring 1 EGRESS STATS:

duplicate packets: 0
supervision frames: 0
packets sent on port A: 0
packets sent on port B: 0
byte sent on port a: 0
byte sent on port b: 0

HSR ring 2 EGRESS STATS:
duplicate packets: 472617535
supervision frames: 2908371
packets sent on port A: 472617493
packets sent on port B: 472616962
byte sent on port a: 806518995400
byte sent on port b: 811359936926

**show hsr statistics ingressPacketStatistics**

HSR ring 1 INGRESS STATS:
ingress pkt port A: 0
ingress pkt port B: 0
ingress crc port A: 0
ingress crc port B: 0
ingress danh pkt portAcpt: 0
ingress danh pkt discrd: 0
ingress supfrm rcv port A: 0
ingress supfrm rcv port B: 0
ingress overrun pkt port A: 0
ingress overrun pkt port B: 0
ingress byte port a: 0
ingress byte port b: 0

HSR ring 2 INGRESS STATS:
ingress pkt port A: 4729843950
ingress pkt port B: 5049046881
ingress crc port A: 0
ingress crc port B: 0
ingress danh pkt portAcpt: 5325183746
ingress danh pkt discrd: 3939164759
ingress supfrm rcv port A: 21780902
ingress supfrm rcv port B: 28970004
ingress overrun pkt port A: 0
ingress overrun pkt port B: 0
ingress byte port a: 714469348360
ingress byte port b: 806539236074

clear hsr statistics
Configure HSR-PRP RedBox Using Device Manager

This section assumes that the Cisco IE switch has been installed and configured with an IP address for remote access. For more details on setting up a Cisco IE switch, refer to the corresponding installation guides.

1. Log in to the switch using Device Manager credentials.

   Figure 93  Device Manager Login Screen

2. After a successful login, the Dashboard for the switch loads.
3. Enable the HSR feature on the Cisco IE switch using the options highlighted in Figure 95. Select the Admin tab, select the Feature Mode option, and then select HSR as the required feature mode.
4. Configure HSR-PRP Redbox by selecting the highlighted steps in Figure 96.

Figure 96  Configure HSR Feature

5. Configure HSR-PRP Redbox parameters on the Cisco IE switch using the options highlighted in Figure 97.
To create and enable a PRP channel and group on a supported Cisco IE switch, follow these steps:

1. Enter global configuration mode.
   ```
   configure terminal
   ```
2. Create PRP LAN interface:
3. Attach PRP channel to the physical interface. Follow the guidelines for identifying the switch role and the corresponding interface.

```
interface range gigabitEthernet 1/1
    prp-channel-group 1
    no shutdown
```

### Table 50 PRP RedBox Interface Mapping

<table>
<thead>
<tr>
<th>SKU</th>
<th>Interface Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE4000</td>
<td>PRP channel group 1 always uses Gi1/1 for LAN_A and Gi1/2 for LAN_B</td>
</tr>
<tr>
<td></td>
<td>PRP channel group 2 always uses Gi1/3 for LAN_A and Gi1/4 for LAN_B</td>
</tr>
<tr>
<td>IE4010</td>
<td>PRP channel group 1 always uses Gi1/25 for LAN_A and Gi1/26 for LAN_B</td>
</tr>
<tr>
<td></td>
<td>PRP channel group 2 always uses Gi1/27 for LAN_A and Gi1/28 for LAN_B</td>
</tr>
<tr>
<td>IE5000</td>
<td>PRP channel group 1 always uses Gi1/17 for LAN_A and Gi1/18 for LAN_B</td>
</tr>
<tr>
<td></td>
<td>RP channel group 2 always uses Gi1/19 for LAN_A and Gi1/20 for LAN_B</td>
</tr>
</tbody>
</table>

Configure and Monitor PRP RedBox Using Device Manager

This section assumes that the Cisco IE switch has been installed and configured with an IP address for remote access. For more details on setting up a Cisco IE switch, refer to the corresponding installation guides.

1. Log in to the switch using Device Manager credentials.

**Figure 98 Device Manager Login Screen**
2. After a successful login, the Dashboard for the switch loads.

Figure 99  Device Manager Dashboard

3. Configure PRP by selecting the **PRP** option under the **Configure** tab as highlighted in Figure 100.
4. Configure PRP Channel properties like channel number, switchport mode, allowed VLANs, native VLANs, and so on as highlighted in Figure 101.
5. The status of the PRP Channel would be reflected as soon as the configuration of the PRP channel is completed as highlighted in Figure 102.

**Figure 102  PRP Channel Status**

6. Select the **PRP** option listed under the **Monitor** tab to check details of V DAN and Node table details.
PTP over PRP

PTP is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP is designed specifically for industrial networked measurement and control systems and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

Previously, PTP traffic was allowed only on LAN-A of PRP. However, if LAN-A went down, PTP synchronization was lost. To enable PTP to leverage the benefit of redundancy offered by PRP infrastructure, PTP packets over PRP networks are handled differently than other types of traffic. The current implementation of PTP over PRP does not append a Recovery Control Task (RCT) to PTP packets and bypasses the PRP duplicate/discard logic for PTP packets.

Follow these steps to configure PTP over PRP network.

Note: The PTP feature over HSR ring is currently not supported.
Before You Begin

The grandmaster can be located in a PTP over PRP topology as one of the following:

- A Redbox connected to both LAN A and LAN B (PTP grandmaster as RedBox).
- A VDAN connected to a PRP RedBox (PTP grandmaster connected to a PRP RedBox).
- A DAN (PTP grandmaster clock directly attached to both LANs of PRP).

The PTP grandmaster cannot be attached either to LAN-A or LAN-B because only the devices in LAN-A or LAN-B will be synchronized to the GM.

The switch sends untagged PTP packets on the native VLAN when the switch port connected to the grandmaster clock is configured as follows:

- Switch is in Default Profile mode.
- Switch is in trunk mode.
- VLAN X is configured as the native VLAN.

When the grandmaster clock requires tagged packets, make one of the following configuration changes:

- Force the switch to send tagged frames by entering the global `vlan dot1q tag native` command:
  
  ```
  vlan dot1q tag native
  ```
Networking and Security in Industrial Automation Environments

Availability

- Configure the grandmaster clock to send and receive untagged packets. If you make this configuration change on the grandmaster clock, you can configure the switch port as an access port.

- Force the switch to tag PTP packets by entering the interface level command `ptp vlan <>`. With this configuration change, the switch would tag all PTP packets traversing through the interface with the corresponding VLAN.

  ```
  interface gigabitEthernet1/1
  ptp vlan <vlanID>
  ```

When the network requires Class of Service (COS) values for PTP packets to be set, make one of the following configuration changes:

- The switch by default sets the COS value to 4 to all tagged PTP packets according to the IEEE C37.238 standard in PTP Power profile mode.

- Force the switch to set COS value for PTP packets by entering global `ptp packet` command:

  ```
  ptp packet <cos>
  ```

Recommended Practices

- Disable PTP on interfaces where PTP is not necessary.

- Configure peer-to-peer transparent mode for PTP transparent clocks to reduce jitter and delay accumulation:

  ```
  ptp mode p2ptransparent
  ```

- Configure the switch to process non-PTP compliant PTP Grandmaster sending announce messages without Organization_extension and Alternate_timescale TLVs using the following command:

  ```
  ptp allow-without-tlv
  ```

- In interoperability scenarios, its best to use the default PTP domain value which as per C37.238:2011 standard is 0 (zero). The default PTP domain value on Cisco IE switches is set to 0 (zero). It can also be configured using the following command:

  ```
  ptp domain 0
  ```

Configuring PRP RedBox

PRP is designed to provide zero recovery time after failures in Ethernet networks. PRP allows a data communication network to prevent data transmission failures by providing network nodes two alternate paths for the traffic to reach its destination. Two LANs) provide alternate paths for the traffic over independent LAN segments. A switch configured for PRP mode has one Gigabit Ethernet port connecting each of the two LANs. The switch sends two packets simultaneously to each LAN through the two different ports to the destination node. The destination node discards duplicate packets.

To create and enable a PRP channel and group on a supported Cisco IE switch, follow these steps:

1. Enter global configuration mode:

   ```
   configure terminal
   ```

2. Create PRP LAN interface:

   ```
   interface PRP-channel1
   switchport mode trunk
   ```

3. Attach PRP channel to the physical interface. Follow the guidelines for identifying the switch role and the corresponding interface.

   ```
   interface range gigabitEthernet 1/1
   prp-channel-group 1
   ```
Configuring PTP over PRP

1. Enter global configuration mode:
   ```
   configure terminal
   ```

2. Set the Power Profile:
   ```
   ptp profile power
   ```

3. Specify the synchronization clock mode:
   ```
   ptp mode {boundary pdelay-req|p2transparent|forward}
   ```
   - mode boundary pdelay-req—Configures the switch for boundary clock mode using the delay-request mechanism. In this mode, the switch participates in the selection of the most accurate master clock. Use this mode when overload or heavy load conditions produce significant delay jitter.
   - mode p2transparent—Configures the switch for peer-to-peer transparent clock mode and synchronizes all switch ports with the master clock. The link delay time between the participating PTP ports and the message transit time is added to the resident time. Use this mode to reduce jitter and error accumulation. This is the default in Power Profile mode.
   - mode forward—Configures the switch to pass incoming PTP packets as normal multicast traffic.

4. Specify TLV settings:
   ```
   ptp allow-without-tlv
   ```

5. Specify synchronization algorithm if the switch is configured as PTP Boundary Clock:
   ```
   Switch(config)#ptp transfer {feedforward|filter linear}
   ```
   - feedforward - Very fast and accurate. No PDV filtering.
   - filter linear - Provides a simple linear filter (default).

Troubleshooting PTP over PRP

Use the following commands to check PTP clock type, GrandMaster properties, and clock source:

```
show ptp clock (In case of Boundary clock)
```
PTP Device Profile: Power Profile
Clock Identity: 0x0:BF:77:FF:FE:2C:47:0
Clock Domain: 10
Number of PTP ports: 28
PTP Packet priority: 4
Time Transfer: Feedforward
Priority1: 128
Priority2: 128
Clock Quality:
   Class: 248
   Accuracy: Unknown
   Offset (log variance): N/A
Offset From Master(ns): 12
Mean Path Delay(ns): 20
Steps Removed: 1
Local clock time: 14:02:47 IST Dec 13 2018

show ptp clock (In case of Peer to Peer Transparent clock)
PTP CLOCK INFO
PTP Device Type: Peer to Peer transparent clock
PTP Device Profile: Power Profile
Clock Identity: 0x0:BF:77:FF:FE:27:D3:80
Clock Domain: 10
Number of PTP ports: 28
PTP Packet priority: 4
Delay Mechanism: Peer to Peer
Local clock time: 08:40:51 UTC Dec 13 2018

show ptp parent
//shows the parent to which the PTP is synchronized with//
PTP PARENT PROPERTIES
Parent Clock:
   Parent Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
   Parent Port Number: 17
   Observed Parent Offset (log variance): N/A
   Observed Parent Clock Phase Change Rate: N/A
Grandmaster Clock:
   Grandmaster Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
   Grandmaster Clock Quality:
      Class: 6
      Accuracy: Within 250ns
      Offset (log variance): N/A
      Priority1: 128
      Priority2: 128

show clock detail
08:41:04.904 UTC Thu Dec 13 2018
Time source is PTP

show prp statistics ptpPacketStatistics
PRP channel-group 1 PTP STATS:
   ingress lan a: 45
   ingress drop lan a: 0
   ingress lan b: 48
   ingress drop_lan b: 0
   egress lan a: 90
   egress lan b: 93
PRP channel-group 2 PTP STATS:
   ingress lan a: 0
   ingress drop lan a: 0
   ingress lan b: 0
   ingress drop_lan b: 0
   egress lan a: 0
   egress lan b: 0
On a Cisco IE 5000 switch acting as PRP Redbox and also as PTP grandmaster, the PTP state on PRP member ports can be checked using the following command. Both the PRP member ports should have a port state of MASTER.

```
show ptp port gigabitEthernet 1/17
PTP PORT DATASET: GigabitEthernet1/17
  Port identity: clock identity: 0x0:BF:77:FF:FE:2C:36:80
  Port identity: port number: 17
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 23
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000
```

On a Cisco IE 5000 switch acting as PRP Redbox and PTP Boundary clock, the PTP state on PRP member ports can be checked using the following command. The state of the active port should be SLAVE and the other as PASSIVE_SLAVE. If the active port fails, the other port changes the state to SLAVE.

```
show ptp port gigabitEthernet 1/17
PTP PORT DATASET: GigabitEthernet1/17
  Port identity: clock identity: 0x0:BF:77:FF:FE:2C:47:0
  Port identity: port number: 17
  PTP version: 2
  Port state: SLAVE
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 20
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000

show ptp port gigabitEthernet 1/18
PTP PORT DATASET: GigabitEthernet1/18
  Port identity: clock identity: 0x0:BF:77:FF:FE:2C:47:0
  Port identity: port number: 18
  PTP version: 2
  Port state: PASSIVE_SLAVE
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 38
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000
```

**Cisco IE 5000 as PTP Grandmaster**

Cisco Industrial Ethernet switches are capable of accurate time distribution using PTP or IRIG-B, but previously relied on an external source to provide accurate time. The Cisco IE 5000 switch has a built-in Global Navigation Satellite System (GNSS) receiver that enables the switch to determine its own location and get accurate time from a satellite constellation. The switch can become the PTP Grandmaster clock for time distribution in the network.
Before You Begin

GNSS is supported only on Cisco IE 5000 switches with SKUs that have Version ID (VID) v05 or higher and GNSS firmware version 1.04 or higher. Verify using `show version` output:

```bash
show version | i Version ID
Version ID                      : V06
```

```bash
show version | i GNSS
GNSS firmware version           : 1.04
```

The GNSS feature is available for all feature sets (lanbase, ipservices) and does not require a separate license.

GNSS can be used as time source for PTP default and Power profiles only.

GNSS can be used as time source for PTP in GMC-BC mode only.

Configuring PTP Grandmaster

1. Enter global configuration mode:
   ```bash
   configure terminal
   ```

2. Enable GNSS.
   ```bash
   gnss
   ```

3. Configure the switch for grandmaster-boundary clock mode:
   ```bash
   ptp mode gmc-bc
   ```

Troubleshooting PTP Grandmaster

```
Switch#show gnss status
GNSS status: Enable
Constellation: GPS
Receiver Status: OD
Survey progress: 100
Satellite count: 11
PDOP: 1.00    TDOP: 1.00
HDOP: 0.00    VDOP: 0.00
Alarm: None
```

```
Switch#show clock detail
14:09:13.378 IST Thu Dec 13 2018
Time source is GNSS
```

```
Switch#show gnss satellite all
SV Type Codes: 0 - GPS, 1 - GLONASS, 2 - Beidou
```

```
All Satellites Info:
SV PRN No Channel No Acq Flg Ephemeris Flg SV Type Sig Strength
10 0 1 1 0 44
32 1 1 1 0 42
21 2 1 1 0 40
20 3 1 1 0 44
11 4 1 1 0 40
18 6 1 1 0 44
26 7 1 1 0 40
25 8 1 1 0 39
27 9 1 1 0 24
```
Quality of Service

This section describes how Quality of Service (QoS) works in industrial automation environments and specifies the major QoS design considerations when deploying Cisco industrial switches into industrial automation networks.

QoS is an enabling technology inside the industrial automation network. Cisco Industrial Switches employ a built-in Express Setup and Smart-ports method to facilitate simple deployment without having to take additional steps. However, studying and understanding the QoS solution and its performance implication is a very important task for the industrial automation solution development team.
Quality of Service

QoS refers to network control mechanisms that can provide various priorities to different industrial automation devices or traffic flows or to guarantee a certain level of performance of a traffic flow in accordance with requests from the application program. By providing dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics, QoS can ensure better service for selected network traffic.

Traffic Flows

Traffic flows in an industrial automation network have very different traffic patterns compared to client server-based applications in the IT network. For example:

- Cyclical I/O data is communicated on very short intervals (milliseconds) from devices to controllers and human-machine interfaces (HMIs) or workstations, all on the same network segment and mainly remaining in the local Cell/Area Zone.

- Industrial devices utilize unique Differentiated Services Code Point (DSCP) marking to identify itself with IT management traffic flows. For example, PTP event marked with DSCP 59, PTP management marked with DSCP 47, ODVA, Inc. Common Industrial Protocol (CIP) class urgent marked with DSCP 55, etc.

- Different types of industrial automation network traffic (Motion, I/O, and HMI) have different requirements for latency, packet loss, and jitter. The service policy should differentiate service for these types of traffic flows.

- OT traffic typically is pulse-based with very small packet size.

- IT and OT traffic often coexist together inside the industrial automation network. OT traffic take precedence over other IT management network traffic flows.

Figure 105, Table 52, and Table 53 illustrate a typical industrial automation network traffic flow, traffic types, and differentiated service marking.
**Figure 105 Industrial Automation Plant Manufacture Zone Traffic Flow**

![Diagram of traffic flow in an industrial automation environment.]

**Table 52 Industrial Automation Plant Manufacture Zone Traffic Types**

<table>
<thead>
<tr>
<th>Refer Number in Figure</th>
<th>From Description</th>
<th>To Description</th>
<th>Protocol</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a,b,c</td>
<td>Producer (for example, VFD Drive)</td>
<td>Consumer (for example, controller)</td>
<td>A producer (for example, VFD Drive, or controller) communicates data via CIP Implicit I/O (UDP multicast) traffic to multiple consumers. a—Represents device to controller IO. b—Represents controller–controller I/O. c—Represents controller reporting real-time status to HMI.</td>
<td>EtherNet/IP</td>
<td>UDP</td>
</tr>
<tr>
<td>2</td>
<td>Producer</td>
<td>Consumer</td>
<td>Producers can communicate data via CIP I/O as UDP unicast traffic to a consumer.</td>
<td>EtherNet/IP</td>
<td>UDP</td>
</tr>
</tbody>
</table>
Quality of Service

Table 52 Industrial Automation Plant Manufacture Zone Traffic Types

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>CIP Priority</th>
<th>DSCP enabled by default</th>
<th>802.1D Priority (default)</th>
<th>CIP Traffic Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event (IEEE 1588)</td>
<td>N/A</td>
<td>59 (111011)</td>
<td>7</td>
<td>PTP event messages, used by CIP Sync</td>
</tr>
<tr>
<td>PTP management (IEEE 1588)</td>
<td>N/A</td>
<td>47 (101111)</td>
<td>5</td>
<td>PTP management messages, used by CIP Sync</td>
</tr>
<tr>
<td>CIP class 0/1</td>
<td>Urgent (3)</td>
<td>55 (110111)</td>
<td>6</td>
<td>CIP Motion</td>
</tr>
</tbody>
</table>
Industrial automation plants adopt a common and well-understood Purdue model (reference ISBN 1-55617-265-6) for Control Hierarchy so as to segment network devices and functions into different functioning zones for easy management. Every segment deploys many different kinds of switches and routers with different network architecture and feature sets. In order to streamline all traffic flow and different network services and reduce packet loss, jitter, and latency, a well-designed QoS model is very important to guarantee network performance and operation.

Figure 106 shows a typical QoS model designed for cell/zone area inside an industrial automation plant, where multiple Cisco IE switches (Cisco IE 2000, Cisco IE 3x00 Series Switch, Cisco IE 4000, Cisco Catalyst 3850 and Cisco Catalyst 9300, etc.) inter-connected form an ingress and egress pipeline to classify and police network traffic flows.

### Table 53 Industrial Automation Plant Manufacture Zone Traffic Flow Marking

<table>
<thead>
<tr>
<th>Class</th>
<th>Mark</th>
<th>Priority</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled (2)</td>
<td>47 (101111)</td>
<td>5</td>
<td>Safety I/O I/O</td>
</tr>
<tr>
<td>High (1)</td>
<td>43 (101011)</td>
<td>5</td>
<td>I/O</td>
</tr>
<tr>
<td>Low (0)</td>
<td>31 (011111)</td>
<td>3</td>
<td>No recommendation at present</td>
</tr>
<tr>
<td>CIP UCMM All</td>
<td>27 (011011)</td>
<td>3</td>
<td>CIP messaging</td>
</tr>
<tr>
<td>CIP class 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Network Devices and QoS Models**

Industrial automation plants adopt a common and well-understood Purdue model (reference ISBN 1-55617-265-6) for Control Hierarchy so as to segment network devices and functions into different functioning zones for easy management. Every segment deploys many different kinds of switches and routers with different network architecture and feature sets. In order to streamline all traffic flow and different network services and reduce packet loss, jitter, and latency, a well-designed QoS model is very important to guarantee network performance and operation.
Quality of Service

Cisco IE 2000 Industrial Ethernet Switch

The Cisco IE 2000 mainly assumes an access switch role to bridge industrial Program Logic Controller (PLC). The Cisco IE 2000 utilizes Multilayer Switch QoS (mls) globally and establishes the trust boundary for the overall network. This is achieved by correctly classifying network traffic flows based on their protocol, ports, and QoS marking. The ingress side has two queues consisting of priority Queue and Shaped Round Robin (SRR) shared queue. Through a transmit ring, network traffic feeds into the egress side policed with one priority queue and three shared SRR queues for weighted bandwidth allocation and traffic enters into a transmit ring to exit the egress interface.

Cisco IE 3x00 Series Industrial Ethernet Switch

The Cisco IE 3X00 switch is the next generation switch replacing the Cisco IE 3000. It utilizes a Modular QoS Class (MQC) model along with ASIC pre-programmed Traffic Profile to classify network traffic and establish trust boundary. A simplified hardware architecture enables a QoS data plane entirely on an ASIC. Ingress side packet classification, marking, and policing are performed using either ASIC codepoint-based tables or TCAM rules. Packet enqueue and scheduling profile are decided based on the QoS Profile. Egress side packet enqueueing, scheduling, and shaping are performed. Different QoS packets will be mapped into packet 128 QoS profiles. Shaped Deficit Weighted Round Robin (SDWRR) provide dynamic enqueue and dequeue handling as compared with Weighted Round Robin (WRR). A Strict Priority Arbiter (SPA) can expedite mission critical packet handling in egress ports.

Cisco IE 4000 Industrial Ethernet Switch

The Cisco IE 4000 with more port density, compute power, and multiple industrial protocol support assumes either access layer switch or a distribution switch. It utilizes MQC and QoS Group to classify traffic and police them into the correct queue. A class-based Weighted Fair Queue (WFQ) with Priority Queue (PQ) is chosen to police traffic on the egress side. The Cisco IE 4000 does not have a SRR transmit ring.

Cisco Catalyst 3850 Network Switch

Cisco Catalyst 3850 StackWise switches are the cell/zone area gateway devices to interconnect Layer 2 device ring/chain with Layer 3 network infrastructures. The Cisco Catalyst 3850 switch utilizes MQC and QoS-Group for ingress traffic classification and policing. Network traffic enters into a StackWise ring and feeds into egress 1 Priority Queue and 3 Weighted Fair Queue (WFQ). An egress port SRR shaper provides weighted bandwidth allocation between different traffic classes.

Cisco Catalyst 9300 Network Switch

Cisco Catalyst 9300 StackWise switches provide a cloud ready software defined access (SD-Access). It utilizes policy-based automation from edge to cloud, which can incorporate mobility, IoT, cloud, and security in one portfolio. The Cisco Catalyst 9300 utilizes a similar QoS model as the Cisco Catalyst 3850 StackWise switch. UADP 2.0 Application-Specific Integrated Circuit (ASIC) incorporates template-based configurable QoS entries to ensure Superior QoS, including granular wireless bandwidth management, fair sharing, 802.1p Class of Service (CoS), Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port.

Traffic Classification

The first element in a QoS policy is to classify/identify the traffic that is to be treated differently. Classification and marking tools set this trust boundary by examining any of the following:

- Layer 2 parameters—802.1Q class-of-service (CoS) bits
- Layer 3 parameters—IP Precedence (IPP), Differentiated Services Code Points (DSCP), IP Explicit Congestion Notification (ECN), and source/destination IP address
- Layer 4 parameters—Layer 4 protocol (TCP/UDP) and source/destination ports
Layer 7 parameters—Application signatures

The QoS model implemented in Cisco IE switches focuses on the Differentiated Services or DiffServ model. One of the key goals of DiffServ is to classify and mark the traffic as close to the source as possible. This allows for an end-to-end model where intermediary routers and switches simply forward the frame based on the predetermined marking. Do not trust markings that can be set by users on their PCs or other similar devices, because users can easily abuse provisioned QoS policies if permitted to mark their own traffic.

Following classification, marking tools can set an attribute of a frame or packet to a specific value. Such marking (or remarking) establishes a trust boundary that scheduling tools later depend on.

**Figure 107 Industrial Automation Plant Manufacture QoS Trust Boundary**

The following steps describe ingress QoS implementation:

1. Establish ACLs for each industrial automation network traffic type. This will allow the industrial Ethernet switch to filter the network traffic based upon key characteristics like transport protocol (UDP or TCP), port type (CIP Explicit messages or Implicit I/O), or existing DSCP value.

2. Set up class-maps to match the ACL-filtered traffic with a classification.

3. Set up a policy map that assigns classification to class-maps.

4. Assign the service policy to each port that transports industrial automation network traffic.
Policing, Queuing, and Scheduling

Network device egress port can use policing, queuing, and scheduling tools to manage traffic flow priority by putting mission critical traffic into priority queue and allocating the correct amount of bandwidth across all traffic classes. The following sections describe each of the building blocks of an egress QoS model.

Policing

Policing is a mechanism to limit the bandwidth of any traffic class and can be used on any port.

Policing can result in three actions:
- No action if the bandwidth is not exceeded.
- If the bandwidth is exceeded, the packet may be dropped.
- If the bandwidth is exceeded, the packet may be "marked down" where the classification is modified to presumably lower its priority.

Queuing

Queuing establishes buffers to handle packets as they arrive at the switch (ingress) and leave the switch (egress). Each port on the switch has ingress and egress queues. Both the ingress and egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedence for different traffic classifications. Each queue has three thresholds to proactively drop packets before queues fill up. Traffic classes assigned to thresholds 1 or 2 will be dropped if the queue buffer has reached the assigned threshold. Traffic classes assigned to a threshold of 3 for a specific queue will only be dropped if that queue has filled its buffer space.

Table 54  Industrial Automation Plant Manufacture Zone Traffic Type and Queue Allocation

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>PTP Event</th>
<th>CIP Urgent</th>
<th>PTP Mang., CIP Scheduled, CIP High</th>
<th>Network Control</th>
<th>Voice Data</th>
<th>CIP Low, CIP Class 3</th>
<th>Voice Control</th>
<th>Best Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>59</td>
<td>55</td>
<td>47, 43, 48</td>
<td>46</td>
<td>31, 27</td>
<td>24</td>
<td>The rest-</td>
<td></td>
</tr>
<tr>
<td>CoS</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>2 1 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>PTP Event</th>
<th>CIP Motion</th>
<th>PTP Mang., Safety I/O, I/O</th>
<th>STP, etc.</th>
<th>SIP, etc.</th>
<th>CIP Explicit Messages</th>
<th>SIP</th>
<th>All the rest</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS-to-Ingress Queue</td>
<td>Queue 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>map</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress Queue</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threshold</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| CoS-to-Egress Queue   | Queue 3   | Queue 4    | Queue 2                     |           |           |                       |     |
| map                   |           |            |                             |           |           |                       |     |
| Egress Queue          | 3         | 3          |                             | 3         | 3         | 2                     | 3   |
| Threshold             | 3         |            |                             |           |           |                       |     |
Quality of Service

Table 55  Industrial Automation Plant Manufacture Zone Ingress Queue Allocation

<table>
<thead>
<tr>
<th>Ingress Queue</th>
<th>Queue #</th>
<th>CoS-to-Queue Map</th>
<th>Traffic Type</th>
<th>Queue Weight</th>
<th>Queue (Buffer) Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRR Shared</td>
<td>1</td>
<td>0, 1, 2</td>
<td>All the rest</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>Priority</td>
<td>2</td>
<td>3, 4, 5, 6, 7</td>
<td>PTP, CIP, Network Control, Voice, Video</td>
<td>60%</td>
<td>60%</td>
</tr>
</tbody>
</table>

Table 56  Industrial Automation Plant Manufacture Zone Egress Queue Allocation

<table>
<thead>
<tr>
<th>Egress</th>
<th>Queue #</th>
<th>CoS-to-Queue</th>
<th>Traffic Type</th>
<th>Queue</th>
<th>Queue Size for Gb</th>
<th>Queue Size for 10/100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>1</td>
<td>7</td>
<td>PTP Event</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>SRR Shared</td>
<td>2</td>
<td>0, 1, 2, 4</td>
<td>All the rest</td>
<td>19</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>SRR Shared</td>
<td>3</td>
<td>5, 6</td>
<td>PTP Management, CIP Implicit I/O, Network Control &amp; Voice data</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>SRR Shared</td>
<td>4</td>
<td>3</td>
<td>CIP Explicit Messages</td>
<td>40</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

Scheduling

Both the ingress and egress queues are serviced by either Shared Round-Robin (SRR) scheduling or Strict Priority Arbiter (SPA, Cisco IE 3x00 Series Switch), which controls the rate at which packets are sent.

The following are the general configuration steps for egress side QoS:

1. Enable priority queue out (queue 1) on all switch ports carrying IACS network traffic (access and trunk ports). This ensures the highest priority traffic assigned to the queue will be serviced quickly. This queue will no longer be serviced as a shared round-robin and any SRR settings for that port will not be in effect.

2. Assign specific queues for IACS network traffic and other priority traffic, if it exists (e.g., Voice and Network Routing traffic). These queues are then assigned buffers and scheduling weights to minimize packet loss and optimize scheduling. Maintain 1 ingress and egress queue for other traffic. For ingress, queue 1 is for other traffic. For egress, queue 2 (of 4) is for best effort traffic.

3. Map IACS network traffic to specific queues via COS and DSCP maps for each queue and threshold. IACS network traffic should be assigned to the third threshold to avoid packet loss. Packet loss will occur if the queues buffers are full, but not until then. The queue that they are assigned to will define the minimum amount of bandwidth they receive and will define how quickly they are serviced, where the priority queue is always handled first.

4. Assign SRR Queue bandwidth share weightings for all ports to assign weights to the egress queues for that port. This represents the relative amount of bandwidth dedicated to traffic in a queue when congestion occurs. When a queue is not using its bandwidth, the bandwidth is made available to other queues.

5. Define output/egress queue buffer sets that are assigned to a port to allocate the buffer space to a queue. By allocating more queue space to IACS network traffic queues, packet-loss is avoided. The above settings allow for specific priority to be assigned to CIP network traffic while maintaining a basic service for other types of traffic. These settings are aligned with the ODVA, Inc. recommendations for QoS and ensure that IACS devices that cannot mark their own CIP traffic receive the same preferential QoS treatment as IACS devices that mark their CIP traffic. No specific configuration is required to apply these QoS recommendations to the Cisco industrial Ethernet switch beyond using Express Setup and selecting the appropriate Smartport.

For configuration examples, refer to QoS Configuration Examples, page 222.
Management and Configuration Tools

The following configuration tools are used in this guide for configuration and management of Cisco IE switches.

Device Manager

You can use Device Manager, which is in the switch memory, to manage individual and standalone switches. This web interface offers quick configuration and monitoring. You can access Device Manager from anywhere in your network through a web browser. For more information, see the Device Manager online help.

Some of the features that can be configured with Device Manage are:

- Port Settings
- Etherchannels
- REP
- Smartports
- STP
- VLAN
- VTP
- AAA
- Multicast
- QoS

Cisco IOS CLI

The switch CLI is based on Cisco IOS software and is enhanced to support desktop-switching features. You can fully configure and monitor the switch. You can access the CLI either by connecting your management station directly to the switch management port, or a console port, or by using Telnet or SSH from a remote management station.

Smartports

Smartports macros provide a convenient way to save and share common configurations. You can use Smartports macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

Each Smartports macro is a set of CLI commands that you define. Smartports macros do not contain new CLI commands; they are simply a group of existing CLI commands.

When you apply a Smartports macro to an interface, the CLI commands within the macro are configured on the interface. When the macro is applied to an interface, the existing interface configurations are not lost. The new commands are added to the interface and are saved in the running configuration file.

Refer to Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide for Smartports configuration details:
Cisco Industrial Network Director

Cisco IND provides an easy-to-use interface designed especially for operations staff to be able to get a clear picture of their plant floor network and attached automation endpoints. For additional information, refer to the official product documentation available at:

- [http://www.cisco.com/go/ind](http://www.cisco.com/go/ind)

Deploying a New Industrial Switch

When configuring a new switch, use Express Setup and configure an IP address to manage the switch remotely.

Use one of the following options to configure the switch:

- Use Plug and Play feature in Industrial Network Director as described below.
- Use Smartports macros and Device Manager to apply configuration as described below.
- Use Smartports macros and CLI to apply the configuration.

Cisco IND Plug-N-Play Feature

The Cisco IND Plug-N-Play feature provides the OT technician with a way to efficiently replace or add a new network device to their current network topology. The following section describes the steps to add a device to an existing ring using a configuration template in IND and the plug-n-play feature.

Creating a Template

IND requires a template be saved with a .ftl file extension, apache freemarker. The template is created using a copy of standard configuration on a existing switch. After that, values that may change, like host names, are replaced with input variables that are configured when pushed to a new device. The template is saved with a ftl extension by utilizing File -> Save As.. and changing the .txt extension to .ftl.

**Note:** If you are copy a running configuration and modifying it as a template, be sure to remove any crypto self-signed certificate configurations. If you push a configuration with a certificate in the template, the self-signed certificate will be overwritten with the old one and will prevent the web UI from functioning.
Management and Configuration Tools

**Figure 108 Replacing File Extension**

![Image of replacing file extension]

**Loading a Template**

Go to Design -> Plug and Play -> Config Templates -> Upload and select the template previously created.

**Figure 109 Loading Template**

![Image of loading template]

**Template Validation**

In the current template you will notice the $(hostname) variable. Utilizing $({}) you can define a variable in a template that will require the user to input the required value when pushing the configuration.
Out of the box, a switch will guide you through initial configuration. Configure the basics such as switch name, management, etc. Ensure the IP address of the device is reachable by IND. After initial configuration, configure the device to utilize plug-n-play and point it towards IND:

```
pnp profile <profile-name>
transport http ipv4 <ip address of IND server> port 8088
```

### Pushing Configuration Template

1. Once device is configured for UPNP and is placed on the network, you should see the device under **Design -> Plug-n-Play -> Unclaimed Devices**. You should now be able to select the device to push a configuration template.

2. To push a configuration template, we must first create a new profile to define some attributes.
3. Devices that need to be configured are matched via serial number.

4. Enter the proper values in the variable fields.
5. Validate that the configuration is correct and click **Claim**.

6. Verify that the new device has been configured correctly. Status should read Config Success.

### Applying Global Smartports

After running the express setup you could apply the following configuration macros through CLI:

**cisco-global**

cisco-global macro applies the following configurations:

- Enable dynamic port error recovery for link state failures.
- Enable aggressive mode UDLD on all fiber uplinks.
- Enable Rapid PVST+ and Loopguard.
Networking and Security in Industrial Automation Environments

Management and Configuration Tools

To apply use the following command in configuration mode:

```
macro global apply cisco-global
```

cisco-ie-global

cisco-ie-global macro applies the following configurations:

- Access List and Policy Map for CIP QoS.
- Configures ip igmp snooping and ip igmp snooping querier.
- Configures spanning-tree mode to MST and Loopguard.

To apply use the following command in configuration mode:

```
macro global apply cisco-ie-global
```

IND for Plantwide PTP Time Synchronization Management

IND for PTP infrastructure discovery and management requires CIP and SNMP features and begins with IND release 1.7. It includes the following steps:

- Industrial network devices discovery
- Industrial network devices inventory and licensing
- Industrial network devices PTP topology and PTP attributes validation

System Requirements

Table 57  System Requirements

<table>
<thead>
<tr>
<th>Desktop Requirements</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Operating System (OS)</td>
<td>Windows 7 Enterprise or Professional with Service Pack 2 or Windows 10</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When using Windows 2016 Server (64-bit version), you may not be able to select the Uninstall option from the Windows Start program window. If this occurs, log out of Windows 2016 and then log in again. If you do not see the Uninstall option in the Windows menu, then restart the PC.</td>
</tr>
<tr>
<td>Browser</td>
<td>Chrome: Version 50.0.2661.75, 53.0.2785.116</td>
</tr>
<tr>
<td></td>
<td>Firefox: 55.0.3, 57.0.4,63.0.3 or above</td>
</tr>
<tr>
<td>CPU</td>
<td>Quad-Core 1.8 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

The IND software package requires:

- No other FTP server is running and listening on port 21.
- No other instance of PostgreSQL is installed on port 5432 or any other port on the system.
The host name of the Windows machine must start with a letter of the alphabet (A-Z or a-z).
- You may use special characters within your password such as digits (0-9), minus sign (-), and period (.) as well as alpha characters.

The following ports are open for both inbound traffic on the firewall:

TCP ports:
- 21—FTP active port for ODM file transfer in regular mode
- 8088—HTTP for PnP
- 8443—HTTPs for Web UI and PnP
- 50000-50050—FTP passive ports for ODM file transfer in regular mode

UDP port:
- 30162—SNMP traps

The following ports are open for outbound traffic on the firewall:

TCP ports
- 443—HTTPs for WSMA/JSON-RPC in secure mode
- 80—HTTP for WSMA/JSON-RPC in regular mode
- 22—SSH/SCP in secure mode
- 23—Telnet in regular mode
- 44818—CIP
- 102—PROFINET
- 502—ModBus
- 4840—OPC-UA
- 139—NetBios TCP/IP
- 1812—RADIUS

UDP ports:
- 161—SNMP
- 67—DHCP server if the IND PnP DHCP helper is being used
- 2222—CIP
- 34964—PROFINET
- 4840—OPC-UA

The following ports are open for both inbound and outbound traffic on the firewall:

TCP ports:
- 8910—HTTPs for pxGrid
Management and Configuration Tools

- 47808—BacNet

**Note:**

- The above listed ports are default ports. If any of the above ports are customized as part of the installation or in an access profile, then the corresponding ports should be open in the firewall.
- Industrial Network Device local user need to have privilege level of 15.

Cisco Industrial Network Directory Installation


IND Industrial Network Devices Discovery

IND for PTP discovery requires the following features to be enabled in industrial network devices:

- CISCO-PTP-MIB for SNMP supported devices
- CIP object 43 for CIP supported devices

In order for Industrial network devices to be discoverable by IND, the following SNMP and CIP related configuration needs to be manually enabled:

```plaintext
IE5K-1#show run int v1a 18
! interface Vlan18
cip enable
end
!
IE5K-1#show run | inc snmp
!
snmp-server group IA-IoT-PTP v2c
snmp-server community cisco RW
!
```

System Requirements

Creating Device Access Profiles

Create a Device Access Profile and provide the corresponding SNMP community string and version setting, Select the **Advanced** option to provide ssh/telnet related credentials as shown in Figure 116.
Creating Device Inventory with IP Scan

Based on the network infrastructure and IP mapping, create an IP Scan discovery profile as shown in Figure 117.
Industrial Network Device Discovery is based on SNMP MIB and related CIP features being enabled inside network devices. IND IP Scan will send an SNMP probe as specified in the Device Discovery Profiles IP range above and populates Inventory tables and constructs device connectivity in the background. Figure 118 is the built-up Inventory table; each inventory device reflects its detailed device related information.

Industrial Network Devices are started inside IND in an “Unlicensed” state as shown in Figure 120.
Industrial Network Devices have to be toggled into a “Licensed” state for management PTP related features as shown in Figure 119.
During the license state change, a bootstrap configuration is pushed into each of the network devices to enforce license subscription management. The following is a bootstrap sample configuration:

Bootstrap Configuration
The system pushes the following configuration when you move the device to the Licensed state in the system:
# Secure-mode only
# Only if user selected self-signed certificate for device certificate in access profile
# If the device has a self-signed certificate with RSA key pair length < certificate key length given in access profile (or) if the device does not have a self-signed certificate in nvram
crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR modulus {certificate-key-length}
crypto pki trustpoint IND_HTTPS_CERT_KEYPAIR
enrollment selfsigned
subject-name OUT="IOT"
rsakeypair IND_HTTPS_CERT_KEYPAIR
hash sha256
crypto pki enroll IND_HTTPS_CERT_KEYPAIR
# Enable SCP server
# Used for transferring ODM file from the system to device
Networking and Security in Industrial Automation Environments

Management and Configuration Tools

# For insecure mode the system uses FTP to transfer ODM file
ip scp server enable

# If AAA is not enabled on the device
ip http authentication local
# Secure mode only
ip http secure-server
ip http secure-port {secure-mode-access-port}
# Insecure mode only
ip http server
ip http port {regular-mode-access-port}

# Configure WSMA
# The system uses WSMA for management
wsma agent exec
profile exec
# Secure-mode only
wsma profile listener exec
transport https path /wsma/exec
# Insecure mode only
wsma profile listener exec
transport http path /wsma/exec

# SNMP configuration
# Trap destination. The system supports both v2c and v3
snmp-server host <system-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp-server host {system-ip-address} version 3 {snmpv3_mode} {snmpv3_username} udp-port 30162

# Bootstrap configuration for SNMPv3
# The system needs the following configuration to be able to query bridge-mib with SNMPv3 security in
# IOS devices.
# This bridge-mib is required by inventory service to get MAC-Table from SNMP when the system moves
device from new to managed state.
snmp-server group {group_name} v3 {snmpv3_mode} context vlan- match prefix
# Enable RFC2233 compliant for linkDown and linkUp trap
snmp-server trap link ifet

# Enable traps supported by the system
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rep
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps flash insertion removal
snmp-server enable traps envmmon fan shutdown supply temperature status
snmp-server enable traps alarms informational
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold

# Configure SNMP to retain ifindex across reboots
snmp ifmib ifindex persist

# Enable dual-power supply
# Not applicable for S5410, IE5K, CGS2K, IE3010
power-supply dual

# Enable SD card alarm
# Not applicable for S8000, CGS2K, IE2000U, IE3010, IE3K, IE3200, IE3300, IE3400 and S5800
alarm facility sd-card enable
alarm facility sd-card notifies

# Turn on notifies for selected facility alarms
alarm facility temperature primary notifies
alarm facility temperature secondary notifies
# Following not application for CGS2K, IE3010
alarm facility power-supply notifies
no alarm facility power-supply disable
Bootstrap Configuration for IE 1000 Switches

# Traps for IE 1000
snmp.config.trap_source.add coldStart
snmp.config.trap_source.add warmStart
snmp.config.trap_source.add linkDown
snmp.config.trap_source.add linkUp
snmp.config.trap_source.add topologyChange
snmp.config.trap_source.add authenticationFailure
snmp.config.trap_source.add entConfigChange
snmp.config.trap_source.add fallingAlarm
snmp.config.trap_source.add risingAlarm
snmp.config.trap_source.add newRoot

# Trap destination
snmp.config.trap_receiver.add <system-ip-address> version 2c {snmpv2-read-community} udp-port 30162

# Trap destination for v3 security
snmp.config.trap_receiver.add {system-ip-address} version 3 {snmpv3_mode} {snmpv3_username} udp-port 30162
Management and Configuration Tools

Figure 120 IND License Apply into Industrial Devices
Creating PTP Topology and Display PTP Attributes

For licensed industrial network devices, IND topology will enable the PTP layer to display the PTP-related topology and each PTP device’s attributes as shown in Figure 122, Figure 123, Figure 124, and Figure 125.
Figure 122 Topology and Device Attributes—PTP Hierarchy
Figure 123 Topology and Device Attributes—PTP GrandMaster Device
Figure 124  Topology and Device Attributes—PTP Boundary Clock Device
Using Device Manager

The following sections contain some features that are configured using device manager. For a complete list and configuration details and options, see the Device Manager online help.

Traffic Segmentation

- VLAN in Configuration -> Layer 2 -> VLAN

Interface Configurations

- SVIs in Configuration -> Layer 2 -> VLAN
- Interface settings in Configuration -> Interface -> Ethernet
- Etherchannel in Configuration -> Interface -> Logical
Management and Configuration Tools

Redundancy
- Etherchannel in Configuration -> Interface -> Logical
- REP in Configuration -> Layer 2 -> REP

Routing
- Default Gateway in Configuration -> Routing Protocols -> Static Routing
- Static routes in Configuration -> Routing Protocols -> Static Routing

Security
- ACL in Configuration -> Security -> ACL
- AAA in Configuration -> Security -> AAA
- User creation in Administration -> Management -> User Administration

Other Configuration
- VTP in Configuration -> Layer 2 -> VTP
- Interface smartports macros in Configuration -> Layer 2 -> Smartports
- IGMP snooping in Configuration -> Services -> Multicast
- QoS in Configuration -> Services -> Multicast
- PTP in Administration -> Management -> Time
- NTP in Administration -> Management -> Time
- CIP in Administration -> Management -> CIP

CLI Specific Configuration
The following sections contain some configurations that are not possible using Device Manager and should be configured using CLI.

Line Passwords Encryption
The password encryption service is enabled in the global configuration with the following command:

```
service password-encryption
```

Logging Settings
To configure the logging buffer size or the time stamping service:

```
logging buffered 16384
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```
QoS Configuration Examples

Error Disable

To fully configure the error-disable feature, use the following commands:

```
errdisable recovery cause udld
errdisable recovery cause bpdu-guard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pAgp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause pSecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery interval 30
```

VTY Line Configuration

If desired the VTY lines must be configured to use SSH only. By default they accept both SSH and Telnet. Add the following configuration under line settings:

```
transport input ssh
```

QoS Configuration Examples

**Cisco IE 2000:**

```
! 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
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
  set qos-group 1
 class CIP-Implicit_dscp_47
  set qos-group 1
 class CIP-Implicit_dscp_43
  set qos-group 1
 class CIP-Implicit_dscp_any
  set qos-group 2
 class CIP-Other
  set qos-group 2
 class 1588-PTP-Event
  set qos-group 0
 class 1588-PTP-General
  set qos-group 1
!
```

QoS Configuration Examples

```plaintext
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-Other
    match access-group 105
class-map match-all CIP-Implicit_dscp_any
    match access-group 104
class-map match-all CIP-Implicit_dscp_43
    match access-group 103
class-map match-all CIP-Implicit_dscp_47
    match access-group 102
class-map match-all CIP-Implicit_dscp_55
    match access-group 101

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

Cisco IE 4000:

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 106 permit tcp any eq 44818 any
access-list 107 permit udp any eq 319 any

policy-map CIP-PTP-Traffic
    class CIP-Implicit_dscp_55
        set qos-group 1
    class CIP-Implicit_dscp_47
        set qos-group 1
    class CIP-Implicit_dscp_43
        set qos-group 1
    class CIP-Implicit_dscp_any
        set qos-group 2
    class CIP-Other
```
Networking and Security in Industrial Automation Environments

QoS Configuration Examples

```
set qos-group 2
class 1588-PTP-Event
set qos-group 0
class 1588-PTP-General
set qos-group 1
!
policy-map PTP-Event-Priority
class qos-group-0
  priority
class qos-group-1
  bandwidth remaining percent 40
class qos-group-2
  bandwidth remaining percent 40
class class-default
  bandwidth remaining percent 20
!
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-Other
  match access-group 105
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
!
class-map match-all qos-group-2
  match qos-group 2
class-map match-all qos-group-1
  match qos-group 1
class-map match-all qos-group-0
  match qos-group 0
!

Cisco IE 3X00

!
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
!
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
```
QoS Configuration Examples

class 1588-PTP-General
  set ip dscp 47
!
policy-map PTP-Event-Priority
  class class-0
    priority
    class class-1
      bandwidth remaining percent 40
    class class-2
      bandwidth remaining percent 20
    class class-default
      bandwidth remaining percent 40
  !
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-Other
  match access-group 105
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
!
class-map match-all class-2
  match ip dscp ef
class-map match-all class-1
  match ip dscp 47
class-map match-all class-0
  match ip dscp 59
!

Cisco Catalyst 3850:
!
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
!
policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
    set qos-group 1
  class CIP-Implicit_dscp_47
    set qos-group 1
  class CIP-Implicit_dscp_43
    set qos-group 1
  class CIP-Implicit_dscp_any
    set qos-group 2
  class CIP-Other
    set qos-group 2
  class 1588-PTP-Event
    set qos-group 0
  class 1588-PTP-General
QoS Configuration Examples

```plaintext
set qos-group 1
!
policy-map PTP-Event-Priority
class qos-group-0
  priority level 1
class qos-group-1
  bandwidth remaining percent 40
class qos-group-2
  bandwidth remaining percent 40
class class-default
  bandwidth remaining percent 20
!
class-map match-any 1588-PTP-General
  match access-group 107
class-map match-any 1588-PTP-Event
  match access-group 106
class-map match-any CIP-Other
  match access-group 105
class-map match-any CIP-Implicit_dscp_any
  match access-group 104
class-map match-any CIP-Implicit_dscp_43
  match access-group 103
class-map match-any CIP-Implicit_dscp_47
  match access-group 102
class-map match-any CIP-Implicit_dscp_55
  match access-group 101
!
class-map match-any qos-group-2
  match qos-group 2
class-map match-any qos-group-1
  match qos-group 1
class-map match-any qos-group-0
  match qos-group 0
!
Cisco Catalyst 9300:
!
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
!
policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
    set qos-group 1
  class CIP-Implicit_dscp_47
    set qos-group 1
  class CIP-Implicit_dscp_43
    set qos-group 1
  class CIP-Implicit_dscp_any
    set qos-group 2
  class CIP-Other
    set qos-group 2
  class 1588-PTP-Event
    set qos-group 0
  class 1588-PTP-General
    set qos-group 1
!
policy-map PTP-Event-Priority
```

226
Configuring the Infrastructure

This section describes how to configure Cell/Area Zone Networking and Security Solution infrastructure components such as Cisco ISE, Cisco IE and Industrial Ethernet switches, and IND based on the design considerations in Cell/Area Zone Security Design Considerations, page 86. This section provides screen shots for the specific features and also the CLI configuration of an IES. It includes the following major topics:

- IND configuration
- Cisco ISE configuration
- IES configuration

Industrial Network Director (IND)

This section describes validated configuration for the IND needed for the following features:

- Creation of Asset discovery profiles for IACS assets and networking devices.
- Creation of Access Profiles that will be used in discovering IACS assets and networking devices.
- Creation of groups for IACS assets and networking devices based on the Cell/Area Zone Groups.
- Creation of assetTags that will be used to provide additional attributes to Cisco ISE for profiling IACS assets.
- Detailed steps for pxGrid integration between IND and Cisco ISE.
Installation

The installation notes for IND can be found at:

Creating Asset Discovery Profile

The objective of creating an asset discovery profile is to define an IP address scope of different IACS assets and networking devices and scan those assets. If the IACS or networking device is reachable, then IND scans the device, discovers the attributes, and moves them to the asset-inventory section. Figure 126 shows how different asset discovery profiles are defined in IND.

Figure 126 Creating the Asset Discovery Profile

As shown in the first row of Figure 126, IACS profile is performing an IP scan for the IP address range 10.17.10.1-10.17.10.254. The Access Profile used for this scan is IACS_PROFILE (explained in the next section) and all these devices are attached to a group called IACS_devices (also explained in the section below).

Configuring Access Profiles

The Access Profile is a template that has the common configuration parameters: username, password, and the SNMP community string information. When a group of devices use a different set of parameters, then a separate Access Profile can be defined. The Access Profile created in this section is tied to the Discovery Profile. Figure 127 shows the details of an Access Profile named IACS_PROFILE.
Asset Inventory

IND maintains list of devices that it has discovered in the Asset Inventory. Each element of the Asset Inventory provides information such as an IES that is attached to an IACS asset, the device type (Controller, IO, and other device types), the interface between the IACS device and the IES, the protocol used to communicate with the IACS asset, IP address of the IACS asset, group information of the device, vendor information, and so on. There are filters available for OT control system engineers to search for devices based on different criteria. Figure 128 shows a list of controllers that support the CIP protocol. As shown in Figure 128, IND displays important information about the IACS asset.
Group Management

Managing devices in separate groups not only simplifies the management of devices, but can also allow an OT control system engineer to influence an access policy for IACS assets. Figure 129 shows three groups that have been created based on the Cell/Area Zone topology.

Configuring Security Tags

IND release 1.4 and greater supports another important feature called security tags. An OT control system engineer can tag a device with a security tag. This feature allows an OT control system engineer to express an intent for an IACS asset (for more information about intent, see OT Managed Remote Access to Plant Floor, page 109. Figure 130 show how security tags can be created. In Figure 130 the security tag of 10 has been assigned to two devices.
Licensing

IND comes up with a base license that allows an OT operator to create Asset Discovery Profiles, scan the assets, and export the asset attributes to Cisco ISE. To perform these tasks, no special license is required. However, if the OT operator would like to have access to features of IND for managing IES devices, then licenses must be purchased.

Licensing features include:

- Switch diagnostics and monitoring such as:
  - Port utilization
  - Interface statistics
  - Syslog
  - CPU and memory usage
  - SD Flash capacity
  - Power supply status
  - Connected devices
  - Alarms
  - MAC and VLAN tables
  - Configuration backup and archives
  - DLR data
- CIP backplane bridging (does not work with Trustsec)


Configuring Cisco ISE

This section gives details on how to configure Cisco ISE for the following components:

- Distribution deployment
Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

- pxGrid between Cisco ISE and IND
- Enabling profiling and configuring different profiling policies
- TrustSec configuration

Distribution Deployment

As mentioned in Cisco ISE Deployment Considerations, page 101, distributed deployment of ISE was chosen for this CVD and also validated with the distribution deployment model. Figure 131 shows how different instances of ISE were used to achieve the distribution model.

Figure 131 Devices Present in Distributed ISE Deployment

Table 58 describes the role for each of the ISE instances.

Table 58 ISE Instance Roles

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>cidm-ise-2</td>
<td>Primary role is for Administration and Secondary role is for Monitoring</td>
</tr>
<tr>
<td>cidm-ise-1</td>
<td>Primary role is for Monitoring and Secondary role is for Administration</td>
</tr>
<tr>
<td>cidm-ise-4</td>
<td>Policy Service Node</td>
</tr>
<tr>
<td>ise24</td>
<td>Policy Service Node</td>
</tr>
</tbody>
</table>

As shown in Table 58, cidm-ise-2 is the PAN node for this design, and all the administration tasks such as configuration of network devices, authentication policies, authorization policies, certificate management, checking logs and all other tasks must be done on this PAN. No configuration is done on the PSN nodes. The network access devices will use the IP address of the PSN node for RADIUS and CTS configuration. The network access devices must not point to the PAN node. In this CVD, when displaying information on navigation it would be mentioned as (ISE admin web), which means configuration is done on the PAN node.

Configuring pxGrid between Cisco ISE and IND

Enabling pxGrid registration between IND and Cisco ISE involves a couple of steps. The pxGrid framework needs certificate-based authentication. So, both Cisco ISE and IND need to present their certificates to each other for the registration process to be completed. The next sub-sections describe the following steps that need to be performed:

- Enabling pxGrid in Cisco ISE, page 233
- Enabling pxGrid Service in Cisco ISE Certificate, page 233
- Exporting the Cisco ISE Certificate, page 234
- Downloading IND Certificate, page 234
- Importing IND Certificate to Cisco ISE, page 235
- Configuring pxGrid on IND, page 235
Enabling pxGrid in Cisco ISE

The pxGrid service needs to be enabled in the Cisco ISE. To enable pxGrid service, go to (ISE admin web)→Deployment. Figure 132 shows how to enable pxGrid services in the Cisco ISE.

Figure 132 Enabling pxGrid Service in the Cisco ISE

Enabling pxGrid Service in Cisco ISE Certificate

For pxGrid registration between IND and Cisco ISE to work, the root certificate for Cisco ISE needs to be exported into IND. This step is done on the PAN PRI. The first step is to pick a certificate in (ISE admin web)→Administration→Certificate→System Certificate and then enable pxGrid services in that certificate. Figure 133 shows pxGrid service enabled for a self-signed certificate in Cisco ISE.
Figure 133 Cisco ISE Certificate with pxGrid Services Enabled

Exporting the Cisco ISE Certificate

The next step is to export the above certificate so that the exported certificate can be imported to IND. After the export option is selected, the file will be downloaded into the local computer. The downloaded certificate needs to be saved and is used in the IND pxGrid registration to ISE, which is shown in Configuring pxGrid between Cisco ISE and IND, page 232.

Figure 134 Exporting Cisco ISE Certificate

Downloading IND Certificate

The self-signed certificate of the IND must be exported from the IND and must be imported to Cisco ISE as a trusted certificate. This step is mandatory because for the Cisco ISE to trust IND, it must know the root certificate of IND. Figure 135 shows the option for downloading the IND certificate. When Download .pem IND certificate is selected, the certificate is downloaded to the computer which must, in the next step, be imported into Cisco ISE.
Importing IND Certificate to Cisco ISE

The IND certificate must be imported into: (ISE admin web)→Administration→Certificates→Trusted Certificates store. With this step completed, the root certificates of both IND and Cisco ISE are in each other’s trusted store. Figure 136 shows the status on Cisco ISE after the IND certificate is imported into the Cisco ISE Trusted Certificates list.

Configuring pxGrid on IND

On the IND, pxGrid registration needs to be performed. Figure 137 shows the parameters that must be provided for successfully registering IND to Cisco ISE. The server information is the FQDN name of the Cisco ISE server and it must be resolvable by the IND either by using DNS or using a local host to IP address mapping in the IND server. The Node Name can be any name that is easier to remember and the Certificate field is the certificate that was downloaded in the previous step. When the connection is initiated from IND for pxGrid set up, the acknowledgment must say that pxGrid registration is successful. If no response is received, then further troubleshooting must be performed. When the registration is successful, the IND will be listed under the web-clients list in Cisco ISE, which is shown in Figure 138.
Configuring the Infrastructure

Approving IND Client in Cisco ISE

The IND web-interface may report that the registration between IND and Cisco ISE is successful. But the IT security architect must approve the IND registration request on Cisco ISE as shown in Figure 138.

Profiling in Cisco ISE

Profiling in Cisco ISE happens using several probes such as RADIUS, DHCP, SNMP, and so on. Cisco ISE can profile different types of assets, but this CVD focuses on profiling IACS assets using pxGrid probe.

Enabling pxGrid Probe in Cisco ISE

To discover IACS assets, Cisco ISE uses pxGrid probe to discover and profile IACS assets. To enable pxGRID probe, navigate to (ISE admin web)→Administration→Deployment and then select the appropriate PSN (ise24 in this CVD) and then select the profiling tab where an option is provided to enable the pxGRID probe. Figure 139 shows how to enable pxGrid probe in Cisco ISE.
Creation of User Groups

In this CVD some example groups were create to explain how OT control system engineers and IT security architects can create groups of devices and profile them. Table 59 gives an example on different roles for IACS assets in a plant-wide architecture. The description in Table 59 shows the permission needed for a particular user group. For example, a device classified as Level_3 group is a device that needs access to all the devices in the plant-wide architecture. Similarly, a device classified as Level_0_IO device has access to devices that are located in a particular Cell/Area Zone. The main intent of the Table 59 access policy example is only to provide a reference example for designing an access policy using TrustSec in a plant-wide network.

<table>
<thead>
<tr>
<th>Device</th>
<th>Location in Plant-wide Network</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering Workstation (EWS)</td>
<td>Level 3 site operations</td>
<td>Must have access to all the devices in the plant-wide architecture</td>
</tr>
<tr>
<td>Controller Interlocking</td>
<td>Cell/Area Zone</td>
<td>All the interlocking PACs must have access to another inter-locking PAC</td>
</tr>
<tr>
<td>Level_2_HMI</td>
<td>Cell/Area Zone</td>
<td>LEVEL_2_HMI must have access to all the devices in Level_0 and Level_1</td>
</tr>
</tbody>
</table>
Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

Profiling Policies in Cisco ISE

Profiling policies in Cisco ISE are used to profile IACS assets. This section shows how to create different profiling policies based on Table 59. The profiling policies shown here are meant as an example and should not be considered a method for the actual deployment.

Level_1_controller Policy

This policy is used to profile an IACS asset which is a controller. The key attributes used to profile this device are shown in Figure 140. As shown in Figure 140, the IOTASSET dictionary is used to match different conditions like protocol, assetVendor, and assetDeviceType. The values for the attributes assetVendor and assetDeviceType are obtained by ISE via the integration to IND. When a new IACS asset is discovered by IND, it provides the details of the asset to Cisco ISE and this information is used to fill in the attribute values of the IOTASSET dictionary.

Figure 140 Attributes Used to Profile a Controller

When a match is found for each condition, the certainty of the device matching the profile increases. If a profiling policy matches all three conditions, then the certainty factor goes higher. There is an option to specify the minimum certainty factor. For example, in Figure 140, if each condition match gives a certainty factor of 10, then if all three conditions match the certainty factor becomes 30. The profiling policy for the previous example can be made stringent by only allowing a device to be profiled if it gets certainty factor of 30 or it can be made very lenient by classifying it as Level_1_Controller if it matches at least one of the conditions. In this CVD, the stringent choice was made when classifying a controller. Figure 141 shows the Level_1_controller policy defined in Cisco ISE.

### Table 59 Creation of Device Access Profile Groups (continued)

<table>
<thead>
<tr>
<th>Device</th>
<th>Location in Plant-wide Network</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level_1_Controller</td>
<td>Cell/Area Zone</td>
<td>Access restricted to a particular Cell/Area Zone</td>
</tr>
<tr>
<td>Level_0_IO</td>
<td>Cell/Area Zone</td>
<td>Access restricted to a particular Cell/Area Zone</td>
</tr>
<tr>
<td>Level_0_Robot</td>
<td>Cell/Area Zone</td>
<td>Access restricted to a particular Cell/Area Zone</td>
</tr>
<tr>
<td>Level_0_Drive</td>
<td>Cell/Area Zone</td>
<td>Access restricted to a particular Cell/Area Zone</td>
</tr>
<tr>
<td>Level_0_Generic</td>
<td>Cell/Area Zone</td>
<td>Access restricted to a particular Cell/Area Zone</td>
</tr>
<tr>
<td>LOCAL_PARTNER</td>
<td>Cell/Area Zone</td>
<td>Access restricted to a particular Cell/Area Zone</td>
</tr>
<tr>
<td>REMOTE_ACCESS</td>
<td>Cell/Area Zone</td>
<td>Access to a remote desktop server</td>
</tr>
<tr>
<td>REMOTE_DESKTOP</td>
<td>Level 3 site operations</td>
<td>Access to a device with SGT value = REMOTE_ACCESS</td>
</tr>
<tr>
<td>Production user (PROD_USER)</td>
<td>Level 3 site operations</td>
<td>Access to all devices in the plant-wide architecture</td>
</tr>
<tr>
<td>Operator Workstation (OWS)</td>
<td>Level 3 site operations</td>
<td>Access to all devices in the plant-wide architecture</td>
</tr>
</tbody>
</table>

When a match is found for each condition, the certainty of the device matching the profile increases. If a profiling policy matches all three conditions, then the certainty factor goes higher. There is an option to specify the minimum certainty factor. For example, in Figure 140, if each condition match gives a certainty factor of 10, then if all three conditions match the certainty factor becomes 30. The profiling policy for the previous example can be made stringent by only allowing a device to be profiled if it gets certainty factor of 30 or it can be made very lenient by classifying it as Level_1_Controller if it matches at least one of the conditions. In this CVD, the stringent choice was made when classifying a controller. Figure 141 shows the Level_1_controller policy defined in Cisco ISE.
Figure 141 Level_1_controller_policy in Cisco ISE

The Level_0_IO_policy is used to profile I/O assets, which usually have a role which is very local to the Cell/Area Zone and will rarely have access outside the Cell/Area Zone. Figure 142 shows the high level idea for Level_0_IO_policy and Figure 143 shows the profiling policy used to profile I/O IACS assets.

Figure 142 High Level Attributes for Level_0_policy
Configuring the Infrastructure

Figure 143  Level_0_IO_policy

Custom Attributes

Cisco ISE uses attributes defined in a dictionary to restrict access to IACS assets and other devices. In Figure 141 and Figure 143, IOTASSET dictionary was used to match attributes that were meant to match IACS assets. In addition, Cisco ISE allows a user to create custom attributes that a user can specify. A combination of pre-defined attributes provided by Cisco ISE along with user attributes allows an IT security architect to create more granular policies. In this CVD, two custom attributes—assetGroup and assetTag—were used to create more granular policies. These attributes were sent from IND to Cisco ISE using the pxGrid API in addition to the normal attributes. Configuring security tags shows how an OT control system engineer can use IND to define security tags; this tag information is seen in Cisco ISE as assetTag. Figure 144 shows how to define custom attributes in Cisco ISE at (ISE admin web)→ Administrator→Identity Management→Settings.

Figure 144  Enabling Custom Attributes in Cisco ISE

Figure 145 shows how to define the custom attributes by going to (ISE admin web)→ Administration→Identity Management→Endpoint Custom Attributes.
Level_3_policy

Level_3_policy is used to profile IACS assets that need to access IACS assets across the Cell/Area Zones. For example, a Level_1_Controller in a Cell/Area Zone may need to access another Level_1_Controller in another Cell/Area Zone. This access may not be needed for all the Level_1 Controllers, but only for a few of them. Cisco ISE profiles a device as a Level_1_Controller based on the device attributes defined in the IOTASSET dictionary. There is a need for an additional attribute along with the normal attributes to classify a Level_1_Controller as Level_3. Custom attributes that were discussed in the previous section could be used in conjunction with the device attributes to classify as Level_3. Figure 146 shows the general idea of classifying the device as Level_3.

Remote_Access

This profiling access policy is used to classify IACS assets that are given access by a remote user to access the device. For example, an IACS asset in Cell/Area Zone currently classified as a Level_1_Controller needs to be accessed by the remote desktop server in the Industrial Zone. The current policy is that no IACS asset can be accessed by the remote desktop server unless the IACS asset is classified as Remote_Access. To change a Scalable Group Tag for an IACS asset, a Change of Authorization (CoA) must occur. IND allows a control system engineer to express operational intent by changing the assetGroup of the IACS asset. Then Cisco ISE would re-profile the IACS asset, issue CoA to the IACS asset, and push a new Scalable Group Tag to the IACS asset. In this CPwE Network Security CVD DIG, assetGroup = 'Remote' was defined in IND as a group where IACS assets that need Remote_Access are placed by the OT control system engineer. Figure 147 illustrates the profiling policy used to match Remote_Access.
Configuring the Infrastructure

Note: When a new SGT is assigned to an IACS asset, there is a loss of connectivity for a few seconds, during which time no application is able to access the IACS asset.

**Figure 147 Profiling Access Policy for Remote Access**

In this CVD, only the custom attribute assetGroup was used to classify the device. As this policy is meant for all IACS assets, only the assetGroup was used to profile the device. The IT security architect can add additional matching conditions, for example, assetDeviceType="Controller" and assetGroup = "Remote".

**Configuring TrustSec in Cisco ISE**

This section provides configuration details for different components that need to be configured on Cisco ISE to support TrustSec in IES and the Cisco Catalyst 3850.

- Adding IES to Cisco ISE
- Adding Scalable Group Tags
- SXP configuration

**Adding IES to Cisco ISE**

For Cisco ISE to assign Scalable Group Tags to IACS assets, IES details such as IP address and radius pre-shared secret key must be configured on Cisco ISE. Navigate to **(ISE admin web)–>Administration–>Network Devices** to configure the IES details. **Figure 148** shows the information needed to establish successful radius configuration between an IES and Cisco ISE.

**Figure 148 IES Radius Configuration**

**CTS Configuration on Cisco ISE**

In the same frame as show in **Figure 148**, the CTS configuration for IES must be configured, as shown in **Figure 149**.
Configuring SXP in Cisco ISE

This section describes on how to enable SXP in Cisco ISE and configure SXP peers in Cisco ISE.

Enabling SXP Service in Cisco ISE

SXP service is enabled in Cisco ISE by going to (ISE admin web)→Administration→Deployment.
Configuring SXP Peers

The IES are configured as Speakers and Cisco ISE is enabled as a Listener. To configure SXP peer, the source and the destination IP addresses must match at the IES and the Cisco ISE. In Cisco ISE, a default configuration template can be used to fill in the rest of the parameters such as password. The location for configuring SXP can be found by going to (ISE admin web)→Work Centers→SXP.
Configuring the Infrastructure

Figure 151 Configuring SXP Peers in Cisco ISE

![Image of Configuring SXP Peers in Cisco ISE]

Configuring SXP Default Parameters

The default parameters can be configured at (ISE admin web)→Work Centers→TrustSec→Settings.

Figure 152 Configuring SXP Default Parameters

![Image of Configuring SXP Default Parameters]
Configuring SGT Components

IACS assets need to be grouped based on the device function such as controller, IO, HMI, and so on. Each device when it is profiled, authenticated, and authorized has a SGT assigned to the device as an end result. The SGT assignment is done by Cisco ISE and the list of SGTs need to be defined by the IT security architect in Cisco ISE. In this CVD, a few device profiles were tested to illustrate how SGT design could be done in a deployment. Creation of User Groups, page 237 gives an overview on the user groups in an Industrial Automation network architecture. Figure 153 shows an example of SGT assignment in Cisco ISE, which is located at (ISE admin web)—>Work Centers—>TrustSec—>Components.

Figure 153 Configuring SGT Components in Cisco ISE

Configuring TrustSec Access Policy Matrix

This section describes how to design a policy matrix for Cisco ISE. Based on the example illustrated in Table 59, the following are policy matrix rules:

- IACS assets or any other devices that are assigned with the SGT group of Level_3 are allowed to access all the devices in the plant-wide network.
- IACS assets with SGT value of Level_1_Controller are allowed to access only the devices in the same Cell/Area Zone.
- IACS assets with SGT value of Level_0_Controller are allowed to access only the devices in the same Cell/Area Zone.
- IACS assets with Remote_Access are allowed to communicate with another device assigned with SGT value of Remote_Desktop and Level_3 (because Level_3 has access to all the devices).

Figure 154 shows the TrustSec Access Policy Matrix.
As shown in Figure 154, Level_3 Controller is allowed to communicate with all the IACS assets, however Level_1_Controller and Level_0_IO can only communicate if they are present in the same Cell/Area Zone. After defining the TrustSec Policy in the ISE, it is downloaded to all IES and the distribution switch (Cisco Catalyst 3850) by selecting the “Deploy” option, as shown in Figure 154. The TrustSec policy matrix can become larger and it may be difficult to view the entire policy on a single screen. To prevent that problem, an option exists to filter the view that will display the matrix that has desired SGTs only. The Show box on top of the screen will enable that functionality and requires the user to create a custom view.

Authentication Policy

802.1X authentication policy involves three parties:

- The supplicant—A client device that wishes to attach to the network.
- The authenticator—A networking device that accepts authentication requests from the client and sends them to the RADIUS authentication server.
- The authentication server—One that validates a client’s identity and sends back the success or failure RADIUS message.

In this CVD, the supplicant is the IACS asset, the authenticator is the IES, and the authentication server is ISE.

Authentication policies are used to define the protocols used by Cisco ISE to communicate with the IACS assets and the identity sources to be used for authentication. Cisco ISE evaluates the conditions and, based on whether the result is true or false, applies the configured result. The authentication protocol tested in this CVD is called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device to determine what kind of network access to provide. This protocol is used to authenticate end devices that do not support any supplicant software in them, such as 802.1X EAP-TLS, EAP-FAST, and so on. For more information about MAB, see: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html
The authentication policy used in the Cisco ISE for this CVD checks the protocol and the Identity Store as Internal Endpoints. To configure the authentication policy, navigate to (ISE admin web)—>Policy—>Policy Sets—>Default as shown in Figure 155, and select the arrow on the right to configure the authentication policy, as shown in Figure 156.

Note: In the example shown in Figure 156, the default authentication policy set was used. In case the real deployment has a different authentication policy set, then the IT Security Architect must select the correct authentication policy set.

Figure 155 Navigation to Configure Authentication/Authorization Policy

Figure 156 ISE Authentication Policy

Authorization Policies

Authorization policies are critical to determine what the user is allowed to access within the network. Authorization policies are composed of authorization rules and can contain conditional requirements that combine one or more identity groups. The permissions granted to the user are defined in authorization profiles, which act as containers for specific permissions.

Authorization profiles group the specific permissions granted to a user or a device and can include attributes such as an associated VLAN, ACL, or a SGT. This CVD uses SGT to grant permissions to an IACS asset. Configuring TrustSec Access Policy Matrix, page 246 describes how the Policy Matrix was designed in the CVD. When an IACS asset is authenticated and as part of the authorization policy, an appropriate SGT is assigned to the IACS asset. The TrustSec Policy Matrix determines the permissions associated with each IACS asset. Figure 157 shows the high-level steps when an IACS asset is connected to the network. To configure the authorization policy navigate to (ISE admin web)—>Policy—>Policy Sets—>Default and then select Authorization Policy.
The default policy can be designed based on how stringent the requirement is. One option is to assign a default SGT like LEVEL_GENERIC and classify devices that do not meet any of the authorization policy conditions. Or there could be a stringent design where, if an IACS asset is not being profiled by any of the existing conditions, then deny access to the network for that IACS asset. Figure 158 shows the authorization table for this CVD.
Configuring the Infrastructure

Configuring IES

This section provides the configuration details for the IES in the Industrial Automation network architecture described in this CVD. The configuration of key features deployed in the IES, such as TrustSec, NetFlow, and Radius server, are described below.

Configuring RADIUS AAA

Each IES must be configured to communicate with the Cisco ISE AAA server for authorizing IoT devices, users, and other systems. The AAA server shown in this configuration is pointing to the PSN node. The following configurations are performed via the command line interface (CLI) of the device.

1. Enter configuration mode. At the global level specify the interface that has the IP address configured in Cisco ISE that will be used to source authentication requests. Enable AAA.

```
aaa new-model
!
!
aaa group server radius ISE
  server name ISE
  
  aaa authentication login no-auth none
  aaa authentication dot1x default group ISE
  aaa authorization network cts-list group ISE
  aaa authorization auth-proxy default group ISE
  aaa accounting dot1x default start-stop group ISE
  aaa session-id common
```

2. Configure Change of Authorization (CoA):

```
aaa server radius dynamic-author
  client <PSN_IP_ADDRESS> server-key 7 <SHARED_KEY>
  
  Note: This configuration done on the IES device must match the configuration done on Cisco ISE. Refer to Figure 148.
```

3. Configure the radius server for TrustSec. In this CVD, the name for the list is cts_list and this name should be tied to the `aaa authorization network` command shown in Step 1:

```
cts authorization list cts-list
```

4. Configure the following RADIUS server attributes:

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
```

5. Configure the RADIUS server, IP address, and shared secret that was entered in Cisco ISE:

```
radius server ISE
  address ipv4 <PSN_IP_ADDRESS> auth-port 1812 acct-port 1813 pac key 7 <PAC_KEY>
  
  Note: This configuration done on the IES device must match the configuration done on Cisco ISE. Refer to Figure 149.
```

6. Configure the AAA group name for RADIUS and specify the server created in step 5:

```
aaa group server radius ISE
  server name ISE
```

7. Globally enable port-based authentication:
Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

```
dot1x system-auth-control
```

Configuring Port-based Authentication

On the IES, the following configurations enable port-based authentication. Configure each interface that will have an endpoint device connected. For MAB and Dot1x methods to co-exist and function as expected, the order and priority must be properly specified as referenced in this application note Configuring MAB: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html

Add the following configuration to the interfaces where the IACS assets could be attached. In this CVD, authentication open was applied to the port to ensure that the device remains connected even if for some reason the port is unable to authenticate to the RADIUS server. The default behavior of the port-based authentication is to block access to the network. By enabling authentication open, the port is not shut down and the IACS asset is able to communicate in the network by using the IP address assigned to it.

```
interface GigabitEthernet1/10
description Connected to a Controller
switchport access vlan 101
switchport mode access
ip flow monitor StealthWatch_Monitor input
load-interval 30
authentication event fail action next-method
authentication host-mode multi-auth
authentication open
authentication order mab dot1x
authentication priority mab dot1x
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication mab
snmp trap mac-notification change added
snmp trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast edge
```

Configuring SDM Templates on IES

SDM templates will allow an OT control system engineer to prioritize resources for different features enabled on an IES. In this CVD, the routing template is required to support SGT assignment on IES. To enable SDM mode to be “routing”, the following steps must be completed:

```
sdm prefer routing
```

After entering the command, the IES must be rebooted.

Configuring CTS Credentials on the IES

Specify the Cisco TrustSec device ID and password for the switch to use when authenticating with Cisco ISE and establishing the PAC file. This password and ID must match the Cisco ISE Network Devices configuration specified earlier in Figure 149.

```
switch# cts credentials id {switch ID} password {password}
```
Configuring SXP Tunnel on an IES

The SXP tunnel between Cisco ISE and an IES must be established because the SGT binding information (SGT value –IP address) should be sent to Cisco ISE, which would push this information to the enforcement point (Cisco Catalyst 3850). The following is the configuration of the SXP tunnel on the IES:

```
ccts sxp enable
cts sxp default password 7 03070A180500701E1D
cts sxp connection peer 10.13.48.184 source 10.17.10.233 password default mode local speaker hold-time 0
```

Configuring NetFlow on IES

Enabling NetFlow on an IES has three components: a Flow Record, a Flow Exporter, and a Flow Monitor. After all three components (explained below) have been configured, the Flow Monitor is applied to a physical interface.

Flow Record

A Flow Record defines the information that will be gathered by the NetFlow process, such as packets in the flow and the types of counters gathered per flow. Custom flow records specify a series of match and collect commands that tell the Cisco device which fields to include in the outgoing NetFlow record.

The match fields are the key fields, meaning that they are used to determine the uniqueness of the flow. The collect fields are extra information that is included in the record in order to provide more detail to the collector for reporting and analysis. When a Flow Record is defined, all of the flow data traffic that enters (ingress) or leaves (egress) the device is captured.

In configuration mode, create ingress or egress flow records using the appropriate interface direction commands. In this CVD, traffic was captured on the ingress interface of the IES to capture the traffic generated by the IACS assets.

This configuration includes required as well as optional flow record fields needed by Stealthwatch.

1. Create Ingress Record, which in this CVD is called a StealthWatch_Record:

```
flow record StealthWatch_Record
description NetFlow record format to send to StealthWatch
match datalink mac source address input
match datalink mac destination address input
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect transport tcp flags
collect interface input
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

Note: When the IES Device Manager was used to configure NetFlow on the ports by using the Stealthwatch template, then the command `collect counter packets long` was not applied to the IES device, and without this command, the Stealthwatch management console was not able to detect any flows coming from the IES device. To mitigate this behavior, the command `collect counter packets long` must be applied using CLI. If the IES CLI is used to configure NetFlow on the IES device, then the above mentioned configuration will work. This problem happens only when the Device Manager was used to configure NetFlow on the IES device.
Flow Exporter

The Flow Exporter defines where and how to send the NetFlow (Flow Records). In actuality, a Flow Exporter defines a flow collector IP address and port as the destination and in this case, the Stealthwatch Flow Collector is the destination.

```
floow exporter StealthWatch_Exporter
    description StealthWatch Flow Exporter
    destination 10.13.48.183
    source Vlan101
    output-features
      transport udp 2055
      option application-table
```

Flow Monitor

A Flow Monitor describes the NetFlow cache or information stored in the cache. Additionally, the Flow Monitor links together the Flow Record and the Flow Exporter. The Flow Monitor includes various cache characteristics such as the timers for exporting, the size of the cache, and, if required, the packet sampling rate (Sampled NetFlow/sFlow). As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the StealthWatch Flow Collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets received for the flow) or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download and standard CIP I/O connections). There are timers to determine if a flow is inactive or if a flow is long lived. The times used in CVD are 30 seconds for inactive time out and 60 seconds for active time out.

2. Create the Ingress flow monitor using the record and exporter created previously:

```
floow monitor StealthWatch_Monitor
    description StealthWatch Flow Monitor
    exporter StealthWatch_Exporter
    cache timeout active 60
    cache timeout update 5
    record StealthWatch_Record
```

3. Once the flow monitor has been created, it can be applied to all the access interfaces in an IES. Apply the flow monitor to an appropriate interface and the appropriate ingress/egress using input/output:

```
interface GigabitEthernet1/10
    description Connected to a Controller
    switchport access vlan 101
    switchport mode access
    ip flow monitor StealthWatch_Monitor input
    load-interval 30
    authentication event fail action next-method
    authentication host-mode multi-auth
    authentication open
```

Note: The IP flow monitor policy can be applied both in ingress and egress directions.
Configuring the Infrastructure

Configuring Distribution Switch—Cisco Catalyst 3850

As described in Cell/Area Zone Segmentation, page 89, the enforcement is moved to the distribution switch, no enforcement occurs in the Cell/Area Zone, and the East-West traffic flow, as explained in IACS Traffic Flows in a Network, page 87, is enforced at the distribution switch. This section describes the steps that need to be configured on the distribution switch to enable enforcement:

Configuring Radius Server

This is very similar to the configuration of IES, so refer to Configuring RADIUS AAA, page 250.

Configuring TrustSec

The configuration of TrustSec has the following components:

- Configuring cts
- Configuring sxp
- Configuring IPDT
- Configuring enforcement

Configuring cts

The cts configuration is similar to the IES, so refer to Configuring CTS Credentials on the IES, page 251.

Configuring sxp

SXP configuration on the distribution switch is similar to the IES, so refer to Configuring SXP Tunnel on an IES, page 252.

Configuring IPDT

There is a change in the way Cisco Catalyst 3850 platforms are configured with device-tracking compared to the IES. In the Cisco Catalyst 3850, the device-tracking feature must be enabled, a device-tracking policy must be created, and this policy must be attached to the interface where the IP device-tracking needs to be enabled. In this CVD, IP device-tracking is enabled on interfaces (Port-channel3) that are attached to IES interfaces.

```
device-tracking tracking
!
device-tracking policy IPDT
  no protocol udp
  tracking enable
!
interface Port-channel3
  switchport trunk native vlan 101
  switchport trunk allowed vlan 101,102
  switchport mode trunk
  device-tracking attach-policy IPDT
end
```

P5-3850-stack-4#

Enforcement

In this CVD, policy enforcement is done only on the Cisco Catalyst 3850 switch. To enable policy enforcement, the following commands must be enabled:

```
crts role-based enforcement
```
Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

cts role-based enforcement vlan-list <vlan-id>

Troubleshooting the Infrastructure

This section includes the following major topics:

- TrustSec Troubleshooting Tips on Cisco IE and Allen-Bradley Stratix IES and Cisco Catalyst 3850 Switches
- Cisco NetFlow Troubleshooting Tips
- NMT Troubleshooting Tips
- Cisco ISE Troubleshooting Tips

TrustSec Troubleshooting Tips on Cisco IE and Allen-Bradley Stratix IES and Cisco Catalyst 3850 Switches

The following section describes certain show commands that can be executed to view potential sources of problems related to Cisco TrustSec.

Note: An IT engineer should have some expertise in TrustSec in order to troubleshoot any problems that are discovered. For complete information on Cisco TrustSec troubleshooting tips, refer to the following URL: https://community.cisco.com/t5/security-documents/trustsec-troubleshooting-guide/ta-p/3647576

IES is Unable to Register with Cisco ISE and Download the SGT Table Information

Verify whether the IES and Cisco ISE have the Right TrustSec Credentials Matched

This is the first step and it is possible that the IT security administrator might have a typo in the password or the ID information in the IES or the Cisco ISE. The credentials may be missing on the IES. Issue the following command:

IE4K-25#show cts credentials
CTS password is defined in keystore, device-id = IE4K-25

Verify Whether the PAC Key Between the IES and the Cisco ISE is Configured Correctly

The PAC key must match between the Cisco ISE and the IES. If there is a mismatch in the IES, then re-configure the key, which will force a new PAC provisioning in the IES. To verify that the PAC is installed:

IE4K-25#show cts pacs
AID: BA6A666C6C10E7045A4CCD0DA18E706
PAC-Info:
PAC-type = Cisco Trustsec
AID: BA6A666C6C10E7045A4CCD0DA18E706
I-ID: IE4K-25
A-ID-Info: Identity Services Engine
Credential Lifetime: 12:45:25 EST Nov 10 2018
PAC-Opaque:
00020000010000040000030001000A91A603CS3109269B2EACF49C
2D0E1D700000135B868AB009091A604EB1C0FBC8F5471B62DA12C4BB434A3BE2D7C13B59FA9D3BA8DF17CB798E18B8785
6DCC50C4F5CA6820FE4E7B8270A163FA73897FAFD7010325AEB38CD208D292A1B7BBD2C483D01CA4EE6B8FB9B7AFBF9CA8A
5B2274ECD5BB9C457674376A48865BADF98C43B2FCFC9FA8B8D3FD72FC538B
Refresh timer is set for 8w4d

IE4K-25#

To clear the credentials:

clear cts credentials
clear cts pac
Verify that RADIUS is Operational from the IES

IE4K-25#show aaa servers

RADIUS: id 1, priority 1, host 10.13.48.184, auth-port 1812, acct-port 1813
  State: current UP, duration 2488903s, previous duration 0s
  Dead: total time 0s, count 5968
  Quarantined: No
  Authen: request 2275, timeouts 0, failover 0, retransmission 0
  Response: accept 20, reject 2255, challenge 0
  Response: unexpected 0, server error 0, incorrect 0, time 32ms
  Transaction: success 2275, failure 0
  Throttled: transaction 0, timeout 0, failure 0
  Author: request 2, timeouts 0, failover 0, retransmission 0
  Response: accept 2, reject 0, challenge 0
  Response: unexpected 0, server error 0, incorrect 0, time 50ms
  Transaction: success 2, failure 0
  Throttled: transaction 0, timeout 0, failure 0
  Account: request 38, timeouts 0, failover 0, retransmission 0
  Request: start 18, interim 0, stop 18
  Response: start 18, interim 0, stop 18
  Response: unexpected 0, server error 0, incorrect 0, time 29ms
  Transaction: success 38, failure 0
  Throttled: transaction 0, timeout 0, failure 0
  Elapsed time since counters last cleared: 4w19h26m
  Estimated Outstanding Access Transactions: 0
  Estimated Outstanding Accounting Transactions: 0
  Estimated Throttled Access Transactions: 0
  Estimated Throttled Accounting Transactions: 0
  Maximum Throttled Transactions: access 0, accounting 0
  Requests per minute past 24 hours:
    high - 15 hours, 42 minutes ago: 2
    low - 0 hours, 0 minutes ago: 0
    average: 0

IE4K-25#

Verify that the CTS server-list is Pointing to the Right Policy Server Node

The command to verify the cts server-list is shown below:

IE4K-25#show cts server-list

CTS Server Radius Load Balance = DISABLED
Server Group Deadline = 20 secs (default)
Global Server Liveness Automated Test Deadline = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = DISABLED

Installed list: CTSServerList1-000B, 1 server(s):
  *Server: 10.13.48.184, port 1812, A-ID 75FD68DL30DA33A44480ED005C93FF49
    Status = ALIVE
    auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadline = 20 secs

IE4K-25#

Verify that the IES has Downloaded the Right SGT Table Information

IE4K-25#show cts environment-data

CTS Environment Data
----------------------
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
  *Server: 10.13.48.184, port 1812, A-ID BAA6AD6CB6C1087045A4C00DA18E706
    Status = ALIVE
Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

\[
\text{auto-test} = \text{FALSE}, \text{keywrap-enable} = \text{FALSE}, \text{idle-time} = 60 \text{ mins}, \text{deadtime} = 20 \text{ secs}
\]

Multicast Group SGT Table:

Security Group Name Table:

- 0-fd:Unknown
- 2-fd:TrustSec_Devices
- 3-fd:LEVEL_1_GENERIC
- 4-fd:LEVEL_1_GENERIC_IO
- 5-fd:LEVEL_0_IO
- 6-fd:LEVEL_3
- 7-fd:LEVEL_1_CONTROLLER
- 8-fd:Remote_Access
- 10-fd:Remote_Desktop
- 255-fd:Quarantined_Systems

Environment Data Lifetime = 86400 secs

Last update time = 10:18:52 EDT Sun Sep 9 2018

Env-data expires in 0:01:08:23 (dd:hr:mm:sec)

Env-data refreshes in 0:01:08:23 (dd:hr:mm:sec)

Cache data applied = NONE

State Machine is running

IE4K-25#

IACS Asset is Unable to Authenticate to Cisco ISE

This section describes how to troubleshoot when an IACS device is unable to authenticate to Cisco ISE. To demonstrate the flow the IACS asset 10.17.10.65 is used to show the process.

Verify the Authentication and Authorization State of IACS Assets Attached to an IES

IE4K-34# show authentication brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>AuthC</th>
<th>AuthZ</th>
<th>Fg</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/14</td>
<td>0000.bc3f.d0ef</td>
<td>m:OK</td>
<td>AZ: SA-</td>
<td>409219s</td>
<td></td>
</tr>
<tr>
<td>Gi1/16</td>
<td>0000.bccd.f76a</td>
<td>m:OK</td>
<td>AZ: SA-</td>
<td>409221s</td>
<td></td>
</tr>
<tr>
<td>Gi1/11</td>
<td>0000.bc2d.20ef</td>
<td>m:CF</td>
<td>UZ: SA- FA-</td>
<td>409221s</td>
<td></td>
</tr>
</tbody>
</table>

Session count = 3

Key to Authentication Attributes:

- RN - Running
- ST - Stopped
- OK - Authentication Success
- CF - Credential Failure
- AD - AAA Server Failure
- NR - No Response
- TO - Timeout
- AR - AAA Not Ready

Key to Authorization Attributes:

- AZ - Authorized, UZ - Unauthorized
- SA - Success Attributes, FA - Failed Attributes
- D: - DACL, F: - Filterid / InACL, U: - URL ACL
- V: - Vlan, I: - Inactivity Timer, O: - Open Dir

Key to Session Events Blocked Status Flags:

- A - Applying Policy (multi-line status for details)
- D - Awaiting Deletion
- F - Final Removal in progress
- I - Awaiting IFID ID allocation
- N - Waiting for AAA to come up
Verify that NMT has Discovered the IACS Asset 10.17.10.65
The first step would be to verify if NMT has discovered the IACS device 10.17.10.65.

![Figure 159 NMT Discovering IACS Asset 10.17.10.65](image)

Verify that the pxGrid Service is Enabled at Cisco ISE
To verify that go to (ISE admin web)→Administration→Deployment and select the PSN (ise24 in this CPwE Network Security CVD):
The next step is to verify if Cisco ISE has learned the IACS asset. Figure 161 shows that Cisco ISE has learned about the IACS asset.

Verify that Profiling Policies are Configured Correctly
ISE profiles the IACS assets based on the profiling policy. If conditions in the profiling policy are not configured correctly, then ISE will not be able to profile the IACS asset.
Verify that Authentication and Authorization Policies are Configured Correctly in Cisco ISE
To assign a SGT to an IACS asset, the authentication and authorization policy conditions must match to the IACS device attributes.

Verify that pxGrid Probe is Enabled at PSN
To verify that, go to *(ISE admin web)→Administration→Deployment→ Select the psn* (ise24 in this CVD) and select the tab profiling configuration.

Figure 162 Verifying that pxGrid Probe is Enabled on the PSN

Verify Live Logs at ISE to Understand the Authentication/Authorization Flow
To see live logs, go to *(ISE admin web)→ Operation→ Live Logs* to get a list of devices that went through the authentication/authorization process.
Selecting the Details option will provide details about the complete exchange.

**3850 Distribution Switch is not Enforcing the Policy Correctly**

Different reasons for this problem to happen exist; it can be troubleshooted by going through the following steps:

**Verify that SGT is Assigned to the Port on the IES**

- `IE4K-25#show cts role-based sgt-map all`
- `Active IPv4-SGT Bindings Information`
Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

<table>
<thead>
<tr>
<th>IP Address</th>
<th>SGT</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.13.15.25</td>
<td>4</td>
<td>INTERNAL</td>
</tr>
<tr>
<td>10.20.25.12</td>
<td>11</td>
<td>LOCAL</td>
</tr>
<tr>
<td>10.20.25.25</td>
<td>4</td>
<td>INTERNAL</td>
</tr>
<tr>
<td>10.20.25.221</td>
<td>5</td>
<td>LOCAL</td>
</tr>
<tr>
<td>10.20.26.25</td>
<td>4</td>
<td>INTERNAL</td>
</tr>
<tr>
<td>10.20.50.5</td>
<td>4</td>
<td>INTERNAL</td>
</tr>
<tr>
<td>192.168.4.25</td>
<td>4</td>
<td>INTERNAL</td>
</tr>
</tbody>
</table>

IP-SGT Active Bindings Summary

Total number of LOCAL bindings = 2
Total number of INTERNAL bindings = 5
Total number of active bindings = 7

IE4K-25#

Verify that SXP tunnel is up Between the Cisco ISE and the IES Device

IE4K-25#show cts sxp connections
SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set

Peer IP : 10.13.48.184
Source IP : 10.20.25.25
Conn status : On
Conn version : 4
Conn capability : IPv4-IPv6-Subnet
Conn hold time : 120 seconds
Local mode : SXP Speaker
Connection inst# : 1
TCP conn fd : 1
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 6:01:28:42 (dd:hr:mm:sec)

Total num of SXP Connections = 1

Verify that SXP Tunnel is Up at Cisco ISE to the IES (IE4K-25)

Navigate to (ISE admin web)—> Work Centers—> TrustSec—> SXP Devices and verify the SXP status.
Verify that Cisco ISE has Received the SGT-IP Mapping Information through the SXP Tunnel

Verify that 3850 is Receiving the SGT-IP Information through SXP Tunnel

```
P5-3850-stack-4# show cts sxp sgt-map brief
SXP Node ID (generated): 0xC0A80A0B (192.168.10.11)
IPv4, SGT: <10.13.15.25, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.10.65, 5:LEVEL_1_CONTROLLER>
IPv4, SGT: <10.17.10.108, 6:LEVEL_0_IO>
IPv4, SGT: <10.17.10.217, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.10.218, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.10.219, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.10.220, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.20.217, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.20.218, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.17.20.219, 4:TrustSec_Device_SGT>
```
IPv4, SGT: <10.17.20.220, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.20.10.5, 4:TrustSec_Device_SGT>
IPv4, SGT: <10.20.25.10, 11:LEVEL_1_GENERIC>

Verify that Policy Matrix is Downloaded to the 3850 Distribution Switch

PS-3850-stack-4#show cts role-based permissions
IPv4 Role-based permissions from group 5:LEVEL_1_CONTROLLER to group 5:LEVEL_1_CONTROLLER:
   Deny IP-00
IPv4 Role-based permissions from group 6:LEVEL_0_IO to group 5:LEVEL_1_CONTROLLER:
   Deny IP-00
IPv4 Role-based permissions from group 8:LEVEL_3 to group 5:LEVEL_1_CONTROLLER:
   Permit IP-00
IPv4 Role-based permissions from group 9:Remote_Access to group 5:LEVEL_1_CONTROLLER:
   Deny IP-00
IPv4 Role-based permissions from group 10:Remote_Desktop to group 5:LEVEL_1_CONTROLLER:
   Deny IP-00
IPv4 Role-based permissions from group 5:LEVEL_1_CONTROLLER to group 6:LEVEL_0_IO:
   Deny IP-00
IPv4 Role-based permissions from group 6:LEVEL_0_IO to group 6:LEVEL_0_IO:
   Deny IP-00
IPv4 Role-based permissions from group 8:LEVEL_3 to group 6:LEVEL_0_IO:
   Permit IP-00
IPv4 Role-based permissions from group 9:Remote_Access to group 6:LEVEL_0_IO:
   Deny IP-00
IPv4 Role-based permissions from group 10:Remote_Desktop to group 6:LEVEL_0_IO:
   Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Cisco NetFlow Troubleshooting Tips

This section discusses some useful show commands for troubleshooting if NetFlow records are not showing up at the Stealthwatch management console.

Show Commands at the IES/3850 Distribution Switch

This section describes the various show commands that can be issued to troubleshoot the problem in a methodical fashion.

Verify that the NetFlow Record is Collecting the Right Parameters

IE4K-25#show flow record
flow record StealthWatch_Record:
   Description: NetFlow record format to send to StealthWatch
   No. of users: 1
   Total field space: 59 bytes
   Fields:
       match datalink mac source address input
       match datalink mac destination address input
       match ipv4 tos
       match ipv4 protocol
       match ipv4 source address
       match ipv4 destination address
       match transport source-port
       match transport destination-port
       collect transport top flags
       collect interface input
       collect interface output
       collect counter bytes long
       collect counter packets long
       collect timestamp sysuptime first
       collect timestamp sysuptime last

IE4K-25#
Verify that the Exporter is Configured with the Right IP Address

IE4K-25#show flow exporter
Flow Exporter StealthWatch_Exporter:
  Description: StealthWatch Flow Exporter
  Export protocol: NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.13.48.183
    Source IP address: 10.20.50.5
    Transport Protocol: UDP
    Destination Port: 2055
    Source Port: 52254
    DSCP: 0x0
    TTL: 255
  Output Features: Used
  Options Configuration:
    application-table (timeout 600 seconds)

Verify that the Flow Monitor is Configured Correctly

IE4K-25#show flow exporter
Flow Exporter StealthWatch_Exporter:
  Description: StealthWatch Flow Exporter
  Export protocol: NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.13.48.183
    Source IP address: 10.20.50.5
    Transport Protocol: UDP
    Destination Port: 2055
    Source Port: 52254
    DSCP: 0x0
    TTL: 255
  Output Features: Used
  Options Configuration:
    application-table (timeout 600 seconds)

Verify that the Flow Monitor is Applied to an Appropriate Interface

IE4K-25#show flow interface gigabitEthernet 1/10
Interface GigabitEthernet1/10
  FNF: monitor: StealthWatch_Monitor
  direction: Input
  traffic(ip): on

Verify that the Flow Information is Cached on the IES/3850 Switch

P5-3850-stack-4#show flow monitor name StealthWatch_Monitor cache
  Cache type: Normal (Platform cache)
  Cache size: Unknown
  Current entries: 3

  Flows added: 412595
  Flows aged: 412592
    - Active timeout ( 60 secs) 184742
    - Inactive timeout ( 15 secs) 227850

  DATALINK MAC SOURCE ADDRESS INPUT: E865.49DF.7E41
  DATALINK MAC DESTINATION ADDRESS INPUT: 0100.5E00.000A
  IPV4 SOURCE ADDRESS: 10.255.255.51
  IPV4 DESTINATION ADDRESS: 224.0.0.10
  TRNS SOURCE PORT: 0
  TRNS DESTINATION PORT: 0
  IP TOS: 0xC0
  IP PROTOCOL: 88
  tcp flags: 0x00
Configuring the Infrastructure

interface output: Null
counter bytes long: 480
counter packets long: 8

Command to clear the flow data

clear flow record StealthWatch-Record-IN
clear flow monitor StealthWatch-Monitor-IN statistics clear flow monitor StealthWatch-Monitor-IN
cache clear flow exporter StealthWatch-Exporter statistics

NMT Troubleshooting Tips

The configuration details for NMT can be found at:


A troubleshooting feature of NMT is to collect log information, which can help an IT security architect isolate a problem. Figure 167 shows how to collect logs for pxGrid in NMT.

Figure 167 Creating a Log File in NMT

After enabling the log files, to download logs select the “?” option in the top right corner as shown in Figure 167.

Cisco ISE Troubleshooting Tips

The following section provides high level troubleshooting information to assist in identifying and resolving problems you may encounter when you use the Cisco Identity Services Engine (ISE).

Note: For complete information on Cisco ISE monitoring and troubleshooting tips, refer to the following URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_011001.html
Checking the Status of pxGrid

On the PSN, execute the following command to check the status of the pxGrid:

```bash
ise24/admin# show application status ise | include pxGrid
pxGrid Infrastructure Service          running          5736
pxGrid Publisher Subscriber Service    running          5880
pxGrid Connection Manager              running          5851
pxGrid Controller                      running          5902
ise24/admin#
```

Verify pxGrid Certificate in ISE PSN

From (ISE admin Web), navigate to Administration—>System—>Certificates—>System Certificates and expand on PSN (ise24 in this CPwE Network Security CVD) to verify that system certificate is used for pxGrid.

**Figure 168  Verifying pxGrid Certificate in ISE PSN**

Verify the NMT pxGrid Status in ISE

From (ISE admin Web), navigate to Administration—>pxGrid Services and verify that NMT is registered as client.
Enable DEBUG on Profiler and pxGrid

In certain situations, it may be desired to enable debug on ISE and verify the exchange of information between the NMT and ISE via pxGrid. This section describes how to enable the debug.

1. From (ISE admin web), navigate to Administration—>System—>Logging—>Debug Log Configuration.

2. Select the PSN on the right panel (ise24 in this CPwE Network Security CVD DIG).

3. Select profiler and change the logging levels to DEBUG and click Save.

4. Select pxgrid and change the logging levels to TRACE and click Save.

To verify the log information, navigate to PSN (ise24) and issue the following command:

```
ise24/admin# show logging application profiler.log | include IND
```

```
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: Looking for new publishers ...
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: New services are: []
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: NODENAME:ind-win10
2018-10-23 12:27:22,519 INFO [ProfilerINDSubscriberPoller-84-thread-1]
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: REQUEST BODY{"offset":"0","limit":"500"} 
2018-10-23 12:27:22,520 INFO [ProfilerINDSubscriberPoller-84-thread-1]
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: Response status={200
2018-10-23 12:27:22,520 INFO [ProfilerINDSubscriberPoller-84-thread-1]
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: Content: "OUT_OF_SYNC"
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: Status is :"OUT_OF_SYNC"
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: NODENAME:ind-win10
2018-10-23 12:27:22,602 INFO [ProfilerINDSubscriberPoller-84-thread-1]
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: REQUEST BODY{"offset":"0","limit":"500"} 
2018-10-23 12:27:22,602 INFO [ProfilerINDSubscriberPoller-84-thread-1]
cisco.profiler.infrastructure.probemgr.INDSubscriber ::::: Response status={200
```
Implementing Site-wide Precision Time Protocol

This section describes the implementation of site-wide Precision Time Protocol (PTP) for Industrial Automation environments.

There are three deployment options based on customer precision requirements:

- High Precision site-wide time distribution using a dedicated grandmaster clock

  The plantwide high precision grandmaster clock time distribution architecture provides a plantwide, highly accurate time feed forward tree to facilitate inter-cell loop or plantwide motion drive cooperation. It normally requires high accuracy oscillators to synchronize with a GNSS source.

  Grandmaster clock source redundancy, transport network device box-level redundancy (for example stack-wise, HSRP over industrial zone), Cell/Area Zone resilient network topology, etc., all provide redundant PTP message source and transport path. This highly resilient network design reduces the possibility that any network element will lose its clock source. If, in a very extreme case, the clock source become unavailable, a multi-level boundary clock will enter into a "HOLDOVER" state to assume the master clock role for its lower stratum clock element to maintain normal industrial operations.

  Figure 170 shows the plantwide high precision grandmaster clock architecture.
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Figure 170 Plantwide High Precision GPS Backed PTPv2 Architecture

Where:

- Meinberg LANTIME M600 provides redundant plant-wide grandmaster clocks.
- Cisco Catalyst 9300 core switch is configured as Boundary Clock (BC) over industrial zone.
- Cisco IE 5000 pair switches are configured as BC over distribution layer.
- Cisco IE 4000 pair switches are configured as BC on the top of each ring or start to dual-home to distribution switch pairs.
- Cisco IE 4000 is configured as end-to-end Transparent Clock (TC) inside ring.
- Cisco IE 3000 is configured as end-to-end TC inside ring.
- Cisco IE 3400 is configured as end-to-end TC inside ring.
- Customer PLC controller IP module is configured as Ordinary Clock (OC) to recover clock.
- Underlying resilience protocols vary with MSTP, REP, etc. deployed transport protocols.
- Industrial Ethernet Switch is enabled with PTP-aware QoS for classifying and policing PTP messages.

Note: The Cisco Catalyst 9300 will support PTPv2 over VSS stacking in the future. Cisco IE 5000 stack-wise does not currently support PTP. In the topology in Figure 170, Cisco IE 5000 pairs are configured with HSRP over a Layer 2 trunk link.
Site-wide time distribution using Cisco IE 5000 as grandmaster

Intermediate precision with distributed grandmaster clock design uses Cisco IE 5000 switch to directly connect to a GNSS source over industrial zone distribution switch. This design is targeted for general industrial operation where motion-related operation is not the main consideration when designing time synchronization distribution architecture.

Intermediate precision with distributed grandmaster clock design inherits most of the high precision time distribution design by only removing the high precision dedicate grandmaster clock source located on the core network. The Cisco IE 5000 can either connect to a GNSS source or use the Cisco proprietary NTP-to-PTP (Flywheel) feature to assume the grandmaster clock role. It is not recommended to use an external internet NTP server if NTP-to-PTP grandmaster is a consideration in the PTP network design.

Figure 171 shows the intermediate precision plantwide grandmaster clock architecture.

Figure 171 Plantwide Intermediate Precision GPS Backed PTPv2 Architecture

Where:
- Cisco IE 5000 pair switches connect to GNSS providing redundant plant-wide grandmaster clock.
- Cisco IE 4000 pair switches are configured as Boundary Clock (BC) on the top of each ring or start to dual-home to distribution switch pairs.
- Cisco IE 4000 is configured as end-to-end Transparent Clock (TC) inside ring.
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

- Cisco IE 3000 is configured as end-to-end TC inside ring.
- Cisco IE 3400 is configured as end-to-end TC inside ring.
- Customer PLC controller IP module is configured as Ordinary Clock (OC) to recover clock.
- Underlying resilience protocols vary with MSTP, REP, etc.
- Industrial Ethernet Switch is enabled with PTP-aware QoS for classifying and policing PTP messages.

Note: The Cisco Catalyst 9300 will support PTPv2 over VSS stacking in the future. Cisco IE 5000 stack-wise does not currently support PTP. In the topology in Figure 171, Cisco IE 5000 pairs are configured with HSRP over a Layer 2 trunk link.

The Cisco IE 5000 switch incorporated with stratum 3e Oven Controlled Crystal Oscillator (OCXO) can provide superior frequency stability in short term and high accuracy when in holdover state. High-precision Emerald OCXOs offer ±5 to ±8 ppb stability, 1 to 220 MHz frequency. It can be used as a drop-in replacement of legacy quartz OCXOs in emerging 5G and IEEE 1588 synchronization applications while improving overall system performance and robustness.

- Site-wide time distribution using IACS Time Module

Refer to site-wide time distribution using Rockwell Automation PLCs:

- Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture Design Guide
- Scalable Time Distribution within a Converged Plantwide Ethernet Architecture White Paper

The following section provides a detailed configuration and limitation example for a third-party grandmaster clock and Industrial Ethernet switch (IES).

Configuring Meinberg LANTIME M600

Meinberg LANTIME M600 will provision PTP/NTP service from the core network (Purdue model level 3 above) as close as possible to the distribution network (Purdue model level 3) which connects the Cell/Area Zone. This can reduce PTP hop count and possible routing asymmetry. M600 is configure with IPv4/UDP multicast master with End-to-End(E2E) default profile, where UDP port 319/320 pairs will be used for PTP Event messages (for example: E2E default Profile: Sync/Delay_Req) and PTP general messages (Delay_Resp/Follow_UP):


Meinberg LANTIME M600 PTP Timestamping for Grandmaster Clock

M600 consists of three functional blocks: GPS reference time source will integrate with single board PTP computer via internal USB (169 NET) to get timestamping, PTP messages will be advertised via PTP timestamp unit via IP.
M600 PTP Timestamping

PTP messages transport over UDP port 319 and 320 via multicast addresses 224.0.0.107 and 224.0.0.129. This is handled via M600 single onboard computer. PTP messages advertise through manually configured 10 NET via external Fast Ethernet port as shown in Figure 173.
Figure 173 M600 Timestamping

```
root@PTPv2:~ # netstat -nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window Irtt Iface
224.0.0.192 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
169.254.192.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
169.254.100.0 0.0.0.0 255.255.255.0 U 0 0 0 usb0
0.0.0.0 10.255.18.2 0.0.0.0 0 0 0 eth0
root@PTPv2:~ # netstat -aln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
udp 0 0 224.0.0.192:10000 *:*
udp 0 0 224.0.1.129:10001 *:*
udp 0 0 10.255.18.2:10000 *:
udp 0 0 *:5333 *:
udp 0 0 *:5333 *:

root@PTPv2:~ # exit
Connection to 169.254.100.2 closed.

[LOCAL] IA-M600-OM1 ptp2 #
[LOCAL] IA-M600-OM1 ptp2 # netstat -nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window Irtt Iface
0.0.0.0 172.18.133.1 0.0.0.0 0 0 0 lan0
169.254.192.0 0.0.0.0 255.255.255.0 U 0 0 0 tsu100
169.254.100.0 0.0.0.0 255.255.255.0 U 0 0 0 tsu101
172.18.133.0 0.0.0.0 255.255.255.0 U 0 0 0 lan0
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 lan0

[LOCAL] IA-M600-OM1 ptp2 #
[LOCAL] IA-M600-OM1 ptp2 # netstat -aln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
udp 0 0 localhost:16005 *:*
udp 0 0 192.168.133.161:ntp *:
udp 0 0 ia-m600-gml.cisco:ntp *:
udp 0 0 tsu0.ntp *:
udp 0 0 tsu1.ntp *:
udp 0 0 localhost:ntp *:
udp 0 0 *:ntp *:
udp 0 0 *:5333 *:
udp 0 0 localhost:3569 *:
udp 0 0 localhost:ntp *:
udp 0 0 *:ntp *:
udp 0 0 *:5333 *:

[LOCAL] IA-M600-OM1 ptp2 #
```
# M600 PTP User Interface Configuration

**Figure 174 PTP GPS Status**

<table>
<thead>
<tr>
<th>Common Receiver Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Model</td>
</tr>
<tr>
<td>Serial Number</td>
</tr>
<tr>
<td>Software Revision</td>
</tr>
<tr>
<td>Oscillator Type</td>
</tr>
<tr>
<td>Supported Features</td>
</tr>
<tr>
<td>Number of Programmable Pulse Outputs</td>
</tr>
<tr>
<td>Number of Serial Ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Special Receiver Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>GPS Status</td>
</tr>
<tr>
<td>GPS Position LLA</td>
</tr>
<tr>
<td>GPS Position LLA Degree</td>
</tr>
<tr>
<td>GPS Position XYZ</td>
</tr>
<tr>
<td>Number Of Satellites In View</td>
</tr>
<tr>
<td>Number Of Good Satellites</td>
</tr>
<tr>
<td>Selected Satellite Set</td>
</tr>
</tbody>
</table>
Figure 175  PTP Input Source Priority
Figure 176 PTP Parameters—1

Figure 177 PTP Parameters—2
Implementing Site-wide Precision Time Protocol

Configuring Cisco Catalyst 9300

Cisco Catalyst 9300 PTP Configuration Guide:

Restrictions and Limitations for PTP

- The output of show clock on the device and PTP servo clock displayed in `show platform software fed switch active PTP domain 0` are not synchronized to each other. These are two different clocks used on the switch.
- Inter-VLAN is not supported in PTP Transparent Clock Mode.
- PTP is supported only on the first 16 downlink ports and on all the uplink ports of the C9300-48UXM switch model.
- PTP is not supported in stacked systems.
- PTP is not supported on Layer 3 interface (support will be on release 16.12); currently SVI interface will be supported.
- The switch supports IEEE802.1AS and IEEE1588 default profile and they are mutually exclusive. Only one profile can be enabled on the switch at a time.
- We do not recommend having non-PTP enabled devices in the PTP network since it decreases clock synchronization accuracy.
- Management and signaling messages are not supported in Cisco IOS XE Fuji 16.8.1a. These messages are dropped in the switch without being processed.
- Moving from one PTP mode to the other is not recommended. Clear the existing mode using no PTP mode and then configure a new mode.
- IPv6, VRF, EtherChannel interface, and native Layer 3 ports are not supported

Cisco Catalyst 9300 PTP Default Profile Boundary Clock Configuration

The Cisco Catalyst 9300 is deployed on the enterprise core network to facilitate plantwide high precision grandmaster clock delivering time synchronization services across whole plant, where GM1 and backup GM2 are directly connected to a Cisco Catalyst 9300 core switch. The Cisco Catalyst 9300 will be configured in Boundary Clock (BC) mode to recover clock and regenerate clock for downstream PTP devices.
Table 60  Cisco Catalyst 9300 PTP Default Profile Boundary Clock Configuration

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device#configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ptp transport ipv4 udp</td>
<td>Specifies the synchronization transport mode, clock mode, and clock domain:</td>
</tr>
<tr>
<td></td>
<td>ptp mode boundary delay-req</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ptp priority1 &lt;Value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ptp priority2 &lt;Value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp transport ipv4 udp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp mode boundary delay-req</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp priority1 ppp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp priority2 qqq</td>
<td></td>
</tr>
</tbody>
</table>

Specifies the synchronization transport mode, clock mode, and clock domain:

- boundary—Mode to enable the switch to participate in selecting the best master clock. If no better clocks are detected, the switch becomes the grandmaster clock on the network and the parent clock to all connected devices. If the best master is determined to be a clock connected to the switch, the switch synchronizes to that clock as a child to the clock, then acts as a parent clock to devices connected to other ports. After initial synchronization, the switch and the connected devices exchange timing messages to correct time skew caused by clock offsets and network delays. Use this mode when overload or heavy load conditions produce significant delay jitter.

- Once PTP default profile is enabled globally on the device, PTP is enabled on all the interfaces. To disable PTP selectively on individual interfaces, use the no ptp enable command under interface configuration.

- PTP priority1 and priority2

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ptp vlan &lt;Value&gt;</td>
<td>Specify PTP over SVI:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#interface vlan nnn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#ip address m.m.m.m n.n.n.n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#interface GigabitEthernet/x/yz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#switch mode trunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#switch trunk allow vlan nnn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#ptp vlan nnn</td>
<td></td>
</tr>
</tbody>
</table>

Specify PTP over SVI:

- Within the PTP default profile, PTP messages are processed in VLAN 1 by default. Use the ptp vlan vlan-name command under interface configurations to allow PTP message processing on specific VLAN.

You must add this to the VLAN database of the device.

Cisco Catalyst 9300 PTP Default Profile Boundary Clock Configuration Example

```
### PTP Boundary Clock ###
P5-9300-2#show run | sec ptp
ptp transport ipv4 udp
ptp mode boundary delay-req
ptp priority1 10
ptp priority2 11
```
Implementing Site-wide Precision Time Protocol

```
ptp vlan 118
P5-9300-2# P5-9300-2#
P5-9300-2#show run int gi1/0/48
Building configuration...

Current configuration : 228 bytes
! interface GigabitEthernet1/0/48
   description Connect to Meinberg LANTIME M600-GM1 PTP
   no switchport
   ip address 10.255.18.2 255.255.255.252
   service-policy input CIP-PTP-Traffic
   service-policy output PTP-Event-Priority
end

P5-9300-2#show run int gi1/0/47
Building configuration...

Current configuration : 249 bytes
! interface GigabitEthernet1/0/47
   description Connect to DEVICE Gi1/12 (PTP Static Path)
   switchport trunk allowed vlan 1,118
   switchport mode trunk
   ptp vlan 118
   service-policy input CIP-PTP-Traffic
   service-policy output PTP-Event-Priority
end

P5-9300-2#
P5-9300-2#show run int vlan 118
Building configuration...

Current configuration : 103 bytes
! interface Vlan118
   ip address 10.255.18.6 255.255.255.252
   service-policy input CIP-PTP-Traffic
end
P5-9300-2#P5-9300-2#show ver | inc RELEASE SOFTWARE
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.2, RELEASE SOFTWARE (fc4)
BOOTLDR: System Bootstrap, Version 16.10.1r[FC1], RELEASE SOFTWARE (P)
P5-9300-2#
P5-9300-2#show run | sec ptp
ptp transport ipv4 udp
ptp mode boundary delay-req
ptp priority1 10
ptp priority2 11
ptp vlan 118
P5-9300-2#
P5-9300-2#show ptp brief | inc 48|MASTER|SLAVE
GigabitEthernet1/0/7      0      MASTER
GigabitEthernet1/0/8      0      MASTER
GigabitEthernet1/0/9      0      MASTER
GigabitEthernet1/0/10     0      MASTER
GigabitEthernet1/0/46     0      MASTER
GigabitEthernet1/0/47     0      MASTER
GigabitEthernet1/0/48     0      SLAVE
TenGigabitEthernet1/1/1   0      MASTER
TenGigabitEthernet1/1/3   0      MASTER
TenGigabitEthernet1/1/5   0      MASTER
TenGigabitEthernet1/1/7   0      MASTER
TenGigabitEthernet1/1/8   0      MASTER
GigabitEthernet2/0/48     0      INITIALIZING
```
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

```
P5-9300-2#
P5-9300-2#show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
    Parent Port Number: 1
    Observed Parent Offset (log variance): 17258
    Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
    Grandmaster Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
    Grandmaster Clock Quality:
      Class: 6
      Accuracy: Within 100ns
      Offset (log variance): 13563
      Priority1: 1
      Priority2: 1

P5-9300-2#
P5-9300-2#show ptp port gigabitEthernet 1/0/48
PTP PORT DATASET: GigabitEthernet1/0/48
  Port identity: clock identity: 0x0:BC:60:FF:FE:AD:A5:0
  Port identity: port number: 48
  PTP version: 2
  Port state: SLAVE
  Delay request interval(log mean): 0
  Announce receipt time out: 3
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000

P5-9300-2#
P5-9300-2#show ptp port gigabitEthernet 1/0/47
PTP PORT DATASET: GigabitEthernet1/0/47
  Port identity: clock identity: 0x0:BC:60:FF:FE:AD:A5:0
  Port identity: port number: 47
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 0
  Announce receipt time out: 3
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000
  Port VLAN Id: 118

P5-9300-2#
P5-9300-2#show ptp time-property
PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GPS
  Time Property Persistence: 300 seconds

P5-9300-2#
```
Implementing Site-wide Precision Time Protocol

```
P5-9300-2# show ptp clock
PTP CLOCK INFO
PTP Device Type: Boundary clock
PTP Device Profile: Default Profile
Clock Identity: 0x0:BC:60:FF:FE:AD:A5:0
Clock Domain: 0
Network Transport Protocol: udp-ipv4
Number of PTP ports: 64
Priority1: 10
Priority2: 11
Clock Quality:
  Class: 248
  Accuracy: Unknown
  Offset (log variance): 17258
  Offset From Master(ns): 0
  Mean Path Delay(ns): 115
  Steps Removed: 1

P5-9300-2#
P5-9300-2#
P5-9300-2# show platform software fed switch active ptp domain 0
Displaying data for domain number 0
=======================================
Profile Type : DEFAULT
Profile State: enabled
Clock Mode : BOUNDARY CLOCK
Delay Mechanism: : END-TO-END
PTP clock : 2019-5-24 17:45:57
mean_path_delay 113 nanoseconds
Transport Method : udp-ipv4

P5-9300-2#
```

**Note:** The Cisco Catalyst 9300 PTP default profile only supports Layer 2 in the released software, adding SVI configure.

### Configuring Cisco IE 5000

Cisco IE 5000 PTP Configuration Guide:

### Restrictions and Limitations for PTP

**PTP Messages**
- The Cisco PTP implementation supports only the two-step clock and not the one-step clock. If the switch receives a one-step message from the grandmaster clock, it will convert it into a two-step message.
- Cisco PTP supports multicast PTP messages only.

**PTP Mode and Profile**
- The switch and the grandmaster clock must be in the same PTP domain.
- In Default Profile mode, only the delay_request mechanism is supported. To change to Boundary Clock Mode with the delay_request mechanism, enter the `ptp mode boundary delay-req` command.
Packet Format

- The packet format for PTP messages can be 802.1q tagged packets or untagged packets.
- The switch does not support 802.1q QinQ tunneling.
- Slave IEDs must support tagged and untagged packets.
- When PTP packets are sent on the native VLAN in E2E Transparent Clock Mode, they are sent as untagged packets. To configure the switch to send them as tagged packets, enter the `global vlan dot1q tag native` command.

VLAN Configuration

- Set the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port.
- In boundary mode, only PTP packets in PTP VLAN will be processed. PTP packets from other VLANs will be dropped.
- Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.
- Most grandmaster clocks use the default VLAN 0. In Power Profile mode, the switch default VLAN is VLAN 1 and VLAN 0 is reserved. When you change the default grandmaster clock VLAN, it must be changed to a VLAN other than 0.
- When VLAN is disabled on the grandmaster clock, the PTP interface must be configured as an access port.

Clock Configuration

- All PHY PTP clocks are synchronized to the grandmaster clock. The switch system clock is not synchronized as part of PTP configuration and processes.
- When VLAN is enabled on the grandmaster clock, it must be in the same VLAN as the native VLAN of the PTP port on the switch.
- Grandmaster clocks can drop untagged PTP messages when a VLAN is configured on the grandmaster clock. To force the switch to send tagged packets to the grandmaster clock, enter the `global vlan dot1q tag native` command.

Clock Modes

- Boundary Clock Mode
  - You can enable this mode when the switch is in Power Profile Mode (Layer 2) or in Default Profile Mode (Layer 3).
- Forward Mode
  - You can enable this mode when the switch is in Power Profile Mode (Layer 2) or in Default Profile Mode (Layer 3).
  - When the switch is in Forward mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, e2etransparent, or p2ptransparent).
- E2E Transparent Clock Mode
  - You can enable this mode only when the switch is in Default Profile Mode (Layer 3).
  - When the switch is in E2E Transparent mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, p2ptransparent, or forward).
- P2P Transparent Clock Mode
  - You can enable this mode only when the switch is in Power Profile Mode (Layer 2).
  - When the switch is in P2P Transparent mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, e2etransparent, or forward).
- GMC-BC Clock Mode
You can enable this mode only when the switch is in Default Profile Mode.

**PDV Filtering**
- Adaptive mode (ptp transfer filter adaptive) is not available in Power Profile mode or 802.1AS profile mode.

**PTP Interaction with Other Features**
- The following PTP clock modes do not support EtherChannels:
  - e2etransparent
  - p2ptransparent
  - boundary
  - gmc-bc
- The following PTP clock modes only operate on a single VLAN:
  - e2etransparent
  - p2ptransparent

**NTP to PTP Conversion**
- The NTP to PTP feature supports the Default E2E Profile only.

**Default Settings**
- PTP is enabled on the switch by default.
- By default, the switch uses configuration values defined in the Default Profile (Default Profile mode is enabled).
- The switch default PTP clock mode is E2E Transparent Clock Mode.
- The default BC synchronization algorithm is linear filter.

**GNSS Hardware**
The Cisco IE 5000 uses a GNSS receiver with precise frequency and phase outputs for the host system. When connected to an external GNSS antenna, the receiver contains all the circuitry necessary to automatically acquire GNSS satellite signals, track up to 32 GNSS satellites, and compute location, speed, heading, and time. It provides an accurate one pulse-per-second (PPS) and stable 10 MHz frequency output.

The GNSS chip supports the following frequency bands:
- GPS/NAVSTAR—Global Positioning System–USA: L1
- GLONASS—Global’naya Navigatsionnaya Sputnikovaya Sistema–Russia: L1/G1
- BeiDou—China (including B1–2)
Note: The Galileo satellite system is not currently supported in the released software.

### Table 61  Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Table 61  Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration (continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device#configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>gnss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#gnss</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#antenna cable-delay 500</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#antenna power 3.3</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#constellation gps</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#antenna power 3.3</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#anti-jam</td>
<td></td>
</tr>
<tr>
<td>DEVICE(config-gnss)#end</td>
<td></td>
</tr>
</tbody>
</table>

Enter global configuration mode.

Specifies GNSS parameters: antenna cable-delay, power, constellation, etc. There are two stages in the process for the GNSS receiver to acquire satellites and provide timing signals to the host system:

- **Self-Survey Mode**—On reset, the GNSS receiver comes up in self-survey mode and attempts to lock on to a minimum of four different satellites to obtain a 3-D fix on its current position. It computes nearly 2000 different positions for these satellites, which takes about 35 minutes. Also during this stage, the GNSS receiver is able to generate accurate timing signals and achieve “Normal (Locked to GPS)” state. Note that the timing signal obtained during self-survey mode can be off by 20 seconds; therefore, Cisco IOS collects PPS only during OD mode.

After the self-survey is complete, the results are saved to the GNSS receiver flash, which speeds up the transition to OD mode the next time the self-survey runs. You can manually restart the self-survey process with the gnss self-survey restart Cisco IOS command. After self-survey mode completes again, the results in the GNSS receiver flash are overwritten with the updated results.

- **Over-determined (OD) clock mode**—The device transitions to OD mode when self-survey mode is completed and the position information is stored in non-volatile memory on the device. In this mode, the GNSS receiver outputs timing information based on satellite positions obtained in self-survey mode.

The GNSS receiver remains in OD mode until there is a reason to leave it, such as:

- Detection of a position relocation of the antenna of more than 100m, which triggers an automatic restart of the self-survey.

Self-survey takes about 30 minutes to finish as shown below:

```
May 24 12:52:33.168 EDT: %GNSS-5-GNSS_SELF_SURVEY_COMPLETE: self-survey complete
May 24 12:52:33.168 EDT: %GNSS-5-GNSS_IN_OD_MODE: in OD mode
May 24 12:52:37.177 EDT: %GNSS-5-GNSS_ANTENNA_UP: 1PPS is UP
May 24 13:27:04.169 EDT: %GNSS-5-GNSS_IN_OD_MODE: in OD mode
May 24 13:27:04.169 EDT: %GNSS-5-GNSS_ANTENNA_UP: 1PPS is UP
```
Table 61: Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration (continued)

| Step 4 | ptp mode gmc-bc delay-req  
|        | ptp transfer feedforward  
|        | ptp priority1 <value>  
|        | ptp priority2 <value> |

**Example:**

```
Device(config)# ptp mode gmc-bc delay-req  
Device(config)# ptp transfer feedforward  
Device(config)# ptp priority1 ppp  
Device(config)# ptp priority2 qqq
```  

### Specifies the synchronization transport mode, clock mode, and clock domain:

- **gmc-bc**—The GMC-BC acts like a BC, which is a multi-port device, with a single-port GMC connected to a virtual port on the BC. The GMC-BC switches between acting like a GMC when the GMC-BC is the primary GMC, and acting like a BC when the GMC-BC is a backup. This ensures that all devices on the PTP network remain synchronized in a failover scenario.

- **feedforward**—Very fast and accurate. No PDV filtering.

- **PTP priority1** and **priority2**

### Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration Example

```
IE5K-1#show run | sec gnss  
gnss  
antenna cable-delay 500  
antenna power 3.3  
IE5K-1#  
IE5K-1#show run | sec ptp  
ptp mode gmc-bc delay-req  
ptp priority1 100  
ptp priority2 101  
ptp transfer feedforward  
IE5K-1#  
IE5K-1#show run int gi1/20  
Building configuration...  
Current configuration : 389 bytes  
!  
interface GigabitEthernet1/20  
description Connect to IAPTP-IE4K-01 Gig 1/1  
switchport trunk allowed vlan 10,11,18,19,21,901,918-920  
switchport trunk native vlan 901  
switchport mode trunk  
load-interval 30  
rep segment 15 edge primary  
alarm profile ab-alarm  
spanning-tree link-type point-to-point  
service-policy input CIP-PTP-Traffic  
service-policy output PTP-Event-Priority  
end  
IE5K-1#show run int gi1/17  
Building configuration...  
Current configuration : 370 bytes  
!  
interface GigabitEthernet1/17  
description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17  
switchport trunk allowed vlan 10,11,18,19,21,901,917-920  
switchport trunk native vlan 917  
switchport mode trunk  
load-interval 30  
rep segment 17 edge primary  
spanning-tree link-type point-to-point
```

287
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

```plaintext
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

IE5K-1#show run int gi1/18
Building configuration...

Current configuration : 362 bytes

! interface GigabitEthernet1/18
  ! description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
  ! switchport trunk allowed vlan 10,11,13,19,21,901,917-920
  ! switchport trunk native vlan 917
  switchport mode trunk
  load-interval 30
  rep segment 17 edge
  spanning-tree link-type point-to-point
  service-policy input CIP-PTP-Traffic
  service-policy output PTP-Event-Priority
end

IE5K-1#IE5K-1#show ver | inc RELEASE SOFTWARE|Version|image
Cisco IOS Software, IE5000 Software (IE5000-UNIVERSALK9-M), Experimental Version 15.2(20190515:094847)
BOOTLDR: IE5000  Boot Loader (IE5000-HBOOT-M) Version 15.2(2r)EB, RELEASE SOFTWARE (fc1)
System image file is "sdflash:ie5000-universalk9-mz_backedout_CSCvd47399.SPA"
Version ID : V06
Switch Ports Model SW Version SW Image
IE5K-1#

IE5K-1#show gnss status
GNSS status: Enable
Constellation: GPS
Receiver Status: 0D
Survey progress: 100
Satellite count: 7
PDOP: 1.00  TDOP: 1.00
HDOP: 0.00  VDOP: 0.00
Alarm: None

IE5K-1#show gnss satellite all
SV Type Codes: 0 - GPS, 1 - GLONASS, 2 - Beidou

All Satellites Info:
<table>
<thead>
<tr>
<th>SV PRN No</th>
<th>Channel No</th>
<th>Acq Flg</th>
<th>Ephemeris Flg</th>
<th>SV Type</th>
<th>Sig Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>48</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>41</td>
<td></td>
</tr>
</tbody>
</table>

IE5K-1#show gnss time
Current GNSS Time:
Time: 2019/05/25 01:47:03 UTC Offset: 18

IE5K-1#show gnss location
Current GNSS Location:
  LOC: 35:51.314214449 N 78:52.518730299 W 92.77905 m
IE5K-1#show platform gnss
Board ID: 0x5000000 (Production SKU)
GNSS Chip:
  Hardware code: 3023 - RES SMT 360
  Serial Number: 1275127926
  Build Date: 6/24/2017
IE5K-1#
```
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

IE5K-1#show run | sec ptp
ptp mode gmc-bc delay-req
ptp priority1 100
ptp priority2 101
ptp transfer feedforward
IE5K-1#
IE5K-1#show ptp port | inc MASTER|SLAVE|PORT
PTP PORT DATASET: GigabitEthernet1/1
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/2
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/3
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/4
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/5
PTP PORT DATASET: GigabitEthernet1/6
PTP PORT DATASET: GigabitEthernet1/7
PTP PORT DATASET: GigabitEthernet1/8
PTP PORT DATASET: GigabitEthernet1/9
PTP PORT DATASET: GigabitEthernet1/10
PTP PORT DATASET: GigabitEthernet1/11
PTP PORT DATASET: GigabitEthernet1/12
PTP PORT DATASET: GigabitEthernet1/13
PTP PORT DATASET: GigabitEthernet1/14
PTP PORT DATASET: GigabitEthernet1/15
PTP PORT DATASET: GigabitEthernet1/16
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/17
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/18
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/19
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/20
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/21
PTP PORT DATASET: GigabitEthernet1/22
PTP PORT DATASET: GigabitEthernet1/23
PTP PORT DATASET: GigabitEthernet1/24
PTP PORT DATASET: GigabitEthernet1/25
PTP PORT DATASET: GigabitEthernet1/26
PTP PORT DATASET: GigabitEthernet1/27
PTP PORT DATASET: GigabitEthernet1/28
IE5K-1#
IE5K-1#show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Port Number: 0
    Observed Parent Offset (log variance): N/A
    Observed Parent Clock Phase Change Rate: N/A
  Grandmaster Clock:
    Grandmaster Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
    Grandmaster Clock Quality:
      Class: 6
      Accuracy: Within 250ns
      Offset (log variance): N/A
      Priority1: 100
      Priority2: 101
IE5K-1#show ptp cloc
PTP CLOCK INFO
PTP Device Type: Grand Master clock - Boundary clock
PTP Device Profile: Default Profile
Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
Clock Domain: 0
Number of PTP ports: 28
Time Transfer: Feedforward
Priority1: 100
Priority2: 101
Clock Quality:
  Class: 6
  Accuracy: Within 250ns
  Offset (log variance): N/A
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 0
Local clock time: 21:49:06 EDT May 24 2019

IE5K-1#show ptp time-property
PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GNSS

IE5K-1#show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface GigabitEthernet1/1
  Empty
Interface GigabitEthernet1/2
  Empty
Interface GigabitEthernet1/3
  Empty
Interface GigabitEthernet1/4
  Empty
Interface GigabitEthernet1/5
  Empty
Interface GigabitEthernet1/6
  Empty
Interface GigabitEthernet1/7
  Empty
Interface GigabitEthernet1/8
  Empty
Interface GigabitEthernet1/9
  Empty
Interface GigabitEthernet1/10
  Empty
Interface GigabitEthernet1/11
  Empty
Interface GigabitEthernet1/12
  Empty
Interface GigabitEthernet1/13
  Empty
Interface GigabitEthernet1/14
  Empty
Interface GigabitEthernet1/15
  Empty
Interface GigabitEthernet1/16
  Empty
Table 62  Cisco IE 5000 PTP Default Profile Boundary Clock Configuration

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

Interface GigabitEthernet1/17
Empty
Interface GigabitEthernet1/18
Empty
Interface GigabitEthernet1/19
Empty
Interface GigabitEthernet1/20
Empty
Interface GigabitEthernet1/21
Empty
Interface GigabitEthernet1/22
Empty
Interface GigabitEthernet1/23
Empty
Interface GigabitEthernet1/24
Empty
Interface GigabitEthernet1/25
Empty
Interface GigabitEthernet1/26
Empty
Interface GigabitEthernet1/27
Empty
Interface GigabitEthernet1/28
Empty
IE5K-1#
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Cisco IE 5000 PTP Default Profile Boundary Clock Configuration Example

DEVICE#show run | sec ptp
ptp mode boundary delay-req
ptp priority1 100
ptp priority2 101
ptp time-property persist infinite
ptp transfer feedforward
DEVICE#
DEVICE#show run int gi1/12
Building configuration...

Current configuration : 250 bytes
!
interface GigabitEthernet1/12
description Connect to C9300-1 Gi1/0/47 (PTP Static Path)
switchport trunk allowed vlan 1,118

Table 62 Cisco IE 5000 PTP Default Profile Boundary Clock Configuration (continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device#configure terminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>ptp mode boundary delay-req</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptp time-property persist infinite</td>
<td></td>
</tr>
<tr>
<td>ptp transfer feedforward</td>
<td></td>
</tr>
<tr>
<td>ptp priority1 &lt;value&gt;</td>
<td></td>
</tr>
<tr>
<td>ptp priority2 &lt;value&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Example:
Device(config)# ptp mode boundary delay-req
Device(config)# ptp time-property persist infinite
Device(config)# ptp transfer feedforward
Device(config)# ptp priority1
Device(config)# ptp priority2

Specifies the synchronization transport mode, clock mode, and clock domain:
- boundary—Mode to enable the switch to participate in selecting the best master clock. If no better clocks are detected, the switch becomes the grandmaster clock on the network and the parent clock to all connected devices. If the best master is determined to be a clock connected to the switch, the switch synchronizes to that clock as a child to the clock, then acts as a parent clock to devices connected to other ports. After initial synchronization, the switch and the connected devices exchange timing messages to correct time skew caused by clock offsets and network delays. Use this mode when overload or heavy load conditions produce significant delay jitter.
- PTP time property persist infinite would preserve the time properties, preventing slave clocks from detecting a variance in the time values when the redundant grandmaster clock comes out of standby flapping.
- PTP priority1 and priority2

<table>
<thead>
<tr>
<th>Step 4</th>
<th>ptp vlan &lt;value&gt;</th>
</tr>
</thead>
</table>

Example:
Device(config)#interface vlan nnn
Device(config)#ip address m.m.m.m n.n.n.n
Device(config)#interface GigabitEthernetx/y/z
Device(config-if)#switch mode trunk
Device(config-if)#switch trunk allow vlan nnn
Device(config-if)#ptp vlan nnn

Specify PTP over SVI:
- Within PTP default profile, PTP messages are processed in VLAN 1 by default. Use ptp vlan vlan-name command under interface configurations to allow PTP message processing on specific VLAN.
- You must add this to the VLAN database of the device. PTP VLAN can only be configure after you apply PTP global configure.
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

```
switchport mode trunk
ptp vlan 118
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

DEVICE#show run int vlan 118
Building configuration...

Current configuration : 65 bytes
!
interface Vlan118
  ip address 10.255.18.5 255.255.255.252
end

DEVICE#show run int gi1/20
Building configuration...

Current configuration : 389 bytes
!
interface GigabitEthernet1/20
  description Connect to IAPTP-IE4K-01 Gig 1/1
  switchport trunk allowed vlan 10,11,18,19,21,901,918-920
  switchport trunk native vlan 901
  switchport mode trunk
  load-interval 30
  rep segment 15 edge primary
  alarm profile ab-alarm
  spanning-tree link-type point-to-point
  service-policy input CIP-PTP-Traffic
  service-policy output PTP-Event-Priority
end

DEVICE#

DEVICE#show run int gi1/17
Building configuration...

Current configuration : 370 bytes
!
interface GigabitEthernet1/17
  description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
  switchport trunk allowed vlan 10,11,18,19,21,901,917-920
  switchport trunk native vlan 917
  switchport mode trunk
  load-interval 30
  rep segment 17 edge primary
  spanning-tree link-type point-to-point
  service-policy input CIP-PTP-Traffic
  service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/18
Building configuration...

Current configuration : 362 bytes
!
interface GigabitEthernet1/18
  description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
  switchport trunk allowed vlan 10,11,18,19,21,901,917-920
  switchport trunk native vlan 917
  switchport mode trunk
  load-interval 30
  rep segment 17 edge
```
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority

DEVICE# show ver | inc RELEASE SOFTWARE|Version|image
Cisco IOS Software, IE5000 Software (IE5000-UNIVERSAL-K9-M), Experimental Version 15.2(20190515:094847)
[vedasser-7_e_rep 117]
BOOTLDR: IE5000 Boot Loader (IE5000-HBOOT-M) Version 15.2(2r)EB, RELEASE SOFTWARE (fc1)
System image file is "sdflash:ie5000-universalk9-mz_backedout_CSCvd47399.SPA"
Version ID : V06
Switch Ports Model SW Version SW Image
DEVICE#
DEVICE# show run | sec ptp
ptp mode boundary delay-req
ptp priority1 100
ptp priority2 101
ptp time-property persist infinite
ptp transfer feedforward

DEVICE#
DEVICE# show ptp port | inc MASTER|SLAVE|PORT
PTP PORT DATASET: GigabitEthernet1/1
PTP PORT DATASET: GigabitEthernet1/2
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/3
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/4
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/5
PTP PORT DATASET: GigabitEthernet1/6
PTP PORT DATASET: GigabitEthernet1/7
PTP PORT DATASET: GigabitEthernet1/8
PTP PORT DATASET: GigabitEthernet1/9
PTP PORT DATASET: GigabitEthernet1/10
PTP PORT DATASET: GigabitEthernet1/11
PTP PORT DATASET: GigabitEthernet1/12
Port state: SLAVE
PTP PORT DATASET: GigabitEthernet1/13
PTP PORT DATASET: GigabitEthernet1/14
PTP PORT DATASET: GigabitEthernet1/15
PTP PORT DATASET: GigabitEthernet1/16
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/17
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/18
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/19
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/20
Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/21
PTP PORT DATASET: GigabitEthernet1/22
PTP PORT DATASET: GigabitEthernet1/23
PTP PORT DATASET: GigabitEthernet1/24
PTP PORT DATASET: GigabitEthernet1/25
PTP PORT DATASET: GigabitEthernet1/26
PTP PORT DATASET: GigabitEthernet1/27
PTP PORT DATASET: GigabitEthernet1/28

DEVICE#
DEVICE# show int gi1/12
Building configuration...

Current configuration : 250 bytes
!
interface GigabitEthernet1/12
Implementing Site-wide Precision Time Protocol

description Connect to C9300-1 Gi1/0/47 (PTP Static Path)
switchport trunk allowed vlan 1,118
switchport mode trunk
ptp vlan 118
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/20
Building configuration...

Current configuration : 389 bytes
!
interface GigabitEthernet1/20
description Connect to IA-PTP-IE4K-01 Gig 1/1
switchport trunk allowed vlan 10,11,18,19,21,901,918-920
switchport trunk native vlan 901
switchport mode trunk
load-interval 30
rep segment 15 edge primary
alarm profile ab-alarm
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/17
Building configuration...

Current configuration : 370 bytes
!
interface GigabitEthernet1/17
description Connect IE5K-2 IA-PTP-HSRP-PO10 Gi1/17
switchport trunk allowed vlan 10,11,18,19,21,901,917-920
switchport trunk native vlan 917
switchport mode trunk
load-interval 30
rep segment 17 edge primary
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/18
Building configuration...

Current configuration : 362 bytes
!
interface GigabitEthernet1/18
description Connect IE5K-2 IA-PTP-HSRP-PO10 Gi1/17
switchport trunk allowed vlan 10,11,18,19,21,901,917-920
switchport trunk native vlan 917
switchport mode trunk
load-interval 30
rep segment 17 edge
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

DEVICE#show ptp parent
PTP PARENT PROPERTIES
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Parent Clock:
Parent Clock Identity: 0x0:BC:60:FP:FE:AD:A5:0
Parent Port Number: 47
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
Grandmaster Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
Grandmaster Clock Quality:
- Class: 6
- Accuracy: Within 100ns
- Offset (log variance): 13563
- Priority1: 1
- Priority2: 1

DEVICE#show ptp clo
DEVICE#show ptp clock
PTP CLOCK INFO
- PTP Device Type: Boundary clock
- PTP Device Profile: Default Profile
- Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
- Clock Domain: 0
- Number of PTP ports: 28
- Time Transfer: Feedforward
- Priority1: 100
- Priority2: 101
- Clock Quality:
  - Class: 248
  - Accuracy: Unknown
  - Offset (log variance): N/A
  - Offset From Master(ns): 8
  - Mean Path Delay(ns): 147
  - Steps Removed: 2
  - Local clock time: 15:04:28 EDT May 24 2019

DEVICE#show ptp tim
DEVICE#show ptp time-property
PTP CLOCK TIME PROPERTY
- Current UTC offset valid: TRUE
- Current UTC offset: 37
- Leap 59: FALSE
- Leap 61: FALSE
- Time Traceable: TRUE
- Frequency Traceable: TRUE
- PTP Timescale: TRUE
- Time Source: GNSS
- Time Property Persistence: Infinite

DEVICE#show ptp fo
DEVICE#show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
- Interface GigabitEthernet1/1
  - Empty
- Interface GigabitEthernet1/2
  - Empty
- Interface GigabitEthernet1/3
  - Empty
- Interface GigabitEthernet1/4
  - Empty
- Interface GigabitEthernet1/5
  - Empty
- Interface GigabitEthernet1/6
  - Empty
- Interface GigabitEthernet1/7
  - Empty
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Interface GigabitEthernet1/8
Empty
Interface GigabitEthernet1/9
Empty
Interface GigabitEthernet1/10
Empty
Interface GigabitEthernet1/11
Empty
Interface GigabitEthernet1/12
Foreign master port identity: clock id: 0x0:BC:60:FF:FE:AD:A5:0
Foreign master port identity: port num: 47
Number of Announce messages: 3
Message received port: 12
Time stamps: 145448162, 145447166
Interface GigabitEthernet1/13
Empty
Interface GigabitEthernet1/14
Empty
Interface GigabitEthernet1/15
Empty
Interface GigabitEthernet1/16
Empty
Interface GigabitEthernet1/17
Empty
Interface GigabitEthernet1/18
Empty
Interface GigabitEthernet1/19
Empty
Interface GigabitEthernet1/20
Empty
Interface GigabitEthernet1/21
Empty
Interface GigabitEthernet1/22
Empty
Interface GigabitEthernet1/23
Empty
Interface GigabitEthernet1/24
Empty
Interface GigabitEthernet1/25
Empty
Interface GigabitEthernet1/26
Empty
Interface GigabitEthernet1/27
Empty
Interface GigabitEthernet1/28
Empty
DEVICE#

Note: The Cisco Catalyst 9300 PTP default profile only supports Layer 2 in the released software, adding SVI configure.
Configuring Cisco IE 4000

For the Cisco IE 4000 PTP Configuration Guide and Restrictions and Limitations for PTP, refer to Configuring Cisco IE 5000, page 282.

Table 63  Cisco IE 4000 PTP Default Profile Boundary Clock

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device#configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ptp mode boundary delay-req</td>
<td>Specifies the synchronization transport mode, clock mode, and clock domain:</td>
</tr>
<tr>
<td></td>
<td>ptp time-property persist infinite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ptp transfer feedforward</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ptp priority1 &lt;value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ptp priority2 &lt;value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ptp mode boundary delay-req</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp time-property persist infinite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp transfer feedforward</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp priority1 ppp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ptp priority2 qqq</td>
<td></td>
</tr>
</tbody>
</table>

Cisco IE 4000 PTP Default Profile Boundary Clock Configuration Example

IAPTP-IE4K-01#show run | sec ptp
ptp mode boundary delay-req
ptp priority1 110
ptp priority2 111
ptp time-property persist infinite
ptp transfer feedforward
IAPTP-IE4K-01#
IAPTP-IE4K-01#show run int gi1/1
Building configuration...

Current configuration : 342 bytes |
! interface GigabitEthernet1/1
description Connect to IESK-1 Gig 1/20
switchport trunk allowed vlan 10,11,18,21,901,918,920
switchport trunk native vlan 901
switchport mode trunk
load-interval 30
rep segment 15
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#show run int gi1/2
Building configuration...

Current configuration : 348 bytes
!
interface GigabitEthernet1/2
description Connect to IAPTP-IE4K-02 Gig 1/1
switchport trunk allowed vlan 10,11,18,21,901,918,920
switchport trunk native vlan 901
switchport mode trunk
load-interval 30
rep segment 15
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#IAPTP-IE4K-01#show ver | inc RELEASE SOFTWARE|Version|image
Cisco IOS Software, IE4000 Software (IE4000-UNIVERSALK9-M), Experimental Version 15.2(20190515:094847)
[vadasser-7_e_rep 113]
BOOTLDR: IE4000 Boot Loader (IE4000-HBOOT-M) Version 15.2(6.2r)E2, RELEASE SOFTWARE
System image file is "sdflash:ie4000-universalk9-mz_backedout_CSCvd47399.SPA"
Version ID : V02
Switch Ports Model SW Version SW Image
IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp port | inc MASTER | SLAVE | PORT
PTP PORT DATASET: GigabitEthernet1/1
  Port state: SLAVE
PTP PORT DATASET: GigabitEthernet1/2
  Port state: MASTER
PTP PORT DATASET: GigabitEthernet1/3
PTP PORT DATASET: GigabitEthernet1/4
PTP PORT DATASET: FastEthernet1/5
PTP PORT DATASET: FastEthernet1/6
PTP PORT DATASET: FastEthernet1/7
PTP PORT DATASET: FastEthernet1/8
PTP PORT DATASET: FastEthernet1/9
PTP PORT DATASET: FastEthernet1/10
PTP PORT DATASET: FastEthernet1/11
PTP PORT DATASET: FastEthernet1/12
PTP PORT DATASET: FastEthernet1/13
PTP PORT DATASET: FastEthernet1/14
PTP PORT DATASET: FastEthernet1/15
PTP PORT DATASET: FastEthernet1/16
IAPTP-IE4K-01#
IAPTP-IE4K-01#show run int gi1/1
Building configuration...

Current configuration : 342 bytes
!
interface GigabitEthernet1/1
description Connect to IE5K-1 Gig 1/20
switchport trunk allowed vlan 10,11,18,21,901,918,920
switchport trunk native vlan 901
switchport mode trunk
load-interval 30
rep segment 15
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#
IAPTP-IE4K-01#show run int gi1/2
Building configuration...

Current configuration : 348 bytes
!
interface GigabitEthernet1/2
description Connect to IAPTP-IE4K-02 Gig 1/1
switchport trunk allowed vlan 10,11,18,21,901,918,920
switchport trunk native vlan 901
switchport mode trunk
load-interval 30
rep segment 15
spanning-tree link-type point-to-point
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp parent
PTP PARENT PROPERTIES
Parent Clock:
  Parent Port Number: 20
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
  Grandmaster Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
  Grandmaster Clock Quality:
    Class: 6
    Accuracy: Within 100ns
    Offset (log variance): 13563
    Priority1: 1
    Priority2: 1

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp clock
PTP CLOCK INFO
PTP Device Type: Boundary clock
PTP Device Profile: Default Profile
Clock Domain: 0
Number of PTP ports: 16
Time Transfer: Feedforward
Priority1: 110
Priority2: 111
Clock Quality:
  Class: 248
  Accuracy: Unknown
  Offset (log variance): N/A
  Offset From Master(ns): -14
  Mean Path Delay(ns): 44
  Steps Removed: 3
  Local clock time: 10:53:39 EDT May 25 2019

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp time-property
PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Current UTC offset: 37
Leap 59: FALSE
Leap 61: FALSE
Time Traceable: TRUE
Frequency Traceable: TRUE
PTP Timescale: TRUE
Time Source: GNSS
Time Property Persistence: Infinite

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface GigabitEthernet1/1
   Foreign master port identity: port num: 20
   Number of Announce messages: 4
   Message received port: 1
   Time stamps: 415643932, 415641933
Interface GigabitEthernet1/2
   Empty
Interface GigabitEthernet1/3
   Empty
Interface GigabitEthernet1/4
   Empty
Interface FastEthernet1/5
   Empty
Interface FastEthernet1/6
   Empty
Interface FastEthernet1/7
   Empty
Interface FastEthernet1/8
   Empty
Interface FastEthernet1/9
   Empty
Interface FastEthernet1/10
   Empty
Interface FastEthernet1/11
   Empty
Interface FastEthernet1/12
   Empty
Interface FastEthernet1/13
   Empty
Interface FastEthernet1/14
   Empty
Interface FastEthernet1/15
   Empty
Interface FastEthernet1/16
   Empty
IAPTP-IE4K-01#

Configuring Cisco IE 3000

For the Cisco IE 3000 PTP Configuration Guide and Restrictions and Limitations for PTP, refer to Configuring Cisco IE 5000, page 282.

Cisco IE 3000 PTP Default Profile Boundary Clock

Note: The Cisco IE 3000 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.
Networking and Security in Industrial Automation Environments

Implementing Site-wide Precision Time Protocol

Cisco IE 3000 PTP Default Profile Boundary Clock Configuration Example
Note: The Cisco IE 3000 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.

Configuring Cisco IE 3400

For the Cisco IE 3400 PTP Configuration Guide and Restrictions and Limitations for PTP, refer to Configuring Cisco IE 5000, page 282.

Cisco IE 3400 PTP Default Profile Boundary Clock
Note: The Cisco IE 3400 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.

Cisco IE 3400 PTP Default Profile Boundary Clock Configuration Example
Note: The Cisco IE 3400 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.
Performance

This section describes the performance characterization results of Cisco products for site-wide precision time. Tests were performed for 24 hours to validate product stability. Table 64 through Table 71 provide the time accuracy values by products.
### Table 64  High Precision Site-wide Grandmaster Clock Time Distribution Model–Cisco Catalyst 9300

<table>
<thead>
<tr>
<th></th>
<th>LANTIME M600 Reference</th>
<th>Cisco Catalyst 9300 Boundary Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Interval Error (TIE)</strong></td>
<td>±1 \times 10^{-12}s/24hours</td>
<td>min 40ns max 40ns</td>
</tr>
<tr>
<td><strong>Maximum Time Interval Error (MTIE)</strong></td>
<td>±1 \times 10^{-12}s/24hours</td>
<td>min 40ns max 40ns</td>
</tr>
<tr>
<td><strong>Time Deviation (TDEV)</strong></td>
<td>NA</td>
<td>min 0.233 max 19.91</td>
</tr>
</tbody>
</table>
### Table 65  High Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 5000

<table>
<thead>
<tr>
<th></th>
<th>LANTIME M600 Reference</th>
<th>Cisco IE 5000 Boundary Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Interval Error (TIE)</strong></td>
<td>±1·10⁻¹²s/24hours</td>
<td>min -3ns max 18ns</td>
</tr>
<tr>
<td><strong>Maximum Time Interval Error (MTIE)</strong></td>
<td>±1·10⁻¹²s/24hours</td>
<td>min 17ns max 21ns</td>
</tr>
<tr>
<td><strong>Time Deviation (TDEV)</strong></td>
<td>NA</td>
<td>min 0.916 max 4.564</td>
</tr>
</tbody>
</table>
### Table 66  High Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 4000

<table>
<thead>
<tr>
<th>Parameter</th>
<th>LANTIME M600 Reference</th>
<th>Cisco IE 4000 Boundary Clock and Transparent Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Interval Error (TIE)</td>
<td>±1 (-10^{-12})s/24hours</td>
<td>min -17ns max 14ns</td>
</tr>
<tr>
<td>Maximum Time Interval Error (MTIE)</td>
<td>±1 (-10^{-12})s/24hours</td>
<td>min 25ns max 31ns</td>
</tr>
<tr>
<td>Time Deviation (TDEV)</td>
<td>NA</td>
<td>min 0.1 max 5.127</td>
</tr>
</tbody>
</table>
### Table 67  High Precision Site-wide Grandmaster Clock Time Distribution Model–Cisco IE 3000

<table>
<thead>
<tr>
<th>LAN TIME M600 Reference</th>
<th>Cisco IE 3000 Transparent Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Interval Error (TIE)</td>
<td>min -52ns max 22ns</td>
</tr>
<tr>
<td>±1 - 10^{-12}s/24hours</td>
<td></td>
</tr>
<tr>
<td>Maximum Time Interval Error (MTIE)</td>
<td>min 56ns max 74ns</td>
</tr>
<tr>
<td>±1 - 10^{-12}s/24hours</td>
<td></td>
</tr>
<tr>
<td>Time Deviation (TDEV)</td>
<td>min 0.188 max 9.532</td>
</tr>
<tr>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

- **LAN TIME M600 Reference**
- **Cisco IE 3000 Transparent Clock**
- **Time Interval Error (TIE)**
  - ±1 - 10^{-12}s/24hours
  - min -52ns max 22ns
- **Maximum Time Interval Error (MTIE)**
  - ±1 - 10^{-12}s/24hours
  - min 56ns max 74ns
- **Time Deviation (TDEV)**
  - NA
  - min 0.188 max 9.532
Table 68  High Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 3400

<table>
<thead>
<tr>
<th>LANTIME M600 Reference</th>
<th>Cisco IE 3400 Transparent Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Interval Error (TIE)</td>
<td>min -25ns max 59ns</td>
</tr>
<tr>
<td>±1 - 10^{-12}s/24hours</td>
<td></td>
</tr>
<tr>
<td>Maximum Time Interval Error (MTIE)</td>
<td>min 67ns max 84ns</td>
</tr>
<tr>
<td>±1 - 10^{-12}s/24hours</td>
<td></td>
</tr>
<tr>
<td>Time Deviation (TDEV)</td>
<td>min 0.247ns max 10.925ns</td>
</tr>
<tr>
<td>NA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IE 5000 Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>Time Interval Error (TIE)</strong></td>
<td>±4.6–6 s/17hours</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Time Interval Error (MTIE)</strong></td>
<td>±4.6–6 s/17hours</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Time Deviation (TDEV)</strong></td>
<td>NA</td>
</tr>
</tbody>
</table>

### Table 69 Intermediate Precision Site-wide Grandmaster Clock Time Distribution Model–Cisco IE 4000

- **Time Interval Error (TIE)**: ±4.6–6 s/17hours
  - Minimum: -38ns
  - Maximum: 49ns

- **Maximum Time Interval Error (MTIE)**: ±4.6–6 s/17hours
  - Minimum: 9ns
  - Maximum: 87ns

- **Time Deviation (TDEV)**: NA
  - Minimum: 1.358 ns
  - Maximum: 5.756 ns
### Table 70 Intermediate Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 3000

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Cisco IE 5000 Reference</th>
<th>Cisco IE 3000 Transparent Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Interval Error (TIE)</td>
<td></td>
<td>min -37ns max 84ns</td>
</tr>
<tr>
<td>±4.6-6 s/17hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Time Interval Error (MTIE)</td>
<td></td>
<td>min 44ns max 121ns</td>
</tr>
<tr>
<td>±4.6-6 s/17hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Deviation (TDEV)</td>
<td>NA</td>
<td>min 2.9 max 7.537</td>
</tr>
<tr>
<td>NA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 71  Intermediate Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 3400

<table>
<thead>
<tr>
<th>Cisco IE 5000 Reference</th>
<th>Cisco IE 3400 Transparent Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Interval Error (TIE)</strong></td>
<td><strong>min -98ns max 35ns</strong></td>
</tr>
<tr>
<td>±4.6–6 s/17hours</td>
<td><strong>Maximum Time Interval Error (MTIE)</strong></td>
</tr>
<tr>
<td></td>
<td>min 62ns max 133ns</td>
</tr>
<tr>
<td><strong>Time Deviation (TDEV)</strong></td>
<td><strong>min 3.053 max 9.374</strong></td>
</tr>
<tr>
<td>NA</td>
<td><strong>Mean [ppb]</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Min [ppb]</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Max [ppb]</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Max-Min [ppb]</strong></td>
</tr>
</tbody>
</table>

- **Time Interval Error (TIE)**: ±4.6–6 s/17hours
- **Maximum Time Interval Error (MTIE)**: min 62ns max 133ns
- **Time Deviation (TDEV)**: min 3.053 max 9.374
- **Mean [ppb]**: 0
- **Min [ppb]**: -0.003
- **Max [ppb]**: 0.002
- **Max-Min [ppb]**: 0.006
Site-wide Precision Time Protocol Troubleshooting

Syslog:

Table 72  PTP Debug CLI

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`debug ptp {bmc</td>
<td>clock-correction</td>
</tr>
<tr>
<td></td>
<td>▪ <code>bmc</code>—Display the PTP best master clock algorithm debug messages.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>clock-correction</code>—Display the PTP clock-correction messages.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>error</code>—Display the PTP error debug messages.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>Event</code>—Display the PTP state event debug messages.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>messages</code>—Display the PTP state event debug messages.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>transparent-clock</code>—Display the PTP transparent-clock debug</td>
</tr>
<tr>
<td></td>
<td>messages.</td>
</tr>
</tbody>
</table>

Table 73  PTP CLI Showing Configuration and Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ptp {clock</td>
<td>foreign-master-records</td>
</tr>
<tr>
<td></td>
<td>▪ <code>clock</code>—Displays PTP clock information.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>foreign-master-records</code>—Displays PTP foreign-master-records.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>parent</code>—Displays PTP parent properties.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>port FastEthernet</code>—Displays PTP properties for the FastEthernet IEEE 802.3 interfaces.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>port GigabitEthernet</code>—Displays PTP properties for the GigabitEthernet IEEE 802.3z interfaces.</td>
</tr>
<tr>
<td></td>
<td>▪ <code>time-property</code>—Displays PTP clock-time properties.</td>
</tr>
</tbody>
</table>

Third-party PTP-related Equipment and Application Troubleshooting Resources
Meinberg LANTIME Configuration and Management Manual
Previous and Related Documentation

This design and implementation guide is an evolution of a significant set of industrial solutions issued by Cisco. In many ways, this document amalgamates many of the concepts, technologies, and requirements that are shared in industrial solutions. The vertical relevance will be maintained, but shared technical aspects are essentially collected and referred to by this document.


- The Cisco Catalyst 9300 and Cisco Catalyst 3850 are positioned as the distribution switches where there is a controlled IT environment.

- Cisco Catalyst 3850 StackWise—480 configuration:
  - For Cisco Catalyst 3850
    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg Chapter_010.html#reference_5415C09868764F0FA05F88897F108139
  - For Cisco Catalyst 9300


- Cisco IE 3x00 Series Switch

- Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000:
  - Switch Software
  - Switch Software Smartports configuration

- Cisco Industrial Network Director:
  - http://www.cisco.com/go/ind
  - Network Management for Operational Technology in Connected Factory Architectures

- IEC Standards:
Networking and Security in Industrial Automation Environments

Previous and Related Documentation

IEC 61588 Precision clock synchronization protocol for networked measurement and control systems

Table 74 Previous Industry Documentation

<table>
<thead>
<tr>
<th>Industry</th>
<th>Solution</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manufacturing     | Connected Factory—CPwE
                  | Solution to assist manufacturers seeking to integrate or upgrade their Industrial Automation and Control System (IACS) networks to standard Ethernet and IP networking technologies. |
|                   | Connected Factory—PROFINET
                  | Solution for PROFINET-based industrial environments to integrate Cisco Industrial Ethernet switches into the automation network.                                                                           |
|                   | Connected Factory—CC-Link IE
                  | Solution for CC-Link IE-based industrial environments to integrate Cisco Industrial Ethernet switches into the automation network.                                                                             |
|                   | Connected Machine
                  | Enable rapid and repeatable machine connectivity, providing business improvements such as overall equipment effectiveness (OEE) and machine monitoring.                                                       |
|                   | Connected Factory—Network Management for Operational Technology
                  | Discusses the use of Cisco’s Industrial Network Director application for monitoring industrial network assets and discovering automation devices within the context of the Connected Factory solution. |
| Oil & Gas         | Connected Pipeline—Control Center
                  | Secure, virtualized Control Center design for Oil & Gas pipeline operators, including secure remote access and operational support                                                                 |
|                   | Connected Pipeline—Operational Telecoms
                  | Best practice, secure, design guidance for Oil & Gas pipeline wide area networks and pipeline station networks. This includes networks between Control Centers, from Control Centers to pipeline stations, and inside pipeline stations |
|                   | Connected Refinery and Processing Facility
                  | Best practice, secure design guidance leveraging industrial wireless and mobility for next generation refining and processing                                                                             |