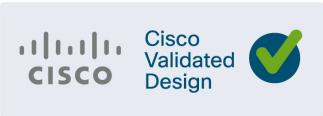
Substation Automation Local Area Network and Security

Version 2.3.2

Design and Implementation Guide

First Published: February 2019



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Contents

Substation Automation Local Area Network and Security

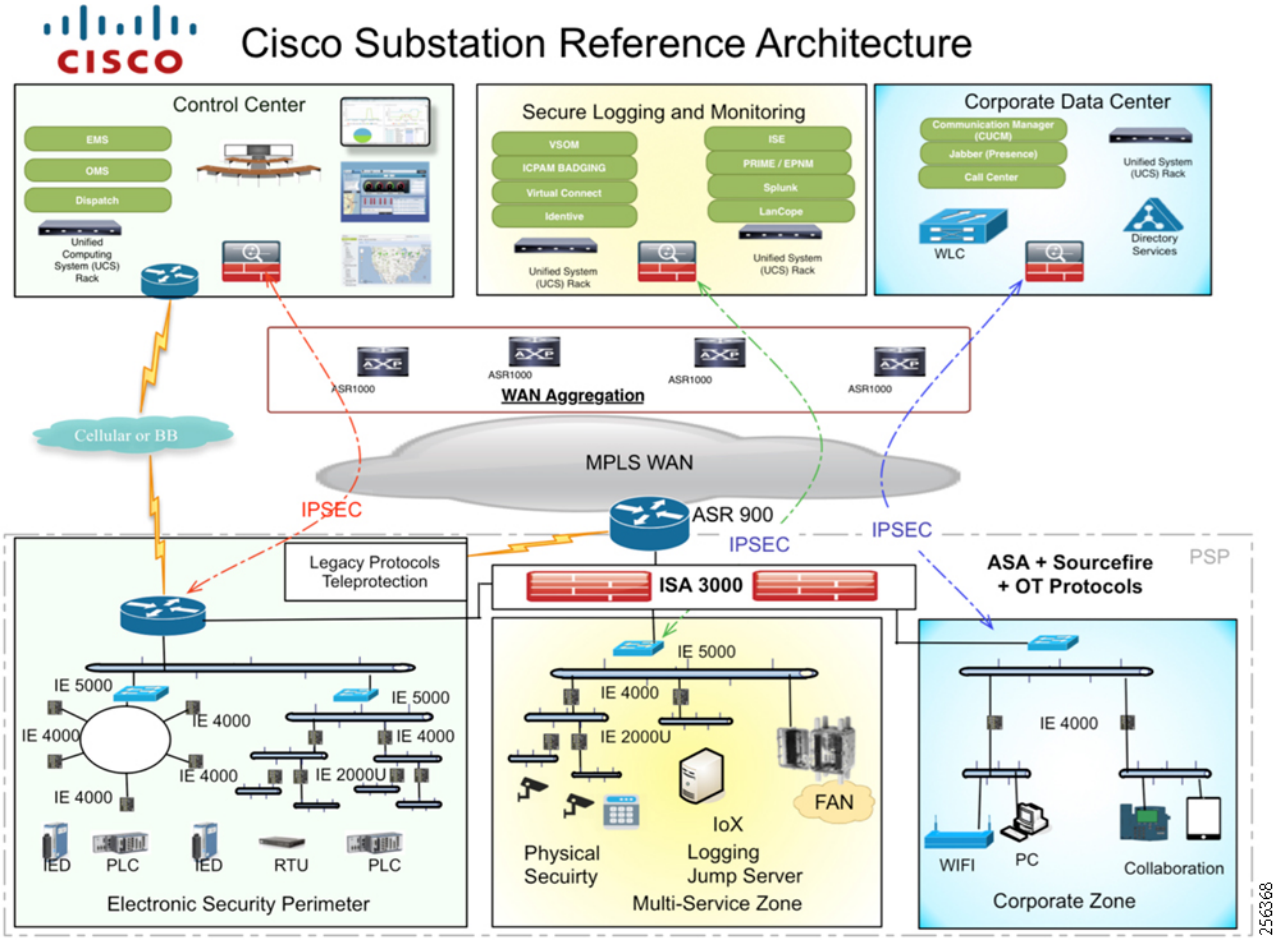
Preface

Cisco is committed to providing a holistic substation automation solution that implements a scalable, secure, and resilient multiservice-enabled network. Solution releases continue to address evolving, real life customer deployment scenarios. In addition to substation automation, management, and reporting, the use cases covered in previous solution releases included architectures for physical security, remote engineering access, remote workforce management, and precise timing distribution. Cisco Validated Designs (CVDs) are available with extensive content on serial and Ethernet-based deployments, topologies for Electronic Security Perimeter (ESP), multiservice, and corporate network zones, Quality of Service (QoS), high availability, and more.

This Substation Automation Local Area Network and Security Design and Implementation Guide CVD (SA LAN and Security CVD) version 2.3.2 is an update that describes developments to the Cisco validated substation automation solution architectures. The purpose of the solution release associated with this document was to further enhance the electrical utility substation automation design and implementation experience and to identify recently-added hardware and software capabilities on the Cisco Industrial Ethernet (IE) switching product line.

The SA LAN and Security CVD version 2.3.2 is a continuation of solution versions 1.5, 2.2.1, and 2.3.1. Version 2.3.2 of the solution is **not** meant to revisit every topic already addressed by previous releases. For historical designs that are still valid and recommended, the reader should refer to earlier solution documentation (see Related Documentation, page 76). The Cisco substation automation reference architecture is depicted in Figure 1.

Figure 1 Cisco Substation Automation Reference Architecture



The SA LAN and Security CVD version 2.3.2 utilizes recent developments in the following areas for modern substation automation designs based on architectures with Ethernet-connected endpoints aligned with the IEC 61850 standard recommendations:

- An evolution in network resiliency protocols with the availability of:
  - High-Availability Seamless Redundancy (HSR) singly-attached node (SAN)
  - Parallel Redundancy Protocol (PRP)-HSR dual RedBox
- An evolution of network-based timing with the introduction of:
  - Global Navigation Satellite System (GNSS) and Global Positioning System (GPS) support
  - Precision Time Protocol (PTP) 1588 v2 timing protocol over both PRP LANs (A and B)
- Security advancements with Cisco NetFlow and Stealthwatch for traffic flow anomaly monitoring
- QoS to predictably service a variety of network applications and traffic types
- Validate a recently-introduced industrial Ethernet switch, the Cisco IE 4010, for use in a substation LAN

Configuration details for each technological development are highlighted to aid field engineers with initial deployments and triaging network-related issues.

Disclaimers

- The content of this CVD applies mainly to utilities who have adopted Ethernet-connected intelligent end devices (IEDs).
- Although substation zones are mentioned, this release of the SA LAN and Security CVD version 2.3.2 focuses mainly on enhancements to the ESP zone design.
- Refer to older releases of the solution document for designs relevant to endpoints communicating using serial-based protocols such as Modbus or DNP3.
- If you do not have access to any of the Cisco SalesConnect links in Related Documentation, page 76, ask your Cisco account team to help provide you with the documentation. However, some of the documents require a non-disclosure agreement (NDA) with Cisco.

Introduction

The SA LAN and Security CVD version 2.3.2 is an update that describes developments to Cisco validated substation automation solution architectures. The purpose of the solution release associated with this document was to further enhance the electrical utility substation automation design and implementation experience by leveraging recently-added hardware and software capabilities on the Cisco Industrial Ethernet (IE) switching product line.

Prerequisite Knowledge

To fully comprehend the information in this document, you should:

- Have a strong foundation in how the utility operational technology (OT) world functions
- Be familiar with relevant utility industry standards and mandates, such as IEC 61850 and NERC CIP

What is Substation Automation?

Substation Automation is an intelligent electrical delivery system integrated with communications and information technology to enhance grid operations, improve customer service, lower costs, and help enable new environmental benefits. The Cisco advanced substation automation solution describes how to use the utility network to monitor and manage electrical systems from power generation, through transmission and distribution, to end users in smart buildings, smart homes, and other sites connected to the electrical utility network.

Cisco Substation Automation Solution release 1.5 addressed the following use case scenarios:

- Substation automation with and without IEC 61850 GOOSE messaging
- Substation automation, including phase measurement units (PMUs)
- Physical security (video surveillance and access)
- Remote workforce management (wired only)
- Precise timing distribution
- Remote engineering access to substation devices
- Network management

Cisco Substation Automation Solution release 2.2.1 covered the following security topics:

- Restricting access

- Protecting data
- Logging events and changes
- Monitoring activity in the substation

Cisco Substation Automation Solution release 2.3.1 focused on:

- High Availability (HA) in the ESP zone topology with PRP and REP
- GOOSE validation
- Dying Gasp
- Cisco CGR2010 4G/LTE offload
- CIP zone badge reader
- PTP in LAN
- Firewall redundancy

Ethernet-Based Substation Automation Implementation Benefits

Substation automation goes beyond traditional supervisory control and data acquisition (SCADA) to help provide added capabilities and information that can further improve operations and maintenance, increase system and staff efficiencies, and leverage and defer major capital investments.

An intelligent communications network is a foundation to building a smart grid. Utilities are investing in communications networks to improve their situational awareness of grid assets in order to control, automate, and integrate systems. Value is created when utilities “smooth out” peak load demand, forgo the use of costly spinning reserves, and alleviate the need for long-term capital investments in new generation plants and other capital investments such as reconducting for capacity improvement.

Cisco believes that substation automation is a key first step to achieving a smarter grid. The grid must be observable and measurable before it can be controlled and automated. Substation automation helps utilities add sophisticated protection and control functions while also providing greater visibility into the performance and health of grid infrastructure.

Ethernet Evolution and Standardization for Utilities

In order to integrate substation protection, control, measurement, and monitoring applications, new communication protocols have been developed and standardized under the umbrella of International Electrotechnical Commission (IEC) 61850, Communication Networks and Systems in Substations. These protocols leverage and build upon already existing Ethernet standards.

Legacy serially-connected devices now have modern Intelligent electronic device (IED) counterparts available with Ethernet ports that implement these new protocols. IEDs typically contain multiple protection, control, monitoring, and communication functions.

One specific IED that warrants special consideration because of its unique latency requirements is the phasor measurement unit (PMU). PMUs are devices capable of measuring voltages and reporting data. PMUs are used to help synchronize grid devices to ensure phase imbalance does not occur across segments of the power grid.

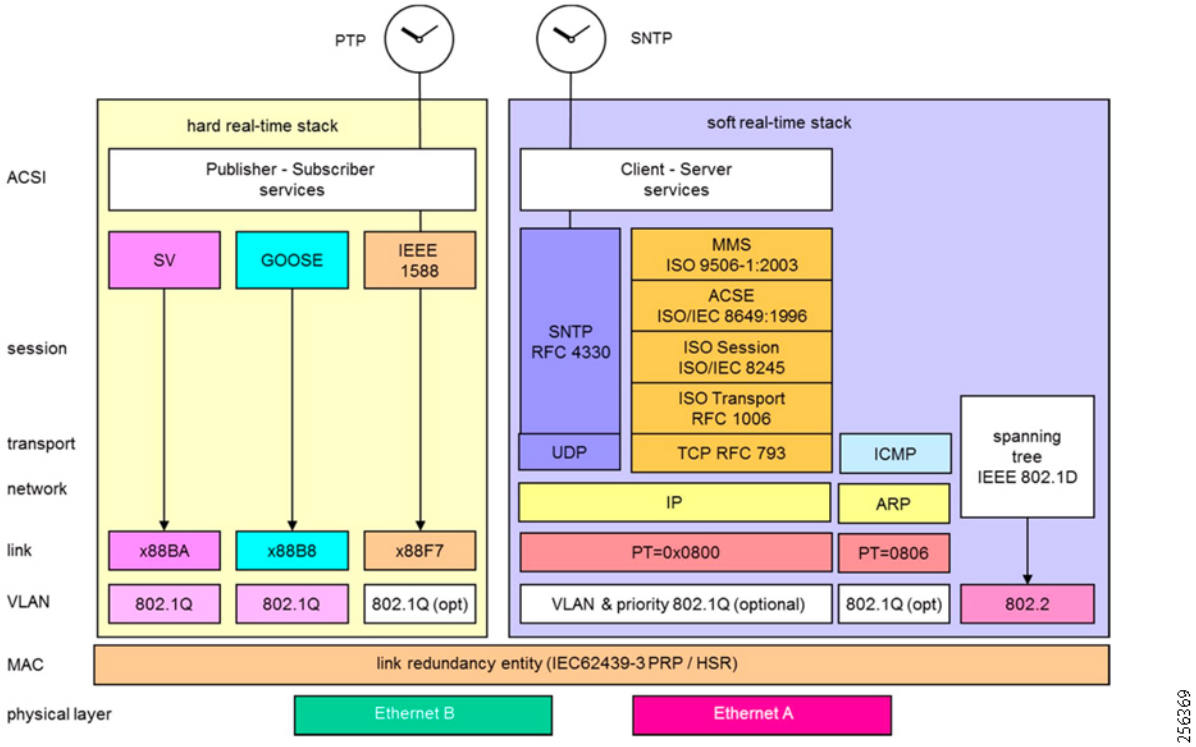
IEC 61850 Goals

IEC 61850, a set or over 25 standards and technical reports (TRs), has been adopted by many electrical utilities around the world. The Utility Communications Architecture International Users Group (UCA IUG) that developed the standards did so with a desire for interoperability (between devices and systems), ease of configuration (allocation of functions to devices), long term stability (layered, object-model based design), and extensibility.

IEC 61850 Protocol Stack

The IEC 61850 protocol stack defines a network architecture for the substation LAN. Figure 2 shows the basic IEC 61850 protocol stack as derived from IEC-61850-90-4 Ed1.

Figure 2 IEC 61850 Protocol Stack



The IEC 61850 protocol stack is divided into a hard-real time stack supporting the services of Sampled Values (SV), Generic Object-Oriented Substation Events (GOOSE), and the Precision Time Protocol (PTP). The IEC 61850 protocol stack also offers a soft real-time stack supporting the network time synchronization SNTP, the manufacturing message specification (MMS) communication and ancillary services mentioned in IEC 61850-8-1. These protocols rely on the services of the Media Access Control (MAC) layer, which may support 802.1Q VLANs and priorities and redundancy.

Cisco Alignment to IEC 61850 Standards

Considering the importance of IEC 61850 and the alignment of many utilities around the globe to the standards' recommendations, Cisco decided it was important to be actively involved in some of the standard body's technical working groups. Cisco also participates in conformance and interoperability testing conducted by the UCA IUG membership (composed of end users and vendors). Cisco substation automation architectures align with the IEC 61850 modern substation standards recommendations.

New Developments for Substation Automation

The capabilities offered by the Cisco SA LAN and Security solution have evolved since the previous validation effort. This version of the SA LAN and Security CVD version 2.3.2 emphasizes some of the more significant developments since the validation cycle of late 2016:

- An evolution in network resiliency protocols with the availability of:

  - High-Availability Seamless Redundancy (HSR) singly-attached node (SAN)
  - Parallel Redundancy Protocol (PRP)-HSR dual RedBox
- An evolution of network-based timing with the introduction of:
  - Global Navigation Satellite System (GNSS) and Global Positioning System (GPS) support
  - Precision Time Protocol (PTP) 1588 v2 timing protocol over both PRP LANs (A and B)
- Security advancements with Cisco NetFlow and Stealthwatch for traffic flow anomaly monitoring
- QoS to predictably service a variety of network applications and traffic types
- Validate a recently introduced Industrial Ethernet switch, Cisco IE 4010, for use in a substation LAN

This document starts with an overview of Ethernet in the electronic security perimeter (ESP) zone, explores some challenges associated with Ethernet-based substation automation implementations, and then expands on how Cisco technological advancements can help overcome these challenges.

A new industrial switch has since been built by Cisco, namely the Cisco Industrial Ethernet (IE) 4010. Similar to the Cisco IE 4000, the Cisco IE 4010 boasts a robust feature set applicable to many industries. It differs from the Cisco IE 4000 in form factor. There are differences in resilient protocol support, the details of which will be covered later in this document. The Cisco IE 4010 is at a better price point for those customers who do **not** need all of the high-bandwidth and timing capabilities of the Cisco IE 5000.

This document then explores the addition of High-Availability Seamless Redundancy (HSR) single attached node (SAN) protocol. If a customer decided to jointly implement HSR and Parallel Redundancy Protocol (PRP) lossless protocols, Cisco now offers the capability for some IE switches to serve as dual RedBoxes (that can bridge HSR and PRP networks). This section also examines the pros and cons for PRP verses HSR, since resiliency protocols are not created equally. Each has advantages and disadvantages.

An evolution of network timing functionality on Cisco IE switches has also occurred since the validation from late 2016. Cisco IE 5000 switches now support GNSS and GPS via the onboard receiver. Native GNSS and GPS capabilities on a Cisco IE 5000 switch alleviates the need for procuring and maintaining external clock sources in the substation automation environment, a capability that can save money particularly in greenfield deployment scenarios. The GNSS and GPS receiver allows the Cisco IE 5000 to directly act as a Precision Time Protocol (PTP) 1588 v2 grandmaster (GM) for the substation LAN and the Cisco IE 5000 can directly provide PTP 1588 v2 power profile to the intelligent end devices (IEDs) that require a high-precision, network-based timing input.

The Cisco solution now supports and recommends the deployment of PTP 1588 v2 over both PRP LANs and PTP frames will be protected like other protocol traffic.

This document then explores security advancements with the evolution of Cisco NetFlow support (beyond just NetFlow-lite). Cisco Stealthwatch can now leverage Cisco NetFlow for Layer 3 and higher traffic visibility. Stealthwatch provides anomaly detection of Layer 3+ traffic flows on Cisco IE switches.

The document ends with design considerations for the Cisco substation automation solutions by reviewing quality of service (QoS). QoS is what facilitates the network to predictably transport a variety of network applications and traffic types with service differentiation.

New Software Feature Support Matrix

The SA LAN and Security CVD version 2.3.2 of the solution has the features and recommended hardware platform combinations shown in Table 1.

Table 1 SA LAN and Security CVD 2.3.2 Feature Matrix

Feature	Cisco IE Switches	Cisco IOS Software
PRP RedBox PTP over PRP	Cisco IE 2000U Cisco IE 4000 Cisco IE 4010 Cisco IE 5000	15.2.6E2a
HSR Single Attached Node RedBox (SAN)	Cisco IE 4000 Cisco IE 4010 Cisco IE 5000	15.2.6E2a
HSR to PRP Dual RedBox	Cisco IE 4000	15.2.6E2a
GNSS/GPS Receiver PTPv2 GM	Cisco IE 5000	15.2.6E2a
Cisco IE Switch Embedded Device Manager	Cisco IE 4000 Cisco IE 4010 Cisco IE 5000	15.2.6E2a
Cisco NetFlow Security	Cisco IE 4000 Cisco IE 4010 Cisco IE 5000	15.2.6E2a

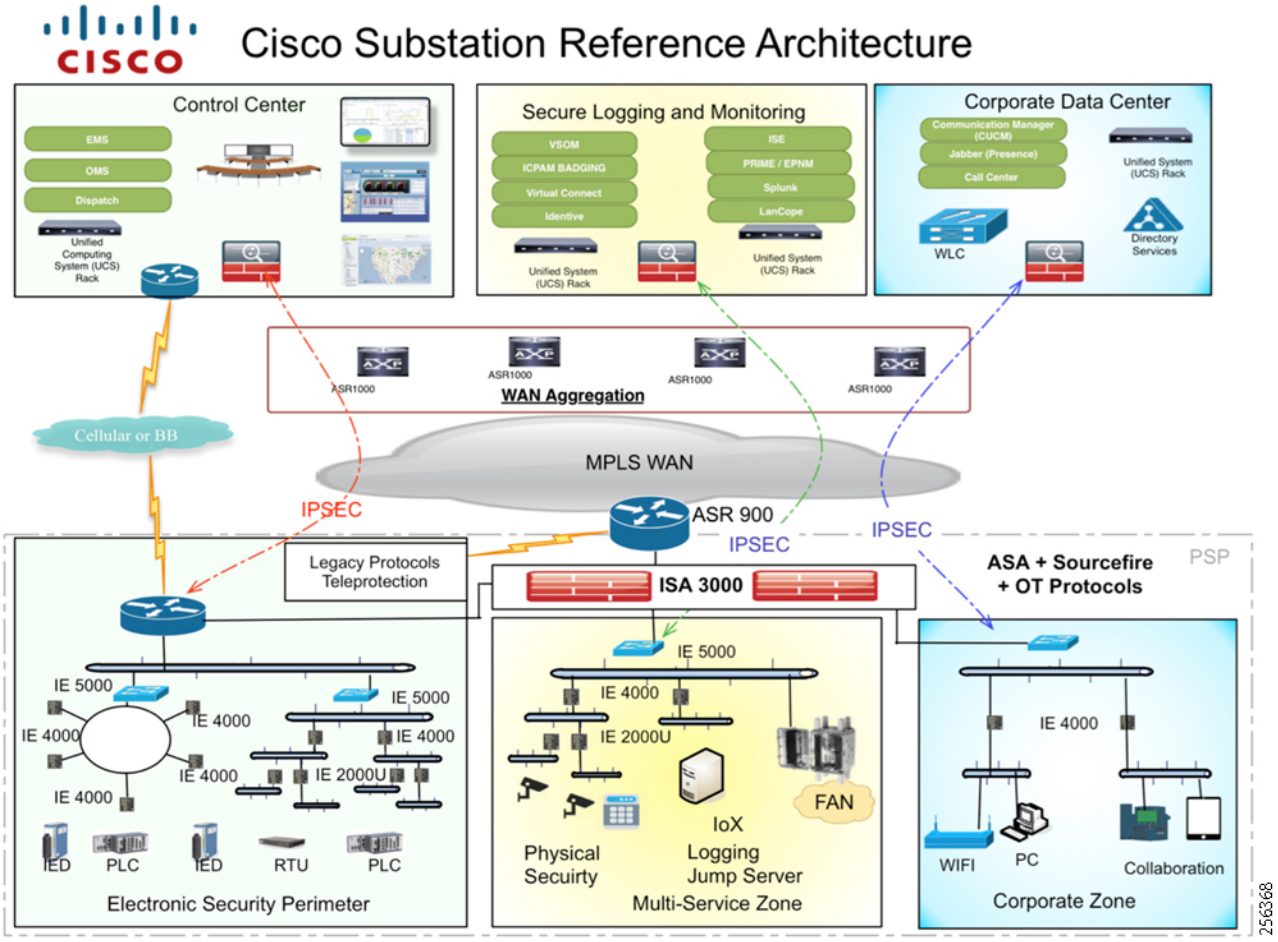
Summary

The SA LAN and Security 2.3.2 CVD builds on previous solution releases through new technology validations in Cisco solution labs in the areas of the Cisco IE 4010 switch, new IOS software release 15.2.6E2a for Cisco IE switches, and new software features related to resiliency, timing, and security. This CVD helps to provide guidance on where the new technology fits in the Cisco overall substation automation solution. This new technology can enhance the design and deployment of a substation automation network by Cisco.

Cisco IEC 61850 Substation Architecture

A modern electrical utility network overall is a distributed environment wherein the grid operators and controllers are **not** located physically within a substation. Utility operators in fact typically work from a remote operations and control center connecting across a wide area network (WAN) infrastructure. Refer to the Cisco substation reference architecture in Figure 3.

Figure 3 Cisco Substation Automation Reference Architecture



The WAN is an extension of the utility enterprise environment. The WAN can be privately owned by the utility or the utility may procure a leased line service over a service provider network. This results in a unique design where a Demilitarized Zone (DMZ) is required at the substation edge. All communications into and out of the substation network must pass through the DMZ firewall. The zone traffic egressing the substation edge should be encrypted using IPSec and separated into separate, logical networks using Layer 3 Virtual Private Network (L3VPN) technology.

Substation automation network design best practices by Cisco include a recommendation to separate L3VPNs for zone traffic traversing the WAN. This allows a shared infrastructure to carry zone traffic over common physical but logically separated networks. Multi-protocol Label Switching (MPLS) in the utility-owned private WAN or leased line services from a service provider help enable this model. This aligns with Cisco security recommendations for segmentation.

The DMZ firewall at the substation edge helps provide controlled access into substations. It also provides segmentation and separation between substation zones. The substation LAN environment, as specified in IEC 61850 standards, comprises three functional component blocks or zones:

- Multiservice
- Corporate Substation
- Electronic Security Perimeter

Multiservice Zone

The Multiservice Critical Infrastructure Protection (CIP) zone contains physical security components like Ethernet-connected badge readers, video surveillance cameras, local authentication, authorization, and accounting (AAA), and logging applications. If remote access from a control center into the substation ESP zone is required, Cisco recommends that a jump server, or a computer used to manage devices in a separate security zone, be installed in the multiservice zone. The multiservice zone is a likely location for security applications such as Cisco Identity Services Engine (ISE), Splunk, and downstream utility applications requiring services such as an application gateway or broker functions. Segmentation of these applications and services is highly recommended even within this zone and it can be achieved with virtual LAN (VLAN).

Corporate Substation Zone

The Corporate Substation (CorpSS) zone is an extension of the corporate network in the substation. It is where wireless Ethernet connectivity (Wi-Fi), voice services, and general Ethernet connectivity for employees to access email, web, or the Internet (via the central site) are provided. This is an extended enterprise located remotely within the substation. This zone is the least secure zone and includes devices and services such as IP phones, video end points, and Wi-Fi connected or hardwired PCs for corporate applications.

Electronic Security Perimeter Zone

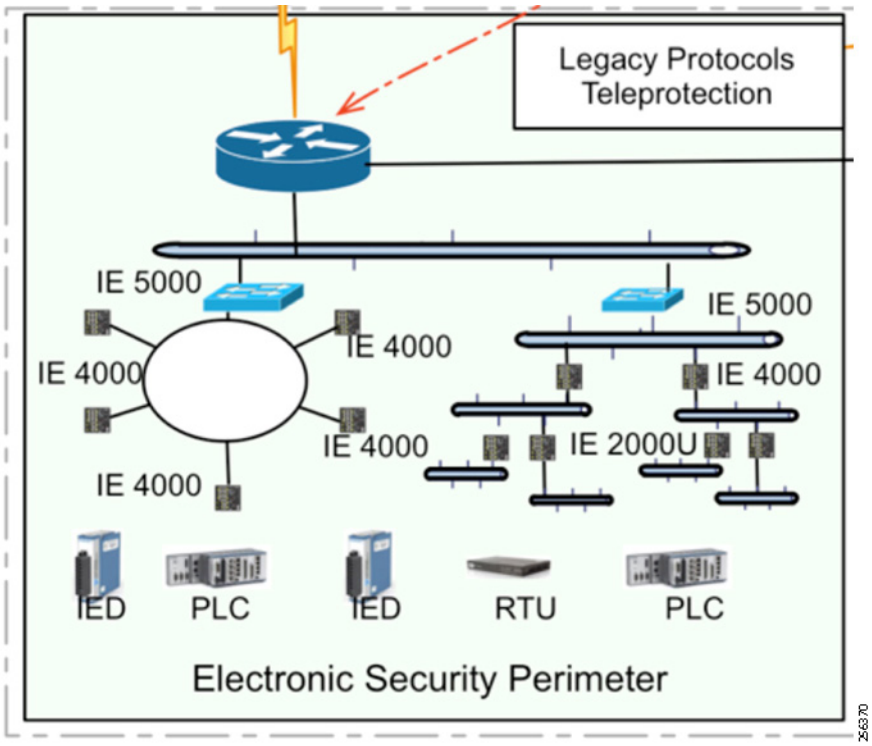
The Electronic Security Perimeter (ESP) zone includes all grid operations infrastructure and is the highest security zone. It is highly recommended that this be further segmented by application such as SCADA, protection services, transformer ops, and so on. The ESP is the most critical zone in the substation and requires the highest level of security and availability. One method of achieving Ethernet network segmentation is with VLANs terminating at the substation edge firewall.

Deployment models are typically based on the size of the substation's ESP zone. Substation IEDs can connect to Cisco IE switches built in one of a variety of topological options, namely hub and spoke, ring, or tree. Cisco offers high-availability redundancy mechanisms such as Resilient Ethernet Protocol (REP), Parallel Redundancy Protocol (PRP), and Highly-Available Seamless Ring (HSR). Choice of the topology style and redundancy protocol will depend on application requirements. Redundancy and resiliency are described in more detail later in this CVD.

Electronic Security Perimeter Zone

The Electronic Security Perimeter (ESP) is the zone where critical utility monitoring and controlling infrastructure reside. Devices like remote terminal units (RTU), Intelligent Electronic Devices (IED), programmable logic controllers (PLCs), relays, and so on reside within the ESP zone. The ESP Zone contains the station and process buses as defined by IEC 61850 standards. See Figure 4 for a depiction of a Cisco ESP zone reference architecture.

Figure 4 Cisco ESP Zone Reference Architecture



Station Bus

The station bus connects the entire substation and helps provide connectivity between central management and individual bays. The station bus connects IEDs within a bay, distributed controllers, and human machine interfaces (HMIs). It connects bays to each other and connects bays with the gateway/gateway router. It may connect up to hundreds of IEDs, often segmented physically or logically, based on communication parameters or application/purpose.

Process Bus

The process bus connects primary measurement and control equipment to the IEDs. The process bus conveys unprocessed power system information (voltage and current samples and apparatus status) from the switch-yard source devices—such as current transformers (CTs), potential transformers (PTs), data acquisition units (DAUs), and merging units (MUs)—to the IEDs and relays that process data into measurements and control and protection decisions.

Typically, the process bus is limited to a bay, however busbar protection and differential protection traffic might span multiple bays.

ESP Traffic Classes Per IEC 61850

The following are the traffic class definitions as taken from IEC-61850-107D C160 9073 EB38 A493 0266 7153 D440 18AD 53F4 Ed1:

> [Manufacturing Message Specification] MMS traffic defined in IEC 61850-8-1, which allows an MMS client such as the SCADA, an OPC server or a gateway to access 'vertically' all IED objects. This traffic flows both on the station bus and on the process bus, although some process bus IEDs do not support MMS. The MMS protocol is a client-server (unicast) protocol operating at the network layer (Layer 3). Therefore, it operates with IP addresses and can cross routers. In one operating mode, the MMS client (generally the SCADA or the gateway) sends a request for

a specific data item to the MMS server of an IED, identified by its IP address. The server returns the requested data in a response message to the IP address of the client. In another mode, the client can instruct the server to send a notification spontaneously upon occurrence of an event.

[Generic Object Oriented Substation Events] 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. GOOSE uses short informational messages and GOOSE requirements specify a low probability of loss and a budget delay of only a few milliseconds.

The Sampled Values protocol (SV; specified in IEC 61850-9-2) 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, for instance, for busbar protection and phasor measurement.

ESP Traffic Requirements

As per the IEC 61850-8-1 standards, GOOSE uses publisher/subscriber communications for time sensitive and critical communications. GOOSE is a control model in which any format of data (status, value) is grouped into a data set and transmitted. GOOSE data is directly embedded into Ethernet data frames and includes mechanisms to help ensure transmission speed and reliability.

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. GOOSE uses short informational messages and GOOSE requirements specify a low probability of loss and a budget delay of only a few milliseconds.

GOOSE is one of the IEC 61850 traffic types within the substation that is time sensitive in nature and requires low-latency forwarding. It uses well known EtherType of 0x88b8 for easy identification and classification within the Layer 2 domain. SV packets, on the other hand, use a well-known EtherType of 0x88bA.

GOOSE traffic can deal with some jitter or some delay in interarrival time. GOOSE can have a slightly lower priority treatment when compared to SV traffic (also Layer 2 multicast).

IEC 61850 prescribes that GOOSE and Sampled Values (SV) frames are priority-tagged using a VLAN ID of 0, marked by IEDs, in order for the network to use PCP for classification and help provide preferential treatment. IEEE C37.238-2011 mandates the use of VLAN tags. Future revisions may make VLANs optional. Defaults for GOOSE, SV, and C37.238-2011 are priority-tagging with priority code point (PCP) value of 4.

IED QoS priority markings are assigned at the power systems engineering stage and recorded in the substation configuration description (SCD) file. Consider the impact to engineering design if the network decides to remark QoS values.

There are multiple types and classes of GOOSE traffic that have latency requirements ranging from 3ms to 100ms. IEC 61850-90-4 QoS classification states that GOOSE frames for tripping and inter-tripping should have high priority. GOOSE frames for interlocking should have medium priority. Finally, other GOOSE frames like heartbeats and analog values should be assigned medium priority.

Table 2 highlights the different GOOSE, SV, MMS, and time synchronization messages along with details that can help distinguish their application and communication requirements.

Table 2 IEC 61850 Protocols and Requirements

Communication Bus	Function Type/Message		Protocol	Max Delay	Bandwidth	Priority	Application
Process	1A. Trip	GOOSE	Layer 2 Multicast	< 3 msecs	Low	High	Protection
Process	1B. Other	GOOSE	Layer 2 Multicast	< 200 msecs	Low	High	Protection
Process and Station	2. Medium Speed	MMS	IP/TCP	< 100 msecs	Low	Medium Low	Control
Process and Station	3. Low Speed	MMS	IP/TCP	< 500 msecs	Low	Medium Low	Control
Process	4. Raw Data	SV	Layer 2 Multicast	< 208.3 msecs	High	High	Process Bus
Process and Station	5. File Transfer	MMS	IP/TCP/FTP	< 1000 msecs	Medium	Low	Management
Process and Station	6. Time Sync	Time Sync	PTP (Layer 2)		Low	Medium High	General Phasors, SV
Station Bus	7. Command	MMS	IP		Low	Medium Low	Control

Protocol Locations in Station Bus and Process Bus

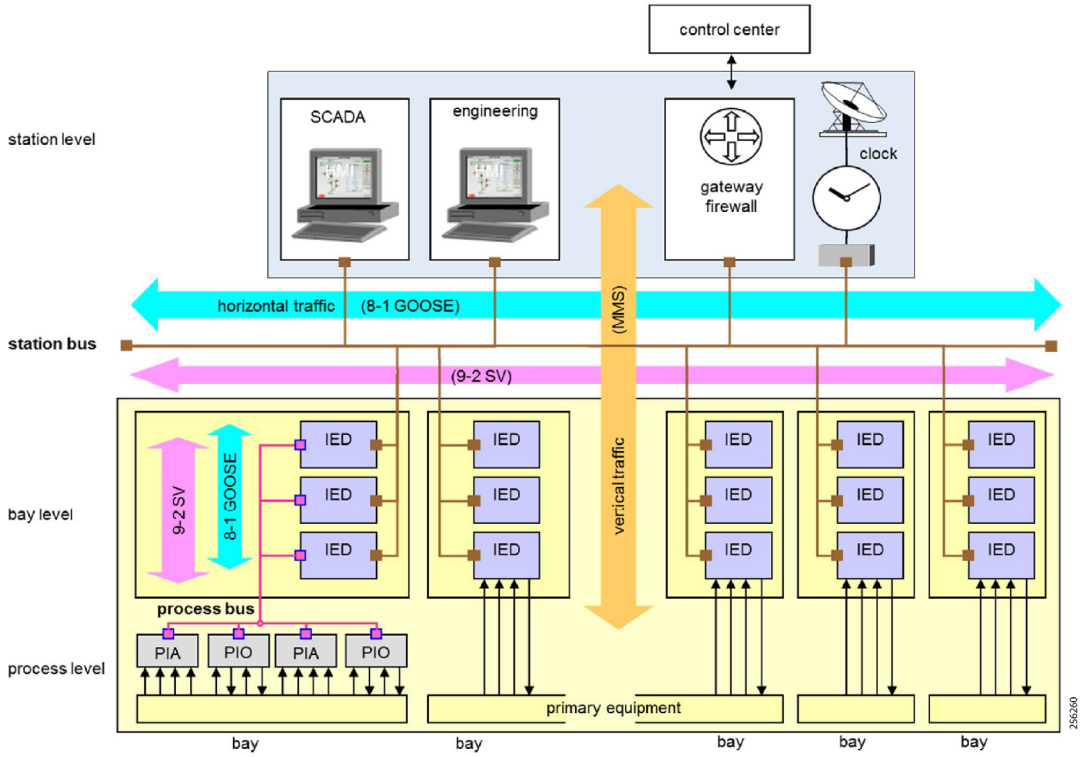
The protocols typically found on a station bus include GOOSE (Layer 2 multicast), MMS, SNTP, SNMP, FTP, and others (Transmission Control Protocol—TCP/IP or User Datagram Protocol—UDP/IP Layer 3 unicast).

The protocols found on a process bus are SV (Layer 2 multicast), sometimes GOOSE (Layer 2 multicast), and often MMS (Layer 3 unicast) traffic. The infrastructure connecting process bus devices is expected to provide real-time quality of service to critical traffic.

There is no hard requirement forcing SV traffic out of the station bus; in fact bus-bar protection might dictate the need for SV traffic in the station bus. If this is the case, QoS would need to be in place to preserve the lower jitter and latency tolerance of such SV traffic in the station bus.

Figure 5 is derived directly from IEC 61850 standards and illustrates where in the station and process buses you would typically find MMS, GOOSE, and SV traffic.

Figure 5 Where to Find MMS, GOOSE, and SV in Station and Process Bus



Combining the Station Bus and Process Bus

While it is possible to fit station bus and process bus into one network structure from a networking perspective (if sufficient bandwidth is available, such as 1 Gbit/s or higher), it is prudent to separate them for various reasons. For instance, consider separating buses to reduce station bus load due to chatty application traffic on the process bus. If you must combine them, think about avoiding single points of failure when coupling process and station buses.

Refer to IEC 61850-90-4 for additional details, including many possible topology design options.

Summary

The traffic flows in the substation are modeled on the 61850 standards. GOOSE and SV traffic demand high priority treatment and low latency requirements. GOOSE data has latency requirements in the 3-100 msec range, while Sample Values are in the 3-10 msec range. Timing is also extremely important when transported within and between substations. Network-based timing can be carried across the station over Ethernet using the IEEE-based Precision Time Protocol 1588 v2 (PTP v2).

Given this summary of the basics about utility substation automation Ethernet-connected applications and advantages in an Ethernet-based substation design, what are some of the main challenges that need to be overcome in order to design an efficient Ethernet-based substation ESP network?

Challenges in Substation ESP Design

This section explores some of the main challenges that need to be overcome to design an efficient substation automation ESP zone, including:

Challenge 1—Latency and Jitter

The first challenge is to design for low latency. Latency is directly impacted by buffering in the network. Buffering happens when links are oversubscribed and congested. Latency therefore correlates to bandwidth availability and quality of service.

Cisco offers different Industrial Ethernet switches with varying interface bandwidth capacities. Do your applications require 10 Mb Ethernet connections? What about 100 Mb? Have you analyzed the bandwidth consumption once application traffic is enabled?

At Layer 2, latency is kept to a minimum because switches are designed to forward frames using hardware lookups. Layer 3 boundaries (where routing comes into the picture) add software lookups and buffering, hence traffic crossing a Layer 3 boundary will incur a higher latency. Layer 2 traffic that is restricted within a local substation zone will experience much lower latency than traffic that needs to cross a Layer 3 boundary (through the DMZ).

Jitter is variation in the latency or inter-arrival time of frames/packets. Assuming you complete your capacity planning activity, what happens if and when link oversubscription occurs? Not all traffic is sensitive to latency and jitter, meaning not all traffic classes require the lowest possible latency. Are the important traffic classes being offered preferential treatment via QoS classification, marking, and prioritization?

In summary, to deal with low latency, choose network switches that offer a high enough bandwidth capacity for your applications and design a proper QoS model that offers differentiated services in order for higher priority traffic to be passed through your network before medium and lower priority traffic. With the help of a well-planned QoS design for packets granted the same treatment, latency should not vary much between one frame/packet and the next. Hence, jitter would be kept to a minimum.

Challenge 2—Fast Convergence

The second challenge is to design for fast convergence. Convergence is all about recovery time; how long does it take for your traffic flows to recover in the event of a link or node failure.

As discussed, certain applications and protocols have differing latency requirements. Note what makes ESP traffic latency requirements more difficult to achieve is that if there ever was a network outage due to a link or node failure, the ESP traffic is still expected to abide by the protocol requirements. Convergence needs to be as fast as possible because convergence events will add latency when a failure occurs.

Protocol selection should be based on the most demanding application's requirements in the substation's ESP zone. A summary of resilient protocol convergence performance times is provided in Table 3.

Table 3 Resilient Protocol Convergence Performance

Protocol	Typical Convergence Time
RSTP	Milliseconds to seconds

Table 3 Resilient Protocol Convergence Performance (continued)

Protocol	Typical Convergence Time
REP	50 - 250 milliseconds
PRP	0 milliseconds (lossless)
HSR	0 milliseconds (lossless)

Challenge 3—Scale

The third challenge is to design for scale. From a pre-emptive planning perspective, a network can be designed for scale and protected from oversubscription with a proper traffic segmentation model. Knowing that substation traffic like GOOSE and SV are Layer 2 multicast traffic types, which effectively behave like a Layer 2 broadcast, it is important to consider which GOOSE/SV endpoints need to subscribe to one another and hence need to "listen" to each other's traffic. Scale can be planned using:

- VLANs—Assign VLANs to limit broadcast storms. Assign switch access ports to a VLAN and only devices on the same VLAN would ever receive the traffic from devices on the same VLAN. Note that the intelligent end devices themselves may have the ability to natively define the VLAN so that traffic egressing is already marked. Ports on the switches need to understand and look for the VLAN headers by configuring them as dot1q trunk ports.
- Multicast filtering—Layer 2 access lists can be implemented that filter and only allow traffic with specific Layer 2 multicast addresses. Insight into what multicast addresses are in use and for which devices across the network is critical to create meaningful access lists.

Cisco utility substation automation designs recommend the network administrator consider both methods of planning for scale.

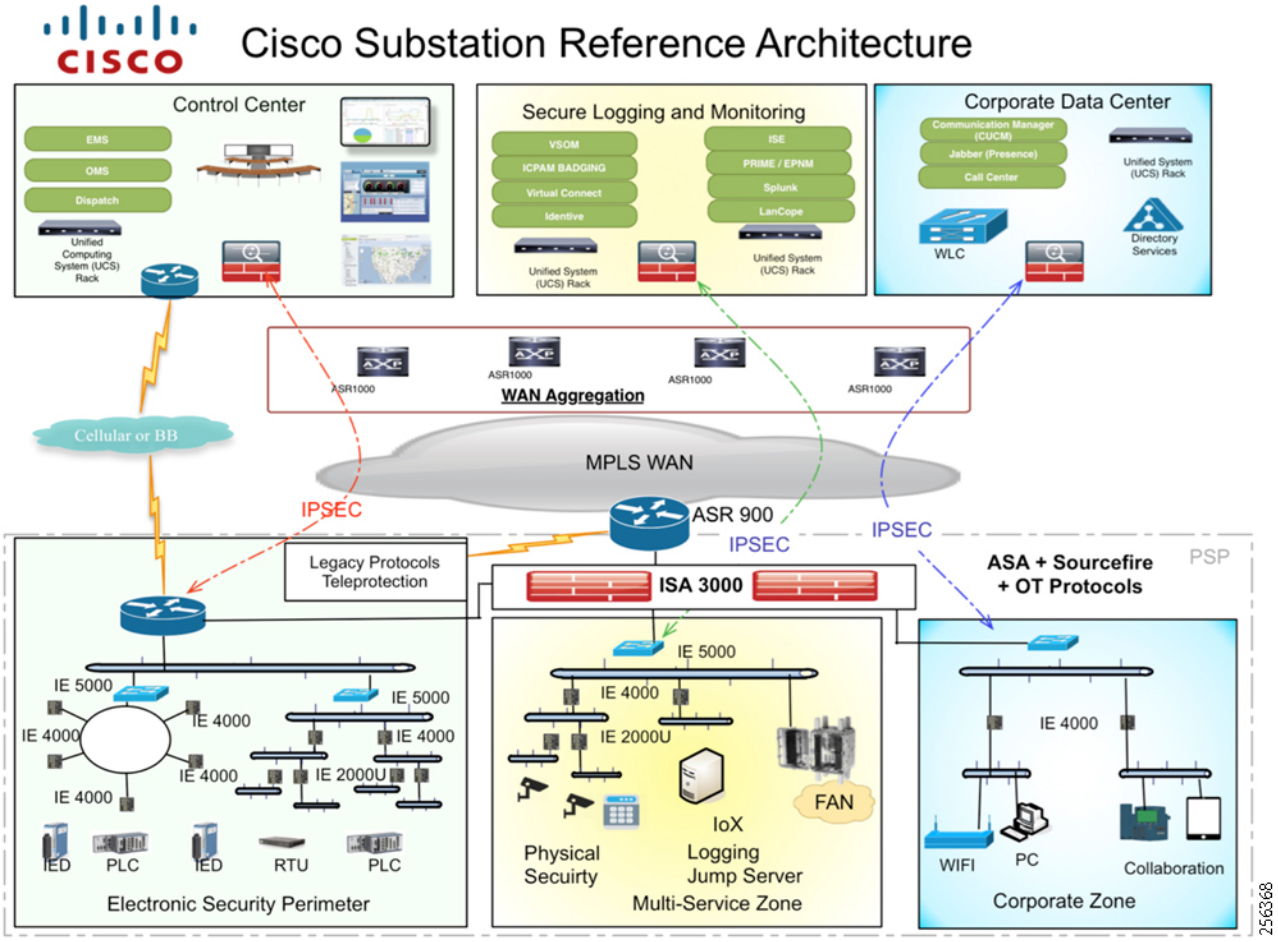
One might think scale can be resolved by adding more equipment into the infrastructure. Adding more equipment with more ports is fine for scaling available access ports for device connectivity, but do not lose sight of what happens to all of the access traffic as it traverses the zone between switches. The appropriate amount of bandwidth should be available at aggregation points to allow the traffic through.

Some protocols have a limit in terms of recommended number of nodes participating. Ring size will ultimately be impacted by the recommendations for each protocol. Consider the protocols in use, the amount of traffic for each application flow, and factor this information into your ring size planning activities.

Challenge 4—Security

The forth challenge is to design for security. Security can be achieved using traffic segmentation.

Figure 6 Cisco Substation Automation Reference Architecture



Referring to the reference architecture in Figure 6, Cisco recommends that the substation network be segmented in the following ways:

- Zones—At this point, the CVD already highlighted the need for separation of functional zones (multiservice, CorpSS, and ESP zones). Extended enterprise and other traffic should never mix with the critical (ESP) grid monitoring and controlling application traffic.
- Inside the ESP zone, Layer 2 traffic can and should be separated by VLAN.
- Beyond the ESP zone Layer 2 boundary, a router or firewall can encrypt outgoing traffic and map logically-segmented traffic zone traffic destined to the control center.

Storm control, a Layer 2 network security protocol, prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when frames flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.

Be mindful when implementing security protocols that the effectiveness quickly diminishes should any devices or network switches lack support for the security protocols. Utilities with mixed vendor deployments cannot fully implement a single vendor's proprietary technology. Hence, mixed vendor environments are limited to implementing industry standard protocols on all devices.

For Layer 3 traffic in the ESP zone (for example, MMS, Modbus TCP, and DNP3 IP), consider enabling features like Cisco NetFlow and leveraging security applications like Stealthwatch. CIsco NetFlow aides Stealthwatch to provide anomaly detection within the ESP zone because Cisco NetFlow helps provide visibility into the traffic traversing the zone's

infrastructure. Stealthwatch can aid with troubleshooting and highlighting abnormal behaviors due to malware infections. With the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000, Cisco NetFlow can be enabled to help provide data flow metrics to Stealthwatch. Stealthwatch takes the flow data from the network then helps offer real-time situational awareness of all users, devices, and traffic. Stealthwatch has many in-built machine learning algorithms that can assist in analyzing all of this data and detecting anomalies in the network.

Challenge 5—Field Serviceability

Devices in the ESP zone are designed to be easily replaceable should the need arise for field maintenance. How do Cisco Industrial Ethernet switches and routers accomplish this?

First, the devices can be configured to send what is called a "dying gasp" to alert the operations team that a critical failure has occurred. A dying gasp is a notification message which signifies a critical event, such as loss of power or a link going down. Dying Gasp notifications are available through Ethernet Operations and Maintenance (OAM) frames, SYSLOG messages, and SNMP traps.

Next, Cisco hardened switches and routers leverage replaceable flash disks containing the software and configuration files necessary for the devices to function. Simply swapping out the flash disks from the old to the new devices helps ensure that the new devices will boot and function exactly like the devices they are replacing.

Challenge 6—Network Management

Utility substation deployments can mimic in size an enterprise branch office deployment, which in total can contain hundreds or even thousands of switches, routers, and security appliances. Network management of large installations can be challenging. To meet these challenges, Cisco provides a robust set of mechanisms referred to as the network management system (NMS) through which the operator configures and monitors the performance of the substation LAN deployment. Several management platform options are available, including Cisco Industrial Network Director (IND), Cisco Prime Infrastructure (PI), and each of the Cisco IE switches that are configurable using an embedded device manager.

During the validation phase of this CVD, the embedded device manager, which is a web-based graphical user interface, was tested as an alternative to the functionality provided by the command line interface (CLI). We recommend using the embedded device manager as an alternative to the CLI in some cases, however not all CLI-available functionality is present in the device manager at this time. See the implementation sections for more details.

Note that Cisco IND and Cisco PI were **not** validated in this release. However, they are both regularly used in Cisco IoT solution validation.

Network management traffic would span between control center and substations, traversing the WAN. A dedicated management L3VPN is recommended to segregate management traffic from other traffic types that travel across the utility's distributed architecture. Once inside the substation, network management traffic should map to a consistent VLAN across the ESP zone. For all network management traffic on IE switches, Cisco recommends that the administrator designate a management port and an IP address for device communication.

This document now examines in more detail how Cisco hardware and software products can help build a better substation automation network by overcoming the ESP zone design challenges.

Cisco Industrial Ethernet Switch Portfolio

This section explores changes in the Cisco IE switch product line.

Cisco offers a variety of switches for the utility substation LAN, from lightly managed, low speed, and low port density products to best-in-class, Layer 2/Layer 3, high port density, high bandwidth, feature rich devices.

- Cisco IE 1000
  http://www.cisco.com/go/ie1000

- Cisco IE 2000U
  http://www.cisco.com/go/ie2000u
- Cisco CGS 2520
  http://www.cisco.com/go/cgs2520
- Cisco IE 4000
  http://www.cisco.com/go/ie4000
- Cisco IE 4010
  http://www.cisco.com/go/ie4010
- Cisco IE 5000
  http://www.cisco.com/go/ie5000
- Cisco Industrial Switch Portfolio At a Glance
  https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-734999.pdf

Common features across the Cisco industrial grade switching product portfolio include:

- IEEE 1613 and IEC 61850-3 Compliant—All go through KEMA third-party validation
- No moving parts
- Advanced IOS Software capabilities with added utility specific functionality
- PoE/PoE+ support on specific models of every switch series
- Layer 2 LanBase or Full Layer 3 IP Services images available
- Common power supplies across product lines
- Redundant power inputs or power supplies
- Extended Power Supply Support (low and high voltage AC/DC supported)
- IEEE 1588 v2 PTP support C37.238 (Power Profile)
- Modbus Memory Map Support (View only statistics)
- -40C to +75C operating temperature support
- Alarm contacts—input and output
- 5-year limited hardware warranty covering all components (including power supplies)
- Swap drives for easy field replacements

Table 4 compares the feature sets of the various Cisco IE switches.

Table 4 Cisco IoT Industrial Switching Portfolio

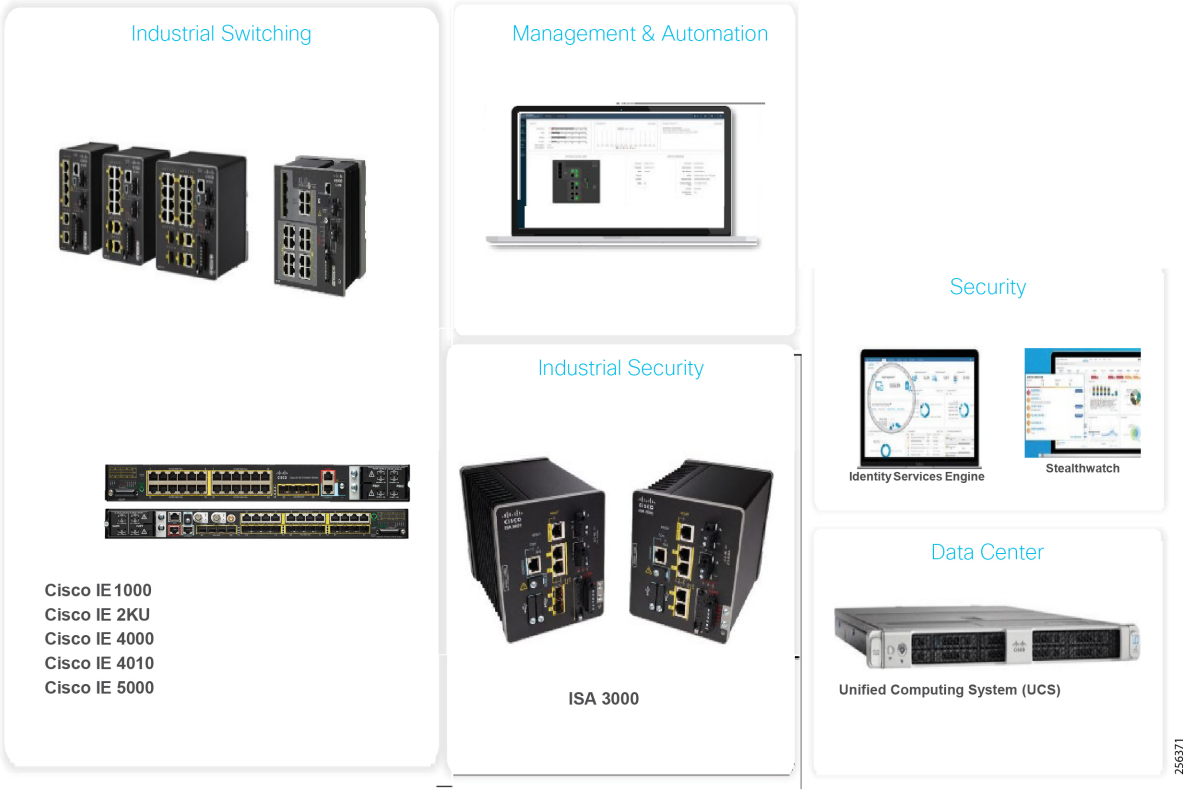
	Cisco CGS 2520	Cisco IE 2000U	Cisco IE 4000	Cisco IE 4010	Cisco IE 5000
Place in the Network	Access	Access	Access or Distribution	Access or Distribution	Access or Distribution
19 Inch Rack-Mount	Yes	No	No	Yes	Yes
DIN Rail-Mount	No	Yes	Yes	No	No

Table 4 Cisco IoT Industrial Switching Portfolio (continued)

QoS	Yes	Yes	Yes	Yes	Yes
Cisco NetFlow	No	No	Yes	Yes	Yes
RSTP	Yes	Yes	Yes	Yes	Yes
REP	Yes	Yes	Yes	Yes	Yes
HSR-SAN	No	No	Yes	Yes	Yes
HSR-PRP	No	No	Yes	No	No
PRP (RedBox)	No	No	Yes	Yes	Yes
PTP Power Profile	Yes	Yes	Yes	Yes	Yes
PTP GM	No	No	No	No	Yes
Embedded Device Manager	Yes	Yes	Yes	Yes	Yes

Figure 7 illustrates the Cisco industrial switching portfolio for utility substation environments. Multiple platforms are available to accommodate various feature requirements. Cisco IND is the management platform that supports the industrial switches in these environments.

Figure 7 Cisco IoT Industrial Switching Portfolio



New Hardware Availability—Cisco IE 4010

This section describes the newest Cisco IE switch, the Cisco IE 4010. The IE designation means this switch is meant to be deployed in non-carpeted, rugged locations that experience extreme high or low temperatures and that require passive cooling capabilities and no internal moving parts.

- The Cisco IE 4010 switch boasts a robust feature set applicable to many industries.
- The Cisco IE 4010 form factor fits into a 19" rack mount (rather than being DIN-rail mounted like the Cisco IE 4000).
- The Cisco IE 4010 is at a better price point for those customers who do **not** need the higher 10 Gbps uplink bandwidth or built-in timing capabilities (GNSS, GPS, and IRIG-B) of the Cisco IE 5000.
- The Cisco IE 4010 comes in a either a 12- or a 24-port configuration with 200 watts of power over Ethernet (PoE) budget usable for IP cameras and access points (APs).
- The Cisco IE 4010 offers 1 Gigabit up/downlinks.
- The Layer 2 and Layer 3 feature sets on the Cisco IE 4010 are similar to the Cisco IE 4000 and Cisco IE 5000 offerings, however there are some differences:
  - Cisco IE 5000 supports PTP GM
  - Cisco IE 4000 supports HSR-PRP RedBox

Deployment Locations for the Cisco IE 4010

Consider deploying the Cisco IE 4010 switch in the following places in the substation automation network:

- Electronic Security Perimeter (ESP) zone
  - Station bus
  - Process bus
- Multiservice zone
  - Physical security and badge-reader connectivity
  - Wireless access point connectivity
- Corporate zone—Providing connectivity to corporate users

ESP Design Challenges the Cisco IE 4010 Addresses

The Cisco IE 4010 was purpose-built with industrial environment demands in mind. It forwards Layer 2 frames using hardware lookups, so Ethernet frames are forwarded with ultra-low latency. With a proper QoS configuration to protect real-time, latency sensitive traffic, latency and jitter should not be a problem as long as traffic stays inside the Layer 2 ESP zone.

The Cisco IE 4010 supports all the variants of fast convergence protocols like RSTP, REP, PRP, and HSR. It supports segmentation using VLANs and multicast filtering. It is one of the platforms that supports Cisco NetFlow collectors and works with Stealthwatch. It supports field serviceability and network management.

Resiliency for Utility Networks

This CVD provides a brief summary of PRP and an in-depth look at HSR. Cisco now offers the capability for some of its IE switches to serve as dual RedBoxes (meaning a RedBox that can bridge HSR and PRP networks).

Legacy Resiliency Protocols

Depending on whether or not a utility decides to fully embrace IEC 61850 design recommendations, several resiliency protocols are available from which to choose. For utilities that need more time before they can migrate the substation implementation to Cisco and IEC 61850-based standards, a few legacy resiliency protocols are available to choose from within ring topology deployments:

- Rapid Spanning Tree (RSTP)—A variant of spanning tree protocol (STP) that is known, used, and trusted by IT professionals who have previously used Cisco switches.
- Resilient Ethernet Protocol (REP)—A Cisco proprietary protocol described in Resilient Ethernet Protocol.

Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) is an evolution of the STP IEEE 802.1D standard. Like its predecessor, RSTP creates spanning-tree instances. RSTP addresses many convergence issues that existed with STP. The CPU and memory requirements are higher than what is needed for 802.1D. RSTP speeds the recalculation of the spanning tree when the Layer 2 network topology changes. It does so by immediately changing a blocked port to a forwarding state without waiting for the network to converge. RSTP can achieve much faster convergence in a properly configured network. RSTP is compatible with STP networks.

Cisco IE switches support RSTP. RSTP, however, takes on the order of milliseconds (at best) to seconds (at worst) to converge in the event of a link or a node failure in the ring topology.

Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) is a Cisco-proprietary protocol designed to meet fast convergence requirements in a large scale, Layer 2 network, particularly for ring topologies. REP avoids the need for Spanning-tree in simple ring-based topologies and is designed to operate with standard Ethernet hardware. REP is implemented on Cisco Connected Grid (CG), Industrial Ethernet (IE), and Carrier Ethernet (CE) platforms. It delivers fast and predictable convergence in a ring topology with convergence typically in the 50 - 250 msec range in most cases. It is deterministic, scalable, and it coexists with spanning tree. An industry standard protocol, G.8032, was later derived from REP.

Other Resiliency Protocols

When following IEC 61850 implementation standards in the station bus and process bus, high performance applications in the utility substation mandate a number of key requirements that should be addressed. The substation architecture must meet design requirements for GOOSE and Sample Values, both of which are multicast traffic types. This includes high availability (HA) and topology choices to meet scale, segmentation, and communications requirements. IEC 61850-5 provides guidance for HA and communication requirements. There are two choices:

- Parallel Redundancy Protocol (PRP) supports either tree or ring topologies with no limits on node counts and it can deliver a zero msec failover/recovery requirement. However, PRP has one drawback. PRP requires duplicate LANs (named LAN-A and LAN-B) and double the networking equipment hardware.
- Highly Available Seamless Ring (HSR) also delivers a zero msec fail-over/recovery requirement but is only available in a ring topology. HSR scales to a limited number of devices based on application bandwidth requirements. HSR does **not** require duplicate LANs (double the switching infrastructure) in the ESP.

Protecting the Resilient Network With Storm Control

With HSR and PRP resiliency protocols, Cisco recommends protecting the network from storms as they can very quickly multiply even faster considering the packet replication that occurs by applying a redundancy feature. Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance.

How Lossless Resiliency Protocols Solve ESP Design Challenges

Lossless resiliency protocols like PRP and HSR ultimately help ensure that critical, real-time traffic in the substation ESP zone gets delivered in time, even in the event of a network failure. An Ethernet link or an entire switch can suffer downtime without leading to any overall loss of critical application traffic. Hence, latency requirements are maintained.

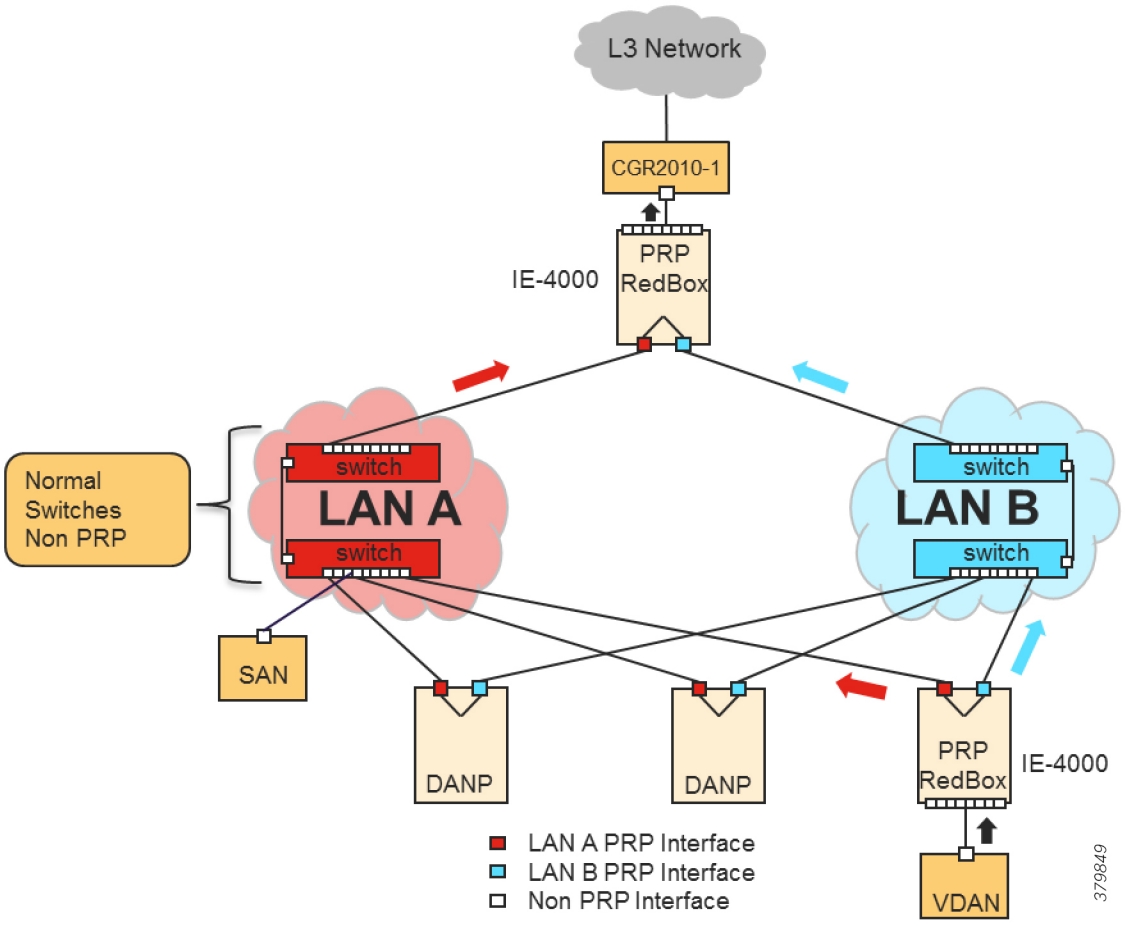
PRP Support on Cisco IE Switches

This section of the SA LAN and Security CVD version 2.3.2 is meant to help provide a brief refresher on PRP, as the Cisco PRP implementation has evolved since the previous CVD release was published. It first covers PRP basics and then looks at what has changed.

PRP is defined in International Standard IEC 62439-3 Clause 4 and PRP is deployed in Ethernet environments that require lossless redundancy for applications on occurrence of a link or node failure.

PRP helps offer redundancy by connecting IEDs and Cisco IE switches to two independent parallel networks called LAN-A and LAN-B. The connections to LAN-A and LAN-B require two separate interfaces at the connecting device, which is known as the Dual Attached Node (DAN). DANs have redundant paths available to all other DANs in the network. Figure 8 shows an overview of PRP.

Figure 8 PRP Overview



DANs can be either dual-homed IEDs that natively support PRP or they can be Layer 2 switches that support PRP protocol. Switches offering PRP functionality to non-PRP capable IEDs are called redundancy boxes (RedBox). A wide range of Cisco IE switches can serve as PRP RedBoxes. Once connected to a RedBox, a singly attached IED becomes what is called a virtual dual attached node (VDAN).

The topology contained within LAN-A or LAN-B can be ring or tree-based. A node that purposely attaches to only one of the LANs (either LAN-A or LAN-B) without a RedBox is known as a singly attached node (SAN) and **will not** communicate with devices outside of the LAN to which it is connected.

Note: In order to keep each LAN resilient, Cisco recommends the use of REP inside PRP LAN-A and LAN-B, assuming all switches in these LANs are Cisco IE switches. For interoperability of Cisco IE switches and non-Cisco switches, we recommend the use of RSTP to keep LAN-A and LAN-B resilient.

More details on PRP can be found in preceding solution releases, namely in the SA LAN and Security version 2.3.1 CVD. See Related Documentation, page 76 for relevant URLs.

PRP Support—New Features on Cisco IE Switches

At the time the previous Cisco SA LAN and Security CVD version 2.3.1 solution was validated, PRP interoperated with PTP 1588 v2 on Cisco IE switches. However, support then was limited to carrying PTP frames over a single LAN (LAN-A). It was Cisco's recommendation to block PTP frames from traversing LAN-B.

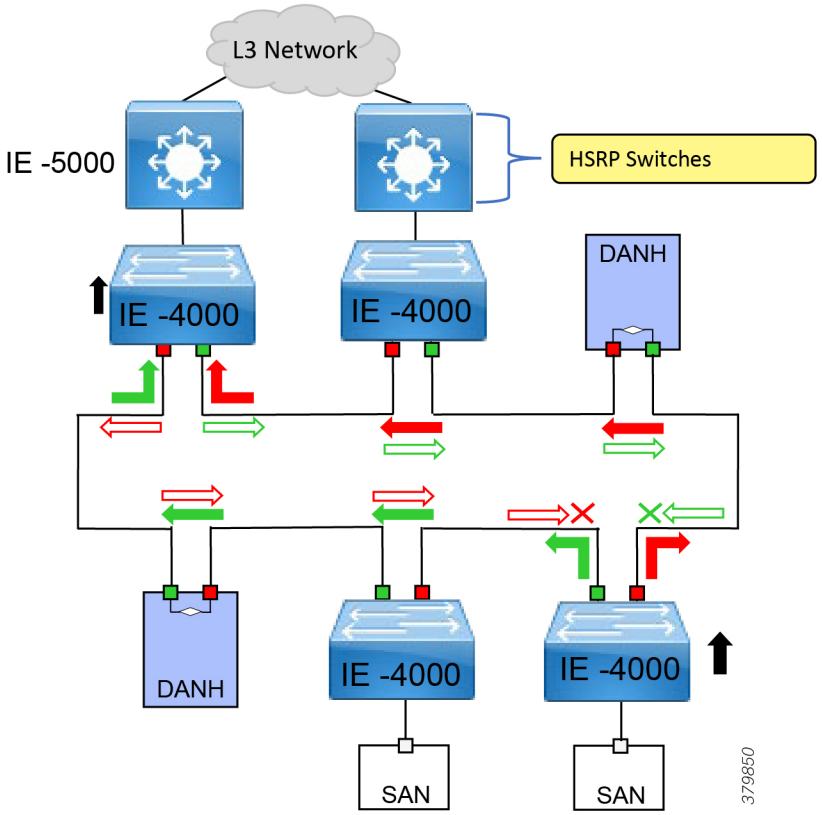
With the current SA LAN and Security CVD version 2.3.2, PTP protocol support has been extended to operate over both PRP LANs. Once the network administrator enables PTP frames to be carried over both LANs, PTP frames become protected just like other Layer 2 protocol frames and the loss of a single node or a link in either of the LANs will result in a loss-less convergence of the PTP 1588 v2 protocol. This means that IEDs will continue to stay in synchronization with a precise time source should one of the paths experience a failure.

PRP resiliency support, including PTP over PRP, is available on 8/16 port Cisco IE 2000U, Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 series switches. Operations staff can rest assured that Cisco's current PRP implementation offers as a resiliency protocol that meets the need for applications requiring precise timing via PTP 1588 v2 protocol.

HSR Support on Cisco IE Switches

HSR is defined in International Standard IEC 62439-3-2016 clause 5. HSR is a lossless protocol similar to PRP, however HSR is designed to work in a ring topology. HSR defines a ring with traffic in opposite directions. One HSR-aware port sends traffic counter clockwise in the ring and a second HSR-aware port sends traffic clockwise in the ring. HSR's frame duplication mechanism helps provide lossless redundancy in the event of a single failure within the ring. Figure 9 shows an overview of HSR.

Figure 9 HSR Overview



The HSR frame format includes additional protocol-specific information sent within the frame header. The header contains a sequence number that is used to determine if the received data is a first or a duplicate arrival of the frame.

IEDs with two interfaces attached to the HSR ring and that support the HSR protocol are referred to as Doubly Attached Nodes implementing HSR (DANHs). SANs must attach to the HSR ring through a RedBox. Once connected to a RedBox, a singly-attached IED becomes what is called a virtual dual attached node (VDAN).

An HSR RedBox acts as a DANH for all traffic for which it is the source or the destination. Cisco IE switches implement HSR RedBox functionality and connect to the HSR ring using Gigabit Ethernet ports.

HSR resiliency support is available on the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 switches.

HSR Loop Avoidance

To avoid loops and use network bandwidth effectively, an HSR RedBox does not transmit frames that have already been transmitted in the same direction. See Figure 9 for an illustration of this behavior.

To avoid loops, when a an HSR RedBox injects a frame into the ring, the frame is handled as follows:

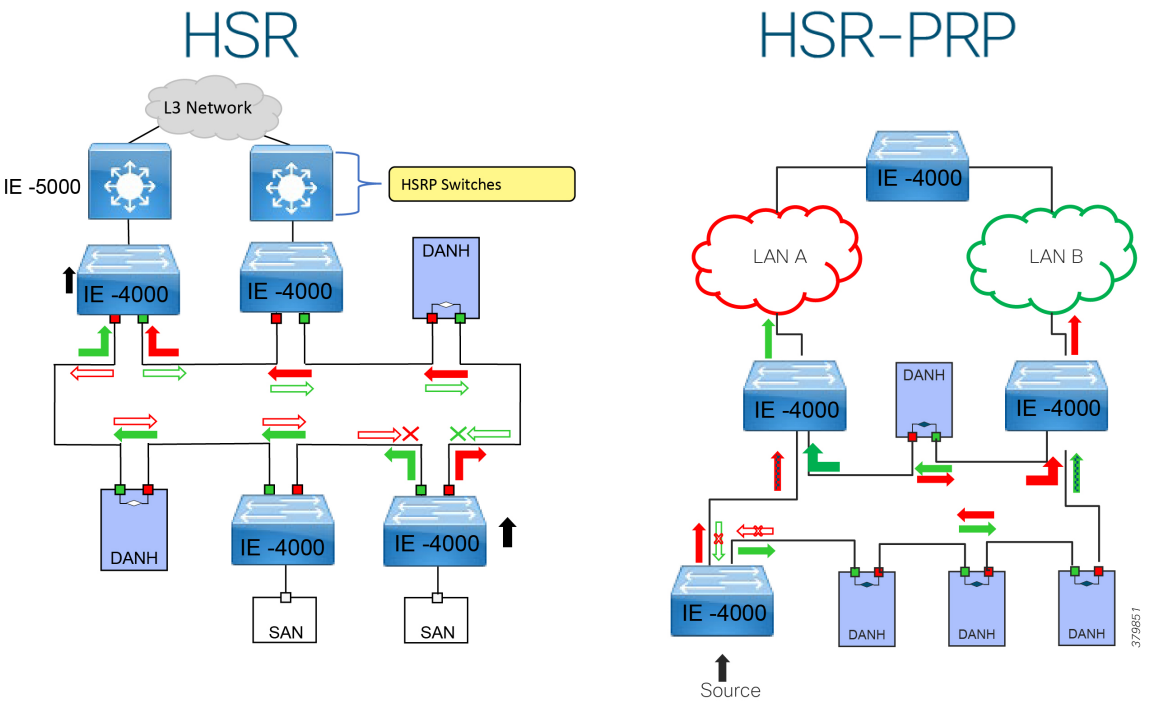
- Unicast frame with destination inside the HSR ring—When the unicast frame reaches the destination node, the frame is consumed by the respective node and is no longer forwarded.
- Unicast frame with destination not inside the ring:
  - Since this frame does not have a destination node in the ring, it is forwarded by every node in the ring until it reaches the originating node.
  - Every node has a record of the frames it had previously sent, along with the direction in which it was sent.
  - Every node will check whether it has already forwarded the received packet through its outgoing interface.
  - Once the originating node detects that frame has completed the loop, it drops the frame.
- Multicast frame:
  - A multicast frame is forwarded by each HSR node because there can be more than one consumer (intended receiver) of this frame.
  - For this reason, a multicast frame always reaches the originating node.
  - Every node will check whether it has already forwarded the received packet through its outgoing interface.
  - Once the originating node detects that frame has completed the loop, it drops the frame.

HSR RedBox Modes of Operation

An HSR RedBox can operate in one of the following modes:

- 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 data from the PRP frame and generates the HSR frame using this data. It performs the reverse operation for packets in the opposite direction. Figure 10 depicts HSR SAN and HSR-PRP operating modes and how they work.

Figure 10 HSR SAN and HSR-PRP Operating Modes



Comparing PRP and HSR Support on Cisco IE Switches

Although PRP and HSR are both resilient protocols and provide lossless failover capabilities, each protocol has advantages and disadvantages that should be examined since this information can influence protocol and deployment design selection.

Table 5 PRP and HSR Support on Cisco IE Switches

Area for Comparison	PRP	HSR
Native support available on IEDs	Yes	Yes
Can be implemented with legacy switches	Yes[1]	No All IEDs and switches in an HSR ring **must** support HSR.
Requires special Ethernet frames	No	Yes
RedBox capability	Yes	Yes
Supported topologies	LANs can be rings or trees	Ring topology only
Node count limit	No limit	Depends on aggregation link bandwidth. IEC 61850 recommends: ■ Station Bus–Up to 20 nodes ■ Process Bus–Up to 6 nodes[2]

Table 5 PRP and HSR Support on Cisco IE Switches (continued)

Implementation cost	Higher More network infrastructure	Lower Reuse same network infrastructure
Resilient support for PTP	Yes	No
VLAN support	Yes	Yes
Packet overhead	Yes[3]	Yes[3]

1. Legacy switches may be used in conjunction with a PRP network assuming that IEDs support PRP natively. Legacy switches can be placed in LAN-A and LAN-B. RedBox functionality is only available on select Cisco IE switches.
2. HSR's node limit is influenced by whether or not a utility chooses to implement IEC 61850 SV in the process bus. SV can consume several Mbps of bandwidth per publisher/subscriber flow and the amount of bandwidth available on an HSR ring quickly diminishes as frames are duplicated. The recommended aggregation link (links between HSR switches) bandwidth will be based on the number of SV publishers/subscribers. Cisco IE switches support up to 1 Gbps on the aggregation links. Cisco IE 5000 10 Gbps uplinks are typically reserved for WAN-facing traffic.
3. PRP adds overhead to the frame trailers. The PRP redundancy control trailer (RCT) is added to each frame. HSR adds overhead to the frame headers, which is called the HSR header. Both include a sequence number that is used to discard duplicates.

Precision Timing in Substation Automation

Precision time is a key requirement for all industrial applications. A special profile of Precision Time Protocol version 2 (PTPv2) was developed for utilities called the power profile. it differs from the default profile of PTP v2 used in Industrial Automation because power profile produces Layer 2, multicast Ethernet traffic. The power profile, as defined in IEEE C37.238, uses peer-to-peer delay measurements and time is accurate to 1 μsec over a span of up to 16 hops. The following Wikipedia article describes some of the commonalities and differences between the PTP profiles in the industrial automation space:
https://en.wikipedia.org/wiki/Precision_Time_Protocol_Industry_Profile.

GNSS and GPS on Cisco IE 5000

Cisco Industrial Ethernet switches are capable of accurate time distribution using PTP, but the switches previously relied on an external source to help provide accurate time.

A significant enhancement is the new, built-in Global Navigation Satellite System (GNSS) receiver on the Cisco IE 5000 switch. The GNSS and GPS receiver enables the switch to determine its location and get an accurate time reference from a satellite constellation. The Cisco IE 5000 switch can now serve as the PTP grandmaster clock and offer precise time in the substation LAN.

Note: Select Cisco IE 5000 switches with SKUs that have Version ID (VID) v05 or higher and GNSS firmware version 1.04 or higher.

PTP Over PRP

Precision Time Protocol (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. PTP can now leverage the redundancy benefits offered by PRP infrastructure, however PTP packets are handled differently than other types of traffic over PRP networks. The current Cisco implementation of PTP over PRP does not append an RCT to PTP packets and bypasses the PRP duplicate/discard logic for PTP packets.

PTP Grandmaster Redundancy

The following are possible ways that the PTP GM can be positioned in a PRP topology:

- A single PTP GM can be a Redbox that connects to both PRP LANs (LAN-A and LAN-B).
- A single PTP GM can be a VDAN that connects to a PRP RedBox.
- Dual Star Topology—Two PTP GMs can be Redboxes and each PTP GM connects to both PRP LANs (LAN-A and LAN-B). This is the Cisco recommended approach.

As with any critical protocol in the ESP zone, timing redundancy should be considered when designing the ESP network. As such, Cisco recommends deploying redundant PTP GMs in the ESP zone in a dual-star topology.

Security—Cisco NetFlow and Stealthwatch Enhancements

Although some attack vectors can be reduced using physical security, there are others that are more difficult to control because they use trusted personnel or equipment.

Some classical IT techniques to prevent Ethernet Layer 2 attacks could be applied to protect critical frames, like GOOSE. These practices are well documented, known by IT staff, and include but are not limited to:

- Set dedicated VLANs.
- Disable unused ports and set them as switch ports in an unused VLAN.
- Consciously place ports in trunking and non-trunking modes depending on what is connected.
- Create an access or prefix list based on user/device credentials.
- Avoid the use of shared Ethernet such as WLANs or hubs.

Securing the management plane is extremely important because it helps provide 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 Cisco 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 ESP traffic, which has the advantage of keeping the device reachability independent of any issues that may be occurring in the ESP network. If an out-of-band network is not possible, a logically separated network using a dedicated network management VLAN should be utilized.

Security Principles

The following fundamental principles should be adopted by the utility network operator to ensure secure systems:

- Visibility of all devices in the substation LAN 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 in the substation.
- 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. Segmenting a network using zones helps provide an organized way of managing access within and across zones. Segmenting the network-connected devices further reduces the risk of an infection spread if or when a device is subjected to malware.
- Identification and restricted data flow— All the devices in the substation must be identified, authenticated, and authorized. The network must enforce policies when users and utility assets attach to the network.

- Network anomalies—Any unusual behavior in network activity must be detected and examined to determine if the new behavior is intended or is due to a malfunction of the device. Detecting network anomalies as soon as possible gives operations teams the means to remediate network abnormality sooner, thereby reducing possible downtimes.
- Malware detection and mitigation—Unusual behavior displayed by an infected device must be detected immediately and security tools should allow remediation actions to the infected device.
- Deep packet inspection—Traditional firewalls are not built for industrial environments. There is a need for industrial firewalls which can perform deep packet inspection on industrial protocols to identify anomalies in traffic flow.
- Environmental—Secure infrastructure hardening of the networking assets in the substation.
- Security standards and assessments—Abiding by North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) mandates for critical substations in North America and following guidelines from NERC CIP and NIST elsewhere. Security risk assessments identify control systems and their level of criticality.

Security Using Cisco NetFlow and Stealthwatch for Anomaly Detection

This version of SA LAN and Security CVD heavily leverages the validation outcomes available in *Networking and Security in Industrial Automation Environments Design and Implementation Guide* (IA CVD): https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html

The IA CVD offers design guidance for enabling Cisco NetFlow and leveraging Stealthwatch to help provide anomaly detection. Visibility into the traffic traversing the utility network can aid with troubleshooting and highlight abnormal behaviors. With the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000, Cisco NetFlow can be enabled on these devices that can help 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.

Note that within substation ESP zones, Cisco NetFlow and Stealthwatch can be used to detect anomalies with Layer 3 traffic flows (for example, MMS, MODBUS TCP, and DNP3 IP). However, since GOOSE and SV protocols are Layer 2 only, Cisco NetFlow collections are not applicable and Stealthwatch dashboards would not show GOOSE and SV Layer 2 frame flows.

A more detailed CVD solution release is being planned that will be devoted to the topic of network security for utilities. For now, refer to the *Networking and Security in Industrial Automation Environments Design and Implementation Guide* for ideas on designing and implementing Cisco NetFlow and Stealthwatch for a utility substation ESP zone.

QoS and Protecting Real-time Traffic

The goal of end-to-end Quality of Service (QoS) deployment in Cisco CVD solutions is to control and predictably service a variety of network applications and traffic types. Implementing QoS guarantees complete control of resources (bandwidth, equipment, and so on) and coexistence of several traffic types (network management, physical security management, and so on) with mission-critical traffic (SCADA, PMU, and GOOSE). Careful solution design and validation of QoS helps to mitigate loss of mission-critical traffic and helps ensure efficient utilization of available resources for various applications by:

- Supporting dedicated bandwidth
- Reducing loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

QoS is important for networks supporting substation automation that need to transport loss, latency, and jitter-sensitive data, especially in cases where there is a limited amount of bandwidth. Latency-sensitive applications in the substation include real-time control and protection messaging (C37.118 synchrophasor data, 61850 GOOSE, synchrophasor messaging, and so on).

QoS policies can be defined to classify ingress packets based on EtherType or class of service (CoS), set appropriate QoS group values, and use the QoS group for further treatment on egress. Cisco recommends classifying GOOSE/SV packets on ingress based on Ether-type and inserting GOOSE/SV packets into the priority queue on egress. Remaining traffic can go into a class with guaranteed bandwidth.

Table 6 lists some different possible traffic types found in Substation Automation LAN, corresponding latency requirements, the bus in which these packets flow, and the corresponding recommended Ingress and Egress classification and QoS treatment. Each deployment may incorporate variations on the recommended prioritization. To that end, the recommendations incorporate a template model, allowing for the insertion of additional granularity when needed.

Table 6 Substation Traffic Types

Traffic Type	Classification Criteria	Egress			Notes
Mechanisms	Ingress QoS Group Marking	Shaping	Bandwidth Guarantee	Congestion Avoidance	
GOOSE/GSSE/SV	1	Priority Queuing (policing option available)	Priority Queuing (policing option available)	No	Applicable to Station and Process Bus
Network Management	2	No	Yes	Optional	Applicable to Station and Process Bus
Physical Security	3	No	Yes	Optional	Applicable to Station and Process Bus
Network Service	2	No	Yes	Optional	Applicable to Station and Process Bus
Command Center Remote	2	No	Yes	Optional	Applicable to Station and Process Bus
Mobile Remote Engineering	2	No	Yes	Optional	Applicable to Station and Process Bus
Remote Workforce	4	No	Yes	Optional	Applicable to Station and Process Bus
PTP	4	No	Priority Queuing (policing option available)	No	Applicable to Station and Process Bus

Industrial Ethernet switches like the Cisco IE 4000 support up to four queues. They support Modular QoS command line interface. The modular approach can be implemented using the following steps.

1. Identify and classify the traffic—Various classification tools like access control lists (ACLs), IP addresses, CoS, and IP Differentiated Services Code Point (DSCP) can be used. The choice of the tool depends on traffic types.

2. Perform QoS functions on the identified traffic—A few of the available QoS functions are queuing, policing, marking, and shaping. Functional selection depends on ingress or egress application traffic flow requirements.

3. Apply the appropriate policy map to the desired interfaces.

The next sections provide a detailed examination of each of the areas above, all of which influence ESP zone design.

Implementing HSR SAN

HSR protocol has been validated on the platforms in Table 7, all of which are deployable in the utility substation LAN.

Table 7 HSR and Platform Validation

HSR Feature	Cisco Validated Platforms
Single Attached Node RedBox (SAN)	Cisco IE 4000 Cisco IE 4010 Cisco IE 5000
HSR to PRP Dual RedBox	Cisco IE 4000

The following HSR deployment topologies are not yet recommended on Cisco platforms:

- Single HSR network to multiple PRP networks
- Multiple HSR networks to a single PRP networks

HSR SAN

A maximum of two ports are configurable for HSR SAN on Cisco IE switches. Specific interfaces are reserved for use of the HSR SAN feature. HSR is configurable using CLI and the web-based, embedded device manager tool available for Cisco IE switches.

When configuring a Cisco IE switch in SAN mode, a non-HSR aware IED can be connected as a Virtual Doubly Attached Node (VDAN). The Cisco IE switch in SAN mode becomes a proxy for the VDAN and allows the VDAN traffic to be protected.

Commands are available for troubleshooting the HSR SAN feature, including the ability to view:

- Configuration details
- HSR ring state
- Statistics for HSR components
- All MAC addresses accessible to the SAN switch using the HSR interface (other HSR nodes in the ring and VDANs)
- The HSR VDAN (proxy node) table
- Neighboring switch information
- HSR alarms

The HSR SAN implementation on Cisco IE switches supports VLAN-tagging of the HSR supervision frames.

HSR SAN is interoperable with many protocols and features on Cisco IE switches, including but not limited to the following:

- HSRP

- LLDP
- CDP
- SNMP
- QoS (Layer 2 CoS)
- VLAN untagged and tagged traffic

Note that HSR SAN is **not** interoperable with the following protocols on Cisco IE switches:

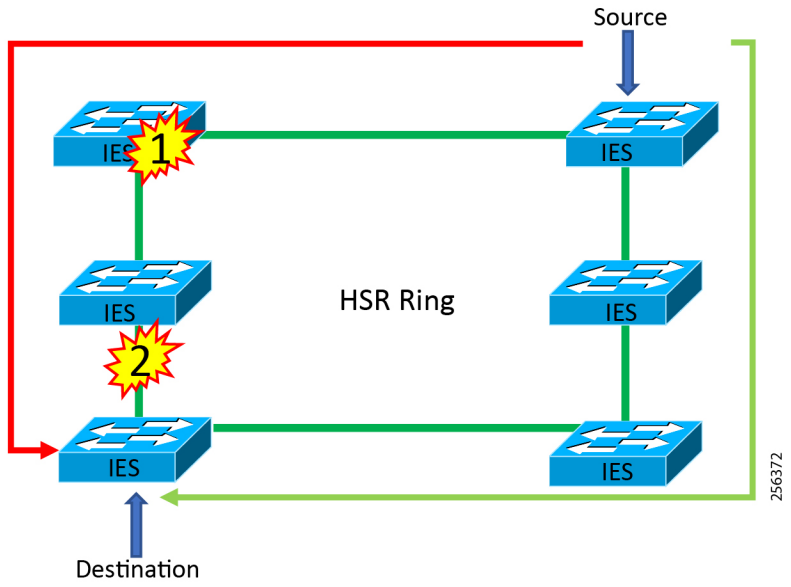
- Flex Link
- Ether Channel
- REP
- PTP

Single HSR Ring Process Bus

High-availability Seamless Redundancy (HSR) is defined in International Standard IEC 62439-3-2016 clause 5. HSR is designed to work in a ring topology. Instead of two parallel independent networks of any PRP 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.

Figure 11 shows an example of an HSR Ring for Substation Automation Process Bus using Cisco IE 4000 variant switches. Traffic in the network consisted of Sample Values (tagged—VLAN 0 and VLAN 110), GOOSE (VLAN 120), and untagged IP packets.

Figure 11 Process Bus as HSR Ring



To validate the resiliency and the corresponding latency requirements of the network, failures like switch failure and link flap were introduced at different points as highlighted and numbered in Figure 11:

- (1)—A redundant network switch

- (2)—A redundant network link

Refer to Table 8 for device role information for HSR SAN.

Table 8 HSR SAN Cisco IE Switches and Roles

SKU	Role	IOS Version
Cisco IE 4000	HSR SAN	15.2.6E2a

Configuring HSR SAN Using CLI

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, note:

- HSR ring ports can only be configured in Layer 2 mode.
- It is recommended to configure settings like media-type, speed, and duplex settings of the port before configuring ring membership.
- Once a port is part of HSR ring, the port cannot be shut down. Instead the HSR Ring interface can be shut if required. However, this operation would shut down both of the member ports.

```
Switch# config t
Switch(config)# interface HSR-ring1
Switch(config-if)# shutdown
Switch(config-if)# end
```

- HSR VLAN(s) should be enabled on the switch using the following commands:

```
Switch# config t
Switch(config)# vlan 100
Switch(config-vlan)# no shutdown
Switch (config-vlan)# end
```

- When an 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.

```
Switch# config t
Switch(config)# interface GigabitEthernet 1/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1
Switch(config-if)# end
```

Summary of Steps

1. Activate HSR feature mode:

```
Switch# 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.

Refer to the following configuration guide for more details on licensing:
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.pdf

2. Verify that the HSR feature is activated:

```
Switch# show version | include Feature
Feature Mode: 0x25 Enabled: HSR (Disabled: MRP TSN)
```

3. Enter global configuration mode:

```
Switch# configure terminal
```

4. Enter interface configuration mode and disable PTP on the ports to be assigned to the HSR ring:

```
Switch(config)# interface range GigabitEthernet 1/3-4
Switch(config-if-range)# no ptp enable
```

Note: PTP feature over HSR ring is currently not supported on Cisco IE switches.

5. Shut down the ports before configuring the HSR ring:

```
Switch(config-if-range)# shutdown
```

6. Create the HSR ring interface:

```
Switch(config)# interface HSR-ring2
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

7. Assign HSR ring to the physical interfaces:

```
Switch(config)# interface range GigabitEthernet 1/3-4
Switch(config-if-range)# hsr-ring 2
Switch(config-if-range)# no shutdown
Switch(config-if)# end
```

8. Repeat the steps on remaining switches part of the HSR ring.

Table 9 HSR Interface Mapping

SKU	Interface Mapping
Cisco IE 4000	HSR Ring 1 always uses Gi1/1 and Gi1/2. HSR Ring 2 always uses Gi1/3 and Gi1/4.
Cisco IE 4010	HSR Ring 1 always uses Gi1/17 and Gi1/18. HSR Ring 2 always uses Gi1/19 and Gi1/20.
Cisco IE 5000	HSR Ring 1 always uses Gi1/25 and Gi1/26. HSR Ring 2 always uses Gi1/27 and Gi1/28.

Verifying HSR SAN Using CLI

Verify the functionality of HSR SAN using the following commands:

```
Switch# show hsr ring 1 detail

HSR-ring: HS1
------------
 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: Gi1/1
```

```
   Logical slot/port = 1/1      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/2
   Logical slot/port = 1/2      Port state = Inuse
        Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: 0cd0.f801.7b02
 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: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled

Switch# show hsr ring 1 status

HSR-ring: HS1
------------
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san

HSR-003# show hsr ring 1 ?
  detail   Detail information
  status   HSR-ring status
  summary  Summary per hsr ring

Switch# show hsr ring 1 summary
Flags:  D - down        H - bundled in HSR-ring
        R - Layer3      S - Layer2
        U - in use

Number of hsr-rings in use: 1
Group   HSR-ring     Ports
------+-------------+---------------------------------------
1      HS1(SU)       Gi1/1(H), Gi1/2(H)

Switch# show hsr statistics ingressPacketStatistics

 HSR ring 1 INGRESS STATS:
   ingress pkt port A: 298880
   ingress pkt port B: 519738
   ingress crc port A: 0
   ingress crc port B: 0
   ingress danh pkt portAcpt: 8971
   ingress danh pkt dscrd: 0
   ingress supfrm rcv port A: 295312
   ingress supfrm rcv port B: 514335
   ingress overrun pkt port A: 0
   ingress overrun pkt port B: 0
   ingress byte port a: 25077052
   ingress byte port b: 40761555
 HSR ring 2 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 dscrd: 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

Switch# show hsr statistics egressPacketStatistics

 HSR ring 1 EGRESS STATS:
   duplicate packets: 2710
   supervision frames: 278284
   packets sent on port A: 2710
   packets sent on port B: 2710
   byte sent on port a: 60439946
   byte sent on port b: 44974427
 HSR ring 2 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
```

Recommended Practices for HSR-SAN Configuration

- Disable PTP on interfaces where PTP is not necessary.
- Enable storm control for broadcast and multicast traffic on access facing interfaces:

```
Switch# config t
Switch(config)# interface GigabitEthernet1/5
Switch(config-if-range)# storm-control broadcast level pps 1k
Switch(config-if-range)# storm-control multicast level pps 5k
Switch(config-if-range)# storm-control action shutdown
Switch(config-if-range)# storm-control action trap
Switch(config-if-range)# end
```

- Configure different VLANs for different IEDs so as to avoid flooding of multicast and broadcast messages to other devices.

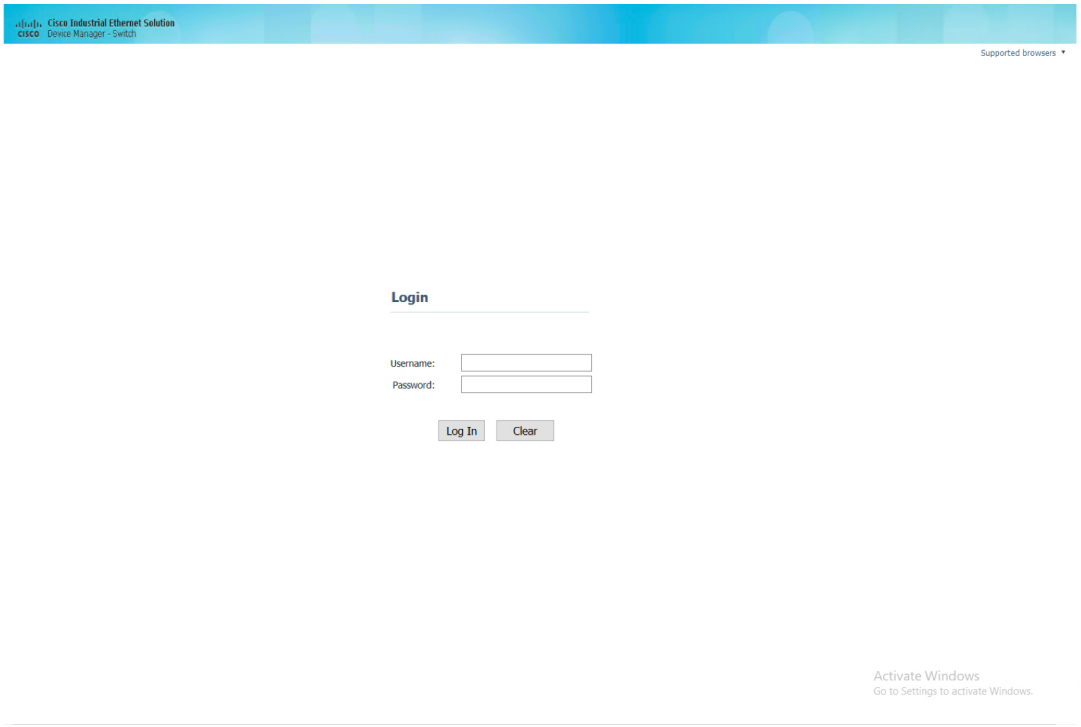
Note: PTP over HSR ring is not currently supported on Cisco IE switches.

Configuring HSR-SAN Using Device Manager

This section assumes that the Cisco IE switch has been installed and pre-configured with an IP address for remote access. For more details on setting up a Cisco IE switch, refer to the Cisco IE switch installation guides.

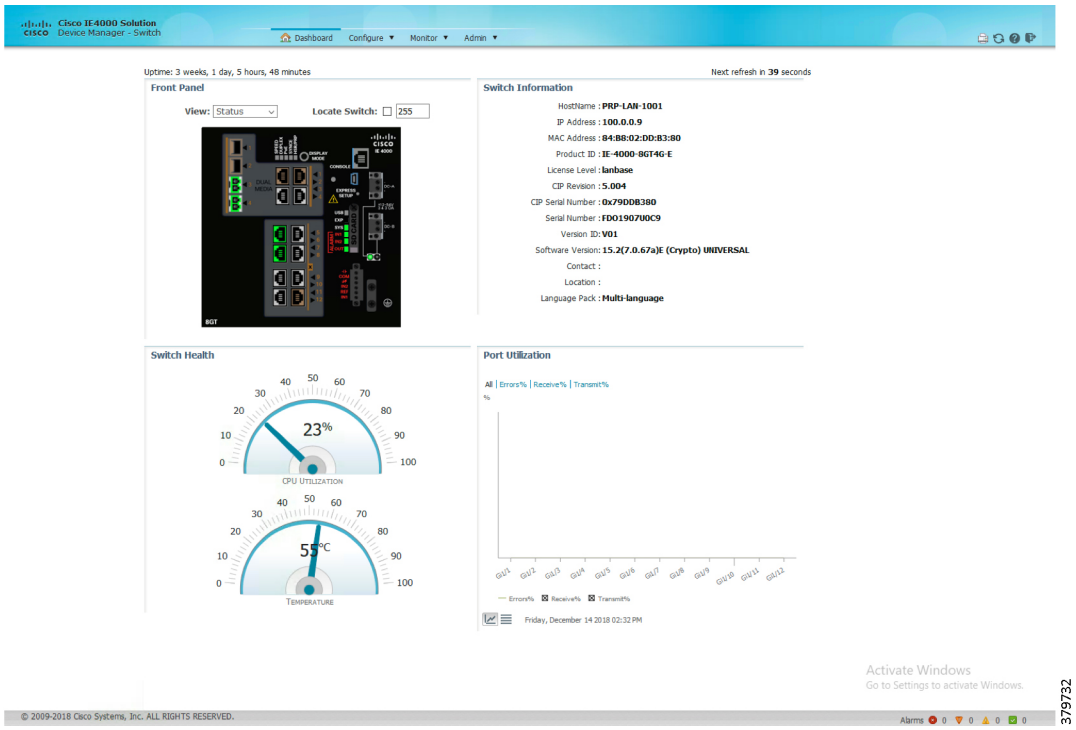
1. Log in to the switch using Device Manager credentials, as shown in Figure 12.

Figure 12 Device Manager Login Screen



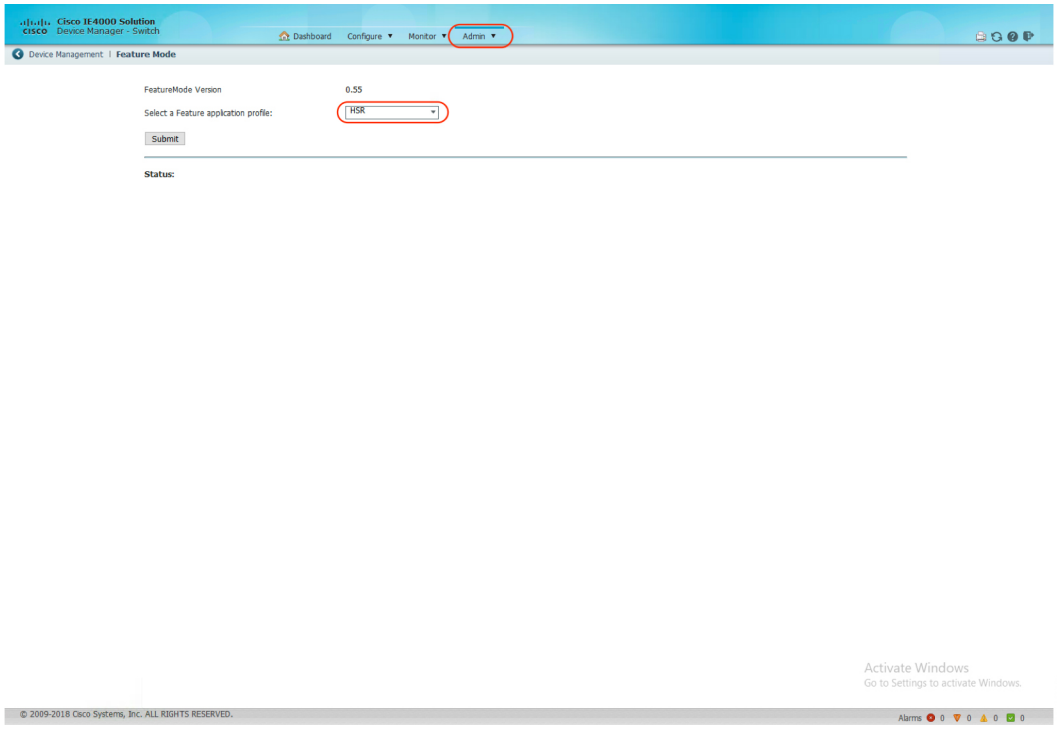
2. After a successful login, the Dashboard for the switch loads, as shown in Figure 13.

Figure 13 Cisco IE 4000 Device Manager Dashboard



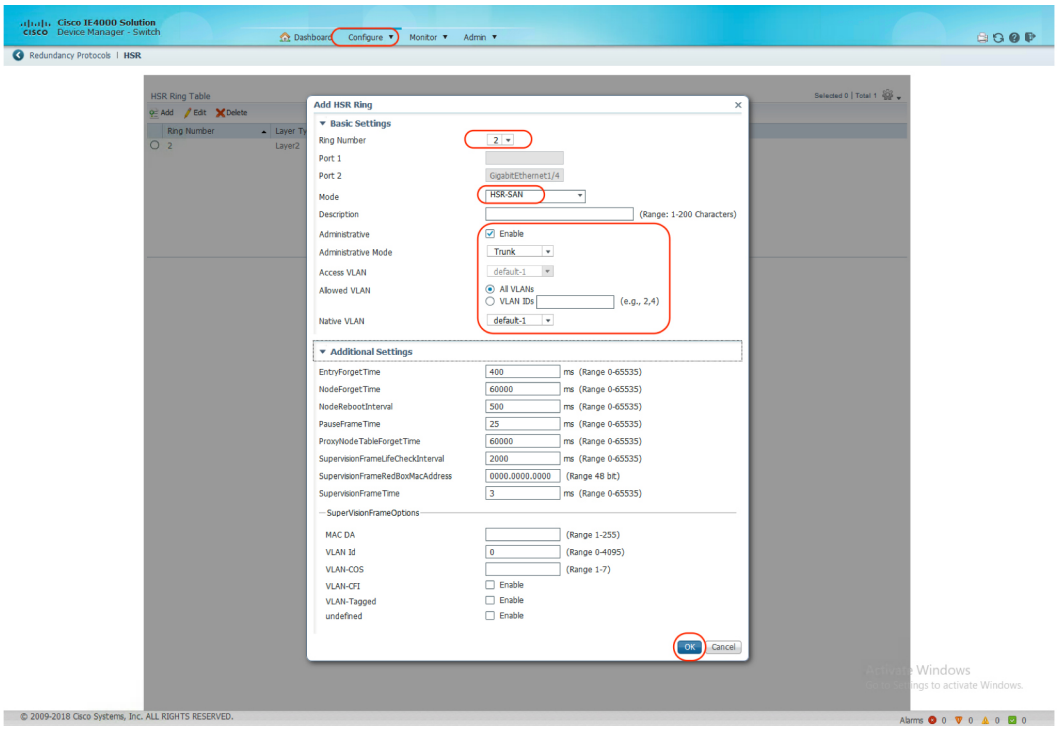
3. Enable the HSR feature on the Cisco IE switch using the options highlighted in Figure 14.

Figure 14 Enable HSR Feature



4. Configure HSR Ring and its related parameters on the Cisco IE switch using the options highlighted in Figure 15.

Figure 15 HSR Ring Parameters



Implementing HSR-PRP Dual RedBox

HSR to PRP Dual RedBox is used to connect together PRP and HSR networks. This feature is supported on Cisco IE 4000 switching products only (not the Cisco IE 4010). This feature allows HSR and PRP RedBoxes to convert PRP frames to HSR frames and vice versa, all while protecting the network from any loops.

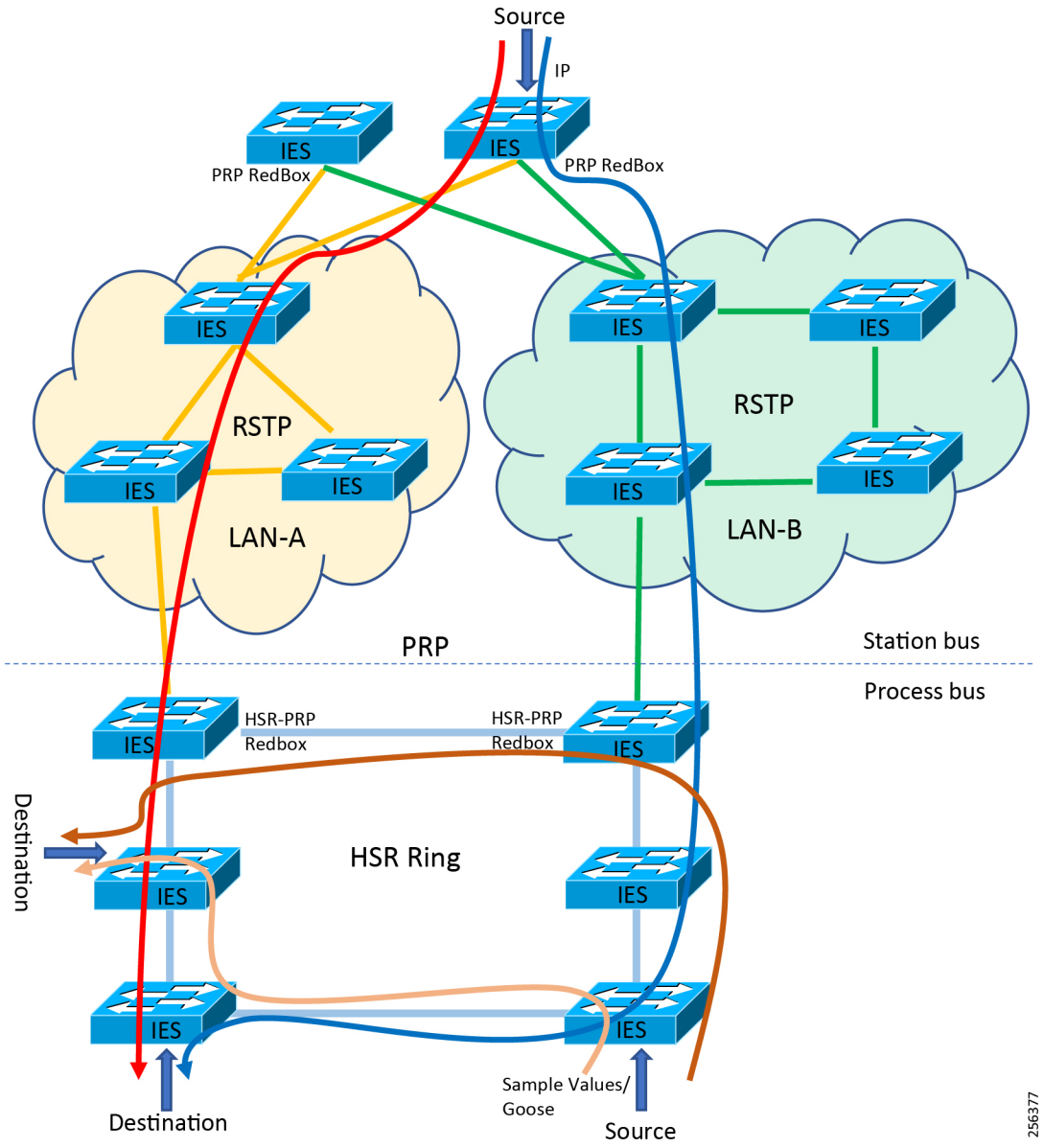
A maximum of two ports are configurable for HSR and a maximum of two ports are configurable for PRP when enabling HSR to PRP Dual RedBox on Cisco IE switches. Specific interfaces are reserved for use of the HSR and PRP features. HSR to PRP Dual RedBox is configurable using CLI and using the web-based device manager tool available for Cisco IE switches.

Note: Cisco recommends increasing the MTU size for switch interfaces participating in PRP LAN-A and LAN-B networks to account for the 6-byte PRP trailer added to every packet.

Remember that since PTP is not yet supported over HSR, PTP would need to be disabled in ports facing the HSR ring direction.

The topology in Figure 16 shows a combination of a station bus and process bus network, but it could also be a second-level station bus. High availability throughout both the station and the process bus network is achieved using a double LAN network on the station bus and an HSR ring of bridging end nodes on the process bus, as shown in Figure 16.

Figure 16 PRP-Based Station Bus and HSR-Based Process Bus



The redundant LAN networks A and B may be closed into a ring structure using RSTP. They are connected to the rings through redundancy boxes working in PRP LAN-A and LAN-B mode.

A typical deployment of 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. RedBoxes do not forward duplicate frames in the same direction to avoid loops. RedBoxes convert PRP frames to HSR frames and vice versa.

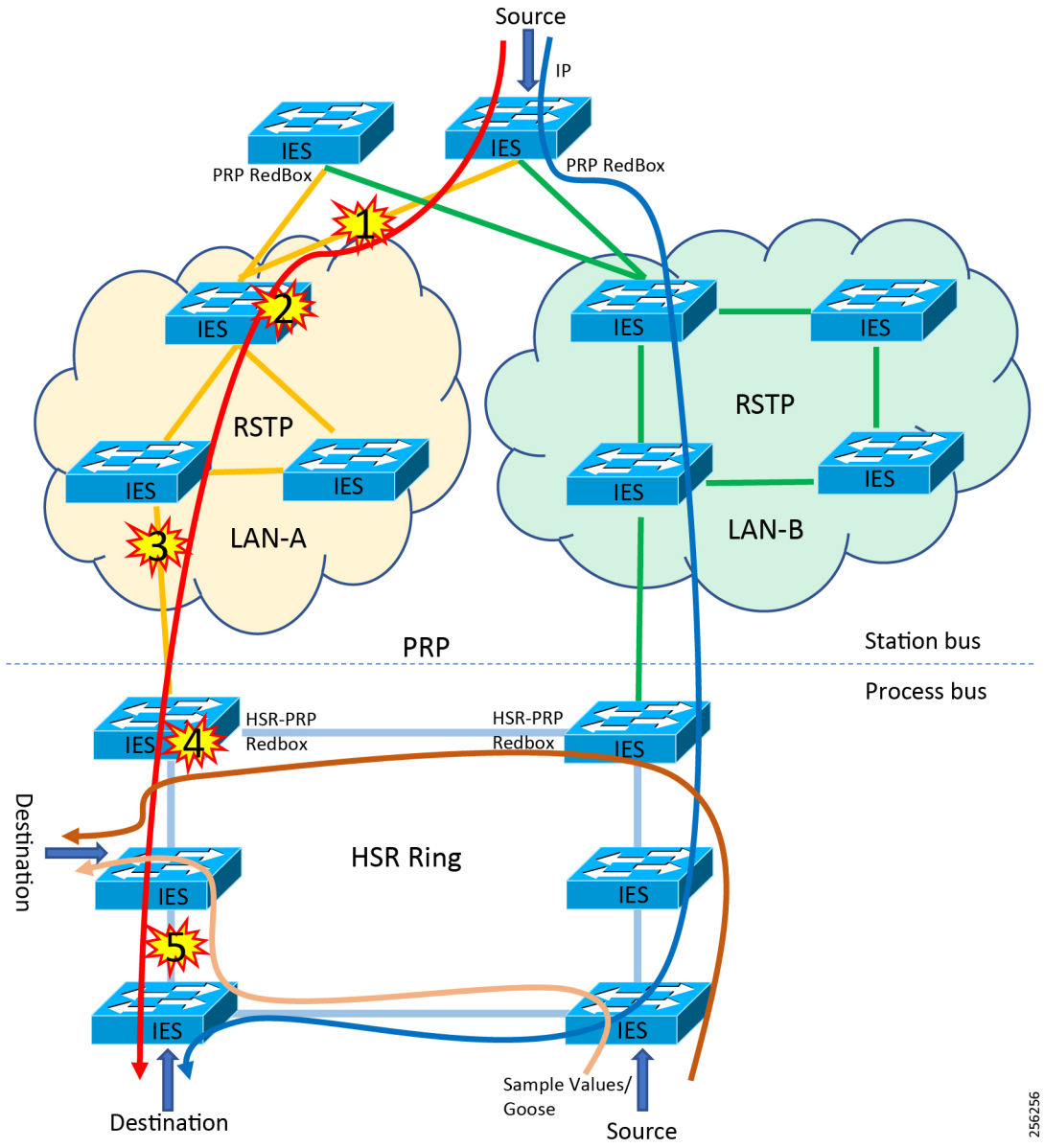
Table 10 lists different Cisco Industrial Ethernet switches and their role in the topology depicted in Figure 16.

Table 10 HSR-PRP Dual RedBox Cisco IE Switches and Roles

Switch	Role	IOS Version
Cisco IE 5000	PRP RedBox	15.2.6E2a
Cisco IE 4000	HSR-PRP Redbox	15.2.6E2a
Cisco IE 4010	RSTP	15.2.6E2a

Figure 17 shows an HSR ring connected to a PRP network through two RedBoxes, one for each LAN. RedBoxes are configured to support PRP traffic on the interlink ports and HSR traffic on the ring ports. In this example traffic flows between PRP and HSR network through RedBoxes. Traffic in the network consisted of Sample Values (tagged—VLAN 0 and VLAN 110), GOOSE (VLAN 120), and untagged IP packets.

Figure 17 PRP-Based Station Bus and HSR-Based Process Bus



To validate the resiliency and the corresponding latency requirements of the network, failures were introduced at different points as highlighted and numbered in Figure 17:

- (1), (3), and (5)—A redundant network link
- (2) and (4)—A redundant network switch

Configuring HSR-PRP Dual RedBox Using CLI

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, note:

- 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 frame. To help ensure that all packets can flow through the PRP network, increase the MTU size for switches within the PRP LAN-A and LAN-B network to 1506 as follows:

```
Switch# config t
Switch(config)# system mtu 1506
Switch(config)# system mtu jumbo 1506
```

- PRP VLANs can be enabled on the switch using the following commands:

```
Switch(config)# vlan 100
Switch(config-vlan)# no shutdown
Switch(config-vlan)# exit
```

- When an IED sends VLAN 0-tagged packets, it is recommended to configure the IED-facing and uplink interfaces as trunk ports allowing VLAN 1 along with other required VLANs:

```
Switch(config)# interface GigabitEthernet 1/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1
Switch(config-if)# end
```

Summary of Steps

1. Activate HSR feature mode:

```
Switch# license right-to-use activate hsr
```

For more details refer to the following configuration guide:
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.pdf

Note: Reload the switch for the license change to take effect by confirming the reload prompt and waiting for the switch to boot.

2. Verify that the HSR feature is activated:

```
Switch# show version | include Feature
Feature Mode: 0x25 Enabled: HSR (Disabled: MRP TSN)
```

3. Enter global configuration mode:

```
Switch# configure terminal
```

4. Enable HSR-PRP mode and select LAN-A or LAN-B and the PRP Net ID:

```
Switch(config)# 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:

```
Switch(config)# no hsr-prp-mode enable
```

6. Enter interface configuration mode and disable PTP on the ports to be assigned to the HSR ring:

```
Switch(config)# interface range GigabitEthernet 1/3-4
Switch(config-if-range) # no ptp enable
```

   Note: PTP feature over HSR ring is currently not supported.

7. Shut down the ports before configuring the HSR ring:

```
Switch(config-if-range)# shutdown
```

8. Create the HSR ring interface:

```
Switch(config)# interface HSR-ring2
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

9. Assign HSR ring to the physical interfaces:

```
Switch(config)# interface range GigabitEthernet 1/3-4
Switch(config-if-range)# hsr-ring 2
Switch(config-if-range)# no shutdown
Switch(config-if)# exit
```

10. Create PRP LAN interface. Repeat the step on the second HSR-PRP RedBox:

```
Switch(config)# interface PRP-channel1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

11. Assign PRP channel to the physical interface. Follow the guidelines for identifying the switch role and the corresponding interface:

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if-range)# prp-channel-group 1
Switch(config-if-range)# no shutdown
Switch(config-if)# end
```

Table 11 HSR-PRP RedBox Cisco IE 4000 Interface Mapping

SKU	HSR Mode	Port Type	Interface Number
Cisco IE 4000	HSR-PRP	PRP-LAN-A (RedBox A)	PRP channel interface: ■ Gi1/1 (Port 3) HSR ring interfaces: ■ Gi1/3 (Port 1) ■ Gi1/4 (Port 2) ■ Note: Gi1/2 is unused
		PRP-LAN-B (RedBox B)	PRP channel interface: ■ Gi1/2 (Port 3) HSR ring interfaces: ■ Gi1/3 (Port 1) ■ Gi1/4 (Port 2) ■ Note: Gi1/1 is unused

- Refer to Implementing HSR SAN, page 31 to configure HSR on Cisco IE switches that participate in the HSR ring.
- Refer to Implementing PRP RedBox, page 50 to configure PRP on Cisco IE switches that participate in the PRP network.
- Per VLAN Spanning Tree protocol is enabled by default on Cisco Industrial Ethernet switches. Refer to the following link to configure other modes of Spanning Tree Protocol on Cisco Industrial Ethernet Switches: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmstp.html

Verifying HSR-PRP Dual RedBox Using CLI

Verify HSR-PRP functionality using the following commands:

```
Switch# 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

Switch# 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
 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: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled

Switch# 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

Switch# 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 dscrd: 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 dscrd: 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

Switch# clear hsr statistics
```

Recommended Practices for HSR-PRP Dual RedBox

- Disable PTP on interfaces where PTP is not necessary.
- Enable storm control for broadcast and multicast traffic on access facing interfaces:

```
Switch(config)# interface GigabitEthernet1/5
Switch(config-if-range)# storm-control broadcast level pps 1k
Switch(config-if-range)# storm-control multicast level pps 5k
Switch(config-if-range)# storm-control action shutdown
Switch(config-if-range)# storm-control action trap
Switch(config-if-range)# end
```

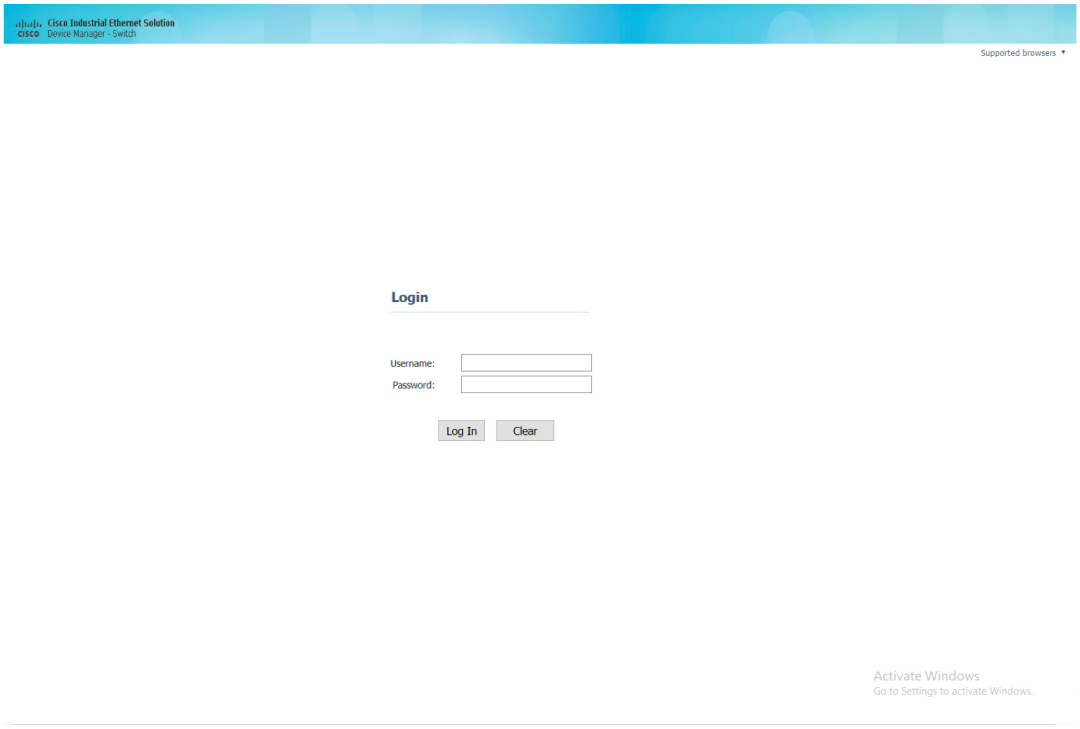
- Configure separate VLANs for different IEDs to avoid flooding of unnecessary multicast and broadcast messages to non-participating devices.

Configuring HSR-PRP Dual RedBox Using Device Manager

This section assumes that the Cisco IE switch has been installed and pre-configured with an IP address for remote access. For more details on setting up a Cisco IE switch, refer to the Cisco IE switch installation guides.

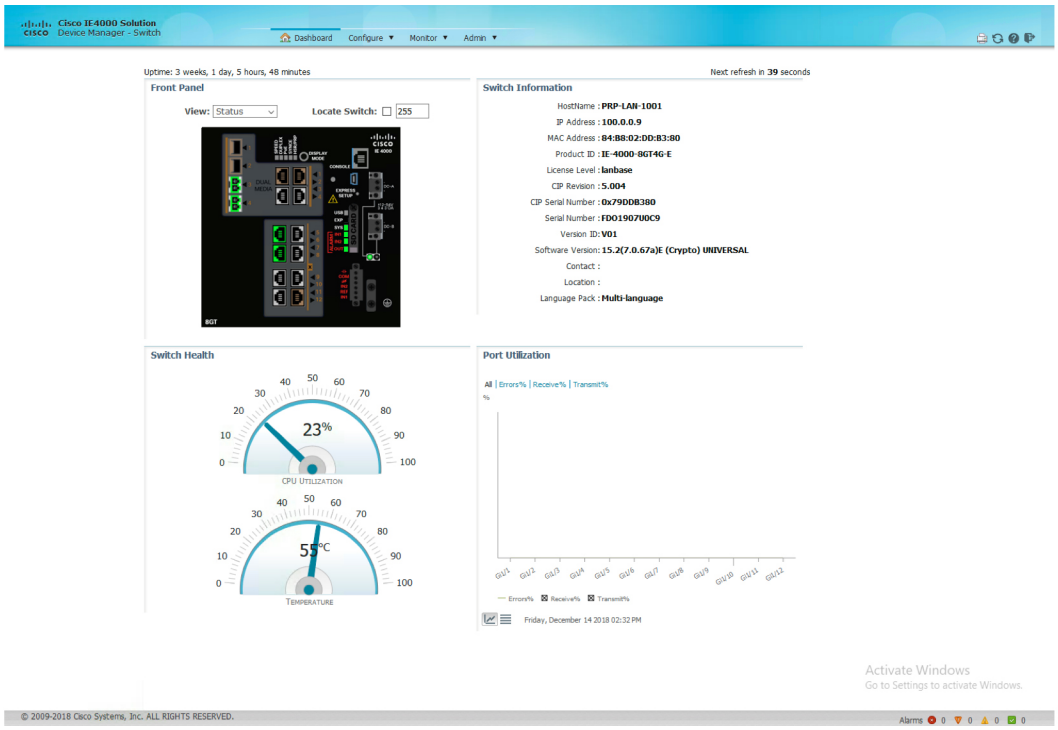
1. Log in to the switch using Device Manager credentials, as shown in Figure 18.

Figure 18 Device Manager Login Screen



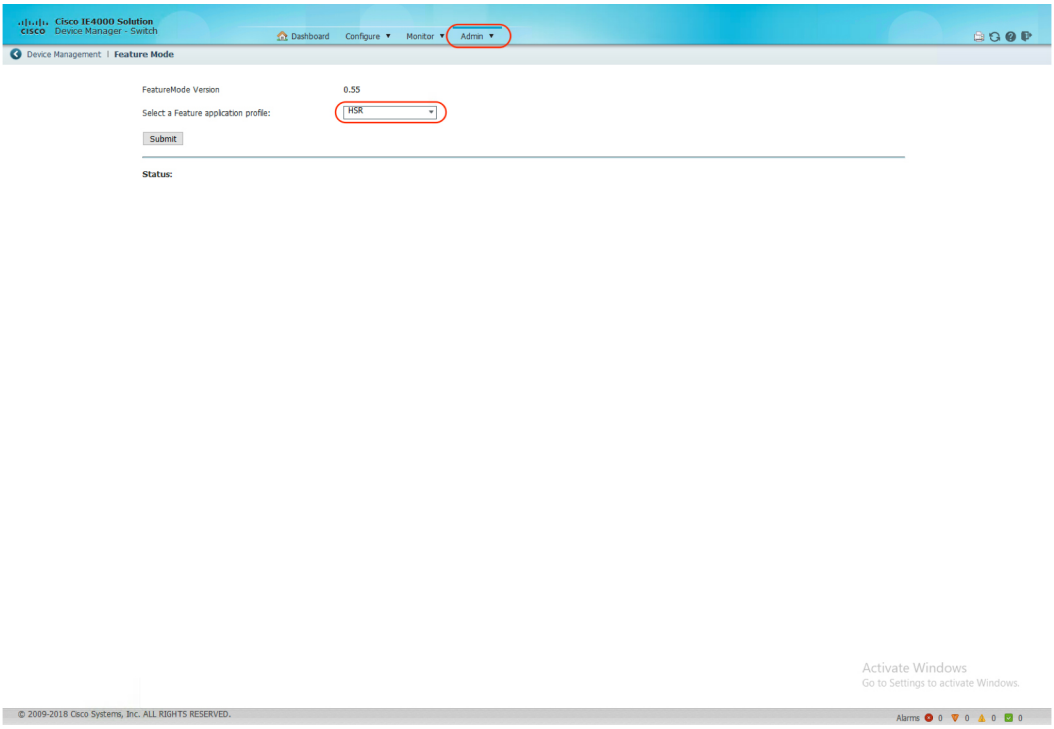
2. After a successful login, the Dashboard for the switch loads, as shown in Figure 19.

Figure 19 Cisco IE 4000 Device Manager Dashboard



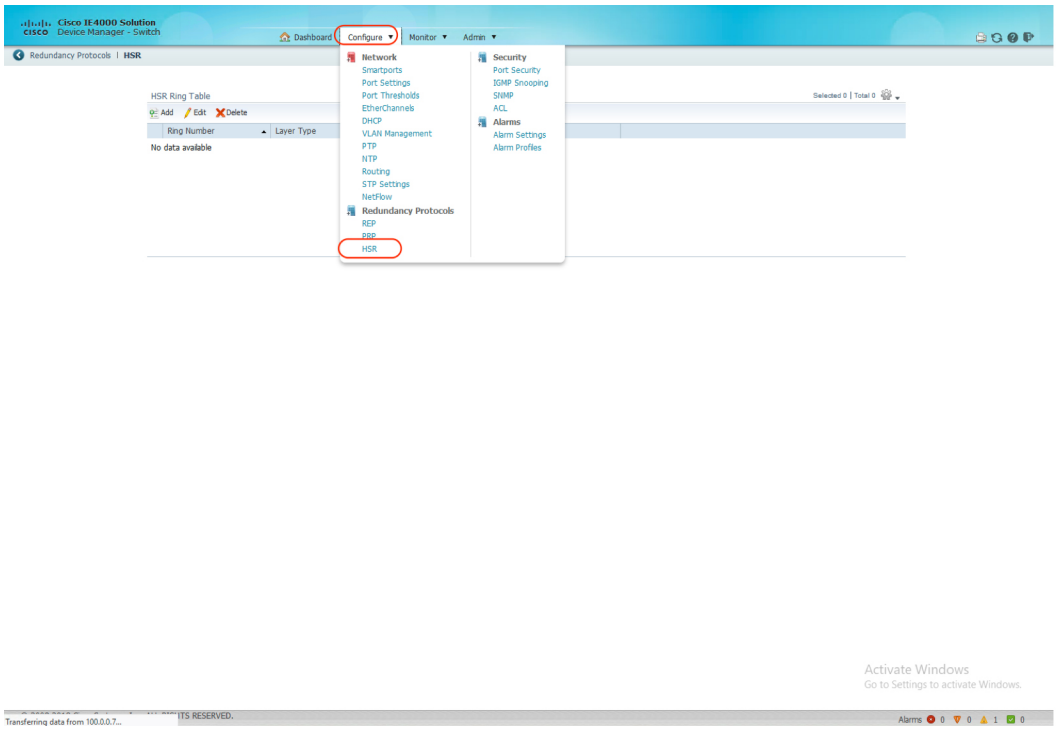
3. Enable the HSR feature on the Cisco IE switch using the options highlighted in Figure 20. Select the **Admin** tab, select the **Feature Mode** option, and then select **HSR** as the required feature mode.

Figure 20 Enable HSR Feature



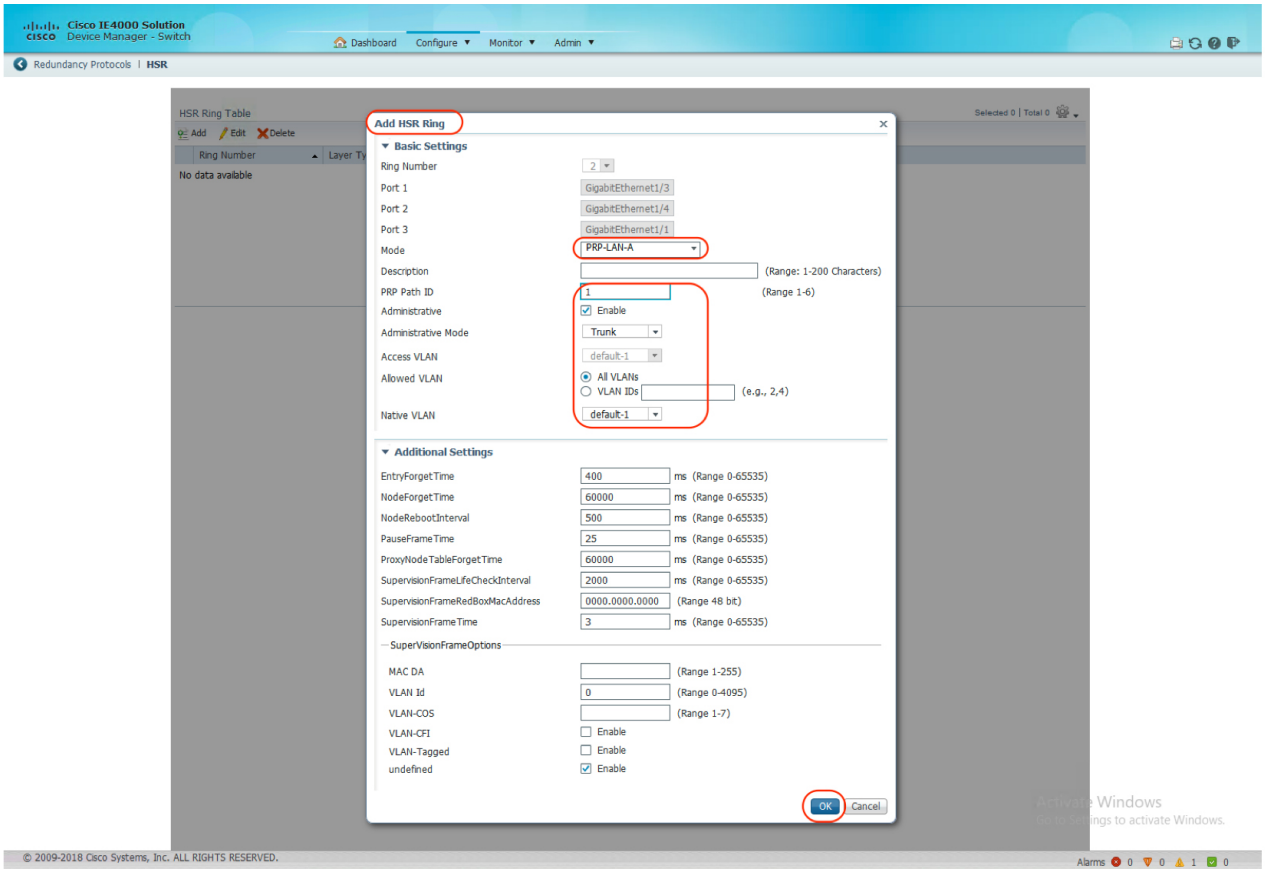
4. Configure HSR-PRP Redbox by selecting the highlighted steps in Figure 21.

Figure 21 Configure HSR Feature



5. Configure HSR-PRP Rebox parameters on the Cisco IE switch using the options highlighted in Figure 22.

Figure 22 Configure HSR-PRP Parameters



Implementing PRP RedBox

PRP protocol has been validated on the following platforms, all of which are deployable in the utility substation LAN:

- Cisco IE 4000
- Cisco IE 4010
- Cisco IE 5000

A maximum of four ports are configurable for PRP, two ports are configurable for each PRP channel, and two PRP channels are available on the Cisco IE switches. Specific interfaces are reserved for use by the PRP RedBox feature. PRP RedBox is configurable using the CLI and using the web-based device manager tool available for Cisco IE switches.

Configuring PRP RedBox Using CLI

Summary of Steps

To create a PRP channel and PRP group on the switch, follow these steps:

1. Enter global configuration mode:

```
Switch# configure terminal
```

2. Create PRP LAN interface:

```
Switch(config)# interface PRP-channel1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

3. Attach PRP channel to the physical interface. Follow the guidelines for identifying the switch role and the corresponding interface:

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if-range)# prp-channel-group 1
Switch(config-if-range)# no shutdown
Switch(config-if)# exit
```

Refer to the following configuration guide for licensing if required:
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.pdf

Table 12 PRP RedBox Interface Mapping

SKU	Interface Mapping
IE4000	PRP channel group 1 always uses: ■ Gi1/1 for LAN_A ■ Gi1/2 for LAN_B PRP channel group 2 always uses: ■ Gi1/3 for LAN_A ■ Gi1/4 for LAN_B
IE4010	PRP channel group 1 always uses: ■ Gi1/25 for LAN_A ■ Gi1/26 for LAN_B PRP channel group 2 always uses: ■ Gi1/27 for LAN_A ■ Gi1/28 for LAN_B
IE5000	PRP channel group 1 always uses: ■ Gi1/17 for LAN_A ■ Gi1/18 for LAN_B PRP channel group 2 always uses: ■ Gi1/19 for LAN_A ■ Gi1/20 for LAN_B

Verifying PRP RedBox Using CLI

Verify HSR-PRP functionality using the following commands:

```
Switch# 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

Switch# show prp statistics ingressPacketStatistics
 PRP channel-group 1 INGRESS STATS:
   ingress pkt lan a: 13198663843
   ingress pkt lan b: 11910141377
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 13428898666
   ingress danp pkt dscrd: 11580279663
   ingress supfrm rcv a: 54393129
   ingress supfrm rcv b: 45261686
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
   ingress oversize pkt a: 0
   ingress oversize pkt b: 0
   ingress byte lan a: 1824139789122
   ingress byte lan b: 1607811647159
   ingress wrong lan id a: 0
   ingress wrong lan id b: 11901970366
   ingress warning lan a: 0
   ingress warning lan b: 1
   ingress warning count lan a: 8
   ingress warning count lan b: 10
   ingress unique count a: 1563991035
   ingress unique count b: 18374154720243
   ingress duplicate count a: 11050581604
   ingress duplicate count b: 11050581604
   ingress multiple count a: 262883304
   ingress multiple count b: 266814778
PRP channel-group 2 INGRESS STATS:
   ingress pkt lan a: 0
   ingress pkt lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
   ingress oversize pkt a: 0
   ingress oversize pkt b: 0
   ingress byte lan a: 0
   ingress byte lan b: 0
   ingress wrong lan id a: 0
   ingress wrong lan id b: 0
   ingress warning lan a: 0
   ingress warning lan b: 0
   ingress warning count lan a: 0
```

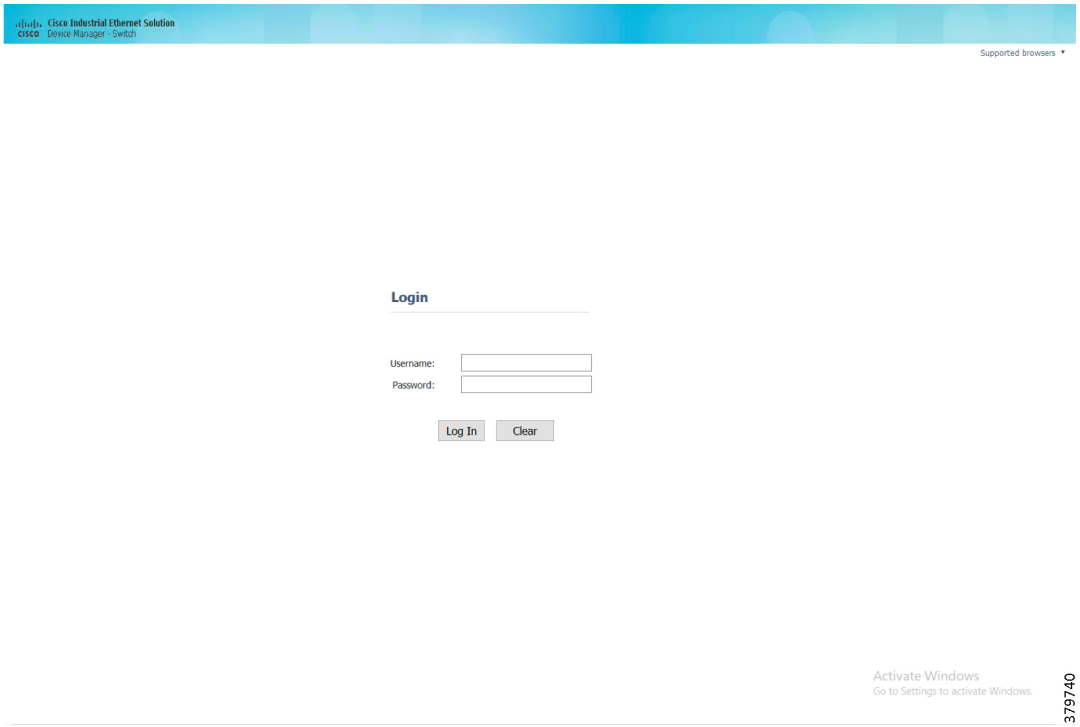
```
   ingress warning count lan b: 0
   ingress unique count a: 0
   ingress unique count b: 0
   ingress duplicate count a: 0
   ingress duplicate count b: 0
   ingress multiple count a: 0
   ingress multiple count b: 0

Switch# show prp statistics egressPacketStatistics
 PRP channel-group 1 EGRESS STATS:
   duplicate packet: 256072256
   supervision frame sent: 3384262
   packet sent on lan a: 256072249
   packet sent on lan b: 247312133
   byte sent on lan a: 96216658798
   byte sent on lan b: 92860115368
   egress packet receive from switch: 270808154
   overrun pkt: 0
   overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
   duplicate packet: 0
   supervision frame sent: 0
   packet sent on lan a: 0
   packet sent on lan b: 0
   byte sent on lan a: 0
  byte sent on lan b: 0
   egress packet receive from switch: 0
   overrun pkt: 0
   overrun pkt drop: 0

Switch# show prp channel 1 detail
PRP-channel: PR1
------------
Layer type = L2
 Ports: 2       Maxports = 2
Port state = prp-channel is Inuse
Protocol = Enabled
Ports in the group:
  1) Port: Gi1/17
   Logical slot/port = 1/17     Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/18
   Logical slot/port = 1/18     Port state = Inuse
        Protocol = Enabled

Switch# show prp channel 1 summary
Flags:  D - down        P - bundled in prp-channel
        R - Layer3      S - Layer2
        U - in use

Number of channel-groups in use: 2
Group  PRP-channel   Ports
------+-------------+-----------------------------------------
1      PR1(SU)       Gi1/17(P), Gi1/18(P)
```

Configuring PRP RedBox Using Device Manager

This section assumes that the Cisco IE switch has been installed and pre-configured with an IP address for remote access. For more details on setting up a Cisco IE switch, refer to the Cisco IE switch installation guides.

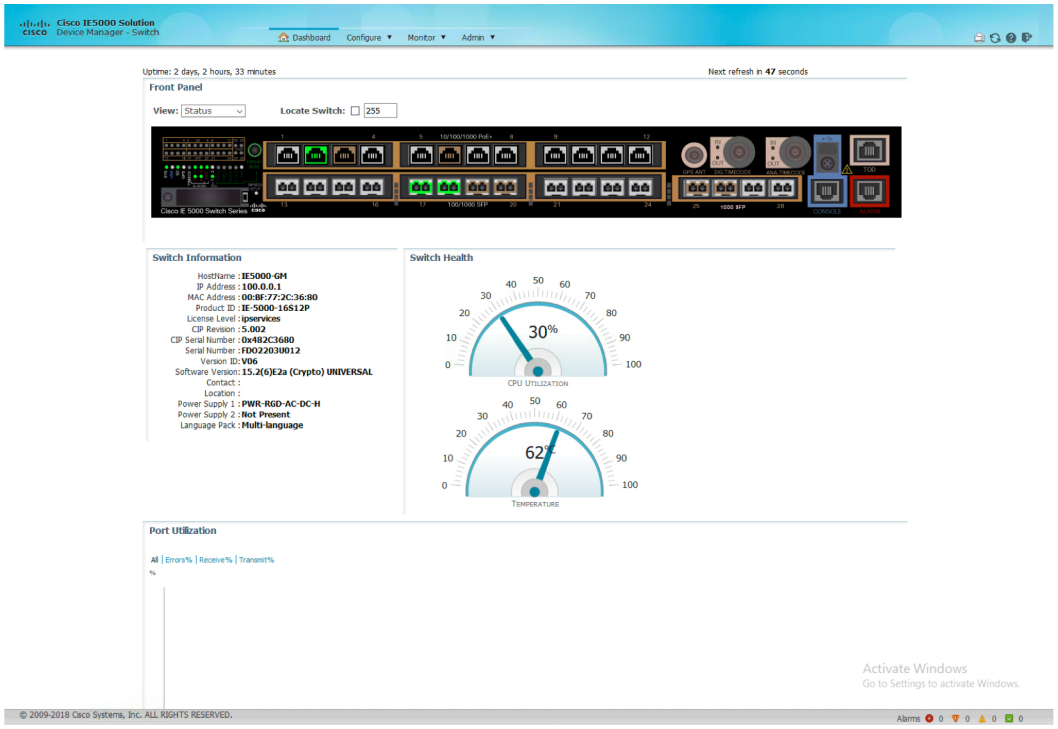
1. Log in to the switch using Device Manager credentials, as shown in Figure 23.

Figure 23 Device Manager Login Screen



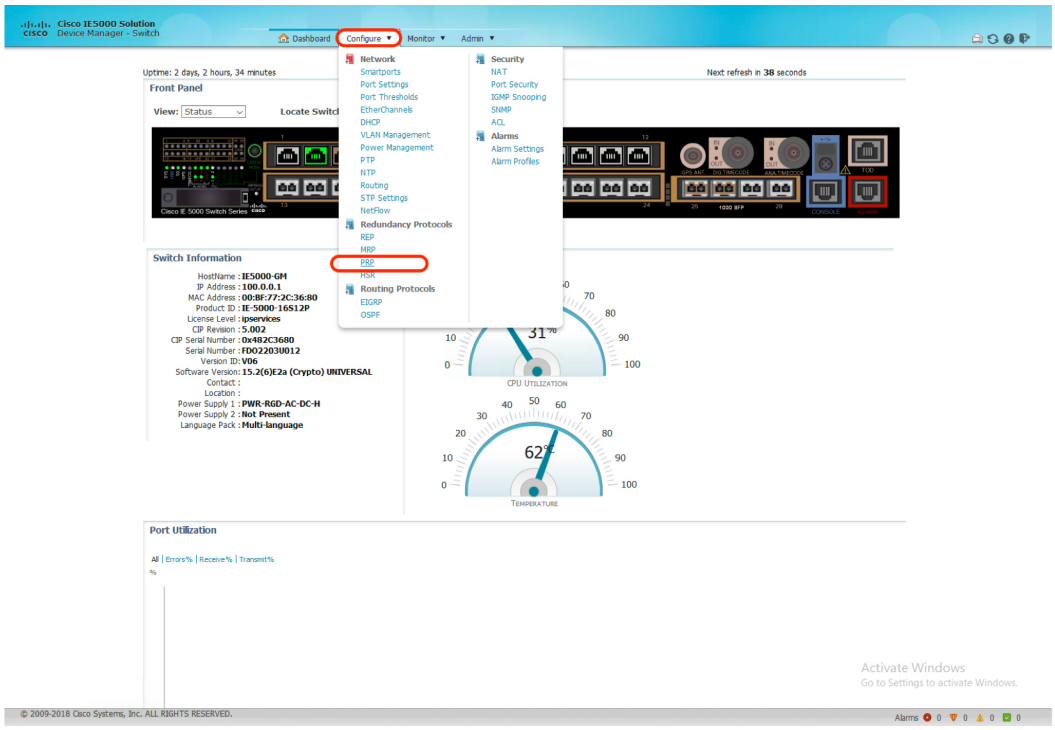
2. After a successful login, the Dashboard for the switch loads, as shown in Figure 24.

Figure 24 Device Manager Dashboard



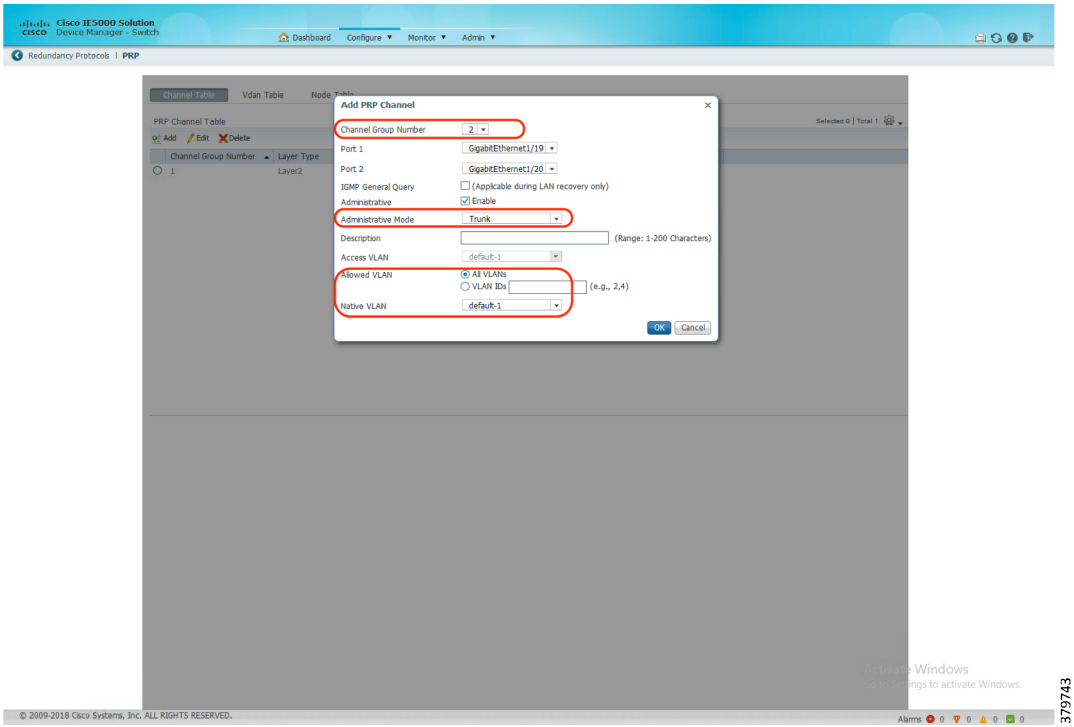
3. Configure PRP by selecting the **PRP** option under the **Configure** tab as highlighted in Figure 25.

Figure 25 Configure PRP Using Device Manager



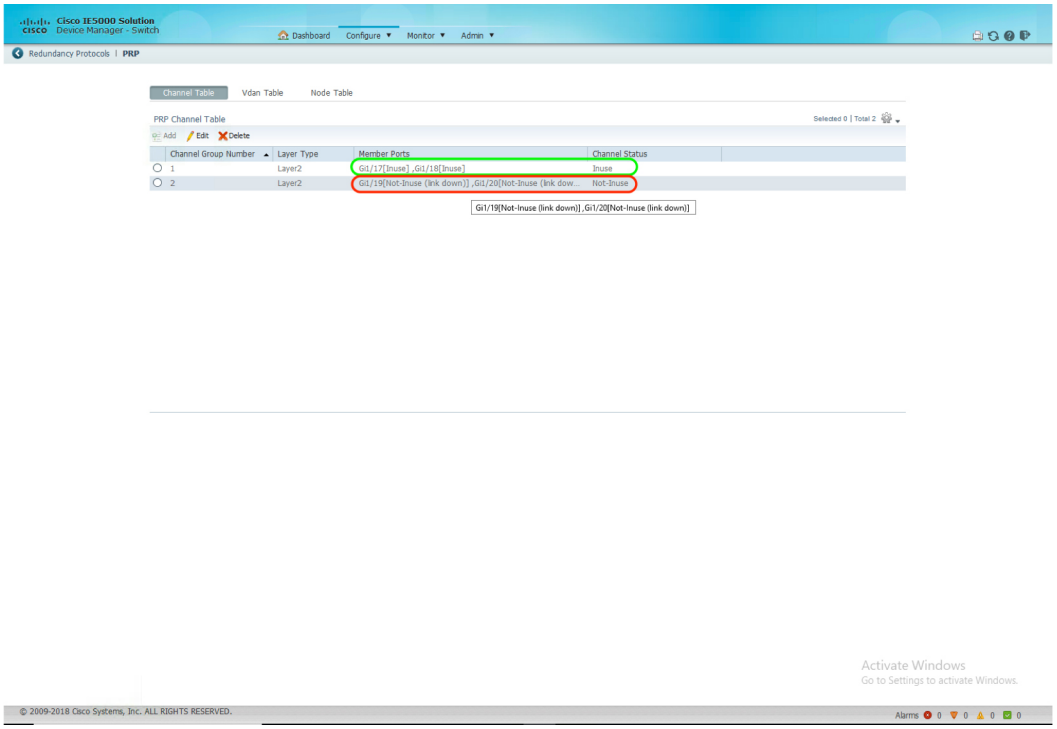
4. Configure PRP Channel properties like channel number, switchport mode, allowed VLANs, native VLANs, and so on as highlighted in Figure 26.

Figure 26 Configure PRP Channel Properties



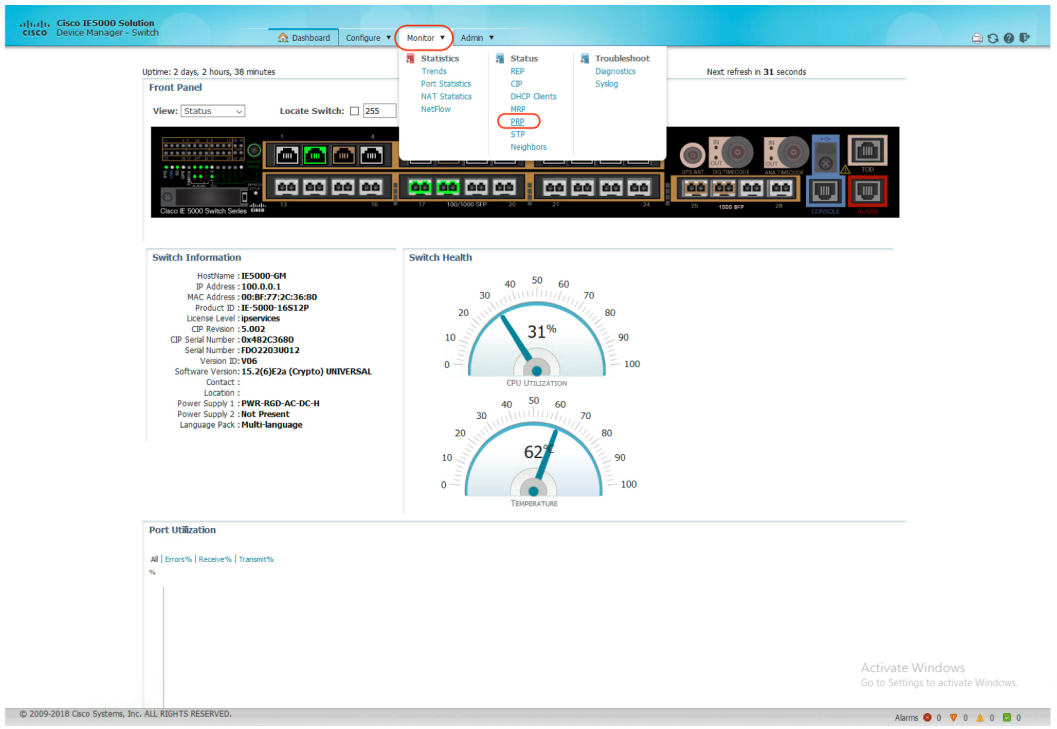
5. The status of the PRP Channel would be reflected as soon as the configuration of the PRP channel is completed as highlighted in Figure 27.

Figure 27 PRP Channel Status



6. Select the **PRP** option listed under the **Monitor** tab to check details of VDAN and Node table details, as shown in Figure 28.

Figure 28 Monitor PRP



Implementing PTP over PRP

PTP over PRP has been validated on the following platforms, all of which are deployable in the utility substation LAN:

- Cisco IE 4000
- Cisco IE 4010
- Cisco IE 5000

Table 13 PTP Over PRP Cisco IE Switches and Roles

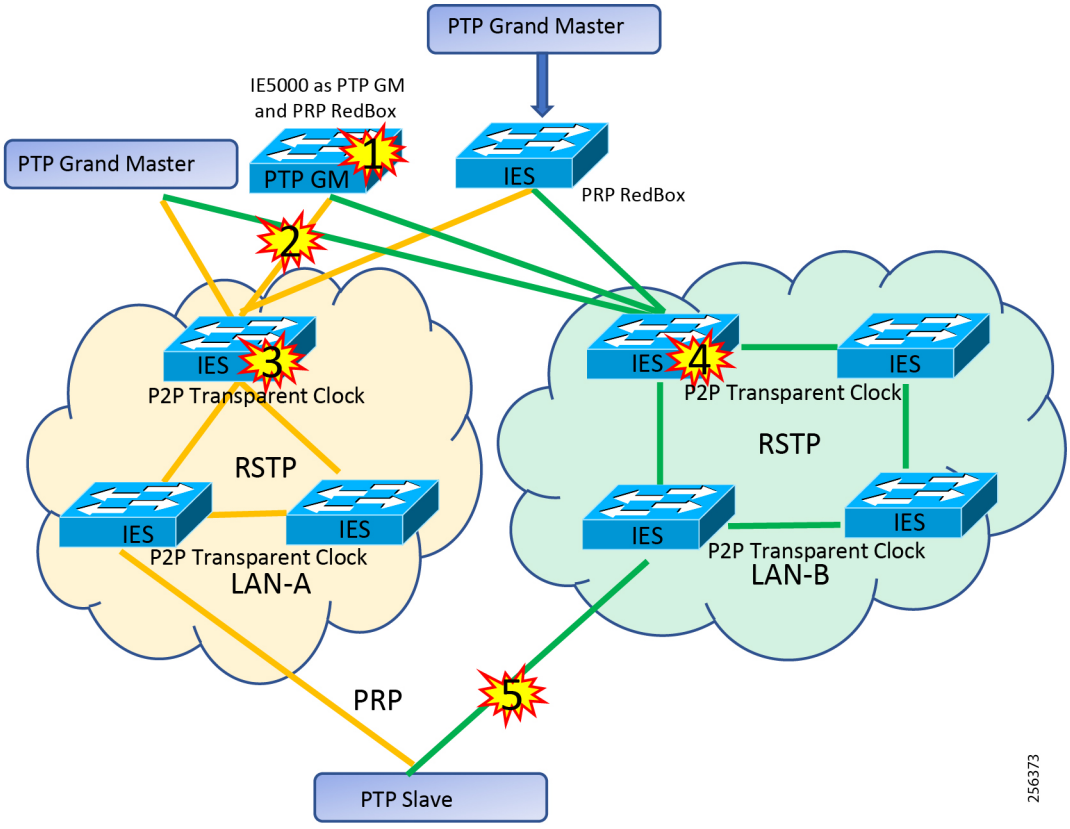
SKU	Role	IOS Version
Cisco IE 5000	PRP RedBox and PTP Grandmaster	15.2.6E2a
Cisco IE 4000	RSTP	15.2.6E2a
Cisco IE 4010	PRP RedBox, RSTP	15.2.6E2a

Cisco recommends that the PTP grandmaster (GM) be connected to both PRP LANs if you want to leverage the PTP over PRP feature. Otherwise, only devices in the single LAN where the PTP GM is connected can be synchronized.

On Cisco IE switches, PTP over PRP supports VLAN tagged and untagged PTP packets. PTP packets, by default, have a QoS CoS bit set to 4. Cisco IE switches allow the network administrator to override the CoS to a different value. Also, note that some other vendors may have the PTP domain setting hard-coded to use domain 0. Cisco IE switches default to the same domain number of 0 and the switches allow the domain to be changed.

The topology in Figure 29 shows the use of a Cisco IE 5000 acting as a PRP Redbox and also as a PTP grandmaster and Cisco IE 4010 acting as PRP Redbox with PTP grandmaster connected to the PRP Redbox, thereby providing the required resiliency for PTP over PRP.

Figure 29 PTP over PRP



To validate the resiliency and the corresponding latency requirements of the network, failures were introduced at different points as highlighted and numbered in Figure 29:

- (1)—PTP Grandmaster
- (2) and (5)—A redundant network link
- (3) and (4)—A redundant network switch

During validation, a Cisco IE 5000 was used as a PTP Boundary Clock/Slave deriving its clock from either of the PTP grandmasters through the PRP network. Cisco IE 4000 and Cisco IE 4010 switches were used as RSTP switches and are configured as P2P Transparent clocks. The network helps provide resiliency in terms of two different PTP grandmasters and network links. Failure of either a network link or one of the PTP grandmasters did not impact the PTP source for PTP Slave/Client devices.

Traffic in the network consisted of Sample Values (tagged—VLAN 0 and VLAN 110), GOOSE (VLAN 120), and untagged IP packets.

Note: PTP feature over HSR ring is currently not supported.

Note that the PTP GM can be positioned in a PRP topology as follows:

- A Redbox connected to both LAN-A and LAN-B and the PTP grandmaster as a RedBox.
- A VDAN connected to a PRP RedBox and the PTP grandmaster connected to a PRP RedBox.
- A DAN and the PTP grandmaster clock directly attached to both PRP LANs.

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.

Configuring PTP over PRP Using CLI

Follow these steps to configure PTP over PRP network. 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:

```
Switch(config)# vlan dot1q tag native
```

- 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 interface level command **ptp vlan <*vlanID*>**. With this configuration change, the switch would tag all ptp packets traversing through the interface with the corresponding VLAN.

  Note: PTP VLAN configuration is supported only in PTP boundary clock mode while using Cisco IOS Version 15.2.6E2a. PTP VLAN configuration for PTP Transparent clock mode will be supported in future releases.

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# ptp vlan <vlanID>
Switch(config-if)# end
```

  Note: When PRP LANs use any of the spanning tree protocols like RSTP for loop avoidance, some type of PTP packets are looped. This issue is observed while using Cisco IOS Version 15.2.6E2a. The corresponding defect is CSCvm17877. In such scenarios, it is recommended to use a Cisco IOS version with a fix for defect CSCvm17877.

When the network requires 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 as per IEEE C37.238 standard in PTP Power profile mode.
- Force the switch to set CoS value for PTP packets by entering global **ptp packet <*cos*>** command:

```
Switch(config)# ptp packet <cos>
```

Summary of Steps

1. Enter global configuration mode:

```
Switch# configure terminal
```

2. Set the Power Profile:

```
Switch(config)# ptp profile power
```

3. Specify the synchronization clock mode:

```
Switch(config)# ptp mode {boundary pdelay-req|p2ptransparent|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 or jitter.

- `mode p2ptransparent`—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:

```
Switch(config)# 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).

Verifying PTP Over PRP Using CLI

Use the following commands to check PTP clock type, grandmaster properties, and clock source:

```
Switch# show ptp clock
//In case of Boundary clock//
 PTP CLOCK INFO
  PTP Device Type: 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

Switch# 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

Switch# show ptp parent
//shows the parent to which the PTP clock 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

Switch# show clock detail
08:41:04.904 UTC Thu Dec 13 2018
Time source is PTP

Switch# 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 PRP Redbox and PTP GM Cisco IE 5000 switch, the PTP state on PRP member ports can be checked as follows. The PTP port state of both PRP member ports should be MASTER:

```
Switch# 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 PRP Redbox and PTP boundary clock Cisco IE 5000 switch, the PTP state on PRP member ports can be checked as follows. The active port state should be SLAVE and the standby port state should be PASSIVE_SLAVE. If the active port fails, the standby port changes to SLAVE state:

```
Switch# 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

Switch# 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
```

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 of PTP packets.

  ```
  Switch(config)# ptp mode p2ptransparent
  ```

- Configure the switch to process a non-compliant PTP grandmaster's announce messages without Organization_extension and Alternate_timescale TLVs using the following command:

  ```
  Switch(config)# ptp allow-without-tlv
  ```

- In interoperability scenarios, it is best to use default PTP domain value, which as per C37.238:2011 standard is 0 (zero). The default PTP domain value on IE switches is set to 0 (zero). It can also be configured using the following command:

  ```
  Switch(config)# ptp domain 0
  ```

Configuring PTP Over PRP Using the Device Manager

The task of configuring PTP over PRP using the embedded device manager is no different than configuring each of the features independently. Refer to:

- Configuring GNSS and GPS on Cisco IE 5000 Using Device Manager, page 66
- Configuring PRP RedBox Using Device Manager, page 54

PTP Grandmaster

When deploying PTP in a utility substation, Cisco recommends deploying the PTP power profile. This profile will be used by the IEDs and the configuration of PTP on the switches needs to match the expectation of the IEDs.

PTP Power Profile settings on Cisco IE switches are:

- Two-step, peer-to-peer (peer delay) transparent clocks
- Layer 2 multicast packets
- PTP announce messages include the following Type, Length, and Value (TLV) message extensions to indicate the GM identifier:
  - Organization_extension
  - Alternate_timescale
  - Note: Cisco IE switches can be configured to process packets from a PTP grandmaster that sends announce messages without Organization_extension and Alternate_timescale TLVs.

Cisco IE 5000 GNSS and GPS

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 GNSS receiver that helps enable 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.

Configuring GNSS and GPS on Cisco IE 5000 Using CLI

Before you begin, note:

- 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:

```
Switch# show version | include Version ID
Version ID                      : V06

Switch# show version | include GNSS
GNSS firmware version           : 1.04
```

- GNSS is available for all Cisco IOS software feature sets for Cisco IE switches (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.

Summary of Steps

1. Enter global configuration mode:

```
Switch# configure terminal
```

2. Enable GNSS:

```
Switch(config)# gnss
```

3. Configure the switch for grandmaster-boundary clock mode:

```
Switch(config)# ptp mode gmc-bc
Switch(config)# end
```

Verifying GNSS and GPS on Cisco IE 5000

Use the following commands to verify GNSS operation on Cisco IE 5000:

```
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
       31           10             1                1           0                49
       14           11             1                1           0                43

Switch# show gnss time
Current GNSS Time:
Time: 2018/12/13  07:07:18 UTC Offset: 18

Switch# show gnss location
Current GNSS Location:
  LOC: 12:56.184485149 N  77:41.767297649 E  828.854749999 m

Switch# show platform gnss
Board ID: 0x5000000 (Production SKU)
GNSS Chip:
  Hardware code: 3023 - RES SMT 360
  Serial Number: 1170159173
  Build Date: 3/15/2017

Switch# show ptp clock
 PTP CLOCK INFO
  PTP Device Type: Grand Master clock - Boundary clock
  PTP Device Profile: Power Profile
  Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Clock Domain: 10
  Number of PTP ports: 28
  PTP Packet priority: 4
  Time Transfer: Feedforward
  Priority1: 128
  Priority2: 128
  Clock Quality:
        Class: 6
        Accuracy: Within 250ns
        Offset (log variance): N/A
```

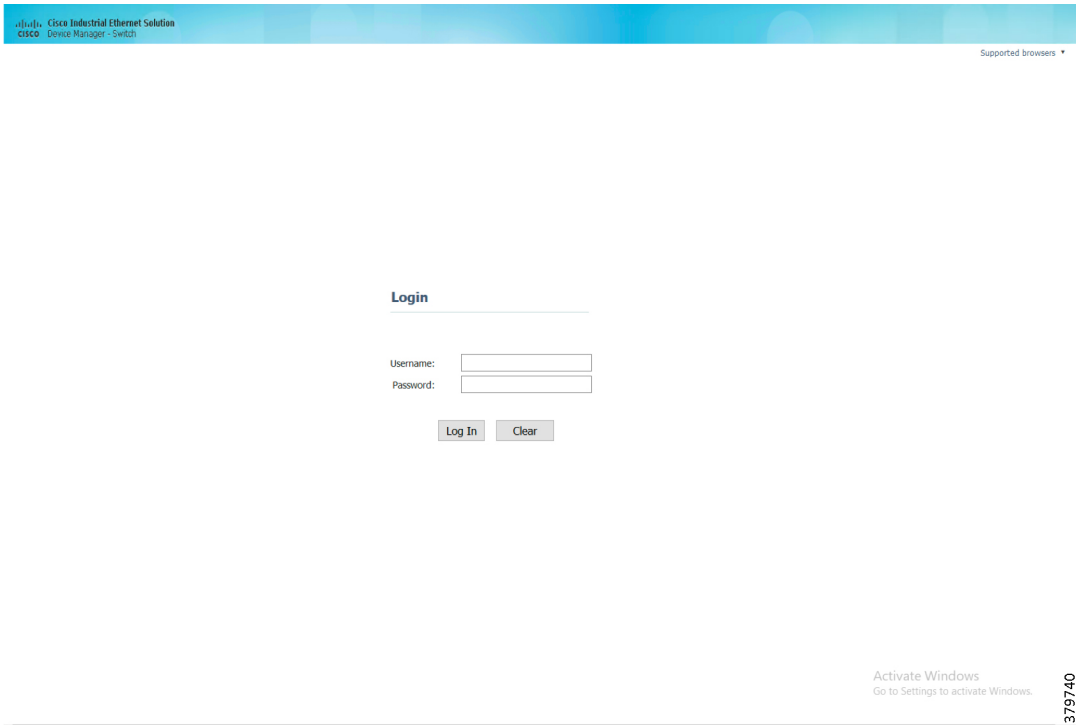
```
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 0
  Local clock time: 12:37:40 IST Dec 13 2018

Switch# 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
```

Configuring GNSS and GPS on Cisco IE 5000 Using Device Manager

This section assumes that the Cisco IE switch has been installed and pre-configured with an IP address for remote access. For more details on setting up a Cisco IE switch, refer to the Cisco IE switch installation guides.

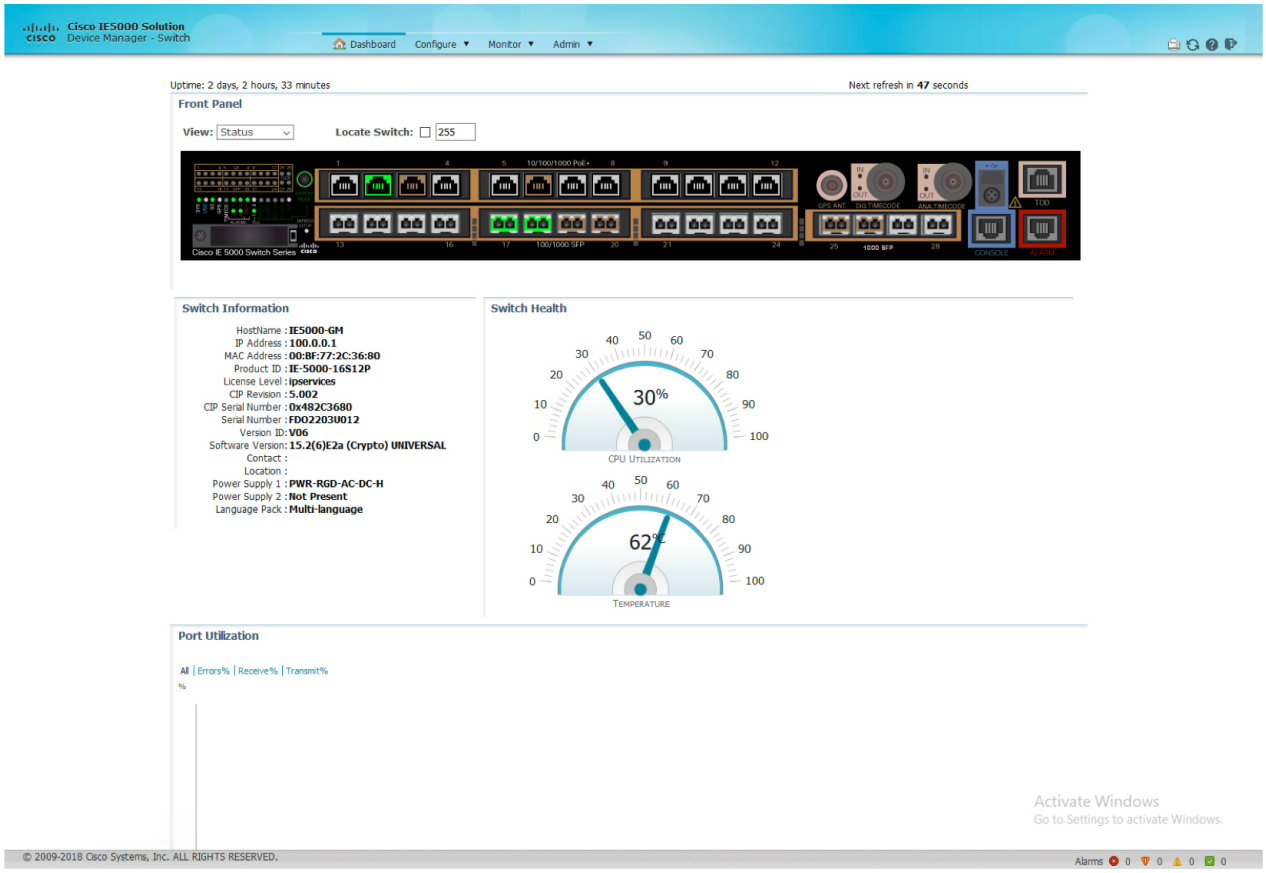
1. Log in to the switch using Device Manager credentials, as shown in Figure 30.

Figure 30 Device Manager Login Screen



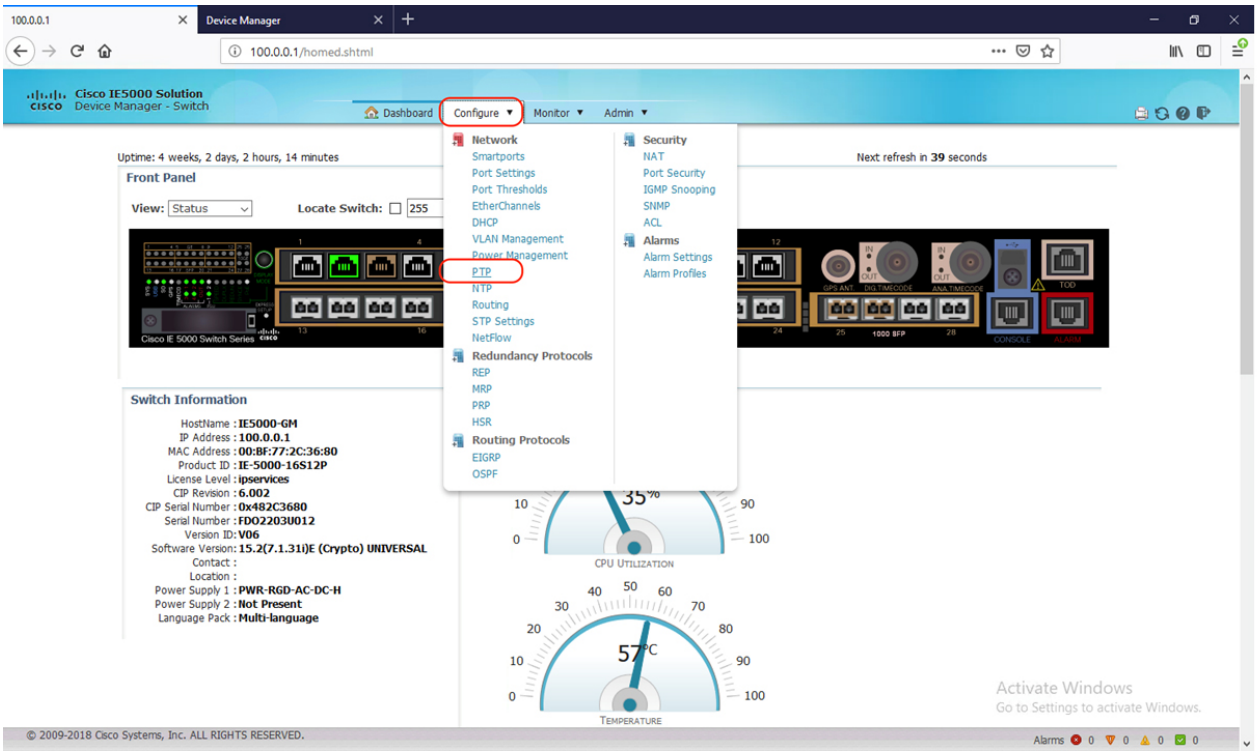
2. After a successful login, the Dashboard for the switch loads, as shown in Figure 31.

Figure 31 Cisco IE Switch Dashboard in Device Manager



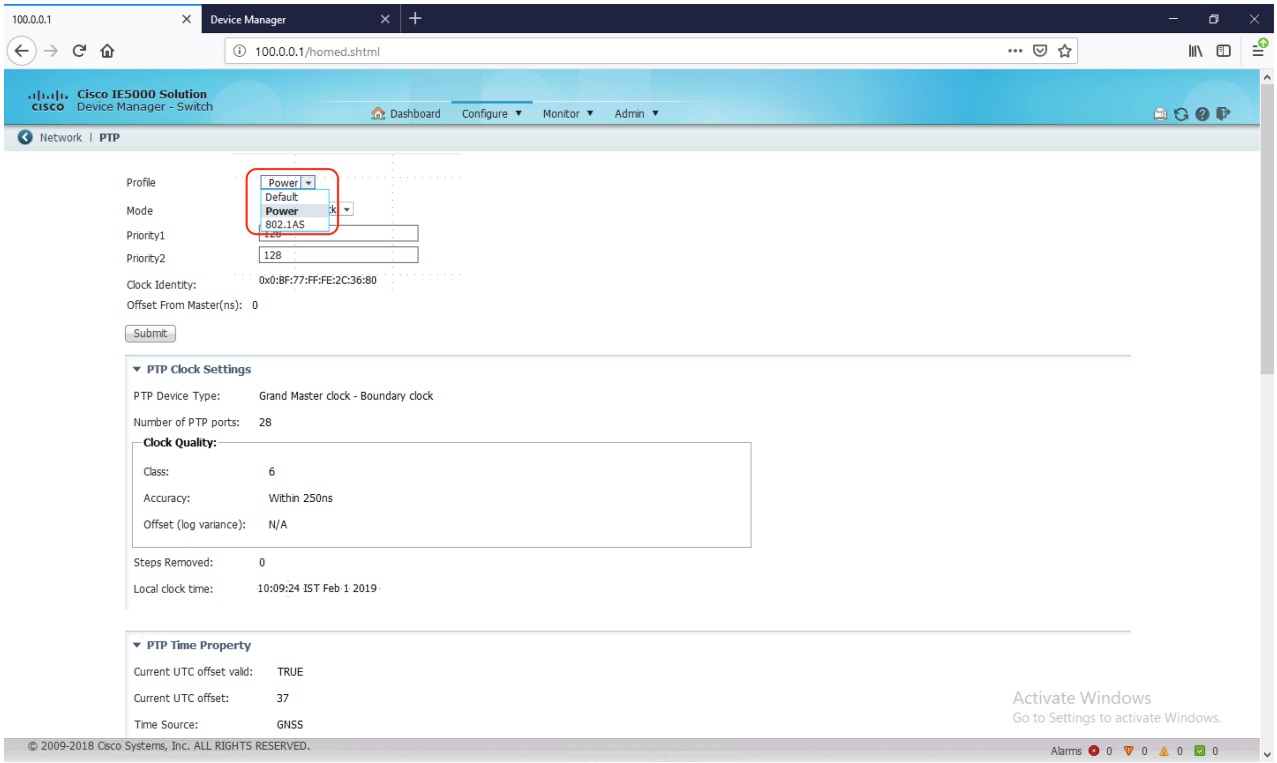
3. Configure PTP by selecting the **PTP** option under the **Configure** tab as highlighted in Figure 32.

Figure 32 Navigating PTP Settings in Device Manager



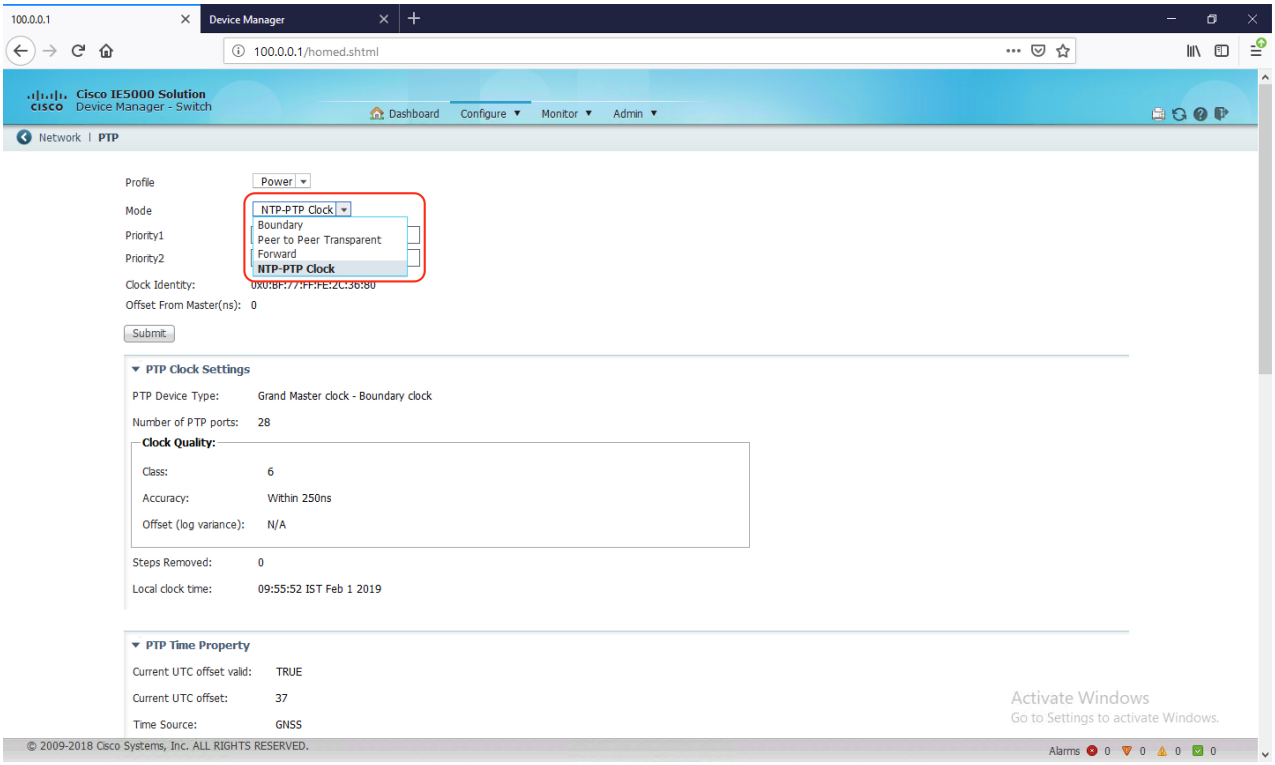
4. Select the **PTP Power** profile as highlighted in Figure 33.

Figure 33 Selecting PTP Power Profile in Device Manager



5. Select **NTP-PTP** mode if the Cisco IE 5000 needs to be configured as a PTP grandmaster. The options can be selected as highlighted in Figure 34.

Figure 34 Selecting PTP Mode in Device Manager



Note: In case of other Cisco IE switches like the Cisco IE 4000 and Cisco IE 4010, the PTP grandmaster function is not supported. Choose an appropriate operating mode according to your requirements.

Implementing QoS for Substation LAN

The Cisco IE 4000, Cisco IE 5000, and Cisco IE 4010 series switches support hierarchical QoS (HQoS) by using the modular QoS CLI (MQC) to help provide a granular and flexible QoS architecture. The modular approach can be implemented using the following steps.

Before you begin, note:

- When the network requires 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 as per IEEE C37.238 standard in PTP power profile mode.
  - Force the switch to set CoS value for PTP packets by entering the following global command:

```
Switch(config)# ptp packet <cos>
```

- Cisco IE switches preserve VLAN 0 CoS in the ingress, but do not in the egress direction unless the native VLAN of the egress trunk interface is changed.
- When an IED sends VLAN 0 tagged packet, it is recommended to configure the IED-facing interface and the uplink interfaces as trunk port allowing VLAN 1 along with other required VLANs:

```
Switch(config)# interface GigabitEthernet 1/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1
Switch(config-if)# end
```

Summary of Steps

1. Identify and classify GOOSE traffic-MAC ACLs were used for classifying GOOSE traffic in this deployment because all GOOSE packets have a common EtherType field of 0x88b8:

```
mac access-list extended GOOSE_Match
 permit any any 0x88B8 0x0
```

2. Identify and classify Sample Value traffic-MAC ACLs were used for classifying SV traffic in this deployment because all Sample Value packets have a common EtherType field of 0x88bA:

```
mac access-list extended SV_Match
 permit any any 0x88BA 0x0
```

3. Create class-maps to classify GOOSE and SV packets by associating respective MAC ACLs:

```
class-map match-all SV
 match access-group name SV_Match
!
class-map match-all GOOSE
 match access-group name GOOSE_Match
```

4. Create an input traffic policy that marks the respective traffic with a QoS group:

```
policy-map TestInputSCADA
 class SV
  set qos-group 1
 class GOOSE
  set qos-group 1
```

5. Create an egress traffic policy to apply QoS functions like queuing, policing, and shaping. The choice of these functions depends on their point of application and requirements. For example, to restrict traffic at an ingress interface, policing should be used. However, to prioritize traffic at the egress, priority queuing is used. If guaranteed bandwidth is required, class-based weighted fair queuing (CBWFQ) is used. It is recommended to classify GOOSE and SV traffic as priority queue traffic.

```
policy-map TestOutSCADA
 class qos_group_1
  priority
  police 100000000
```

6. Attach the appropriate policy to the desired interface:

```
interface GigabitEthernet1/28
 description connected IE4010-006 port-26
 switchport mode trunk
 load-interval 30
 spanning-tree portfast edge
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
```

Verifying QoS in the Substation LAN

Use the following commands to verify QoS operations:

```
Switch# show policy-map interface GigabitEthernet 1/1 output
```

```
 GigabitEthernet1/1
  Service-policy output: TestOutSCADA
    Class-map: qos_group_1 (match-all)
      147413211 packets
      Match: qos-group 1
        Priority
      police cir 100000000 bc 1000000
         conform-action transmit
         exceed-action drop
      conform: 147436751 (packets) exceed: 0 (packets)
      Output Queue:
        Max queue-limit default threshold: 272
        Tail Packets Drop: 0
    Class-map: class-default (match-any)
      11440189 packets
      Match: any
        Output Queue:
          Max queue-limit default threshold: 272
          Tail Packets Drop: 0

Switch# show policy-map interface GigabitEthernet 1/28 input
 GigabitEthernet1/28
  Service-policy input: TestInputSCADA
    Class-map: SV (match-all)
      0 packets
      Match: access-group name SV_Match
    Set qos-group 1
    Class-map: GOOSE (match-all)
      0 packets
      Match: access-group name GOOSE_Match
    Set qos-group 1
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

For additional details on QoS deployment methodology and specific examples, see *Enterprise QoS Solution Reference Network Design Guide*:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSPref.html

Conclusions

Table 14 summarizes utility substation automation considerations.

Table 14 Utility Substation Automation Consideration Summary

Area	Utility Substation Automation Considerations
Industry Needs	■ Operational improvements and modernization ■ Realtime data sensing, collection, analyzing, and logging ■ Monitoring and control ■ Security ■ Operational cost reduction
Types of Control Systems	■ SCADA ■ IEC 61850 ■ PLCs
Requirements	■ Availability ■ Manageability ■ Performance ■ Resiliency ■ Scale
Ruggedization and Environmental	■ Typically required within the ESP Zone ■ Carpeted space *can* begin outside of the ESP zone, but this depends on the utility substation environmental requirements (varies by utility).
Cisco Reference Architecture in this CVD	■ Zone-based within a single substation ■ This CVD explores communications within a single (ESP) zone.
Facilities and Geographical Considerations	■ Decentralized facilities ■ Enterprise can be geographically disconnected from Control Center. ■ The Control Center is geographically disconnected from the Substation. ■ Enterprise, Control Center, and Substations are all interconnected over a WAN. ■ Each Substation has its own DMZ and zones.
Real-time Applications	■ Yes ■ Real-time application support within a network Layer 2 boundary. Crossing into Layer 3 (leaving the substation) diminishes the ability to maintain real-time traffic support. ■ Demanding applications that require low latency and jitter ■ Distribution of precise time

Table 14 Utility Substation Automation Consideration Summary (continued)

Standards	■ IEEE 1613 2009 provides environmental and hardening requirements. ■ IEC 61850, 62351, and 62443 provide recommended best practices and reference topologies. ■ NERC-CIP provides North American regulatory compliance because an end-to-end security architecture is needed to protect power systems. ■ NIST provides a security framework applicable in but more commonly outside of North America.
Protocols	Utility protocols include: ■ SCADA Modbus and DNP3 (serial and IP variants) ■ IEC 61850 GOOSE, SV, and MMS
Functional Segmentation	■ Yes
Operations Team	■ Responsible for grid monitoring and control functions
IT Team	■ Responsible for enterprise applications, security, and network connectivity
IT / OT Convergence	■ Yes ■ Teams are working together to merge the typically siloed application networks, converge capabilities, and drive collaboration.
Zones	Station Edge: ■ DMZ ■ Zone-based firewall ■ Layer 3 boundary to control center Substation contains: ■ ESP Zone – Station Bus – Process Bus – Mostly Layer 2 traffic ■ Multiservice Zone – Physical and cybersecurity Corporate Zone – Extended enterprise Control Center contains: ■ Remote Zones for ESP (operations), Multiservice, and Corporate ■ Each zone connectivity, from Control Center to Substation, is separated over a logical Layer 3 Virtual Private Network (L3VPN).

Table 14 Utility Substation Automation Consideration Summary (continued)

Applications	■ Connect grid devices including sensors, actuators, and controllers and assets such as RTUs, PLCs, and IEDs ■ Enable remote access to production assets and personnel to improve uptime ■ Support utility applications such as Supervisory Control and Data Acquisition (SCADA), historians, and asset management ■ Support relevant network services including DNS, DHCP, timing, authentication, and so on ■ Support a secure infrastructure aligned with IEC 61850/62443 including segmentation, access control, and remote access ■ Enable IoT applications such as predictive analytics and maintenance ■ Remote access to DMZ and security
Safety, Security	■ Yes ■ Logical segmentation across all zones and functions ■ Differences in where the DMZ lives (Substation edge)

Table 14 Utility Substation Automation Consideration Summary (continued)

Performance QoS, Timing	■ QoS to protect real-time traffic, VLAN 0 ■ Segmentation—VLANs and Multicast filtering ■ PTP Power Profile ■ PTP over PRP (both LANs)
Resiliency Requirements	■ Yes ■ Layer 2 fast convergence protocols include: – RSTP – REP – PRP – HSR – HSR + PRP ■ Selection depends on application convergence requirements ■ There are pros and cons to each.
Protocol Support on Purpose-Built Switching Platforms	■ Yes ■ Common platform-set used in a utility substation ESP (and possibly other zones within a substation, depending on environmental requirements). See left column. ■ DIN-Rail Mount: – Cisco IE 1000 – Cisco IE 2000U (utility part identifier) – Cisco IE 4000 ■ Rack-mount: – Cisco IE 4010 – Cisco IE 5000

This SA LAN and Security CVD version 2.3.2 covered:

- Ethernet in the electronic security perimeter (ESP) zone
- The new Cisco IE 4010
- The addition of High-Availability Seamless Redundancy (HSR) single attached node (SAN) protocol
- An implementation option for HSR and Parallel Redundancy Protocol (PRP) lossless protocol “dual RedBox”
- Cisco IE 5000 switch support using the onboard receiver for GNSS/GPS, which allows the Cisco IE 5000 to directly act as a Precision Time Protocol (PTP) 1588 v2 grandmaster (GM)
- Cisco IE switch support for the deployment of PTP 1588 v2 over both PRP LANs

- Cisco's evolving solutions for cybersecurity concerns and the value of enabling Cisco NetFlow and Stealthwatch for higher traffic visibility, segmentation, and anomaly detection on Cisco IE switches.
- Supporting architectures and validated implementation examples for all of the above, demonstrating what can be delivered.

This document intends to make a case for moving forward with Ethernet in substations, since Ethernet can be used to help build an intelligent, easy-to-maintain, flexible, and cost-effective alternative to hard-wired and serial-based substation deployments. The UCA IuG worked diligently on IEC 61850 standards that help offer device and system interoperability, ease of configuration, long term stability, and extensibility.

Cisco validated architectures can be used to help overcome the challenges involved in planning and securing a substation automation implementation.

Related Documentation

Refer to previous iterations of the SA LAN and Security solution CVDs at the following links on Cisco SalesConnect.

Note: If you do not have access to any of these Cisco SalesConnect links, ask your Cisco account team to help provide you with the documentation. However, some of the documents require a signed non-disclosure agreement (NDA) with Cisco.

- 1.5: Smart Grid Substation Automation Design and Implementation Guide
  https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-industries/sasr-design-implementation-guide.pdf
- 2.2.1: Cisco Connected Utilities Substation Security Configuration Guide
  https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/substation-security.pdf
- 2.3.1: Cisco Connected Utilities 2.3.1 Substation Automation LAN and Security
  https://www.cisco.com/c/dam/en/us/products/se/2017/2/Collateral/utilities-validatd-designs.pdf

Other related documentation:

- Networking and Security in Industrial Automation Environments Design and Implementation Guide
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html
- Design Zone for Industry:
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html#~stickynav=1
- Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000:
  - Switch Software
    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.html
  - Switch Software Smartports configuration
    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmacro.html
- Cisco Industrial Network Director:
  - http://www.cisco.com/go/ind
  - Network Management for Operational Technology in Connected Factory Architectures
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD/IND_Connected_Factory_CRD.html

Glossary

The acronyms in Table 15 are used in the SA LAN CVD version 2.3.2.

Table 15 Acronyms

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AP	Access Point
CBWFQ	Class-Based Weighted Fair Queuing
CE	Carrier Ethernet
CG	Connected Grid
CIP	Critical Infrastructure Protection
CLI	Command-Line Interface
CoS	Class of Service
CorpSS	Corporate Substation
CT	Current Transformer
CVD	Cisco Validated Designs
DANH	Doubly Attached Nodes implementing HSR
DAU	Data Acquisition Unit
DMZ	Demilitarized Zone
DSC	Differentiated Services Code Point
ESP	Electronic Security Perimeter
GM	Grandmaster
GNSS	Global Navigation Satellite System
GOOSE	Generic Object-Oriented Substation Events
GPS	Global Positioning System
HA	High Availability
HMI	Human Machine Interface
HQoS	Hierarchical Quality of Service
HSR	High-Availability Seamless Redundancy
IA	industrial Automation
IE	(Cisco) Industrial Ethernet
IEC	International Electrotechnical Commission
IED	Intelligent End Device
IND	Cisco Industrial Network Director
IP	Internet Protocol
IRIG	Inter-Range Instrumentation Group
ISE	Identity Services Engine
IT	Information Technology
L3VPN	Layer 3 Virtual Private Network

Table 15 Acronyms (continued)

Acronym	Definition
LAN	Local Area Network
MAC	Media Access Control
MQC	Modular QoS Command-Line Interface
MMS	Manufacturing Message Specification
MPLS	Multi-protocol Label Switching
MU	Merging Unit
NDA	Non-Disclosure agreement
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NMS	Network Management System
OAM	Operations and Maintenance
OT	Operational Technology
PCP	Priority Code Point
PI	(Cisco) Prime Infrastructure
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PoE	Power Over Ethernet
PRP	Parallel Redundancy Protocol
PT	Potential Transformer
PTP	Precision Time Protocol
QoS	Quality of Service
RedBox	Redundancy Box
REP	Resilient Ethernet Protocol
RCT	Redundancy Control Trailer
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
SA	Substation Automation
SAN	Singly-Attached Node
SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description
STP	Spanning Tree Protocol
SV	Sampled Values
TCP	Transmission Control Protocol
TLV	Type, Length, Value
TR	Technical Report
UCA IuG	Utility Communications Architecture International Users Group
UDP	User Datagram Protocol
VDAN	Virtual Dual Attached Node
VID	Version Identifier

Table 15 Acronyms (continued)

Acronym	Definition
VLAN	Virtual Local Area Network
WAN	Wide Area Network
Wi-Fi	IEEE 802.11x Wireless Ethernet Connectivity

Glossary