# Substation Automation Design Guide – The New Digital Substation

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.

The Substation Automation 3.0 Design Guide CVD is a continuation of solution versions 1.5, 2.2.1, 2.3.1., and 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 Other Relevant Documents, page 7.)

## Introduction

The Substation Automation CVD version 3.0 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 and to introduce software-defined network management capabilities with Cisco DNA-Center for the Substation LAN and vManage for Wide-Area Management (WAN).

## Executive Summary

Utilities are facing greater challenges than ever before. Their grids are being asked to handle more sustainable, distributed, and variable energy sources. At the same time, they are being buffeted by environmental impacts such as fires and extreme weather conditions. Their business models are evolving as they serve a greater variety of customers. In more developed countries, much of the utility workforce is retiring, creating skill and resource gaps. And they are being asked to expand electrical capacity as the world reduces carbon emissions. All this while their operations are under constant threat from ever-evolving cybersecurity risks.

The Cisco® Substation Automation solution enables utilities to support new business models, meet regulatory requirements, expand capacity, integrate renewable energy sources, reduce operational costs, and reduce risks to grid operations. The solution supports more than just the core supervisory control and data acquisition (SCADA) systems, adding key use cases involving protection of key assets and power management. Its technology upgrades and network management capabilities reduce operational costs by reducing the network footprint and automating key tasks. The network infrastructure is capable of supporting more devices and handling more bandwidth with more resiliency and capabilities, such as time synchronization and hosting applications. The Substation Automation solution builds on the visibility and security of our Grid Security solution. The portfolio meets the needs of a wide range of transmission and distribution substations. The updated solution helps utilities overcome the following challenges:

- Growing number of process and station bus devices with higher bandwidth requirements
- Limited space in substations for equipment

- Need to reduce cybersecurity risks by providing visibility into and segmentation of substation devices and communication
- Lack of networking skills in grid operations
- Requirements to Integrate and monitor legacy devices
- Regulatory requirements, especially NERC-CIP security
- Need to scale to support more substations

# Business Case

Deploying the Cisco Substation Automation solution helps Utilities meet a wide variety of business objectives in these areas:

- Protects critical grid assets and improves grid reliability and safety
- Reduces operational costs and improves efficiency
- Reduces security risk and meets regulatory compliance
- Supports moving to sustainable energy sources

## Protection, Reliability, and Safety

Our modern societies rely upon reliable power. Utility operators are measured against reliability goals. And Substation operations are critical to maintaining reliable electrical services. They also procure expensive assets that are expected to be maintained and operational for extended lifetimes. The solution is designed to be provide critical communications needed to monitor and protect critical assets, highly resilient to maintain grid reliability and remotely accessible improving safety.

The solution helps achieve reliability and safety via:

- Support for resilient network topologies and network resiliency protocols for rapid and loss-less network recovery and consistent network services to maintain substation operations through any single point of failure
- Using ruggedized network infrastructure designed to have extremely high Mean Time Between Failure (MTBF) and certified for electrical substation operations (e.g. IEC 61850)
- Resilient network infrastructure to maintain uptime and limit downtime when it occurs
- Enable secure remote access to substation networks and infrastructure
- Network management tools automate deployment to quickly identify problems and outages and resolve them quickly by applying machine-learning and artificial intelligence to identify and respond quickly to network issues

## Operational Cost and Efficiency

Utility operators are very sensitive to operation costs and efficiency as they are often semi-regulated, especially around pricing. Reducing costs and improving efficiency are key considerations. The solution helps achieve these by:

- Support for modern, ethernet-based substation protocols such as IEC 61850, DNP3, Modbus/TCP that are core to driving substation digitization
- Reduce the number of devices that are needed to provide the routing, switching, cybersecurity and networks services (e.g. time synchronization) by consolidating features and capabilities into product lines

- Support more bandwidth and performance on the network infrastructure to increase amount and quality of data available (e.g. more telemetry and sensors), improving predictive maintenance, lifetime and efficiency of existing assets.
- Support products with long operational lifecycles and support
- Support for Software-Defined Wide-Area Networks that enable better efficiency from expensive WAN connections, reducing operational costs
- Introducing network management tools to reduce deployment and management costs via automation and AI-driven problem resolution

## Security and regulatory compliance

Cybersecurity risks to utilities are growing in complexity and frequency. The costs in downtime and recovery are increasing. The regulatory requirements are increasing. This solution entails significant cyber security features designed to help utilities meet the regulatory requirements, decrease the costs associated with cybersecurity events and improve protection of substation operations.

Support for key NERC CIP security requirements outlined in the table below.

**Table 1 Key NERC CIP Requirements and Cisco technology support**

| NERC CIP Requirement | Area | Technologies applied |
|---|---|---|
| CIP-002-5.1a | Critical Cyber Asset Identification | Cisco Cyber Vision, IE3400, IE9300, IR8300 |
| CIP-003-8 | Security Management Controls | IR8300 Zone-based Firewall, Cisco ISA 3000 and Firepower firewalls<br>Cisco's DNA-Center, Identity Services Engine and vManage |
| CIP-005-5 | Electronic Security Permimeter(s) | IR8300 Zone-based Firewall and Cisco ISA 3000, Cisco Duo and Anyconnect |
| CIP-007-6 | Systems Security Management | Cisco's DNA-Center, Identity Services Engine and vManage<br>FirePower Management Center, ISA 3000 and FirePower firewall and SecureX security orchestration |
| CIP-008-5 | Incident Reporting and Response Plan | Cyber Vision, DNA-Center, ISE, vManage, Firepower Management Center and SecureX |
| CIP-010-2 | Configuration Change Management and Vulnerability Assessments | Cisco's Cyber Vision, DNA-Center, ISE and vManage |
| CIP-011-2 | Information Protection | Segmentation with firewalls and TrustSec, network infrastructure with encrypted communications (e.g. VPN and MacSec), Anyconnect, DNA-Center, vManage, and ISE with TrustSec based segmentation |
| CIP-013-1 | Supply Chain Management | IEC62443 Product development certified (62443-4-10 and product 62443-4-20) with TrustAnchor support in the network infrastructure |

Other cyber security features include:

- Establishing the Electronic Security Perimeter as defined by the NERC CIP guidelines to protect substation operations via Industrial Firewalls and Zone-based Firewall services in the new Substation router, Cisco's IE8340

- Support for Substation micro-segmentation to establish zones and conduits with Cisco TrustSec technology in the network infrastructure and deployed and managed via Cisco DNA-Center and Identity Services Engine applications
- Secure network infrastructure operations (e.g. secure boot, secure store, anti-counterfeit mechanisms etc.) with Cisco TrustAnchor in the network infrastructure
- Visibility and security analysis of devices (e.g. IEDs, RTUs, PLCs, etc.) connected and their communications via Cisco Cyber Vision
- Support key processes outlined by NERC CIP such as Critical Asset Identification
- IEC Support for modern, ethernet-based substation protocols such as IEC 61850, DNP3, Modbus/TCP that are core to driving substation digitization
- IEC 62443 (Industrial Cybersecurity) certified products and product development

### Sustainability

As the world has recognized and started to take significant action to tackle climate change and make society more sustainable, electrical utilities have a significant role to play. They must use and incorporate more sustainable energy sources, such as wind and solar which require more agile distribution grids. At the same time, electrification of major systems, (e.g. transportation) in our society, moving away from carbon contributing reliance of fossil-fuel burning, leads to significantly more reliance on our electrical utility systems. Major infrastructure enhancements and improvements almost always include electrical grid.

This solution supports the Electrical utilities sustainability initiatives by:

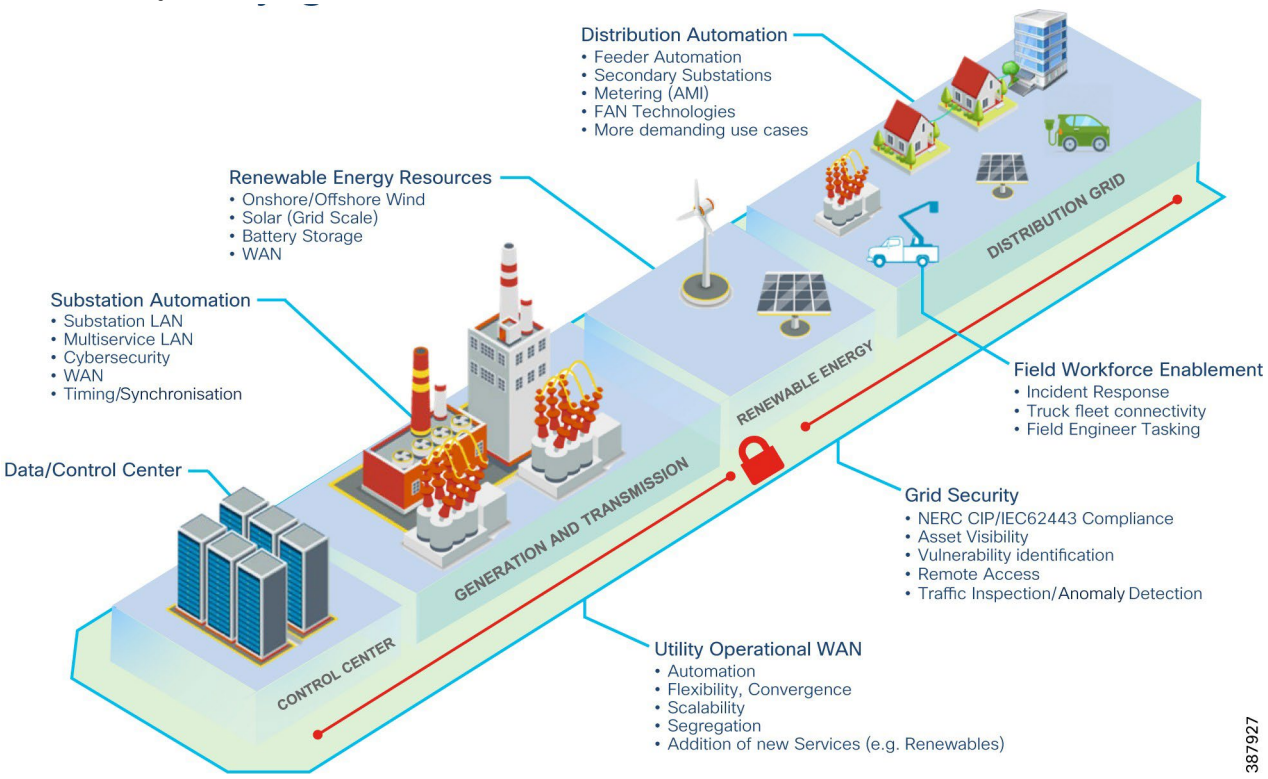
- Enabling further digitalization of the distribution system enabling more real-time control and management to handle the new energy sources and increased demands on the electrical system
- Faster deployment and upgrade to distribution systems with reliable, secure remote access
- Network infrastructure that is more energy efficient, supports Power over Ethernet to efficiently power a range of devices (e.g. cameras, access points, etc.) and is designed for a circular economy

## 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 deploy and implement network and security capabilities to monitor and manage electrical transmission and distribution systems. The solution supports more than just the core supervisory control and data acquisition (SCADA) systems, adding key use cases involving protection of key assets and power management and multi-service networks that exist at or connect through the Substation.

Substation Automation is a critical function in Cisco's solution support for Utility Grid applications. Figure 1 depicts a high-level overview of a Utilities key functions; power generation, distribution automation and field Workforce enablement.

**Figure 1 Utility Grid and Substation Automation Overview**




This solution builds on previous versions that support the following use cases:

- 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

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 in the network infrastructure to provide smoother outages

- PTP in the Substation LAN based upon the 2014 IEEE Precision Time Protocol – Power Profile
- Firewall redundancy

Cisco Substation Automation Solution release 2.3.2 focused on:

- 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

# What's new in Substation Automation

This solution supports and enhances many of the features and use cases listed above. The key new aspects covered in this version include new products and features.

New Features supported in this solution include:

- Substation LAN centralized and automated network deployment and management via Cisco's DNA-Center
- Substation Wide-Area Network (WAN) centralized network deployment and management via Cisco Software-Defined WAN (SD-WAN) technologies (e.g. vManage)

New products introduced to the Substation Automation network and security architecture include:

- The Cisco Catalyst® IE9300 Rugged Series switches with 28 Gigabit Ethernet fiber ports for secure, reliable, low-latency station and process bus communication, IEC 61850-3 and IEEE 1613 compliant and stackable up to 3 units
- The Cisco Catalyst IR8340 multifunctional, modular, rugged Substation router with scalable WAN connectivity, firewall security, application hosting

Both plaftorms are IEC 61850-3 and IEEE 1613 certified and support the following:

- Reliability: a range of resiliency and synchronization protocols (such as High-Availability Seamless Redundancy [HSR] and Parallel Redundancy Protocol [PRP])
- Greater security: a range of features: Zone-Based Firewall (IR8300 only), Cisco Trustsec, IEEE 802.1x Network Access Control, Cisco Trust Anchor, visibility of Substation Automation devices and communication via Cyber Vision and MACsec
- Precision: Support for substation-wide time synchronization (for example, the 2017 IEEE Precision Time Protocol – Power Profile)
- Simplicity: Range of management options, including Cisco DNA Center for switching and Cisco vManage for SD-WAN routing capabilities

## Substation Automation Audience

This document is intended to be used by Utility operators of Electrical Substations and operational Wide-Area Networks and their partners and vendors who deploy, operate and manage electrical grids. 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
- 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, 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.

## Other Relevant Documents

As stated earlier, this solution is based on and integrates with other Utility focused Cisco solutions. Other relevant documents related to Substation Automation include:

Distribution Automation and Secondary Substations:

- Secondary Substation Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG.html
- Secondary Substation Implementation Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/IG/DA-SS-IG.html

Grid Security:

- Grid Security Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/DG/DA-GS-DG.html
- Grid Security Implementation Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/IG/DA-GS-IG.html

- Achieving NERC CIP Compliance https://www.cisco.com/c/en/us/solutions/collateral/industries/white-paper-c11-2396807.html

Virtual RTU:

- Virtual RTU Implementation Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/FAN/Virtual-RTU/IG/CU-VRTU-IG.html

Wide Area Networking:

- Cisco SD-WAN Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

# Substation Automation Architecture

The following section provides an overview of the Substation Automation reference architecture. The architecture is broken down into zones which represent major functions relevant to a grid operators management of Bulk Electric Systems (BES) of which substations are a critical component. The zones break down and definition relies upon definitions and standards set by the North American Electric Reliability Corporation (NERC) for Critical Infrastructure Protection (CIP). Although this is a North American entity, the concepts and functions are applicable to grid operations worldwide.

## Solution Requirements

The Substation Automation architecture is designed to meet the key requirements of Utilities operating their electricity grid. A key set of those requirements are defined by the North American Electric Reliability Corporation (NERC CIP) Critical Infrastructure Protection (CIP) standards.

### Migrating to Ethernet and IP

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.

### NERC CIP Overview

The North American Electric Reliability Corporation (NERC) has established Critical Infrastructure Protection standards “aimed at regulating, enforcing, monitoring and managing the security of the Bulk Electric System (BES) in North America”. Substation operations are a critical function of the BES. These standards describe components of the system, their criticality and protection requirements that Utilities must meet. This solution re-uses the terms and concepts as they are very relevant to Utilities and their Substation Automation operations. It should be noted, this solution cannot be “NERC CIP certified” as that is a Utilities’ responsibility, but it can help customers achieve that objective.

The NERC CIP standard is focused on both physical and cyber security protections for substation operations. For example, there is a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). According to the NERCIP definition of PSP is “The physical border surrounding locations in which Bulk Electrical System Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.” The ESP is a logical “defines a zone of protection around the BES Cyber System”. A BES Cyber System is comprised of BES Cyber Assets,

According to NERCIP definition of PSP is as follows “The physical border surrounding locations in which Bulk Electrical System Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.”. As per Cisco Substation Architecture PSP is further broken down in following zones:

- Substation Core Zone
- Electronic Security Perimeter (ESP) Zone
- Multi Service Zone

- Corporate Substation Zone

The substation integration and automation architecture must allow devices from different suppliers to communicate (interoperate) using an industry-standard protocol. The utility has the flexibility to choose the best devices for each application, provided the suppliers have designed their devices to achieve full functionality with the protocol. The following lists some of the commonly used protocols by Utilities.

Legacy SCADA protocols, which are supported over legacy asynchronous interfaces, include:

- Modbus
- DNP3
- IEC 60870-5-101

Newer SCADA protocols that can be transported over Ethernet interfaces are

- IP-based protocols:
  - Modbus-IP
  - DNP3-IP
  - IEC 60870-5-104
  - IEC 61850 MMS
- Layer 2-based protocols:
  - IEC 61850 GOOSE
  - IEC 61850 SV

## IEC 61850

This international standard defines a communication protocol for “intelligent electronic devices” in electrical substations. As utilities worldwide have focused on transitioning substation automation to digital systems, this standard is being adopted as a key focus for those digital transformations. The standard establishes or references a number of concepts, including those listed below.

- Data and communication models for a range of purposes, including:
  - Manufacturing Message Specification (MMS) for transferring real time process and SCADA data over Ethernet and TCP/IP
  - Generic Object Oriented Substation Events (GOOSE) for transferring data (status, values) between IEDs within the substation in strict time periods (4ms) using multicast Ethernet mechanisms.
  - Sample Values (SV) is a mechanism to publish sampled analog measurements from measurement devices over Ethernet
- Construction, design and operation conditions in which substation equipment, including network infrastructure, must operate.
- Conformance and interoperability testing for substation equipment.

Supporting this protocol is a main focus of this solution. The 61850 communication protocols are described in more detail in the ESP section, where the protocol is largely contained.

## Technical Requirements Summary

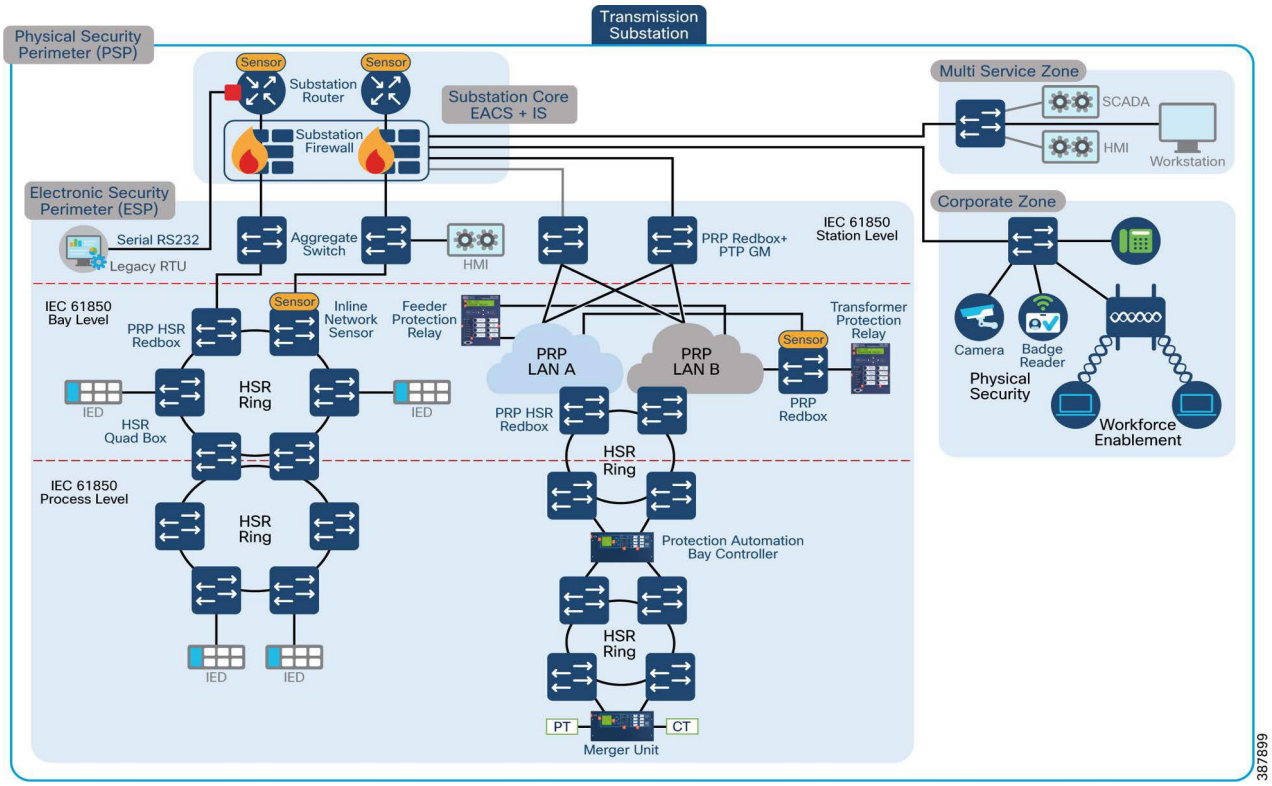
Key Technical Requirements the Substation Automation solution is designed to meet include:

- Maintain low network latency and jitter for the critical Substation communication such as IEC 61850-Goose traffic
- Resilient networks that recover quickly and reduce or eliminate communication loss due to network outages (e.g. link loss, device failure)
- Scale
- Security
- Serviceability
- Usability

# Substation Automation Reference 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. They use Supervisory Control and Data Acquistion (SCADA) applications to manage the remote substations. Figure 2 depicts the Cisco New Digital Substation Automation Reference Architecture.

**Figure 2 Cisco Substation Automation Reference Architecture**




Cisco's New Digital Substation Architecture is comprises an Operations & Control Center, De-Militarized Zone Z), WAN Tier, and Transmission Substation Physical Security Perimeter (PSP) and WAN connectivity for other Secondary substations, local multi-service and corporate networks. Further the PSP is broken into Substation Core, Electronic Security Perimeter (ESP), Multiservice and Corporate (CORP) Zones. Based on IEC 61850 Standard ESP is further subdivided into Station, Bay, and Process Levels.

## Substation Core and WAN Network

Substation Core zone provides two different interfaces as per NERC CIP Electronic Access Point (EAP) and Intermediate System (IS). EAP is Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter. Intermediate System is a Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

Substation Router and Firewall are positioned in Substation Core Zone provide EAP and IS functionalities. Substation router serves as an interface between a local area network in a substation and the utility control or enterprise WAN. Since the WAN comprises, far-flung segments accessed through long-distance data communications, which may be utility-owned or common carrier. When Substation Router is connected as part of Utility Owned backhaul/MPLS network we use define Substation Router on On-Net Substation Router. If Substation Router is connected to public/Cellular network, then Substation Router is named as Off-net Substation Router.

Cisco Substation Router can provide inline firewall (Zone based Firewall) functionality, or we can place dedicated firewall beyond Substation Router to protect ESP, Multi service and Corp Zones. 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

Substation Router provides direct connectivity options to connect Legacy RS232 RTU in Substation ESP premises. Multiple design options exist to transport legacy SCADA traffic towards control center These options are discussed in detail in section Legacy Device connectivity.

External PTP Grand Master can be connected to Substation Router for offering PTP services to ESP Zone.

## Utility WAN

The Utility WAN is often a dedicated WAN infrastructure that connects the Transmission Service Operator (TSO) Control center with various Substations and other field networks and assets. Utility WAN connections can include a host of technologies like Cellular LTE/5G options for public backhaul, Fiber ports to connect utility owned private network, Leased lines or MPLS PE connectivity options as well legacy Multilink PPP backhaul aggregating multiple T1/E1 Circuits.

WAN circuits and backhaul failure options are efficiently designed, provisioned, and managed using Cisco SDWAN Solution. For more details, please refer to the URL:

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

## Electronic Security Perimeter (ESP)

An Electronic Security Perimeter is a logical segmentation used “To manage electronic access to Bulk Electric System (BES) Cyber Systems”, as defined by NERC CIP in CIP-005-5, Cyber Security – Electronic Security Perimeter. The ESP zone includes all grid operations infrastructure in the substation. The ESP is the most critical zone in the substation and requires the highest level of security and availability. Electronic access to the ESP is the role of an Electronic Access Control System (EACS) (reference NERC CIP definitions). In our architecture, the EACS is a key function of the Substation Core and WAN network. The ESP network provides critical communication and cyber security services to the substation infrastructure. SCADA applications in the Operations Control Center require network access to the ESP to collect data from substation infrastructure and manage the substation operations.

## 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). This zone is mapped to NERC CIP Electronic Access Control Systems (EACS) and Electronic Access Monitoring Systems (EAMS).

## Local Corporate Network 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. This zone is mapped to NERC CIP Physical Access Control Systems (PACS) and Physical Access Monitoring Systems (PAMS).

## Operations & Control Center

The Operations & Control Center hosts a number of centralized applications and infrastructure, including:

- Energy Management Systems (EMS) and Outage Management Systems (OMS)
- Headend Router (HER) to aggregate the traffic coming from multiple substations via the Utility WAN,
- A firewall-based DMZ to protect various OT applications
- Network and policy management tools to monitor and manage the Substation networks, such as Cisco's DNAC, ISE, Wireless Lan Controllers (WLC), SDWAN vManage and Firepower Management Center (FMC)
- Industrial cyber security tools such as Cybervison center.

# Electronic Security Perimeter Zone – Design Considerations

The ESP is the network that supports the critical substation operations. The network architecture is designed with high-availability as a key consideration, including the use of loss-less resiliency protocols, such as HSR and PRP. Below is a simplified depiction.

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. Devices like remote terminal units (RTU), Intelligent Electronic Devices (IED), programmable logic controllers (PLCs), relays, transformers, power monitors 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.

Deployment models are typically based on the size of the substation 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 sections CVD.

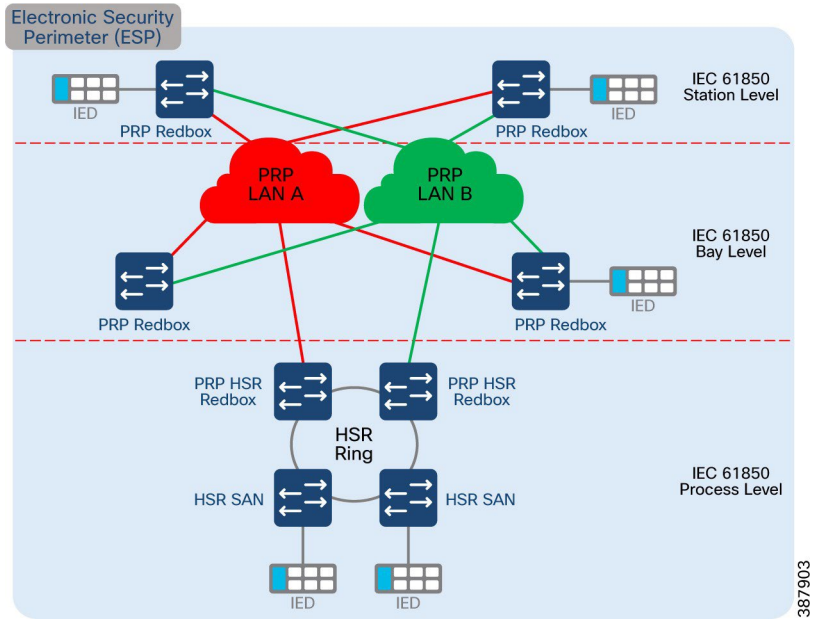
## ESP Architecture

The ESP is the network that supports the critical substation operations. The network architecture is designed with high-availability as a key consideration, including the use of loss-less resiliency protocols, such as HSR and PRP. Below is a simplified depiction. An Electronic Security Perimeter is a logical segmentation used "To manage electronic access to Bulk Electric System (BES) Cyber Systems", as defined by NERC CIP in CIP-005-5, Cyber Security – Electronic Security Perimeter. The ESP zone includes all grid operations infrastructure in the substation. The ESP is the most critical zone in the substation and requires the highest level of security and availability. The ESP network provides critical

communication and cyber security services to the substation infrastructure. SCADA applications in the Operations Control Center require network access to the ESP to collect data from substation infrastructure and manage the substation operations.

The following sample topology depicts various levels of ESP zone.

**Figure 3 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 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.

### 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.

# Applications and Protocols

## IEC 61850

The following are the traffic class definitions as taken from IEC-61850.

[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, 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

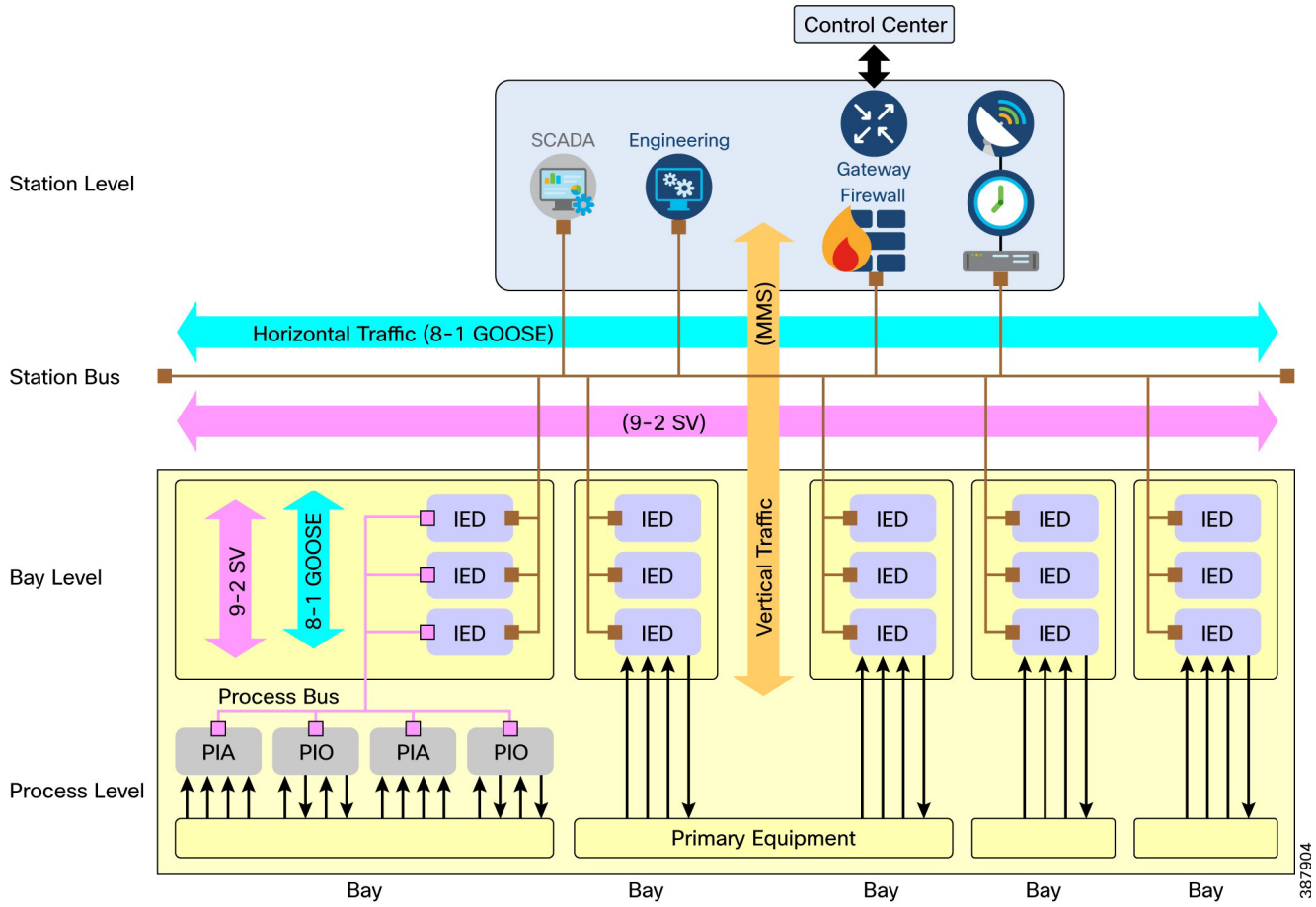
The protocols typically found on a station bus include GOOSE (Layer 2 multicast), MMS, SNTP, SNMP, FTP, and others (Transmission Control Protocol–TCP/IP or User Datagram Protocol–UDP/IP Layer 3 unicast).

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 4 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.

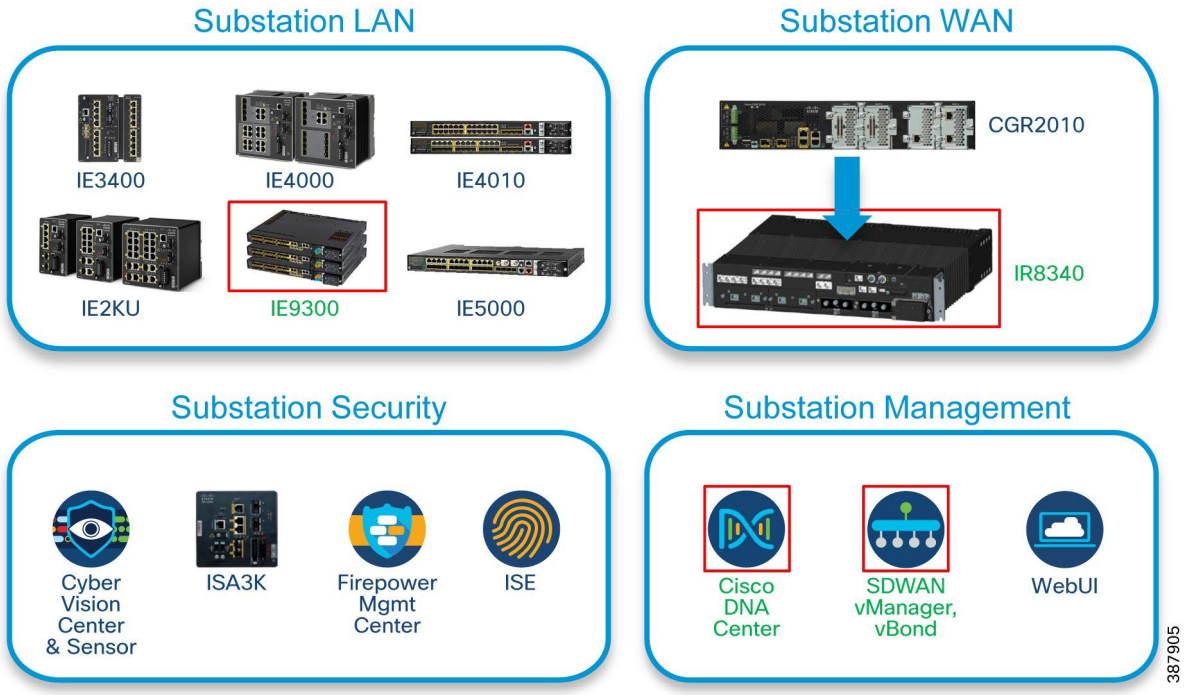
**Figure 4 Where to Find MMS, GOOSE, and SV in Station and Process Bus**




## ESP Portfolio

This section introduces the key products highlighted in the Substation Automation solution for the ESP. It includes the network and security products as they are used to configure, monitor and manage the ESP network and security infrastructure. Design guidance for cyber security and network management tools are in other sections or documents. Below is a depiction of the key pieces of infrastructure for the Substation ESP.

**Figure 5 Substation Automation LAN Portfolio**




There are a number of key roles played by various pieces of the network and cybersecurity portfolio. The below table identifies those roles and the relevant products.

**Table 3 Roles and Products**

| Role | Product |
|---|---|
| Substation Router, Zone Based, Firewall Electronic Access Control System and Intermediate System, Legacy device connectivity | IR8300 |
| Station Bus Switches | IR8300, IE9300, IE5000, IE3400, IE4000, IE4010 |
| Process Bus Switches with Power Profile support | IE9300, IE3400, IE4010, IE4000 |
| Substation Firewall | ISA3000 |
| Corp and CIP Zone Switches | IE5000, IE4000, IE2000 |
| Wi-Fi Access Point in Corp zone | IW6300 |
| Central Headend Router | ASR1K |
| Central Headend Firewall | FPR4150 |
| OT Visibility Manager | Cyber Vision Center |
| OT Inline Sensors | Cyber Vision Sensor running on IE3400, IE9300, IR8300 |
| PRP Redbox | IE5000, IE4000, IE4010, IE9300, IR8340 |
| PRP HSR Redbox and HSR Quadbox | IE4000 |
| PRP Infrastructure Switches | IE4000, IIE2000u, E4010, IE3400, IE9300 |
| HSR SAN | IE4000, IE4010, IE3400, IE5000 |
| PTP Grand Master | IE5000, IR8340 |
| PTP Transparent Clock | IE5000, IE4000, IE4010, IE9300, IR8340 |

**Table 3 Roles and Products**

| Role | Product |
|---|---|
| PTP Boundary Clock | IE5000, IE4000, IE4010, IE9300, IR8340 |
| PTP over PRP | IE5000, IE9300, IE4000, IE4010 |
| Substation LAN Network Management | DN2-HW-APL (include L and XL) |
| Substation WAN Management | vManage |

**Note:** IE2000 SKUs do not support PTP Power Profile.

## Common Substation equipment requirements

The following are some of the common substation equipment requirements. It is recommended to refer to the respective platform guide to get accurate details of the respective equipment.

- IEEE 1613 and IEC 61850-3 Compliance – All products go through KEMA third-party validation
- For longer operational life, network infrastructure with no moving parts
- Advanced IOS Software capabilities with added utility specific functionality
- Combining power and connectivity via 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 to reduce replacement inventory and simplify deployment
- Redundant power inputs or power supplies for resilient operations
- Extended Power Supply Support (low and high voltage AC/DC supported)
- IEEE 1588 v2 PTP support C37.238 (Power Profile) for synchronization of end-device clocks
- Modbus Memory Map Support (View only statistics)
- Extended range of operating temperature support -40C to +75C
- Alarm contacts–input and output
- 5-year limited hardware warranty covering all components (including power supplies)
- Swap drives for easy field replacements
- Dying Gasp
- SD-Flash to simplify device replacement

## Cisco IR 8300

The Cisco Catalyst IR8300 Rugged Series Router is Cisco's first industrial-grade fully integrated routing and switching platform. Built on the Cisco Unified Access Data Plane (UADP) Application-Specific Integrated Circuit (ASIC) and Quantum Flow Processor (QFP), which powers the industry-leading Cisco Catalyst products, the IR8300 is designed to provide outstanding flexibility and adaptability to address the latest needs of the network evolution. The IR8300 supports U.S. public safety FirstNet services and new 5G services and is built for accelerated services, multilayer security, and edge intelligence. It can be deployed in the harsh, rugged environments found in the energy, transportation, and oil and

gas industries. For more details:
https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-ir8300-rugged-series-router/nb-06-cat-ir8340-rugged-ser-rout-ds-cte-en.html.

The IR8300 plays a number of roles in the architecture, include a resilient Transmission or Distribution Substation headend router into the Utility WAN, a EACS, LEAP, resilient Station-bus switch, zone-based Firewall, hosting a Cyber Vision sensor, PTP Grandmaster clock and providing serial-based connectivity for legacy devices. The product is managed by either Cisco's DNA-Center or vManage.

**Figure 6 Cisco IR 8340**

The Cisco Catalyst IR8340 can be deployed as Transmission Substation Router in Substation Core Zone IR8340 can additionally acts as Cyber Vision in network sensor for capturing OT flow and asset visibility as well can acts as inline firewall and VPN terminations.

See the Substation Core and Utility WAN section for more about the IR8340.

## Cisco IE 9300

Cisco Catalyst IE9300 Rugged Series Switch, a high-density fiber port switch, specifically designed for the performance challenges of a substation LAN architecture with a small footprint and ruggedized form factor. It's part of a new way to approach substation automation and management, and together with the recently released Catalyst IR8300 Rugged Series Router, the Catalyst IE9300 provides a validated architecture that unifies the substation LAN and WAN – adding the performance, security, scale and management required for the modernization of the grid.

The Cisco IE9300 can be deployed as PRP LAN infrastructure switch, PRP Redbox in station and process bus. For more details in IE9300 please refer to:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie9300-rugged-series/catalyst-ie9300-rugged-series-ds.html

**Figure 7 Cisco IE9300**

The following table shows Cisco equipment and reference material.

**Table 4 Product and reference material**

| Cisco identifier | Reference URL |
|---|---|
| IE3300 | http://www.cisco.com/go/ie3300 |
| IE3400 | http://www.cisco.com/go/ie3400 |
| IE4000 | http://www.cisco.com/go/ie4000 |

**Table 4 Product and reference material**

| Cisco identifier | Reference URL |
|---|---|
| IE4010 | http://www.cisco.com/go/ie4010 |
| IE5000 | http://www.cisco.com/go/ie5000 |
| CyberVision | https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html |
| ASR1000 | http://www.cisco.com/go/asr1k |

## Resiliency and Topology

Resiliency can be defined as the ability of the communication network to provide services despite network failures and the time to restore such failure in the presence of a failure. Additional network elements like switches and links are introduced to increase dependability and maintain communications in the case of link loss or switch operational failure. Redundancy topologies avoid single points of failure that can disrupt communications and which also impact the non-redundant parts of the network. With Utilities transforming and embracing Ethernet for various network connections, several resiliency protocols are available to choose from. Some of the key considerations before choosing a resiliency protocol are described below.

- Substation application, in particular the criticality of the communications to maintaining operations and
- Network topology, some resiliency protocols were designed with a particular topology in mind,
- Level of tolerable communication, some applications are designed to operate through various levels of communication loss.
- Logical data flows and traffic patterns, understanding the critical flows and which network infrastructure they pass through
- Latency requirements for different types of traffic
- Network management, deployment and monitoring of resiliency protocols may not be supported in many network management applications and may therefore require manual configuration and monitoring
- Time synchronization and accuracy
- Remote connectivity can add to the importance of network resiliency
- Scalability, as some resiliency protocols have limits to their size (e.g. ring-size)
- Upgrade-ability, as resiliency protocols may be invoked and need to be considered when upgrading network infrastructure and
- Interoperability, different network vendors support a range of resiliency protocols, so mixing vendors introduces the need to consider interoperability of selected resiliency protocols
- Cost, resiliency inherently adds costs by adding infrastructure and/or increasing the amount of traffic, generally increasing costs.

Cisco offers high-availability redundancy mechanisms such as Resilient Ethernet Protocol (REP), Parallel Redundancy Protocol (PRP), and Highly Available Seamless Ring (HSR). The following sections will review a variety of resiliency protocols. The protocols include:

- Spanning Tree Protocol (STP) – STP is the most common Layer-2 resiliency protocol and interoperable. It does not recover as quickly or with as little impact as any of the others, so is not recommended for Substation LAN networks.

- Resilient Ethernet Protocol (REP) – REP is a Cisco-proprietary protocol used for rings and concentric ring topologies. It recovers in 30-50 ms, so may be appropriate for some substation application
- Parallel Redundancy Protocol (PRP) – Parallel Redundancy Protocol (PRP) is defined in the International Standard IEC 62439-3. PRP is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks.
- High-availability Seamless Recovery (HSR) – HSR is defined in International Standard IEC 62439-3-2016 clause 5. HSR is a lossless protocol like PRP, however HSR is designed to work in a ring topology.

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.

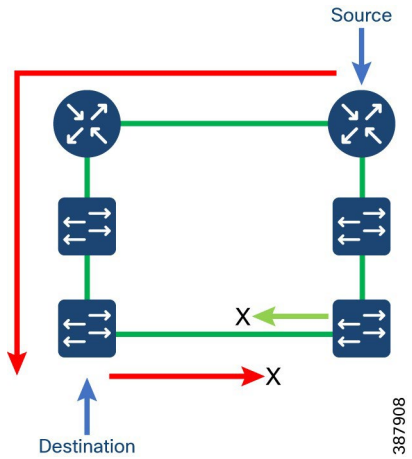
## Spanning Tree Protocol

Spanning Tree Protocol is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology.

Three modes of spanning tree are supported on Cisco Industrial Ethernet routers and switches. They are Per VLAN Spanning Tree (PVST+), Rapid Per Vlan spanning tree (RPVST+) and Multiple Spanning Tree Protocol (MSTP).

**Figure 8 Spanning Tree Protocol**




PVST+—This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. It is the default spanning-tree mode used on all Ethernet port-based VLANs. The PVST+ runs on each VLAN on the switch up to the maximum supported, ensuring that each has a loop-free path through the network.

Rapid PVST+—This spanning-tree mode is the same as PVST+ except that is uses a rapid convergence based on the IEEE 802.1w standard. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries.

MSTP—This spanning-tree mode is based on the IEEE 802.1s standard. You can map multiple VLANs to the same spanning-tree instance, which reduces the number of spanning-tree instances required to support many VLANs. The MSTP runs on top of the RSTP (based on IEEE 802.1w), which provides for rapid convergence of the spanning tree by eliminating the forward delay and by quickly transitioning root ports and designated ports to the forwarding state. You cannot run MSTP without RSTP.

This solution recommends the use of Rapid Per VLAN Spanning Tree protocol and MSTP for interoperability considerations. Typically, Spanning Tree does not recover fast enough for many substation applications, such as IEC61850. It should be noted as a best practice that switch Access ports should have Portfast enabled for quick availability and loop protection that is based on Spanning Tree.

## Design Considerations

- RSTP is primarily intended for automatic LAN configuration and loop prevention. Rapid Spanning Tree Protocol is enabled by default on many of the new Cisco platforms thus automatically avoiding loops as the physical links are connected.
- It provides redundancy against link and bridge failures.
- It does, however, not provide resiliency against link failures to end devices. Loss of a bridge usually causes the loss of all attached devices.
- RSTP does not provide seamless recovery in case of trunk link or bridge failure, it recovers fast enough for most applications that use the station bus.
- It is recommended to refer to IEC 62439-1-2012 that shows how to calculate the worst-case recovery time of RSTP in generalized meshed or tree topologies by being aware of the actual topology of the network and the number of networking devices in the topology.
- If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root. By increasing the priority (lowering the numerical value) of the ideal switch so that it becomes the root, you force a spanning-tree recalculation to form a new topology with the ideal switch as the root. It is recommended to make the gateway router IR8340 as the root.
- When the spanning-tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to an interface that has a higher number than the root port can cause a root-port change. The goal is to make the fastest link, the root port. By changing the spanning-tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical value) than the root port, the Gigabit Ethernet port becomes the new root port.

## 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 Industrial Routers (IR8300), Industrial Ethernet (IE), and Carrier Ethernet (CE) platforms.

Some of the key benefits of REP include:

- 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 and scalable.
- It coexists with spanning tree. An industry standard protocol, G.8032, was later derived from REP.
- It is simple and easy to configure.
- Commonly deployed in Ring topologies.

- Supports rings, segments, and arbitrary topologies with hierarchy of rings and segments.
- Load balancing by blocking selective VLANs at Primary Edge and Alternate Ports.

### Design Considerations

- 1 Gbps fiber inter-switch links are recommended to provide optimum convergence in REP topologies.
- REP Fast can be enabled on platforms and links that support.

  REP Fast resolves the recovery delay for Gigabit Ethernet. It relies on beacons that act as keepalives to detect link failures. When a REP ring interface is configured with REP Fast, it sends a special beacon frame every 3 ms to its directly connected ring neighbor. And it expects to receive a special beacon frame every 3 ms from the same neighbor. Failure to receive three beacon frames in a row translates into a link failure event for REP. In this way REP Fast can detect a link that is down within 10 ms. This is regardless of link speed or media type. REP Fast works on copper as well as fiber links. It resolves the slow detection of link failure by copper Gigabit Ethernet. Once the link failure is detected, the normal REP protocol takes over to recover from the failure and resume Ethernet forwarding over the alternate path.
- Configuration of REP Admin VLAN.
- Consideration must be given to the number of devices and/or switches attached to the REP segment, the number of VLANs configured within the REP segment, and the number of MAC addresses that will be utilized in the REP segment. The combination of factors affects the recovery time of a REP segment during failover.
- Platforms recommended for Utility Substation Automation network do not support stacking that could allow one to enable all relevant features required in a substation over a stack. Hence this design guide recommends the use of a single distribution switch is the preferred design.
- Precision Timing Protocol – Power Profile (c38.238 2011 or 2017) over REP is not supported on some platforms. It is recommended to check the respective platform guide to confirm the support of PTP over REP. Hence it is recommended to use NTP as timing protocol if it is suitable for applications. For example, Substation applications, such as SCADA or disturbance recorders, requires timing accuracy in the millisecond range and can use a network time protocol (NTP) system operating over an existing Ethernet communication network. Station bus deployments typically require timing in the range of milliseconds and use of NTP would be suitable unlike Process bus deployments that requires higher precision and so PTP Power profile can be used for GOOSE and SV messages.

## Parallel Redundancy Protocols (PRP)

Parallel Redundancy Protocol (PRP) is defined in the International Standard IEC 62439-3. PRP is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks. PRP uses a different scheme, where the end nodes implement redundancy (instead of network elements) by connecting two network interfaces to two independent, disjointed, parallel networks (LAN-A and LAN-B). Each of these Dually Attached Nodes (DANs) then have redundant paths to all other DANs in the network. To recover from network failures, redundancy can be provided by network elements connected in mesh or ring topologies using protocols like RSTP or REP where a network failure causes some reconfiguration in the network to allow traffic to flow again (typically by opening a blocked port). These schemes for redundancy can take between a few milliseconds to a few seconds for the network to recover and traffic to flow again.

PRP resiliency support is available on the Cisco IE 4000, Cisco IE 4010, Cisco IE 5000 switches, Cisco IE9300 switches and Cisco IR8340 Substation Automation Router.

### Design Considerations

- PRP LAN_A and LAN_B networks need to meet these criteria:
  - Disjoint – LAN A and LAN B networks cannot be connected to each other using Layer 2 connections to avoid loops.
  - Separate – LAN A and LAN B networks are separate networks with its own independent network devices and physical connections.

  - Independent – A Single Attached node in LAN A cannot communicate with another Single Attached node in LAN B though they can independently communicate with applications such as SCADA in the control center. Any failure in LAN A will only affect the traffic in PRP LAN A, while the traffic in PRP LAN B continues to flow without any loss.
  - Parallel – Both PRP LAN A and LAN B are deployed with a similar LAN topology to transport duplicate packets generated by PRP Redbox connected to these LANs thus providing lossless resiliency in case of network failure in any of the PRP LANs. It is recommended to have similar latency and hops in each of the LANs. An example could be the use of different connectivity options for each of the LANs.

- Do not connect Industrial Ethernet Switches (other than RedBoxes) to both LAN A and LAN B. Direct links between LAN A and LAN B Industrial Ethernet Switches are not allowed. Connecting them directly using Layer 2 path would result in loops.
- system mtu 1506 and system jumbo mtu 1506 needs to be enabled on switches as PRP DANs and Redboxes add a 6-byte PRP trailer to the packet.
- PRP Supervisory frame can be sent on separate VLAN (Optional) and we can mark PRP Supervisory frame for QOS treatment
- LAN A and LAN B can run resiliency protocols like RSTP, REP to provide additional resiliency in each of the LANs for SAN Devices. The LAN can be either a ring or star topology. It is recommended to have similar topology and connectivity for both the PRP LANs so as to avoid higher latency or delays.
- PRP Channel can be configured either as an access port allowing only one VLAN of interest or as a trunk port allowing multiple VLANs of interest. PRP Channel as trunk port can be in a scenario where there are multiple end devices connected to a PRP Redbox and needs to communicate with its peers over VLAN. It can also be used in a scenario where the PRP Redbox is positioned as a Layer3 Gateway aggregating multiple devices connected to the PRP network.

PRP Network can have many different topologies. The following lists a few examples of PRP topologies that could be deployed in a Substation Automation LAN network.

## Topology Examples

### Basic PRP with redundant LAN networks

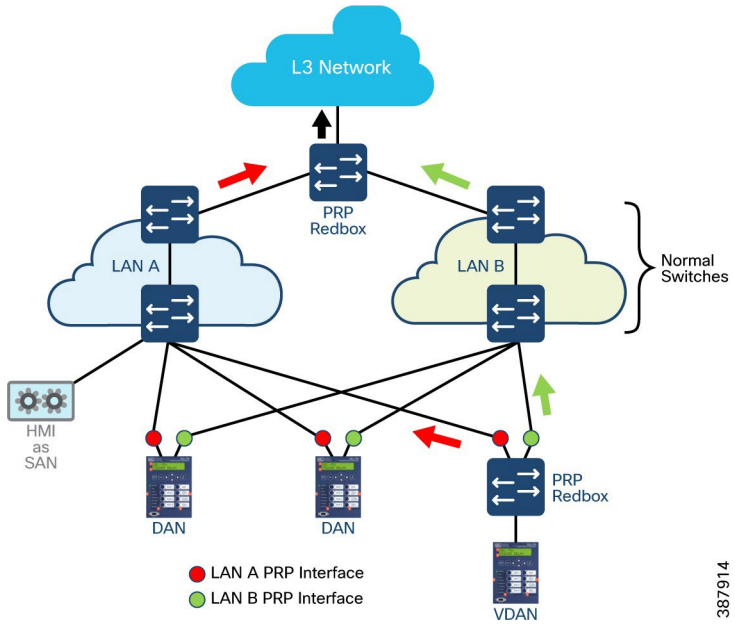
The following Figure shows a PRP topology with two LANs each consisting of many switches as part of the LAN. The switches in each of the LAN can also be in the form of a Ring topology with Spanning Tree or REP configured to avoid loops in the ring. The switches in each of the LAN can provide connectivity to a single attached node. The topology also provides the ability to connect Dual Attached nodes, PRP aware IEDs or network devices with two links, one connected to each LAN thus providing redundancy and resiliency in case of failures.

The DAN sends two packets simultaneously through its two network interfaces to the destination node. A redundancy control trailer (RCT), which includes a sequence number, is added to each frame to help the destination node distinguish between duplicate packets. When the destination DAN receives the first packet successfully, it removes the RCT and consumes the packet. If the second packet arrives successfully, it is discarded. If a failure occurs in one of the paths, traffic continues to flow over the other path uninterrupted, and zero recovery time is achieved.

Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs). The following Figure shows HMI attached as a SAN to one of the switches in LAN-A.

A Redundancy Box (RedBox) is used when an end node that does not have two network ports and does not implement PRP needs to implement redundancy. Such an end node can connect to a RedBox, which provides connectivity to the two different networks on behalf of the device. Because a node behind a RedBox appears for other nodes like a DAN, it is called a Virtual DAN (VDAN). The RedBox itself is a DAN and acts as a proxy on behalf of its VDANs. The following figure shows an IED that doesn't support PRP but needs redundancy is connected to a Cisco Industrial Ethernet switch that supports PRP Redbox function thus providing redundancy and resiliency to the IED.

**Figure 9 Basic PRP with redundant LAN networks**




Key characteristics of this topology include:

- Lossless redundancy over 2 parallel networks
- LAN A & B Switches do not have to understand PRP protocol and can support any topology like star or ring as long as there are no links or shared switches between the LANs.
- Higher Cost due to need for independent LAN A and LAN B network infrastructure and links
- IEC 62439-3 Clause 4 Standard, the standard for both PRP and HSR
- PRP Redbox is supported on IE-4000, IE-4010, IE-5000, IE-9300, IR8340 and select IE-2000u SKU (8,16 port)
- Applications like CyberVision Sensor, Stealthwatch, DNAC work seamlessly. These applications use stateful Layer 3 connectivity. For example, the reachability and the stateful session between CyberVision Center and Sensor over PRP is not impacted as the keepalive for the CyberVision session timeout is higher, in the order of seconds. Similar were the observations for stealthwatch and DNAC. For more details it is recommended to refer to GridSecurity Guide and relevant sections in this guide.

### PRP with redundant Layer-3 connectivity

The following figure shows a PRP topology with two LANs each consisting of many switches as part of the LAN. The switches in each of the LAN can also be in the form of a Ring topology with Spanning Tree or REP configured to avoid loops in the ring. The switches in each of the LAN can provide connectivity to a single attached node. The topology also provides the ability to connect Dual Attached Nodes (DAN), PRP aware IEDs or network devices with two links, one connected to each LAN thus providing redundancy and resiliency in case of failures. The DAN sends two packets simultaneously through its two network interfaces to the destination node. A redundancy control trailer (RCT), which includes a sequence number, is added to each frame to help the destination node distinguish between duplicate packets. When the destination DAN receives the first packet successfully, it removes the RCT and consumes the packet. If the second packet arrives successfully, it is discarded. If a failure occurs in one of the paths, traffic continues to flow over the other path uninterrupted, and zero recovery time is achieved.

Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs). The following Figure shows HMI attached as a SAN to one of the switches in LAN-A.

A Redundancy Box (RedBox) is used when an end node that does not have two network ports and does not implement PRP needs to implement redundancy. Such an end node can connect to a RedBox, which provides connectivity to the two different networks on behalf of the device. Because a node behind a RedBox appears for other nodes like a DAN, it is called a Virtual DAN (VDAN). The RedBox itself is a DAN and acts as a proxy on behalf of its VDANs. The following figure shows an IED that doesn't support PRP but needs redundancy is connected to a Cisco Industrial Ethernet switch that supports PRP Redbox function thus providing redundancy and resiliency to the IED.

The following figure shows that each IR8340 Substation router acts as PRP redbox and connects to each of the LANs respectively. The IR8340 acts as the Layer 3 gateway with HSRP or VRRP being used as gateway redundancy protocol to provide redundancy and resiliency for the L3 traffic flowing between the control center or WAN network and the devices connected in the PRP LAN network. For eg TCP traffic like MODBUS or DNP3 could be a traffic flowing from the SCADA in the control center to one or many of the IEDs connected in the PRP LAN network.

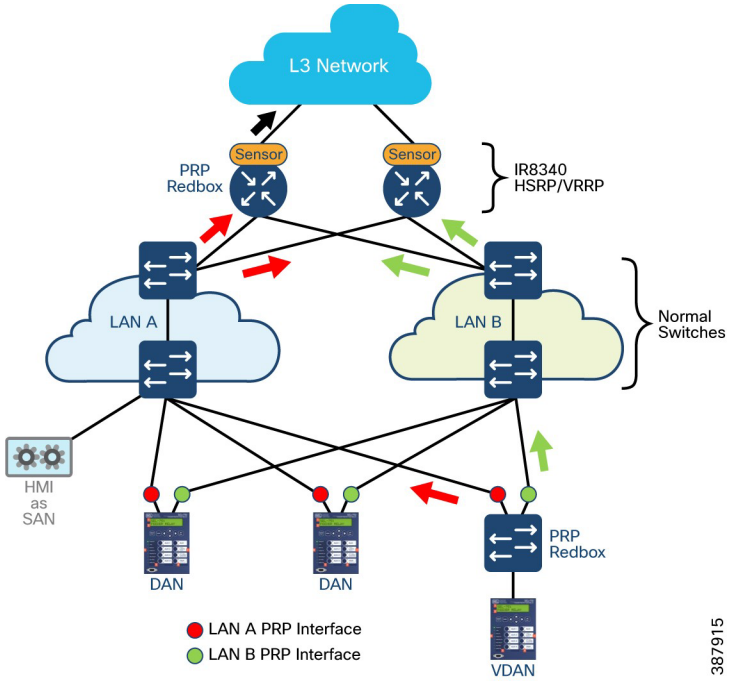
To optimize network redundancy, we need to design our network that aligns both Cisco Layer 3 HSRP and Layer 2 redundancy services with each other. HSRP will assign the active and the standby router based on priority. The highest priority will be the active HSRP router amongst the HSRP group. If the priority is the same, then the highest IP address will be the tie-breaker. It is recommended to manually identify the active router by configuring HSRP priority. When routing is first enabled for the interface, it does not have a complete routing table.

If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table. When the local router has a higher priority than the active router, it assumes control as the active router. As an option a delay can be configured, which will cause the local router to postpone taking over the active role for the number of seconds. HSRP uses two timers: hello interval and hold time. The hello interval defines the frequency that hello packets are sent to the other peer. Hold time indicates the amount of time to wait before marking the peer as down. The hold time should be three or more times greater than the hello interval.

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to HSRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced. The HSRP device with the higher priority can become the active device if it has the standby preempt command configured.

In case of a REP Ring, both edge ports should be located on the primary HSRP node. In case of STP, the root should be located on the primary HSRP node. In case of PRP, it is recommended to manually configure the primary HSRP node using the previously listed HSRP options such as priority, delay, pre-emption. It is also recommended to use BFD for fast peer failure detection.

**Figure 10 Parallel Redundancy Protocol – L3 Gateway Redundancy**




For details on other PRP topology designs that would be suitable for Substation Automation LAN networks refer to Substation Automation Local Area Network and Security Cisco Validated Design Guide.

Key characteristics of this topology include:

- Lossless redundancy over 2 parallel networks
- LAN A & B Switches do not have to understand PRP protocol and can support any topology such as star or ring as long as there are no links or switches shared between the LANs.
- High Cost due to need for independent LAN A and LAN B network infrastructure and links
- IEC 62439-3 Clause 4 Standard
- Supported on IE-4000, IE-4010, IE-5000, IE-9300, IR8340 and select IE-2000u SKU (8,16 port)
- Resilient, but not lossless, connectivity to WAN and Layer 3 networks via the redundant routers
- Applications like CyberVision Sensor, Stealthwatch, DNAC work seamlessly. These applications use stateful Layer 3 connectivity. For example, the reachability and the stateful session between CyberVision Center and Sensor over PRP is not impacted as the keepalive for the CyberVision session timeout is higher, in the order of seconds. Similar were the observations for stealthwatch and DNAC.For more details it is recommended to refer to GridSecurity Guide and relevant sections in this guide.

## Design Considerations

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

## High-availability Seamless Redundancy (HSR)

HSR is defined in International Standard IEC 62439-3-2016 clause 5. HSR is a lossless protocol like 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 counterclockwise 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. The following figure shows an overview of HSR.

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, Cisco IE 5000 switches, Cisco IE9300 switches and Cisco IR8340 Substation Automation Router.

### Design Considerations

The design considerations for HSR are broken up into 3 topologies that interconnect the HSR ring and devices to the rest of the Substation network and WAN.  The 3 ways to interconnect HSR rings are

- via dual Layer-3 switches/routers that then route any valid IP traffic,
- via interconnecting 2 HSR rings via dual switches that form HSR Quad-box
- via interconnecting the HSR ring into two PRP redundant LANs.

## HSR with Layer 3 Gateway Redundancy

HSR is used in HSR-SAN mode to provide redundancy in the access layer where IEDs are connected. The HSR ring can also consist of IEDs that inherently support HSR. Such nodes are called Dual Attached Nodes. The access layer is aggregated by Cisco IR8340 Substation router that also provide a Layer 2/Layer 3 boundary and default gateway for the Layer 2 domain. At the distribution layer, Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol is used to provides stateless redundancy for IP routing. The following figure shows a topology of HSR ring being part of two IR8340 routers and provides Layer 2/Layer 3 resiliency and redundancy.

To optimize network redundancy, we need to design our network that aligns both Cisco Layer 3 HSRP and Layer 2 redundancy services with each other. HSRP will assign the active and the standby router based on priority. The highest priority will be the active HSRP router amongst the HSRP group. If the priority is the same, then the highest IP address will be the tie-breaker. It is recommended to manually identify the active router by configuring HSRP priority. When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table. When the local router has a higher priority than the active router, it assumes control as the active router. As an option a delay can be configured, which will cause the local router to postpone taking over the active role for the number of seconds.

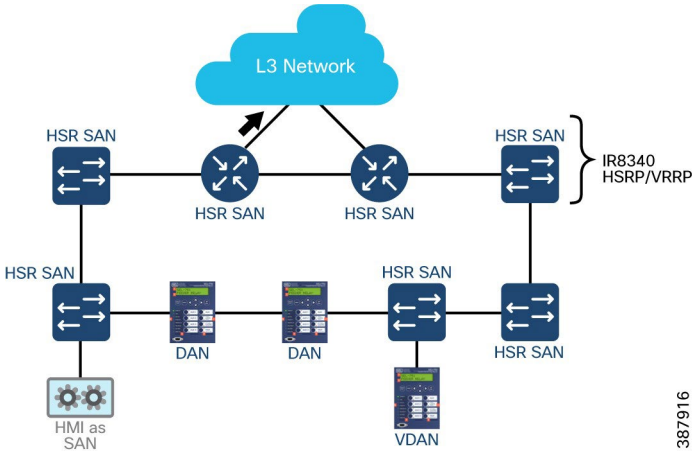
HSRP uses two timers: hello interval and hold time. The hello interval defines the frequency that hello packets are sent to the other peer. Hold time indicates the amount of time to wait before marking the peer as down. The hold time should be three or more times greater than the hello interval.

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to HSRP, either immediately or after a specified delay. The object values

are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced. The HSRP device with the higher priority can become the active device if it has the standby preempt command configured.

In case of a REP Ring, both edge ports should be located on the primary HSRP node. In case of STP, the root should be located on the primary HSRP node. In case of PRP, it is recommended to manually configure the primary HSRP node using the previously listed HSRP options such as priority, delay, pre-emption. It is also recommended to use BFD for fast peer failure detection.

**Figure 11 High-Availability Seamless Redundancy Protocol – L3 Gateway Redundancy**




The following lists the characteristics of HSR on Cisco IR8340. For details of other platforms, refer to the respective platform guides. For details on other HSR topology designs that would be suitable for Substation Automation LAN networks refer to Substation Automation Local Area Network and Security Cisco Validated Design Guide.

Key characteristics of this topology include:

- HSR is supported on the Cisco IE 4000, Cisco IE 4010, Cisco IE 5000 and Cisco IR8340 Substation Router.
- HSR ring ports can only be configured in Layer 2 mode.
- MTU sizes up to 1998 are supported.
- The maximum number of nodes in the node table is 512. Nodes are nothing but all the DANH and VDAN devices that can be connected to the ring at same time.
- Maximum number of nodes in the ring is limited to 50.
- Maximum one ring is supported per box. HSR and PRP cannot be enabled simultaneously on the same IR8340 router.
- The following protocols and features are mutually exclusive with HSR on the same port:
  - PRP
  - EtherChannels
  - Link Aggregation Control Protocol (LACP)
  - Port Aggregation Protocol (PAgP)
  - Resilient Ethernet Protocol (REP)
  - Spanning Tree Protocol
  - PTP

- Once a port is part of a ring, the media-type, speed, and duplex settings of the port cannot be changed. It is recommended to apply those settings before configuring ring membership.
- Once a port is part of ring, the port cannot be shut down. Instead, the HSR Ring interface can be shut if required. However, this operation would shut down both member ports.
- VLAN configuration such as trunk and access mode must be the same on both ports participating in the ring.
- After an interface is added in the HSR ring, only the primary interface counters are updated. Should not check the status of individual physical interfaces after they are added to the HSR ring.
- It is recommended to shut down the ports before configuring the ring on all switches and then re-enable them one by one to avoid MAC flaps.
- Physical interfaces are predefined for the rings and ports in HSR-SAN and HSR-PRP modes and cannot be changed. Port assignments for Cisco IR8340 HSR-SAN mode are shown in the following table. For other devices or modes, refer to the relevant product documentation.

**Table 5 IR8340 and HSR-SAN ports**

| SKU | HSR Mode | Port Type | Interface Number |
|---|---|---|---|
| Cisco IR8340 | HSR-SAN | Ring 1, Port 1 | GE 0/1/4 |
| | | Ring 1, Port 2 | GE 0/1/5 |
| | | Ring 2, Port-A | GE 0/1/6 |
| | | Ring 2, Port-B | GE 0/1/7 |

## HSR-HSR

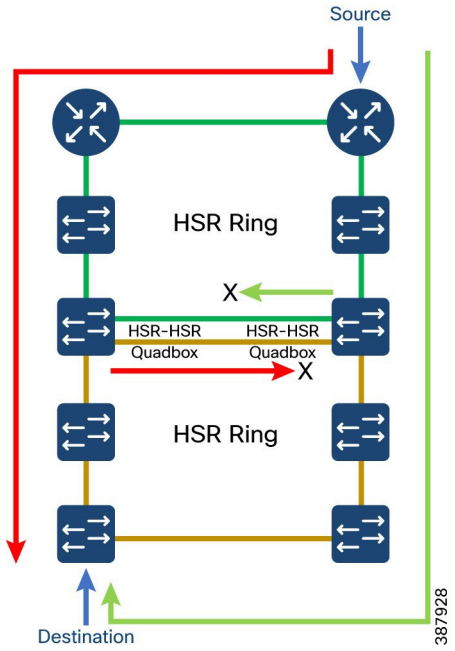
HSR rings can also be implemented in such a way that key switches are participating in two HSR rings, using four interfaces to connect the respective rings, which is known as HSR-HSR or Quadbox. When the HSR-HSR mode is licensed and enabled, the switch shuts all non-HSR ports to avoid traffic interference. Connectivity to the HSR-HSR switch can be done through the HSR-HSR ports or the out-of-band console interface.

HSR-HSR Quadbox functionality is only supported on IE4000. Each QuadBox creates a duplicate frame. More than one QuadBox in the topology can result in multiple copies of the same frame to be generated. However, only one copy is sent on each side of the ring, ensuring that eventually only two copies of a frame are sent on each ring. All subsequent duplicate frames received are dropped by the QuadBox.

To segregate traffic between the two rings, one can configure the QuadBox with VLAN and Multicast filters. This allows one to restrict the specified VLAN and Multicast groups from crossing the rings. VLAN filtering uses the VLAN allowed list to restrict VLANs. Multicast filtering matches packets with same MAC destination address (MACDA) and optional mask as configured in the filters. If there is a match, the packets are dropped. In IEC 61850 substation network, HSR is generally used in small substations or for process bus communications.

An example scenario for HSR-HSR QuadBox is a Station bus ring and subrings with HSR. Following is a simple topology with HSR-HSR QuadBox.

**Figure 12 HSR – HSR Ring**




**Note:** PTP over HSR QuadBox is not supported.

## HSR-PRP Redbox

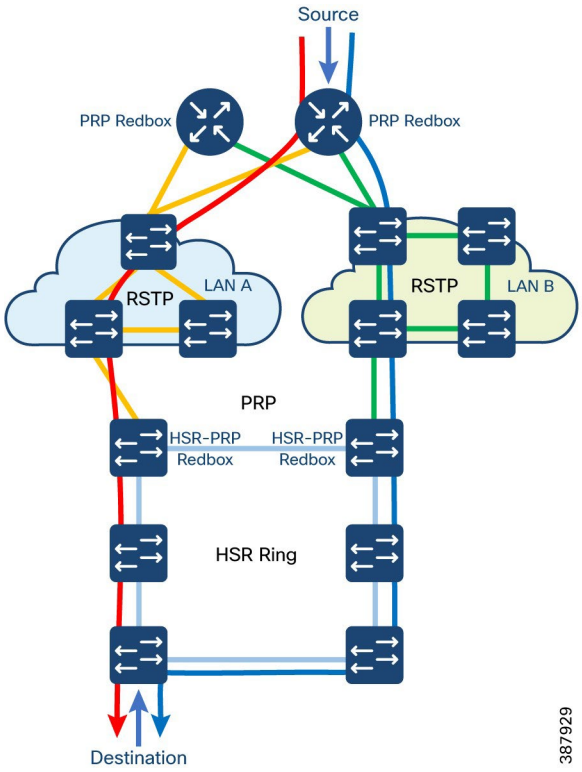
HSR-PRP, also known as Dual Redbox, is used to connect PRP and HSR networks together. It is commonly deployed in utility substations, hence the testing results show GOOSE and Sampled Values but are applicable to other IP protocols. The following topology shows an HSR ring connected to a PRP network through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

An example scenario for HSR-PRP RedBox could be a Station Bus as PRP and Process Bus as HSR. Following is a simple topology with HSR-PRP QuadBox.

### Design Considerations

- In HSR-PRP Dual RedBox mode (IE 4000 only), the device basically functions as a three-port device. All the other interfaces apart from these three interfaces are shut down by the software. These three interfaces are predefined:
  - Gi1/1, Gi1/3 and Gi1/4 for Redbox A
  - Gi1/2, Gi1/3 and Gi1/4 for Redbox B
- A maximum of six PRP networks, identified by the PathId, can be connected to the same HSR ring.
- A PRP network can be connected to any number of HSR rings, but these rings cannot be connected to each other because this would create loops.
- In HSR-PRP Dual Redbox mode, during reload of the HSR-PRP switch when the traffic is in progress, MAC flaps occur once per source MAC address in the switch that is reloaded and also on the PRP device that is transmitting the traffifc. Therefore, if there are 512 different source MAC addresses, then MAC flaps are observed 512 times (once per source MAC address). Also some duplicate packets are seen after this event.

**Figure 13 HSR – PRP Redbox for Station Bus and Process Bus**




## Resiliency Summary

There is no 'best' network topology and no 'best' redundancy protocol. They all have strengths and weaknesses and the correct choice for a given application depends on many factors. There are many possible network topologies that can be designed for IEC61850 based Substation Automation networks. The following table lists a comparison of different protocols that are discussed in this guide.

**Table 6 Resiliency Protocols and Properties**

| Protocol | Topology | Number of Nodes | Typical Convergence |
|---|---|---|---|
| RSTP/MSTP | Any | Max hop 255 | 50ms – 6s |
| HSR | Ring | 50 | 0ms |
| PRP | Dual Independent network | Unlimited | 0ms |
| REP (Cisco proprietary) | Ring | 24 | 50 – 250ms |

The following table lists various flows of traffic and their resiliency requirements and a list of suitable resiliency protocols that can be used for the same.

**Table 7 Substation Automation LAN Traffic and Resiliency Requirements**

| Communicating Partners | Service | Application recovery delay | Recovery delay of communication | Remark |
|---|---|---|---|---|
| SCADA to IED, client-server | IEC 61850-8-1 | 800 ms | 400 ms | Can be handled using REP |
| IED to IED interlocking | IEC 61850-8-1 | 12 ms | 4 ms | Need PRP and/or HSR |
| IED to IED, reverse blocking | IEC 61850-8-1 | 12 ms | 4 ms | Need PRP and/or HSR |
| Protection trip excluding Bus Bar protection | IEC 61850-8-1 | 8 ms | 4ms | Need PRP and/or HSR |
| Bus Bar protection | IEC 61850-9-2 on station bus | < 1 ms | Bumpless – 0 ms | Need PRP and/or HSR |
| Sampled values | IEC 61850-9-2 on process bus | < 4 ms | Bumpless – 0 ms | Need PRP and/or HSR |

## Different Platforms and Resiliency Features

The following table lists some of the lossless resiliency protocols and their different roles that are supported on Cisco Industrial Ethernet switches and Industrial Routers.

**Table 8 Resiliency Protocol – HSR and Roles**

| HSR Roles | IR and ER |
|---|---|
| HSR SAN + PTP GM | IE5000 |
| Station Bus Ring using HSR SAN+ Transparent Clock | IE3400, IE4000, IE5000 |
| Station Bus Ring using HSR SAN+ Boundary Clock | IE4010, IE3400, IE4000 |
| HSR PRP Redbox | IE4000 |
| HSR Quad Box | IE4000 |
| HSR SAN | IE5000, IE4000, IE4010, IE3400, IR8340 |

**Table 9 Resiliency Protocol – PRP and Roles**

| PRP Roles | IR and IE |
|---|---|
| PRP Redbox + PTP GM | IE5000 |
| Station Bus LAN Switch Non-PRP + Transparent Clock | IE9300, IE3400, IE4000, IE4010, IE2000U |
| Process LAN Switch non-PRP + Transparent Clock | IE9300, IE3400, IE4000, IE4010, IE5000 |
| PRP Redbox + HSRP/VRRP | IR8340 |
| PRP HSR Redbox | IE4000 |

# Timing and Synchronization

Substation automation is a mission-critical task and electric power utilities must synchronize across large-scale distributed power grid switches in a substation to enable smooth power transfer and maintain power supply integrity.

Time synchronization is used to precisely synchronize internal clocks in IEDs, Merging Units (MUs), protection and control units, Ethernet switches and wherever processes need to be synchronized in substation automation. It helps to achieve accurate control and precise global analysis of network response and when where and why any faults have occurred.

There are two standard protocols relevant for time synchronization over Ethernet networks in a Substation network, Network Time Protocol (NTP) and Precise Time Protocols (PTP). NTP is the protocol that synchronizes the clocks in typical TCP/IP networks. Servers, workstations, smart phones and the network infrastructure generally support NTP. NTP though can only support synchronization to roughly the second. PTP is a protocol designed to provide much more precision between a network of clocks with time-drift between devices roughly measured in nanoseconds. Precise time synchronization is therefore required to ensure that substation devices have accurate clocks for system control and data acquisition, etc. Time synchronization is especially important for time stamping of sampled values (IEC61850-9-2) of current, and voltage values require accurate clocks inside the merging units.

Time Synchronization over a Local Area Network synchronizes devices and can increase the number of devices driven through one the Ethernet network. It reduces the cabling infrastructure and cost by transporting all time synchronization information together with data communications over the same Ethernet communication medium.

Standard protocols like NTP can be used for synchronizing IEDs connected to a station bus and IEEE 1588 C37.238 PTP power profile for IEC 61850 GOOSE and SV applications in process bus deployments. Cisco Industrial platforms supports both NTP and C37.238 PTP power profile, simultaneously. Depending on the resiliency protocol being used, the application requirements, the appropriate timing protocol should be chosen. And due to the need to compare times across multiple locations and geographies, its important the time synchronization is aligned to Coordinated Universal Time (UTC), the world clock.

## Network Time Protocol

Network Time Protocol is a networking protocol for synchronizing clocks across TCP/IP networks. NTP uses a hierarchical system of clocks to synchronize time across disparate hosts on the network. There are three roles for clocks in the NTP architecture:

- Servers—NTP servers act as a time source for one or more NTP clients.
- Clients—NTP clients synchronize their clocks to one or more servers.
- Peers—NTP peers allow two clocks to synchronize to each other. In essence, peers are clients and servers to each other.

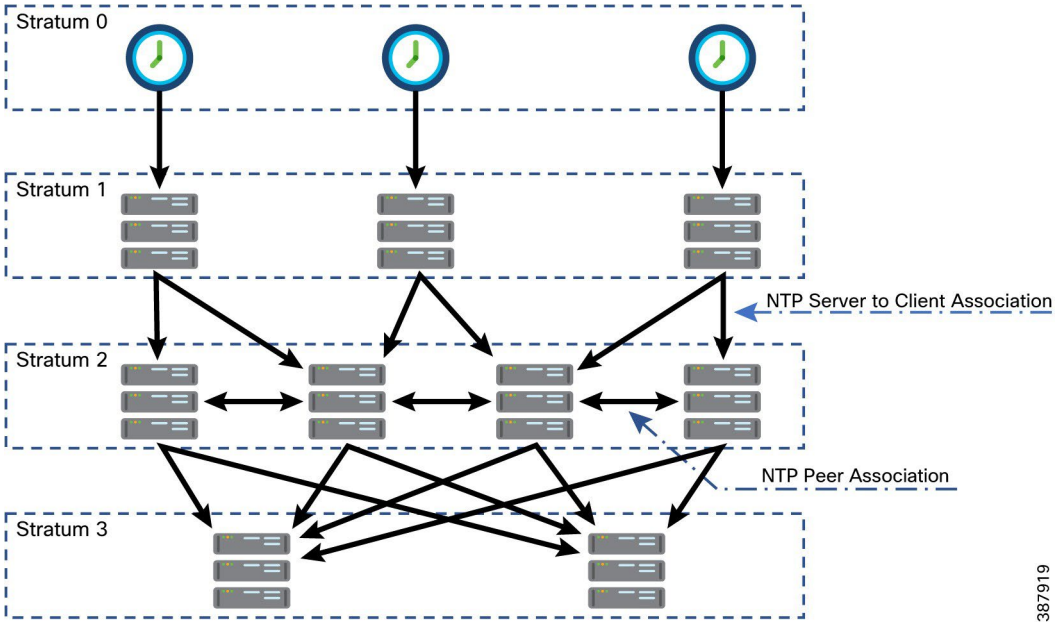
These roles are not exclusive and any device in the Substation Automation architecture can act as one or more of these roles. For example, an NTP server is generally a client to servers higher up in the NTP hierarchy. The network infrastructure is often both a client on the uplinks and a server on the downlinks.

NTP has limited provisions for authenticating timeservers. Most implementations support symmetric keys for authentication. Some recent implementations support the autokey security protocol. NTP authentication is outside the scope for this guide.

The clock hierarchy as showing in the following figure is divided into “stratum” where lower stratum numbers are closer to the reference clock. The reference clock is identified as the stratum 0 clock and is frequently a receiver for a GNSS such as a GPS, but could also be a radio receiver, atomic clock, or another precision time source.

The stratum 0 clock is directly connected to the stratum 1 server and cannot be directly accessed across the network. The stratum 2 servers are the first to synchronize across the network using the NTP protocol. They are clients to several stratum 1 servers and are frequently peers to other stratum 2 servers. The stratum 3 servers are clients to the stratum 2 servers and may be peers to other stratum 3 servers and so on.

**Figure 14 NTP Clock Hierarchy**




The ability of a client (e.g., IED device) to synchronize its clock to the reference depends on its stratum level. Clocks with lower stratum numbers will be more tightly synchronized with the reference clock. NTP clocks will have limited accuracy compared to UTC. They are generally a better fit for substation applications that can tolerate offsets to UTC of tens, if not hundreds, of milliseconds or even seconds.

However, there are several factors that can affect how precisely a client will synchronize to the reference clock:

- Network latency and jitter
- Asymmetric networks
- Number of hops between clocks
- Quality of the internal oscillator
- Operating system capabilities

The NTP clock algorithm supports associating with multiple servers. It will use the multiple inputs to provide better time synchronization of the local clock. The clock algorithm also sanity checks the associated servers. Clock updates from servers that are inconsistent with the pool are invalidated and discarded. Sanity checking reduces the risk of a bad clock source skewing in the NTP client.

Deploy two to four NTP servers in the Utility Operations Center to function as the central clocks for enterprise applications. Depending on the application requirements, these NTP servers could either be directly connected to reference clocks or synchronized to public servers on the Internet. If the decision is made to synchronize to public sources, each of these servers should be synchronized to two to four public sources. There should be some diversity in the public sources, so that a bad clock can be identified and removed from the clock pool. In addition, the Enterprise Zone servers should be peers to each other. Large organizations will likely have additional stratums of NTP servers within the organization to cascade time to the NTP clients. In cases where high accuracy NTP time is needed in the ESP Zone, consider deploying a stratum 1 server within the Substation Automation LAN ESP Zone.

Access to public NTP servers should be controlled at the enterprise edge firewalls. The goal is to have all NTP clients in the organization synchronized to the internal NTP servers. As such, access to public servers should be limited to the internal top-level NTP servers. Moreover, access should be limited to specific public servers that are trusted by the organization. Ideally, use authentication with any external NTP servers to reduce the risk of time synchronization being compromised.

Use NTP to synchronize the clocks in the switches, routers, firewalls, and other network infrastructure deployed in the DMZ and Substation Automation LAN Zones. Synchronizing time for these network devices is important so that syslogs from multiple network devices can be analyzed together to help troubleshoot system level faults.

For more details see https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html

## Precision Time Protocol & Power Profile

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.

Smart grid power automation applications such as peak-hour billing, virtual power generators, and outage monitoring and management, require extremely precise time accuracy and stability. Timing precision improves network monitoring accuracy and troubleshooting ability.

In addition to providing time accuracy and synchronization, the PTP message-based protocol can be implemented on packet-based networks, such as Ethernet networks. The benefits of using PTP in an Ethernet network include:

- Low cost and easy setup by using existing Ethernet networks instead of expensive proprietary timing networks (e.g. IRIG)
- Limited bandwidth is required for PTP data packets

There are different PTP profiles that are supported on Cisco Industrial Ethernet switches and routers. The profiles are:

- Default Profile
- Power Profile (C37.238-2011/IEC 61850-9-3 support)
- 802.1AS Profile
- Extended Power Profile (IEEE C37.238-2017 support—Transparent clock mode only)

Some profiles may not be supported on some platforms. It is recommended to refer to the respective platform guide to confirm the support.

The Power Profile is defined in C37.238-2011 - IEEE Draft Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications. This documentation uses the terms Power Profile mode and Default Profile mode when referring to this IEEE 1588 profile and its associated configuration values.

The IEEE Power Profile defines specific or allowed values for PTP networks used in power substations. The defined values include the optimum physical layer, the higher-level protocol for PTP messages, and the preferred best master clock algorithm. The Power Profile values ensure consistent and reliable network time distribution within substations, between substations, and across wide geographic areas.

The Extended Power Profile supports C37.238-2017 in Transparent clock mode.

The Extended Power Profile has the following characteristics, in comparison with the Power profile (C37.238-2011):

- This profile uses domain-number 254 by default.
- The Transparent clock mode operation increments the " TotalTimeInAccuracy" by approximately 50ns by each node.

## Roles

PTP synchronization behavior depends on the PTP clock mode that is configured on the device. Cisco Industrial Ethernet routers and switches can be configured for one of the following global modes. It is recommended to refer to the respective platform guide to confirm the support.

The key roles covered include:

- Grandmaster – the primary source of time
- Boundary Clock – an intermediary Master clock to distribute time
- Transparent Clock – an intermediary to distribute time where delays on the intermediary are compensated for in PTP traffic

### Grandmaster

The grandmaster clock is the primary source of time in the PTP domain. Grandmaster clocks should have high quality oscillators and be synchronized to UTC. The Grandmaster in a PTP domain is selected through a protocol called the Best-Master Clock Algorithm (BCMA). Once selected, the GM is the central provider of time and responds to slave clocks various requests.

### Boundary Clock

A boundary clock is a multiport device Industrial Ethernet Switch that becomes a slave on one port. As a slave clock, the boundary clock synchronizes its internal clock to the master. The boundary clock then becomes a master to IED devices connected to the other ports on the Industrial Ethernet Switch. Other clocks connected to these ports will become slaves to the boundary clock and synchronize to the boundary clock's internal clock.

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

**Table 10 PTP Boundary Clock and transfer functions**

| Transfer Function | PDV Filtering | Time Convergence |
|---|---|---|
| Default (Linear) | Low | Average |
| Feedforward | None | Fast |
| Adaptive | High | Slow |

The feedforward transfer function can be used in applications that require very accurate time synchronization. Because the feedforward transfer does not filter PDV, it should only be implemented in networks where the IES include PTP support in hardware.

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

Boundary clocks can be a useful consideration in large PTP networks so as to off-load the need of the Grandmaster to respond directly to lots of devices, where the Boundary clock acts as an intermediary for the Grandmaster.

### Transparent Clock

Transparent clocks compensate for latency across the network by inserting delay corrections into the PTP packets. There are two types of transparent clocks defined in the IEEE 1588 specification:

End-to-end transparent (E2E) clocks compensate for latency across a network by measuring how long IEDs and networking devices in the network take to process and forward the PTP packets. These measurements are added to the correction field in the PTP packets.

Peer-to-peer (P2P) transparent clocks assume all devices in a network are PTP aware and therefore only measure the delay to its peers. The peer-to-peer mechanism is not compatible with end-to-end transparent clocks

Transparent clocks (regardless of peer-to-peer or end-to-end) do not become nodes in the PTP hierarchy and are therefore neither master nor slave clocks. Transparent clocks sit in-line between the master and slave clocks and provide time correction between these devices.

Transparent and Boundary clocks can co-exist in a network topology. Transparent clocks are useful in networks where the topology may change the direction from which a node/switch may receive messages from the Master clock (GM or BC), such as a ring topology. Transparent clocks do not have the benefit of relieving upstream Master clocks of processing requests from end devices. **Note:** as of Power Profile 2017, peer-to-peer transparent clocks are mandated.

The following table lists different Cisco Industrial Ethernet platforms and the roles and profiles supported on the respective platforms. It is recommended to refer to the latest platform guide as well to confirm the same.

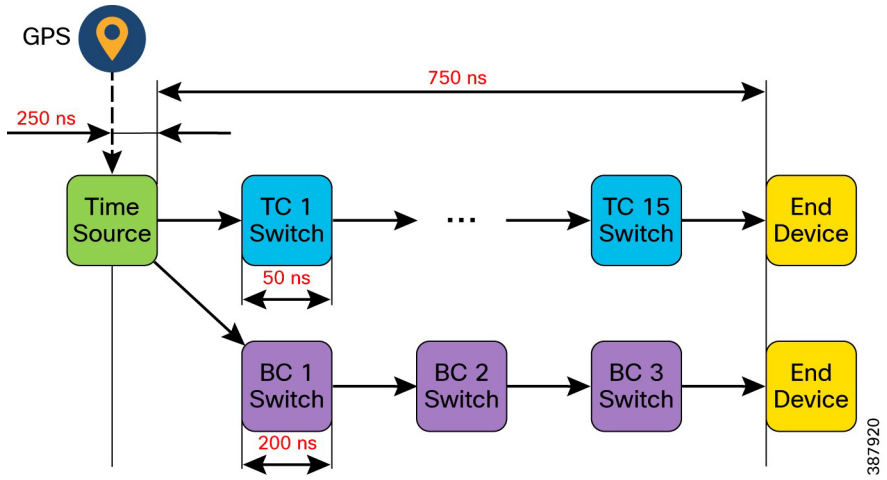
**Table 11 PTP roles and profiles on Cisco Industrial Ethernet products**

| PTP Role | Platform | Profiles supported |
|---|---|---|
| Grand Master | IE5000 | PTP Power profile 2011 |
| PTP Transparent Clock both e2e and p2p | IE9300, IE4000, IE4010, IE3400,IE5000, IE2000U | PTP Power profile 2011<br>PTP Power profile 2017 |
| PTP Boundary Clock | IE9300, IE4000, IE4010, IE3400, IE5000, IE2000U | PTP Power profile 2011 |
| PTP Over PRP Redbox | IE5000, IE4000, IE4010, IE3400 | |
| PTP over HSR | IE5000, IE4000, IE4010, IE3400 | |

## Design Considerations

When building a network, the first step is to locate the reference clocks to minimize the clock inaccuracy. Each transparent clock introduces a time inaccuracy. On the path from the grandmaster to an IED, the time inaccuracy of the different transparent clocks through which the Sync message is transmitted increases by the value of each transparent clock. Each transparent clock enabled on Cisco Industrial Ethernet devices introduces a maximum resident time delay of 50ns. Substation Automation LAN applications demand an end-to-end time delay of 1000ns, starting from the PTP Grand Master till the IED. Boundary clock enabled on Cisco Industrial devices introduces a resident time delay of 250ns and a grandmaster connected to GPS introduces a max resident time delay of 250ns. The same is depicted in the following figure. When Power Profile mode is enabled, Cisco Industrial Ethernet switches or routers drop the PTP announce messages that do not include these two Types, Length, Value (TLV) message extensions: Organization_extension and Alternate_timescale. If the grandmaster clock is not compliant with PTP and sends announce messages without these TLVs, configure the devices to process the announce message by entering the “ptp allow-without-tlv" command.

**Figure 15 PTP Clock and End to End Delay**




Because stricter timing requirements apply to the process bus, the reference clock such as PTP GrandMaster or NTP Master should be located on the station bus and the process bus devices should be synchronized to it. The device connecting station bus and process bus (Ethernet switch or IED with bridging functionality) acts as a PTP transparent clock synchronizing the process bus devices. However, when the reference clock on the station bus becomes unavailable, a device on the process bus, preferably the device connecting the station bus and process bus, should take over as a grandmaster, both towards the station bus (if it still operates) and towards the process bus. When the station bus resumes operation, the connecting device relinquishes its master role to the reference clock. It is recommended to locate the redundant clocks so that a common mode of failure is avoided if feasible and the worst-case number of transparent clocks in the path to an ordinary clock is less or equal to the original grandmaster clock.

Clock synchronization at the process level depends on the considered application and network architecture and topology. In the case of local protection functions such as over current, the relevant data are usually collected by the same merging unit and then no external synchronization is required. If the data are coming from different merging units, e.g., differential protection function, the merging units must be synchronized. How many merging units are required to perform a given function depends not only on the required availability in case of losses, but also on geographical distance and layout of the substation. The number of synchronized merging units should be minimized, e.g., by using bays. Bays could be based on multiple rings or multiple stars as well as multiple point-to-point links.

## Time Source

The GMC-BC mode allows an Industrial Ethernet Switch like IE5000 or Industrial Router like IR8340 to function as the grandmaster in a Substation. In GMC-BC mode, there are two options to synchronize the grandmaster to UTC: the NTP to PTP feature and the GNSS receiver. The Cisco IR8340 and Cisco IE5000 Industrial Ethernet Switch support the NTP to PTP feature. The Cisco Router IR8340 and Cisco IE 5000 Industrial Ethernet Switch also support the GNSS receiver.

IR8340 Timing module has support for IRIG-B (in/out), GNSS, TOD/1PPS and IEEE 1588 v2 (PTP) and SyncE, GNSS support for Stratum 3 NTP redistribution. Cisco IE5000 supports IRIG-B Input and Output interface (B002, B003, B006, B007, B122, B123, B126, B127 timecode), GNSS/GPS.

The GNSS receiver allows the device to synchronize to one of several different satellite constellations:

- GPS/NAVSTAR–Global Positioning System
- GLONASS–Global'naya Navigatsionnaya Sputnikovaya Sistema
- BeiDou–BeiDou Navigation Satellite System

The NTP to PTP feature allows the Industrial Ethernet device to use an NTP server as the reference clock for the PTP domain. In this mode, the Industrial Ethernet Switch synchronizes its clock to one or more NTP servers. How well the switch synchronizes to UTC will depend on the quality of the NTP implementation.

## GM redundancy

The grandmaster clock is the primary source of time in the PTP domain. This solution guide recommends the use of a minimum of two PTP Grandmaster clocks in the Subsation Automation LAN network. The Best Master Clock Algorithm (BMCA) is the basis of PTP functionality. The BMCA specifies how each clock on the network determines the best master clock in its subdomain of all the clocks it can see, including itself. The BMCA runs locally on each port in the network continuously for every Announce interval and quickly adjusts for changes in network configuration. BMCA based on IEEE 1588-2008 uses Announce messages for advertising clock properties.

The BMCA uses the following criteria to determine the best master clock in the subdomain:

- Clock quality (for example, GPS is considered the highest quality)
- Clock accuracy of the clock's time base
- Stability of the local oscillator
- Closest clock to the grandmaster

BMCA based on IEEE 1588-2008 uses its own data set with the received data set to determine the best clock based on the attributes with the following properties, in the indicated order:

- Priority1 - User-assigned priority to each clock. The range is from 0 to 255. The default value is 128.
- Class - Class to which a clock belongs to, each class has its own priority
- Accuracy - Precision between clock and UTC, in nanoseconds
- Variance - Variability of the clock.
- Priority2 - Final-defined priority. The range is from 0 to 255. The default value is 128.
- Unique Identifier - 64-bit Extended Unique Identifier (EUI)

In addition to identifying the best master clock, the BMCA also ensures that clock conflicts do not occur on the PTP network by ensuring that:

- Clocks do not have to negotiate with one another.
- There is no misconfiguration, such as two master clocks or no master clocks, as a result of the master clock identification process.

The BMCA will always select the "best" grandmaster available on the network. In most cases it may be beneficial to use the priority1 and priority2 values to weight the election and force specific devices to become the grandmaster.

Cisco Industrial Ethernet Switch IE5000 and Industrial Router or Substation Router IR8340 can latch onto GNSS and can act as PTP Grandmaster in Power Profile mode. As per the Cisco IOS-XE version that was validated for this solution guide, IR8340 doesn't support PTP over PRP Redbox, REP and HSR resiliency protocols. IE5000 supports PTP over PRP and HSR resiliency protocols.

## Design Considerations

- It is recommended to select a reliable device to be the primary grandmaster for the PTP domain. This device should have an accurate and reliable clock and ideally be synchronized to UTC using a reference clock.
- The primary grandmaster should be protected from faults such as power failures to improve stability of the PTP domain.
- It is also recommended to designate a secondary grandmaster which should use the same PTP timescale and UTC offset to minimize impact to the applications when the secondary grandmaster becomes the grandmaster.

- It is recommended to use Industrial Ethernet Switch in boundary clock mode to propagate time between VLANs.
- Use the time properties persist command to help ride through the loss of the grandmaster.
- Use a redundant star topology to reduce time error in substation automation applications.

## PTP Over PRP

Precision Time Protocol (PTP) can operate over Parallel Redundancy Protocol (PRP) and allows PTP to take advantage of the redundant connections of PRP-nodes thus increasing its resiliency and reliability. Cisco Industrial Ethernet devices follow IEC 62439-3:2016 standard, Annex A and implement an approach that overcomes the challenges of PTP over PRP. Two high-level changes accomplish this:

- PTP packets are not appended with PRP RCT (Redundancy Control Trailer)
- PTP packets bypass PRP duplication and discarding logic (i.e., no duplication of PTP messages), but PTP is inserted into LAN_A and LAN_B via the slave and passive-slave ports (see below)

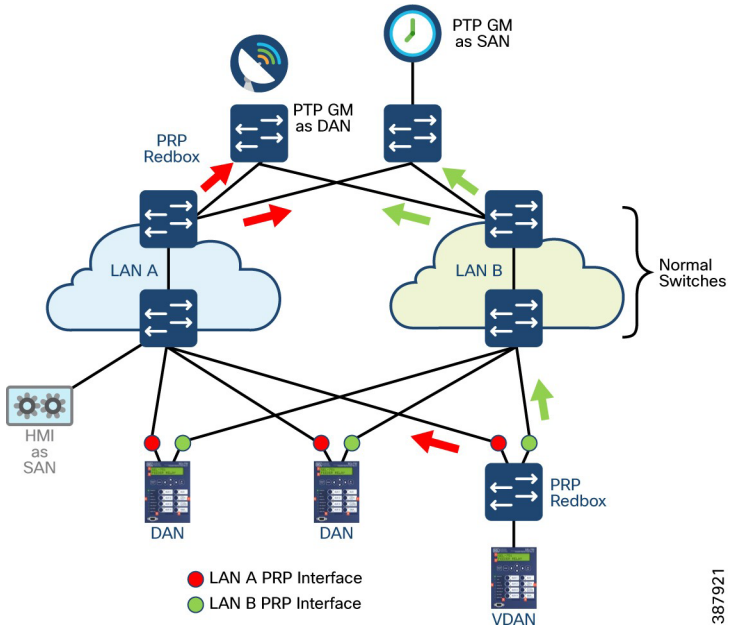
The following are possible ways that the PTP GM can be positioned in a PRP topology:

- 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.

The GM cannot be a SAN attached to LAN-A or LAN-B, because only the devices in LAN-A or LAN-B will be synchronized to the GM.

The following figure shows a sample topology where two PTP Grandmaster clocks are connected to both the LANs. One of the PTP Grandmaster clock is a single attached node connected to one of the Cisco Industrial Ethernet switches that can act as PRP Redbox, and the other clock is enabled on one of the Cisco Industrial Ethernet devices capable of connecting to GNSS and acting as PTP Power Profile Grandmaster.

**Figure 16 PTP Clock over PRP**




Dual-attached nodes (DANs) and PRP-Redbox switches receive PTP synchronization information over both their PRP ports. The LAN-A port and LAN-B port use a different virtual clock that is synchronized to the PTP GrandMaster. However, only one of the ports (referred to as SLAVE) is used to synchronize the local clock (VDAN in the figure). While the LAN-A port is the SLAVE, the LAN-A port's virtual clock is used to synchronize VDAN. The other PRP port, LAN-B, is referred to as PASSIVE_SLAVE. The LAN-B port's virtual clock is still synchronized to the same PTP Grand Master but is not used to synchronize VDAN, unless ifunless LAN-A goes down. Then LAN-B port takes over as the SLAVE and is used to continue synchronizing the local clock

For a VDAN, the PRP RedBox handles the PTP over the two PRP networks. Similarly, all DANs, VDANs and Redboxes shown in the figure continue to remain synchronized. Note that for SANs, redundancy is not available, and in this example, HMI connected as SAN will lose synchronization if LAN-A goes down.

Due to the change, VDAN may experience an instantaneous shift in its clock due to the offset between the LAN-A port's virtual clock and the LAN-B port's virtual clock. The magnitude of the shift would only be a few microseconds at the most, because both clocks are synchronized to the same GM. The shift also occurs when the LAN-A port comes back as SLAVE and the LAN-B port becomes PASSIVE_SLAVE.

The following table lists the Cisco Industrial Ethernet platforms that support PTP Power Profile over PRP. For the most accurate and latest information refer to the platform guide.

**Table 12 Cisco Industrial Ethernet Platforms and PTP over PRP**

| Platform | IE4000 | IE5000 | IE3400 | IE9300 |
|---|---|---|---|---|
| PTP Power Profile over PRP | Yes | Yes | Yes | Yes |

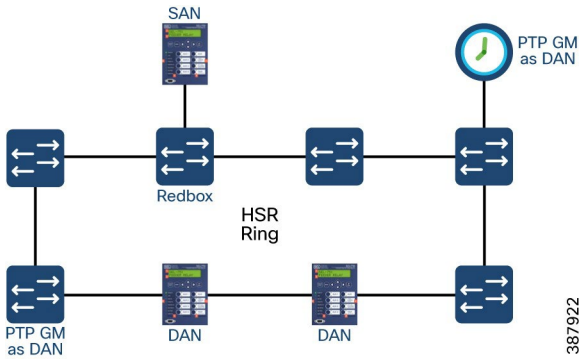
## PTP Over HSR

The HSR duplicate/discard logic is not used for PTP packets to provide high availability for PTP through redundancy.

The following figure describes how PTP clock synchronization works in an HSR network. In this example, a VDAN/SAN is the PTP grandmaster clock. Dually attached devices receive PTP synchronization information over their HSR ports. However, only one of the ports (referred to as SLAVE) is used to synchronize the local clock. The other HSR port (referred

to as PASSIVE) continues to receive synchronization information but is not used to synchronize the local clock. Suppose that RedBox has its port-A as SLAVE and port-B as PASSIVE. When port-A goes down, the portport-B port takes over as the SLAVE and is used to continue synchronizing the local clock on RedBox.

**Figure 17 PTP Clock over HSR**




The PTP grandmaster in an HSR network can be a RedBox, a VDAN/SAN, or a DANH.

The following table lists the Cisco Industrial Ethernet platforms that support PTP Power Profile over PRP. For the most accurate and latest information refer to the platform guide.

**Table 13 Cisco Industrial Ethernet Platforms and PTP over HSR**

| Platform | IE4000 | IE5000 | IE3400 |
|---|---|---|---|
| PTP Power Profile over PRP | Yes | Yes | Yes |

# VLANs and Trunking

Industrial security best practices suggest migrating networks towards architectures compliant with IEC62443 zones and conduits. It is recommended to place assets that do not need to talk to each other into separate network segments or zones to help prevent an attack from spreading to the entire industrial network and infrastructure. NERC CIP compliance dictates multiple segmentation “zones” based on criticality of assets in a substation and between substations. There are a number of mechanisms to implement segmentation in networks including L2 VLANs, L3 VRFs, firewalls and Security Group Tags (which can provide segmentation regardless of VLAN or IP address assignment). VLANs provide a logical separation of networks and can be done on different layers, most common on layer 2. Firewalls to control inbound and outbound traffic into/from different zones. This section describes VLAN.

VLANs is a method to separate types of traffic that share the medium, for instance:

- ESP Zone – OT Traffic Segmentation using VLAN
  - MMS SCADA VLAN
  - DNP3 SCADA VLAN
  - GOOSE VLAN (Process and Station Bus)
  - SV VLAN (Process Bus)
  - Engineering VLAN
  - PTP VLAN
- Corp Zone
  - Video Surveillance VLAN

  - VOIP VLAN
  - Remote Work Force Use case VLAN for WLAN
- CIP Zone
  - VLAN/IP Subnet
  - HMI
  - SCADA MMS

VLANs just separate traffics, there are not intended to reduce trunk traffic. Usually, trunk links have a higher bandwidth than edge links, so it is not necessary to segment them. In principle, a device on VLAN 1 cannot even see that a device on VLAN 2 exists. Devices on different VLANs influence each other only by the bandwidth they consume because they nevertheless share the same physical medium. If necessary, communication between VLANs takes place over a layer 3 router. VLANs divide layer-2 broadcast domains (which define how far broadcast, multicast and unicast traffic travels) and serves as a first security barrier, since the access to the VLAN is entirely governed by the networking device. A device connected inadvertently to the wrong port will not be able to communicate. However, VLANs provide only a weak data security, since any misconfiguration in the network is a potential loophole and configuration is not supervised. The end devices connected to the edge ports are normally VLAN-unaware.

IEC 61850 use 802.1Q priority tagging to privilege time critical bus traffic for protection relevant applications over low priority MMS and management traffic. GOOSE and SV traffic use layer 2 multicast. This traffic propagates across the whole network reaching all bridges and all IEDs. It impacts the bandwidth of all links in the network and adds latency to processing times in all bridges and all IEDs. Therefore, when the station bus extends to numerous devices, it is advisable to divide it into segments separated by bridges that can filter out multicast traffic. A natural way is to split the station bus according to the different voltage levels as shown in the following Figure.

VLAN Trunk refers to a networking configuration that allows multiple VLANs to traverse through a single ethernet link while continuing to keep that traffic in the respective VLANs separated.

## Quality of Service and Protecting Critical 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.

The following table 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 14 Substation Automation LAN Traffic and QoS Requirements**

| Traffic Type | Classification Criteria | Egress | | | Notes |
|---|---|---|---|---|---|
| Mechanisms | Ingress QoS Group Marking | Shaping | Bandwidth Guarantee | Congestion Avoidance | |
| GOOSE/GSSE/SV | 1 | Priority Queuing (policy 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 |

Cisco Industrial Ethernet switches 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.

### Storm Control

Storm control prevents LAN interfaces from being disrupted by a broadcast storm. A broadcast storm occurs when broadcast packets flood the subnet, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a broadcast storm.

## Substation Core and Utility WAN – Design Considerations

The Substation Core is the function that interconnects the various substation zones with the Utility WAN. As specified in NERC CIP standards, to interconnect the ESP, an Electronic Access Control System (EACS) is required and is considered part of the Substation Core. Additionally, it is often the role of the substation router to connect legacy serial devices and provide them connectivity to SCADA applications in the Operations and Command Center via the Utility WAN.

This section discusses the following topics:

- Requirements of the Substation Core and Utility WAN, technical and application protocols
- Equipment Portfolio
- EACS design options for connecting and protecting the ESP
- Legacy Protocol design options
- WAN design options

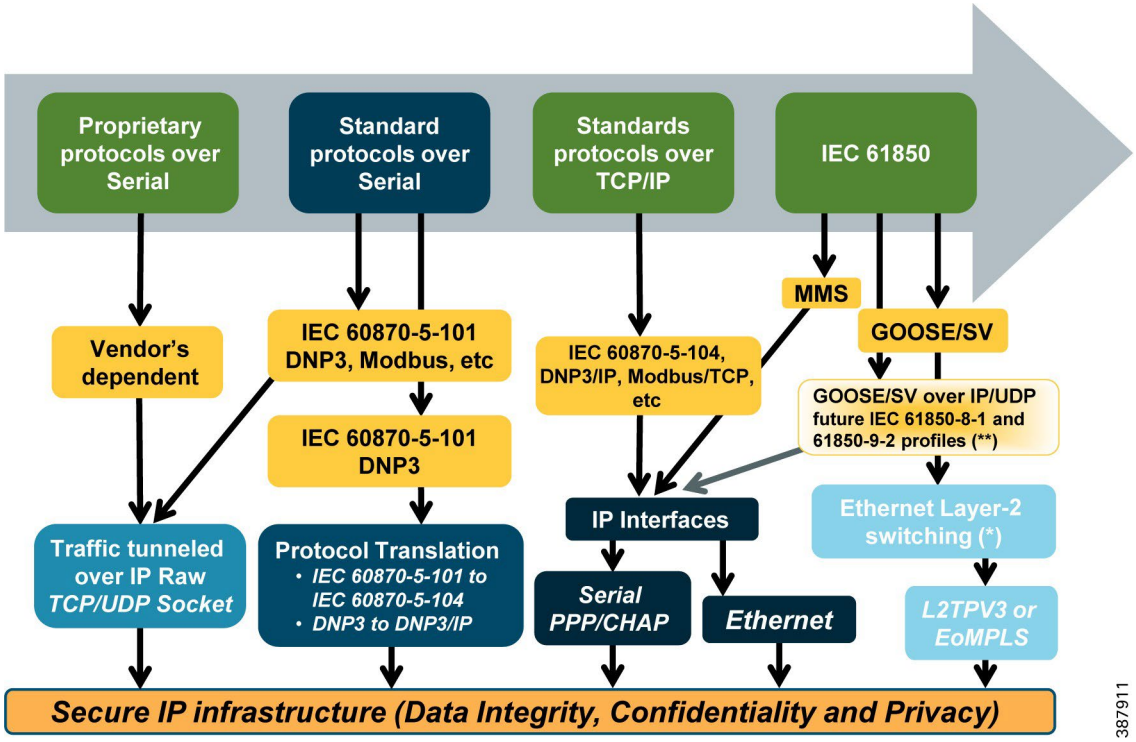
### Substation Core and Utility WAN Networking – Requirements

#### Application and Protocols

Over the last decade or more, substation operators have steadily moved their substation operations to standard network (Ethernet, TCP/IP) based communication protocols, such as IEC 61850, DNP3 TCP, Modbus-TCP and IEC 60870-5-104. All of these are covered as part of the ESP zone. Nonetheless, the substation often contains devices that for a number of reasons cannot easily or are cost prohibitive to migrate to standard network connectivity. These devices often use a range of various serial-based legacy SCADA protocols including DNP, Modbus and IEC 60870-5-101.

As these devices are often critical to substation operations, they must be interconnected to the centralized SCADA applications of the substation operator. The Substation Core provides key connectivity to these devices and communicates the protocols over the utility WAN back to the operations center. This section provided design guidance on connecting and backhauling these protocols.

**Figure 18 SCADA Protocols**




## Technical

## Substation Core – Portfolio

The IR8300 platform has 2 NIM slots and 2 PIM slots as well as a timing module. IR8300 has 12 LAN interfaces. 4 copper with POE, 4 combo SFP/copper and 4 SFP ports as well as 2 combo SFP/copper ports for WAN connectivity.? All LAN & WAN are 1 GE. IRM-NIM-2T1E1  2 port Network Interface T1/E1 Module can be bundled for Multilink PPP WAN backhaul.

The following LTE Pluggable interface modules are supported for WAN connectivity.

**Table 15 IR8340 LTE Pluggable Interface Modules**

| LTE Pluggable interface module | WAN Connectivity |
|---|---|
| P-LTEAP18-GL | 4G/CAT18 LTE Advanced Pro Pluggable – Global |
| P-LTE-MNA | 4G/CAT6 LTE Advanced Pluggable for North American and Europe |
| P-LTE-EA | CAT6 Advanced Pluggable for Europe and North America |
| P-LTE-LA | CAT6 Advanced Pluggable for APAC, LATAM and ANZ |

For more details on WAN modules see:

https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-ir8300-rugged-series-router/nb-06-cat-ir8340-rugged-ser-rout-ds-cte-en.html

Cisco IR8340 Substation Router supports following functions for Utility WAN, VPN and Firewall functions:

- Static and dynamic routing options to route traffic from Substation to one or many control centers
- Interconnect other substations, the multi-service and
- Ability to perform MPLS PE and CE functionality to connect to TSO owned MPLS Backhaul network as shown in below figure for On Net Deployment
- Ability to translate addresses on the LAN to different addresses on the WAN or Internet for proper routing and for cyber security protection of LAN devices using NAT feature.
- Zone-based Firewall to protect substation LAN traffic and devices from unauthorized access.
- Virtual Private Networking (VPN) using any of several standard protocols – establishing an isolated communications tunnel through an insecure public communications network to a secure remote utility server, with strong encryption of messages that protects against disruption or monitoring of message flow.
- Ability to perform QoS functionality in form of Diffserv for prioritizing critical traffic flowing in and out of Substation
- Ability to perform multicast routing based on Substation Use case requirement
- Recognition of external path failures and rerouting of traffic via alternate paths – BGP,OSFP,EIGRP
- First hope redundancy protocols – VRRP and HSRP
- Monitoring, alarming, and logging of traffic behavior and diagnostics
- Network management protocol (SNMP) communications for router and network configuration management.
- Secure shell (SSH) network web server communications with a remote management computer/server – another way of remotely managing the setting and configuration of the router.
- Receiving and serving date/time information to the LAN network time protocol, NTP;and simple NTP or SNTP.
- Ability to function as PTP Power Profile Grand Master or Transparent Clock
- Ability to host applications for distributed computing
- Ability to act as Inline Network Sensor to host Cisco Cybervision Sensor software for OT flow and asset Visibility
- Ability to power up endpoints using POE technology
- GNSS Input

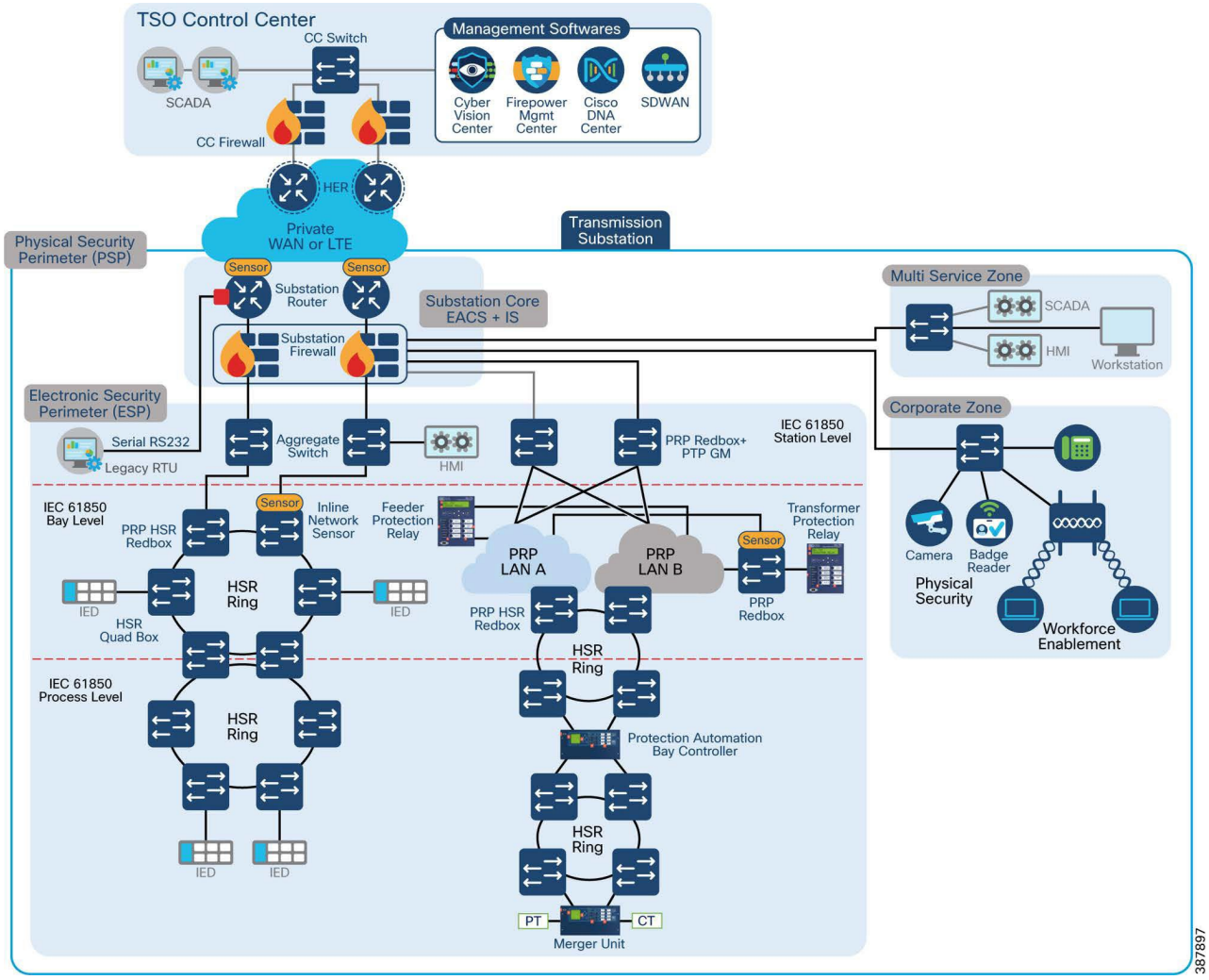
## EACS Design Considerations

### Design Option 1

**Combined EACS and Router**

L3 Routing between ESP Zone and Substation Core Zone. L2 Between Substation Core and Multiservice/ Corporate zones (L2) as depicted in the figure below.

**Figure 19 L3 Routing between ESP Zone and Substation Core Zone**



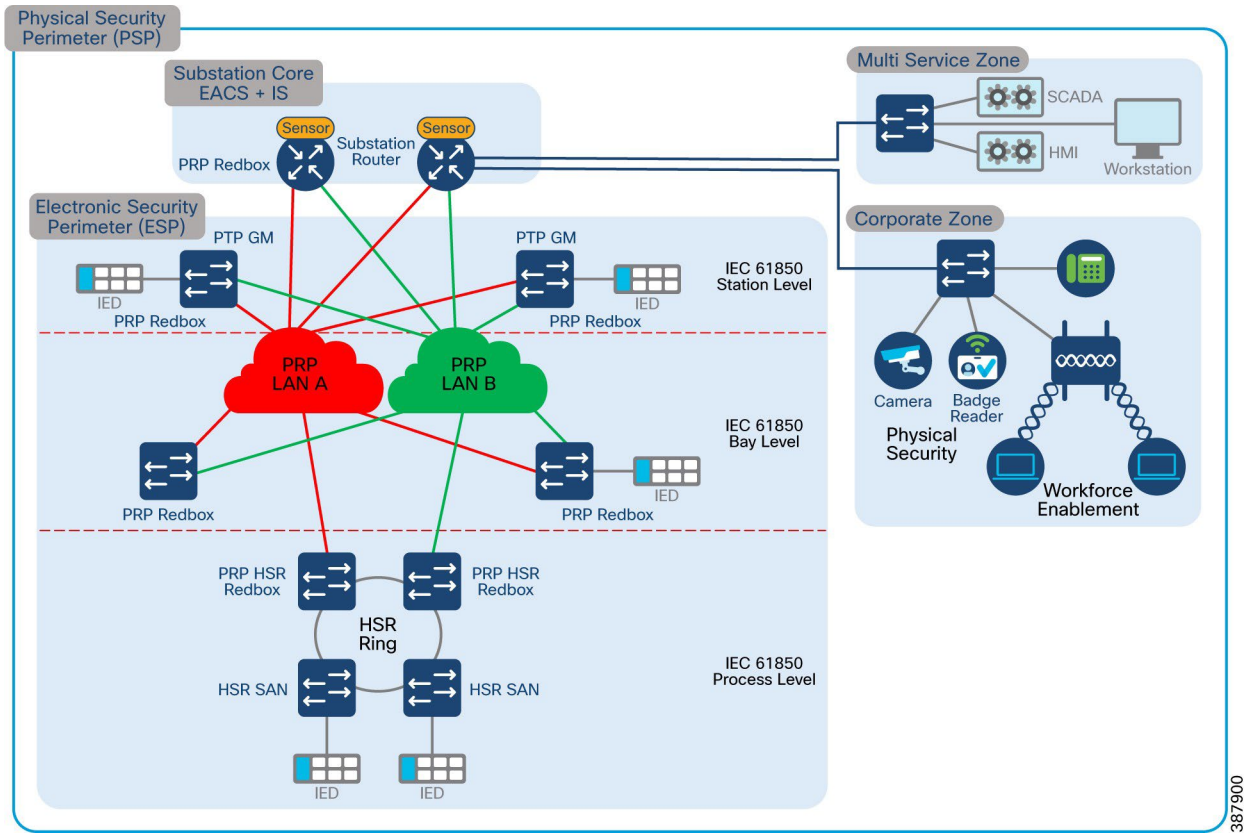

## Design Option 2

Substation Router in Core Zone directly aggregating ESP Station Bus (L2) and Multiservice/ Corporate zones (L2)

There are multiple sub design options for aggregation L2 Traffic from ESP Zone on Substation Router.

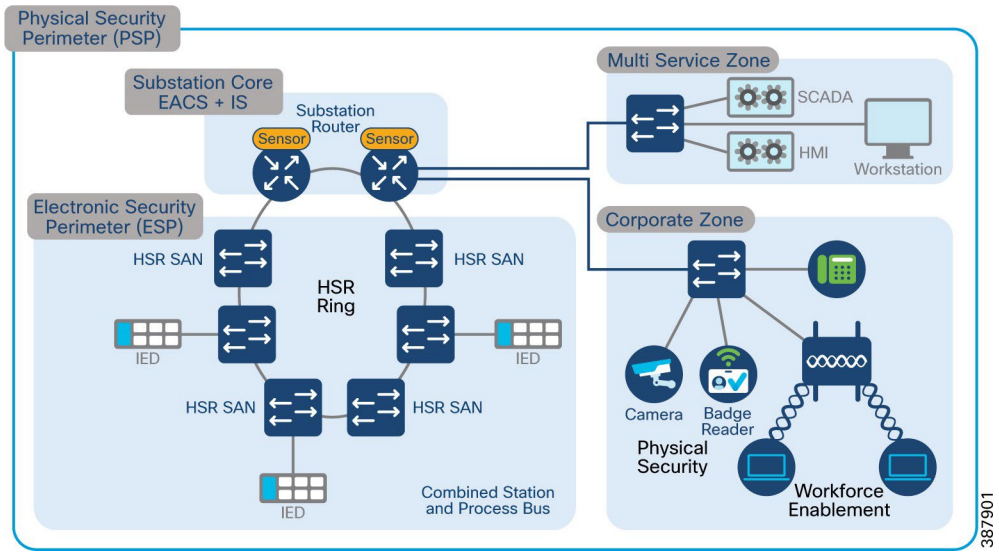
- Option A – Substation Router as PRP Redbox as part of IEC 61850 Station BUS as depicted in below figure. Multi Service and CORP Zones can be connected as star to Substation Router, or we can run L2 Ring protocol like REP or RSTP based on application requirements.

**Figure 20 Substation Router aggregating ESP and Multiservice Zones**



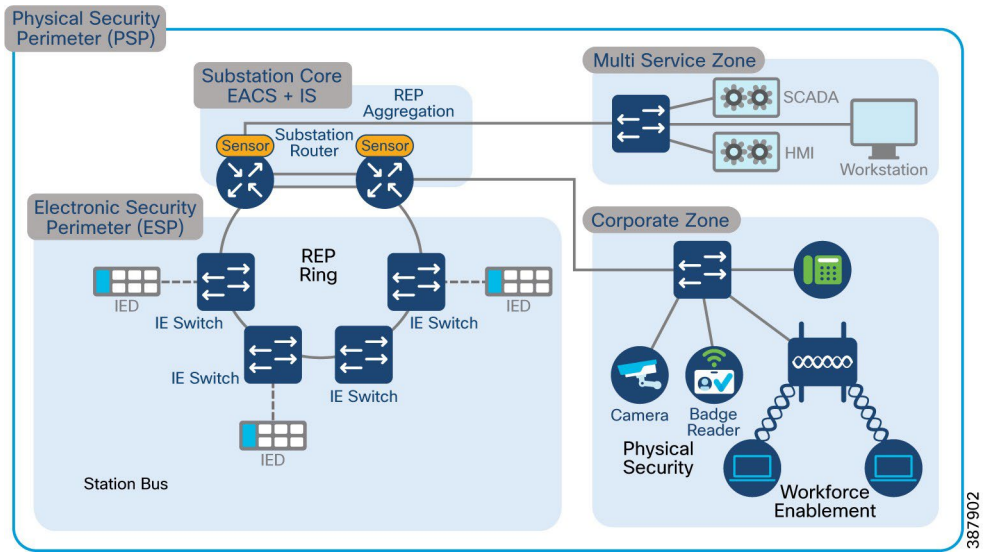

- Option B – Substation Router used as HSR SAN as part of IEC 61850 Station BUS as depicted in the figure below and design for other zones like the option above.

**Figure 21 Substation Router as HSR SAN**




- Option C – Substation Router terminating multiple REP Rings from ESP, Multi Service, and Corp Zones.

**Figure 22 Substation Router with multiple REP rings for different zones**




Pros and cons of different ESP design options are discussed in later section of this CVD. See the Architecture section for options.

# Legacy SCADA protocols design considerations

## Raw Sockets

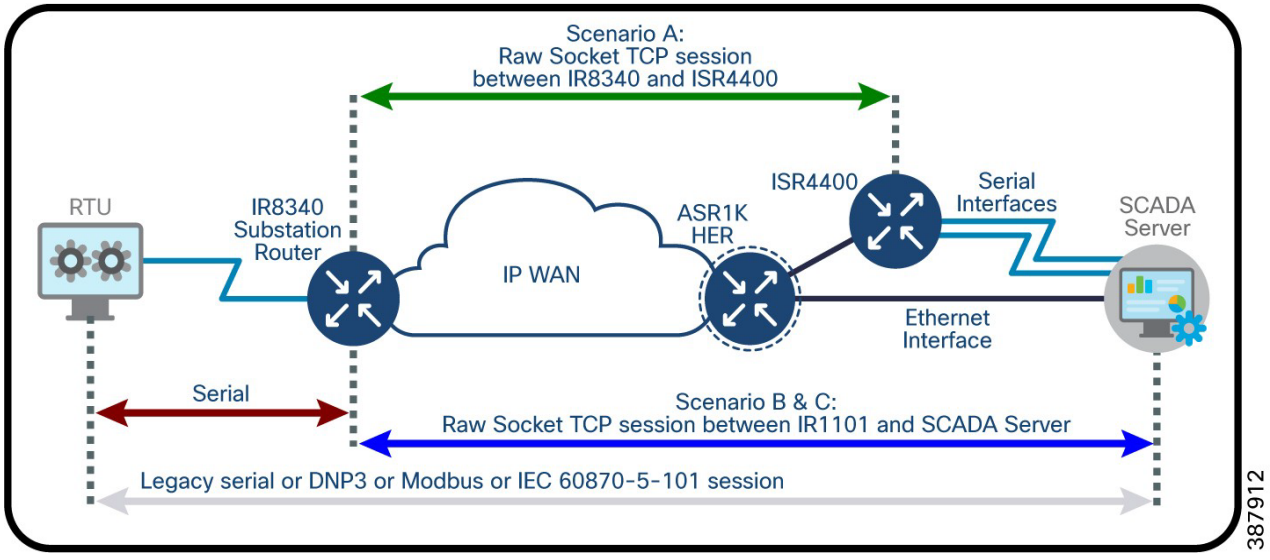
A means to transport streams of characters from one serial interface to another over the IP network for utility application. Serial communications have been the mainstay for Utilities communications for more than a decade using RS232 and RS485 as the physical layer. There is a currently a move within the industry to migrate to Ethernet. However, retrofitting Ethernet and newer IEDs into existing communications systems require supporting a hybrid network of both Ethernet and serial devices. Raw Socket transports Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). Raw Socket supports point-to-point and point-to-multipoint connections over an asynchronous serial line and has a built-in auto TCP connection retry mechanism. Packetization and sending data on a specific packet length, a specific character or upon a timeout are supported sub features within Raw sockets. Monitoring and control (SCADA) data will be routed from the substation to the control center. SCADA communications have latencies ranging from ~500 milliseconds to ~5 seconds.

## Raw Socket TCP Transport

TCP Raw Socket transport uses a client-server model. At most one server and multiple clients can be configured on a single asynchronous serial line. A Raw Socket client receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The Raw Socket client initiates a TCP connection with the Raw Socket server and sends the packetized data across the IP network to the Raw Socket server, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management.

The figure below depicts three different deployment scenarios for point-to-point Raw Socket service.

**Figure 23 Raw Socket TCP Transport**




**Scenario A:** Raw Socket between IR8340 and SCADA Router in headend – no change on SCADA server – communications through COM ports.

**Scenario B:** Raw Socket between IR8340 & SCADA Server – no SCADA application change on server but IP/Serial Redirector software maps COM port to IPv4 address + address + TCP port, running over Ethernet interface.

**Scenario C:** Raw Socket between IR8340 & SCADA Server – SCADA application knows how to directly communicate over a Raw Socket (IPv4 address + TCP port) & Ethernet interface.

**Note:** Scenario A is not scalable. Scenario B or Scenario C for Raw socket deployments is recommended.

## Raw Socket UDP Transport

UDP transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line. The Raw Socket UDP peer receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. Raw Socket UDP peer sends the packetized data across the IP network to the Raw Socket peer at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.

## Protocol Translation

As the Utility industry begins the transition from Legacy based SCADA protocols to IP based protocols, there is a need for a migration strategy to enable both legacy and newer IP based protocols to interoperate. The Protocol translation otherwise known as SCADA Gateway feature on the IR8340 provides this capability.

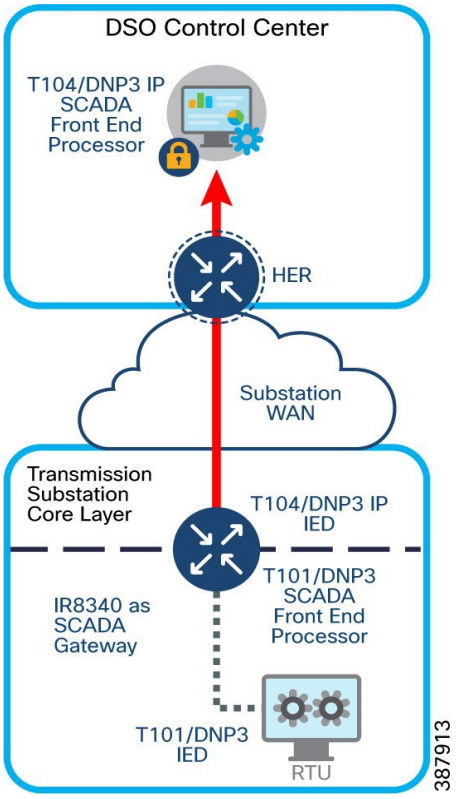
The SCADA Gateway function allows for the following translations between:

- IEC-60870-5-101 and IEC-60870-5-104
- DNP3 Serial and DNP3 IP

The following software stacks are implemented in Cisco Substation Router IR8340

- IEC-101 and DNP3 serial  Protocol Stack
- IEC-104 and DNP3 IP Protocol Stack
- Translation Module to translate between
  - IEC-101 and IEC-104
  - DNP3 Serial and DNP3 IP

**Figure 24 SCADA Protocol Translation**




In the above diagram the IR8340 acts as SCADA gateway to implement T101 Master and T104 slave functionalities. One RTU per serial interface is connected. DA Gateway/ Secondary Substation router will acts as T101 Master for T101 slave RTU. In turn DA Gateway/Secondary Substation router will acts as T104 slave to SCADA T104 Master residing in the control center. This scenario depicts point-to-point protocol translation scenario.

## T101/T104 Protocol translation features

- T101/T104 refers to IEC 60870-5-101 and IEC 60870-5-104 Standard respectively.
- T101 supports point-to-point and multi drop links over serial communications.
- T104 utilizes TCP/IP transport & network protocols to carry the application data (ASDU), which is specified in T101.
- Allows “balanced” and “unbalanced” communication types.
- Balanced mode is limited to point-to-point links where either station can initiate transaction (similar to dnp3 unsolicited response) unbalanced mode is suitable for multi drop links where only master station can send primary frames.

## DNP3/ DNP3 IP Protocol translations features

### Serial Stack

- Poll all data from RTU every 90 seconds
- Provide local time to RTU every 90 seconds
- Support file transfer to and from RTU

- Enable/disable of unsolicited response on RTU

**IP Stack**

- Respond to control center request with local data
- Trigger counter interrogation to RTU when receive such request from control center
- Trigger control transaction to RTU when received such request from control
- Support file transfer to and from control center
- Enable/disable of sending unsolicited response to control center

## Utility WAN design considerations

As explained in architecture section WAN tier aggregates Transmission Service Operator (TSO) Control center and Transmission Substations. Cisco IR8340 deployed as Substation Router serves as an interface between a local area network in a substation and the utility control or enterprise WAN.

- On Net Substation
  - Utility Owned MPLS/IP Backhaul
  - Substation router IR8340 acting as MPLS CE
- Off Net Substation
  - Public Backhaul (Leased Line/ Cellular Backhaul)
  - Substation Router IR8340 acting as IPSEC (FlexVPN/DMVPN) Spoke

**Figure 25 On Net Substation**

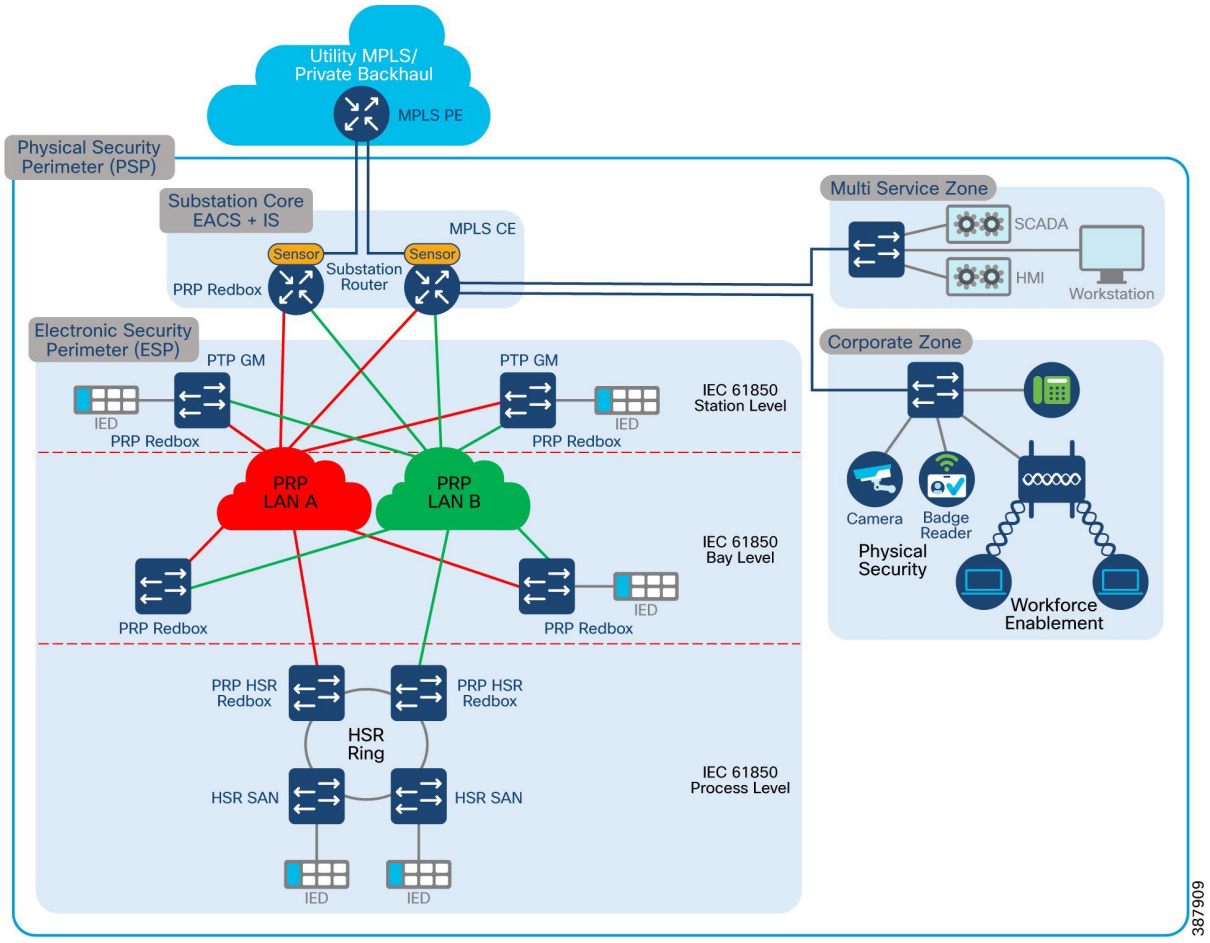
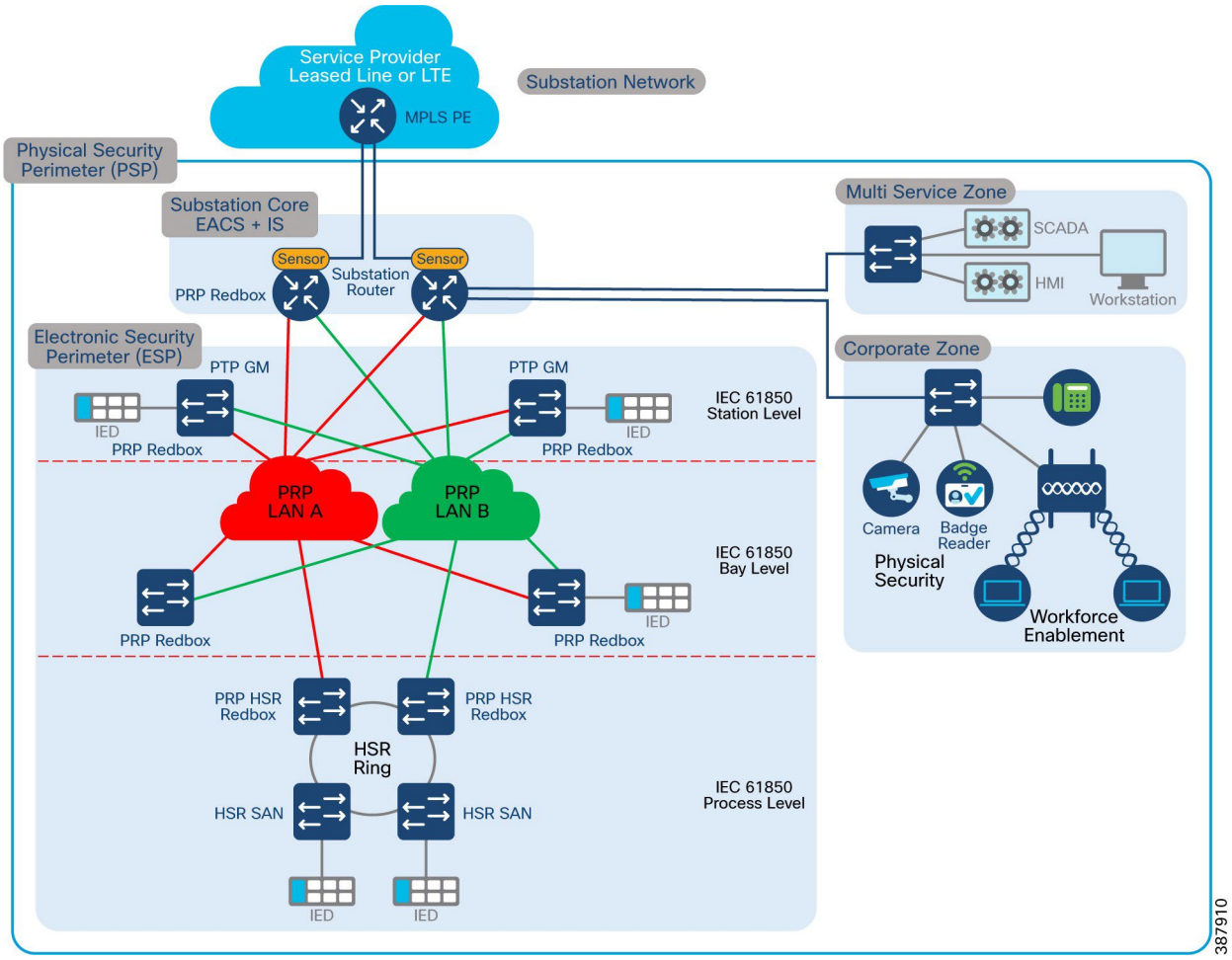


**Figure 26 Off Net Substation**




## WAN Backhaul Redundancy

This scenario addresses the potential failure of a WAN backhaul path.

- SA Router IR8340 can be deployed with different backhaul interfaces that connect different aggregation routers.
- The backhaul interface may be a combination of any Cisco IOS-supported interface's type: Cellular or Ethernet.
- WAN Backhaul Redundancy can be designed with multiple options:
  - Option 1—Single Tunnel FlexVPN tunnel pivot dual backhaul interfaces (dual ISP)
  - Option 2—Dual Tunnel (Active/Active) and dual ISP

Substation Automation Router WAN Backhaul Redundancy is similar to Distribution Automation/Secondary Substation Gateway Design. Refer to the following DA CVD for more details on WAN Backhaul Redundancy design:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG/DA-SS-DG-doc.html

# Network Management

## Substation LAN and Cisco DNA-Center

Cisco DNAC offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides network visibility and uses network insights to optimize network performance and deliver the improved user and application experience. This guide focuses on non-SDA (non-fabric) design. Lack of network health visibility to network administrators and manual maintenance tasks like software upgrades and configuration changes are some of the common network challenges in Substation Automation LAN networks.

It is recommended to place Cisco DNA Center as an application in the TSO Control center but the final decision on location should be made considering the specific customer requirements. Some of the benefits are as follows

- DNA Center performs critical functions to maintain the operational status of the production environment. Those critical functions include Assurance and monitoring of the production network, guided remediation of identified problems and device replacement.
- A separate instance for production environments helps ensure operational requirements are maintained. Production environments have significantly higher and different operational requirements than Enterprise system. A DNA Center instance that supports both Enterprise and Production networks may lead to inadvertent changes or updates impacting the production system that could lead to downtime.

The following are some of the key considerations when adding Cisco DNA Center:

- Cisco DNA Center requires connectivity to all network devices it manages. That means that all devices that need to be discovered and monitored should have an IP address assigned that is routable and able to reach the Cisco DNA Center.
- Cisco DNA Center requires Internet connectivity for licensing information and updates. We recommended using a Smart License proxy. It is also recommended that you allow secure access via the proxy service only to URLs and fully qualified domain names required by Cisco DNA Center. For more details refer to:

  https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html
- If there is an industrial firewall between Cisco DNA Center and managed devices, make sure required ports are allowed on the firewall.
- Latency should be equal to or less than 100 milliseconds to achieve optimal performance for all solutions provided by Cisco DNA Center. The maximum supported latency is 200ms RTT. Latency between 100ms and 200ms is supported, although longer execution times could be experienced for certain functions including Inventory Collection and other processes that involve interactions with the managed devices.
- Cisco ISE must be deployed with a version compatible with Cisco DNA Center. Refer the following link for compatibility information:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

The following are some of the known limitations of Cisco DNA Center:

- Cisco DNA Center does not support managing network devices with management IP address behind a Network Address Translation (NAT) boundary.
- Firewalls running Firepower Threat Defense (FTD) software are not supported on Cisco DNA Center, nevertheless devices connected behind an industrial firewall can be provisioned and managed by Cisco DNA Center.

- Cisco DNA Center does not support automated workflows or assurance for resiliency protocols such as PRP, HSR, REP, DLR. Switches can be still discovered by Cisco DNA Center and benefit from features such as software upgrades, compliance, and device assurance.
- Cisco DNA Center cannot manage products by third party vendors.

The following lists some of the key Cisco DNA Center features:

- Existing switch discovery
- New switch onboarding
- Device Replacement
- Software Upgrades for network infrastructure
- Software, configuration, and security compliance for network infrastructure
- Switch configuration via Cisco DNA Center
- Monitoring of network devices and endpoint network status, including IACS devices
- Troubleshooting and remediation tools provided by Cisco DNA Center
- Network insights
- Security analytics

This section covers planning activities that are required in Cisco DNA Center before discovering and provisioning devices or using assurance.

This section assumes the DNA Center appliance has been installed and the software installed. Those topics will be covered in more detail in the DNA Center for Industrial Automation Implementation Guide. This section covers the following design activities:

- Establish the role-based access control in Cisco DNA Center, which is required to create users with right privileges to perform Cisco DNA Center tasks introduced in the guide.
- Cisco DNA Center assigns users to roles that determine what types of operations a user can perform in the system. The following predefined roles are some of the roles supported by Cisco DNA Center:
  - Network Admin Role
  - Observer Role
  - Super-Admin Role

The following predefined roles are recommended:

- Users that need to provision the network should use the Network-Admin-Role.
- Users that need assurance and inventory visibility should use the Observer-Role.
- Only Cisco DNA Center system administrators should use the Super-Admin-Role.

Define a network hierarchy by creating sites. Sites group devices by physical location and/or function in the network.

- The network hierarchy represents your network locations. It allows for a hierarchy of sites, which contain areas, which, contain buildings and floors. We refer to areas, buildings, and floors as site information. It is possible to create site information to easily identify where to apply design settings or configurations. A site on Cisco DNA Center determines which network settings, software images, and customized templates are applied to a device.

- Configure network settings that apply to those sites such as device credentials, DHCP, and NTP servers. These settings may be applied to devices that belong to a site as part of automation workflows.
- Create network profiles. In the case of switches, network profiles link configuration templates to sites.
- Network profiles are a key concept in Cisco DNA Center to standardize configurations for routers, switches, and WLCs in one or multiple sites. In the case of switches, A profile is used to assign configuration templates to devices based on their site information, device product family, and associated tags. For devices that require a similar configuration, a template helps to reduce the configuration time by using variables and logic statements as placeholders for any unique settings.
- Manage software image repository for network infrastructure upgrades.
- Cisco DNA Center stores all the unique software images according to image type and version. It is possible to view, import, and delete software images.
- It is to be noted that Cisco IR8340 Substation Router is a non-fabric device. Cisco IR8340 needs to be onboarded onto DNAC first using template post which Cisco Industrial Ethernet switch IE9300 needs to be onboarded.

For more details see the following guide:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Networking/DNA_Center_IA/DNA_Center_IA.html

## WAN and vManage

The Cisco SD-WAN solution is an enterprise-grade WAN architecture overlay that enables digital and cloud transformation for enterprises. It integrates routing, security, centralized policy, and orchestration into large-scale networks. It is multitenant, cloud-delivered, highly automated, secure, scalable, and application-aware with rich analytics. The Cisco SD-WAN technology addresses the problems and challenges of common WAN deployments. Some of the benefits include:

- Centralized network and policy management, as well as operational simplicity, resulting in reduced change control and deployment times.
- A mix of MPLS and low-cost broadband or any combination of transports in an active/active fashion, optimizing capacity and reducing bandwidth costs.
- A transport-independent overlay that extends to the data center, branch, and cloud.
- Deployment flexibility. Due to the separation of the control plane and data plane, controllers can be deployed on premises or in the cloud. Cisco WAN Edge router deployment can be physical or virtual and can be deployed anywhere in the network.
- Robust and comprehensive security, which includes strong encryption of data, end-to-end network segmentation, router and controller certificate identity with a zero-trust security model, control plane protection, application firewall, and insertion of Cisco Umbrella™, firewalls, and other network services.
- Seamless connectivity to the public cloud and movement of the WAN edge to the branch.
- Application visibility and recognition in addition to application-aware policies with real-time service-level agreement (SLA) enforcement.
- Dynamic optimization of SaaS applications, resulting in improved application performance for users.
- Rich analytics with visibility into applications and infrastructure, which enables rapid troubleshooting and assists in forecasting and analysis for effective resource planning.

This section provides an overview of the Cisco SD-WAN solution. It discusses the architecture and components of the solution, including control plane, data plane, routing, authentication, and onboarding of SD-WAN devices. The section is based on vManage version 20.8.1.

- The Cisco SD-WAN solution consists of separate orchestration, management, control, and data planes.
- The orchestration plane assists in the automatic onboarding of the SD-WAN routers into the SD-WAN overlay.
- The management plane is responsible for central configuration and monitoring.
- The control plane builds and maintains the network topology and makes decisions on where traffic flows.
- The data plane is responsible for forwarding packets based on decisions from the control plane.

The primary components for the Cisco SD-WAN solution consist of the vManage network management system (management plane), the vSmart controller (control plane), the vBond orchestrator (orchestration plane), and the WAN Edge router (data plane).

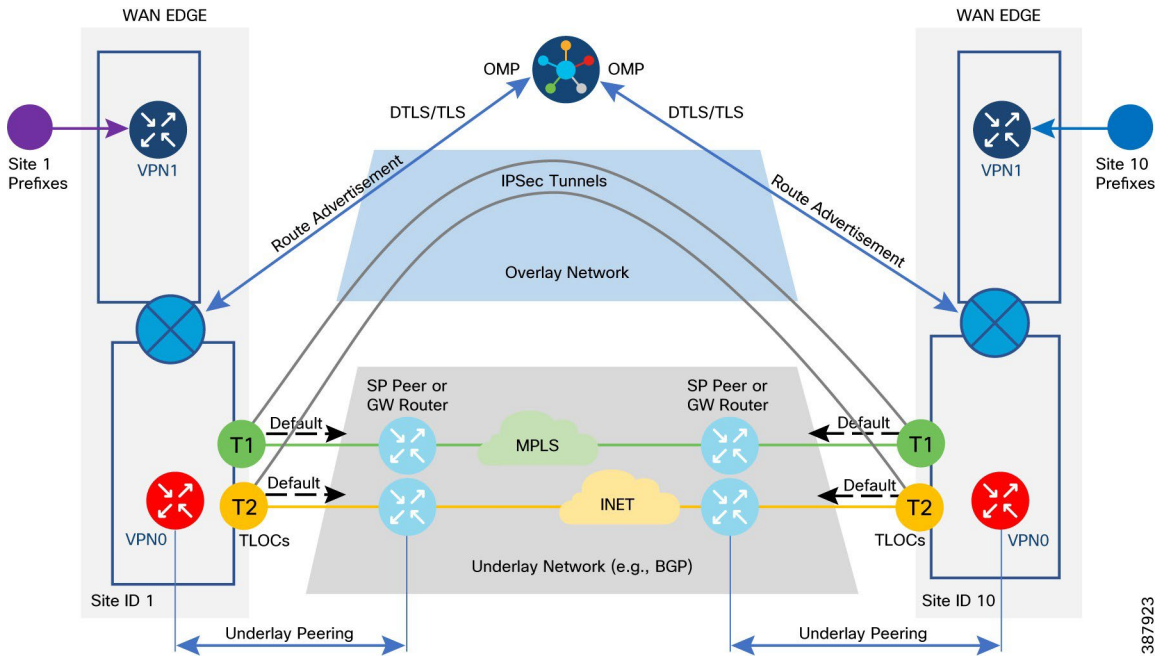
- vManage – This centralized network management system is software-based and provides a GUI interface to easily monitor, configure, and maintain all Cisco SD-WAN devices and their connected links in the underlay and overlay network. It provides a single pane of glass for Day 0, Day 1, and Day 2 operations.
- vSmart controller – This software-based component is responsible for the centralized control plane of the SD-WAN network. It maintains a secure connection to each WAN Edge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the WAN Edge routers by reflecting crypto key information originating from WAN Edge routers, allowing for a very scalable, IKE-less architecture.
- vBond orchestrator – This software-based component performs the initial authentication of WAN Edge devices and orchestrates vSmart, vManage, and WAN Edge connectivity. It also has an important role in enabling the communication between devices that sit behind Network Address Translation (NAT).
- WAN Edge router – This device, available as either a hardware appliance or software-based router, sits at a physical site or in the cloud and provides secure data plane connectivity among the sites over one or more WAN transports. It is responsible for traffic forwarding, security, encryption, quality of service (QoS), routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and more.

The Cisco SD-WAN network is divided into two distinct parts: the underlay and overlay network. The underlay network is the physical network infrastructure which connects network devices such as routers and switches together and routes traffic between devices using traditional routing mechanisms. In the SD-WAN network, this is typically made up of the connections from the WAN Edge router to the transport network and the transport network itself. The network ports that connect to the underlay network are part of VPN 0, the transport VPN.

Getting connectivity to the Service Provider gateway in the transport network usually involves configuring a static default gateway (most common), or configuring a dynamic routing protocol, such as BGP or OSPF. These routing processes for the underlay network are confined to VPN 0 and their primary purpose is for reachability to TLOCs on other WAN Edge routers so that IPsec tunnels can be built to form the overlay network.

The IPsec tunnels which traverse from site-to-site using the underlay network help to form the SD-WAN overlay network. The Overlay Management Protocol (OMP), a TCP-based protocol like BGP, provides the routing for the overlay network. The protocol runs between vSmart controllers and WAN Edge routers where control plane information is exchanged over secure DTLS or TLS connections. The vSmart controller acts a lot like a route reflector; it receives routes from WAN Edge routers, processes and applies any policy to them, and then advertises the routes to other WAN Edge routers in the overlay network.

**Figure 27 SDWAN Logical Network**




There are multiple, flexible controller deployment options available for customers. Controllers can be deployed:

- In a Cisco-hosted cloud controllers can be deployed in AWS or Azure. Single or multiple zones are available for the deployment. Most customers opt for Cisco cloud-hosted controllers due to ease of deployment and flexibility in scaling. Cisco takes care of provisioning the controllers with certificates and meeting requirements for scale and redundancy. Cisco is responsible for backups/snapshots and disaster recovery. The customer is given access to vManage to create configuration templates and control and data polices for their devices.
- In a Managed Service Provider (MSP) or partner-hosted cloud. This is private cloud-hosted or can be public cloud-hosted and deployed in AWS or Azure. The MSP or partner is typically responsible for provisioning the controllers and responsible for backups and disaster recovery.
- On-premise in a private cloud or data center owned by an organization. The customer is typically responsible for provisioning the controllers and responsible for backups and disaster recovery. Some customers, such as financial institutions or government-based entities may choose to run on-premise deployments mainly due to security and compliance reasons.

## On-Premise Controller Deployment

On-Premise Controller Deployment is the recommended deployment option for Utility customers due to security and compliance reasons. In this type of controller deployment, controllers are deployed on-premise in a data center or private cloud, where the enterprise IT organization is typically responsible for provisioning the controllers and responsible for backups and disaster recovery. Some customers, such as financial institutions or government-based entities, may choose to run on-premise deployments mainly due to security compliance reasons.

For on-premise deployments, there are multiple ways to arrange the controllers using NAT, Public IPs, and/or Private IPs. The following are common options for on-premise deployments:

Control connections are established through both the Internet and MPLS transports using publicly routable IP addresses. Publicly routable IP addresses can be assigned directly to the controllers or through one-to-one NAT.

Control connections are established through the MPLS transport using private (RFC 1918) IP addresses and established through the Internet using publicly routable IP addresses. The vBond can use a publicly routable IP address that is accessible from either transport, or it can also be reachable via a private RFC 1918 IP address through the MPLS transport.

## WAN Edge Deployment

WAN Edge routers are deployed at remote sites, campuses, and data centers and are responsible for routing data traffic to and from the sites across the SD-WAN overlay network.

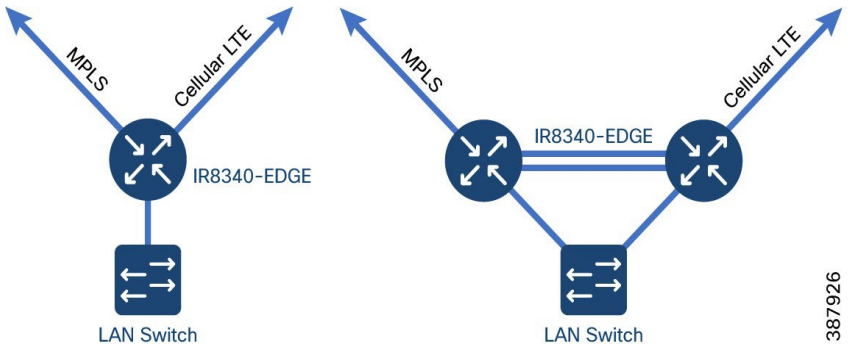
When deploying a WAN Edge router for a site, the platform should be chosen and sized properly for traffic throughput and the number of tunnels supported, etc. A second WAN Edge router is recommended to be added for redundancy. When deploying, WAN Edge routers are commonly connected to all transports for proper redundancy. IPsec-encapsulated tunnels encrypt data traffic to other WAN Edge router locations, and BFD sessions are also formed over these tunnels. User traffic originating from the service VPNs is directed to the tunnels. When a transport or link to a transport goes down, BFD times out and the tunnels are brought down on both sides once the WAN Edge routers detect the condition. The remaining transport or transport links can be used for traffic.

There are many different transport choices and different combinations of transport that can be used. Transports are deployed in an active/active state, and how you use them is extremely flexible. A very common transport combination is MPLS and Internet. MPLS can be used for business-critical traffic, while Internet can be used for bulk traffic and other data. When one transport is down, the other transport can be used to route traffic to and from the site. Internet is reliable in most places and able to meet the SLAs of most applications, so often sites will deploy 2 Internet transports instead.

LTE is used frequently as a transport choice and can be deployed in active mode or as a circuit of last resort, which does not become active unless all other transports become unavailable.

The following are some common WAN Edge deployments. This is not an exhaustive list.

**Figure 28 SDWAN WAN Edge Deployments**




Cisco IR8340 Substation Router can be used as SDWAN Edge router in a Utility Substation Automation network. There are different ways of onboarding a Cisco IR8340 Substation Router.

- Plug and Play
  - Cisco IR8340 Substation router contacts PnP Connect via devicehelper.cisco.com, to get SD-WAN related information.
  - Cisco IR8340 Substation router contacts vBond over a secure tunnel.
  - After authentication, vBond sends the vManage IP and vSmart IP address to the Cisco IR8340 Substation Router.
  - vManage sends the full configuration to the Cisco IR8340 Substation router.

  - Cisco IR8340 Substation router contacts vSmart over a secure tunnel. After authentication, it will join the SD-WAN fabric.

    The template that has been created for the respective Substation Router IR8340, consisting of all the relevant configurations will be applied on the router and the same would be deployed.

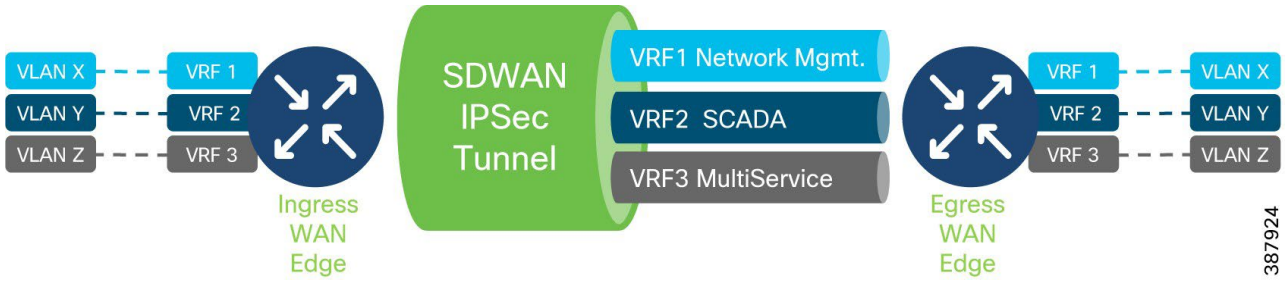
- Onsite BootStrap process
  - Supported on SD-WAN Cisco IOS XE only. IR8340 runs IOS-XE image. The device can also be onboarded using onsite bootstrap process.
  - Use Cisco vManage to generate a configuration file
  - Copy the configuration file to a bootable USB drive and plug the drive into a device, or copy the configuration to the bootflash of a device
  - Boot the device
  - Upon bootup, SD-WAN Cisco IOS XE router will search bootflash: or usbflash: for filename ciscosdwan.cfg
  - The template that has been created for the respective Substation Router IR8340, consisting of all the relevant configurations will be applied on the router and the same would be deployed.

For more details see the implementation guide.

## Other General Design Considerations

- In a Utility Substation Automation network, IR8340 acts as a SDWAN Substation Edge Router and asr1000 series would act as Head End WAN Edge router.
- Traffic should be flowing between substation and Headend in Hub & Spoke design and in some cases, in future between Substations in a Spoke-to-Spoke design.
- Traffic isolation is key to any security strategy. Traffic that enters the router is assigned to a VPN, which not only isolates user traffic, but also provides routing table isolation. This ensures that a user in one VPN cannot transmit data to another VPN unless explicitly configured to do so.
  - VPN 0 is the transport VPN. It contains the interfaces that connect to the WAN transports. Various backhauls like Ethernet, LTE can be configured to be used as WAN transport.
  - VPN 512 is the management VPN. It carries the out-of-band management traffic to and from the Cisco SD-WAN devices.
- Ingress WAN Edge is IR8340 in a Utility Substation Automation deployment and aggregates the traffic from Substation LAN, forwards the same over the IPSec tunnel for further analysis at the Utility control centre. The traffic from the SA LAN can be of different services like SCADA, Network Management , VOIP, Video etc forwarded to the control centre for processing. Each of these traffic streams can be accorded different priorities. The WAN should ensure those different traffic streams are accorded the priorities they require as per the solution.

**Figure 29 SDWAN WAN Edge VRF Deployments**




- WAN Edge routers should exhibit resiliency when one of the WAN backhauls fail. For eg, in an ingress WAN Edge router, if Ethernet WAN Backhaul failure Cellular could be used as backup WAN backhaul.
- Centralized fault, configuration, accounting, performance, and security management as a single pane of glass for Day 0, Day 1, and Day 2 operations on WAN Edge routers using vManage.
- Offer operational simplicity and streamline deployment by using ubiquitous policies and templates, resulting in reduced change control and deployment times of various services like Zone based firewall, QoS policies as applicable, access/trunk ports, NTP, PRP, etc, as supported on IR8340 WAN Edge router.

## Network Management Summary

Cisco SD-WAN technology addresses the problems and challenges of common WAN deployments. Some of the benefits include:

- Centralized network and policy management, as well as operational simplicity, resulting in reduced change control and deployment times.
- A mix of MPLS and low-cost broadband or any combination of transports in an active/active fashion, optimizing capacity and reducing bandwidth costs.
- A transport-independent overlay that extends to the data center, branch, and cloud.
- Deployment flexibility. Due to the separation of the control plane and data plane, controllers can be deployed on premises or in the cloud. Cisco WAN Edge router deployment can be physical or virtual and can be deployed anywhere in the network.
- Robust and comprehensive security, which includes strong encryption of data, end-to-end network segmentation, router and controller certificate identity.
- Seamless connectivity to the public cloud and movement of the WAN edge to the branch.
- Rich analytics with visibility into applications and infrastructure, which enables rapid troubleshooting and assists in forecasting and analysis for effective resource planning.

The following describes Cisco DNA Center features that address some of the challenges in a Utility environment.

- Network monitoring and analytics for proactive remediation—Cisco DNA Assurance enables every point on the network to become a sensor, sending continuous telemetry on application performance and user connectivity in real time. This, coupled with automatic path-trace visibility and guided remediation, means network issues are resolved in minutes—before they become problems.
- Simplified deployment and automation of network maintenance and configuration tasks—Cisco DNA automation provides Zero-touch device provisioning, software image management, device replacement flows, and network provisioning tasks to facilitate device deployment, configuration, and maintenance at scale. Additionally, compliance checks are provided to guarantee the network is compliant with business intent.

- Consistent security policies for endpoints connecting to the network—The solution uses Cisco DNA Center, Cisco Identity Services Engine (ISE), and Cisco Cyber Vision to enhance the visibility of assets and interactions and create security policy to segment the network.

# Conclusions

This Substation Automation – The New Digital Substation CVD version covered:

- Ethernet in the electronic security perimeter (ESP) zone
- The new Cisco IE 9300 and IR8340.
- The support of High-Availability Seamless Redundancy (HSR) single attached node (SAN) protocol and Parallel Redundancy protocol on Cisco IR8340.
- An implementation option for HSR and Parallel Redundancy Protocol (PRP) lossless protocols on Cisco IR8340.
- Cisco IE9300 supporting Precision Time Protocol (PTP) 1588.
- Cisco IE9300 switch support for the deployment of PTP 1588 v2 over both PRP LANs.
- Support of Cisco CyberVision Sensor capabilities on Cisco IR8340 substation router.
- 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 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. Cisco validated architectures can be used to help overcome the challenges involved in planning and securing a substation automation implementation.

# Glossary

Table 16 lists the acronyms and initialisms that may have been used in this SA CVD version 3.0:

**Table 16 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 |

**Table 16 Acronyms (continued)**

| Acronym | Definition |
|---|---|
| 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 |
| 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 |

**Table 16 Acronyms (continued)**

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

Glossary