Substation Automation - The New Digital Substation

Version 3.3 Design Guide

September 2025

Cisco Systems, Inc. www.cisco.com

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

Contents

Substation Automation 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 3.3 Design Guide CVD is a continuation of solution versions 1.5, 2.2.1, 2.3.1, 2.3.2, 3.0, 3.1 and Version 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.

Introduction

The Substation Automation CVD version 3.3 is an update that describes developments to Cisco validated substation automation solution architectures. The purpose of the solution release associated with this document is 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. It also introduces software-defined network management capabilities with Cisco DNA-Center for the Substation LAN and SDWAN Manage for Wide-Area Management (WAN).

New aspects of this 3.3 version are key products and features. New features are listed below.

- PTP Telecom profile over Utility WAN network
- PTP Telecom profile to PTP Power profile conversion on Substation Router Cisco IR8340
- Serial Pseudowire extending serial data from substation router to the headend over Utility WAN
- UTD for IPS on IR8340
- Zone-based Firewall on IR8340 with High Availability

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

- Microchip TP-4100 as substation automation WLAN timing source
- The Cisco Catalyst® IE9300 Rugged Series mixed port switches for secure, reliable, low- latency station and process bus communication, IEC 61850-3, and IEEE 1613 compliant
- The Cisco Catalyst® IE3500 multifunctional, modular, rugged substation switch as PRP Redbox, HSR-PRP Redbox, HSR dual attached node, and application hosting
- Provider connectivity assurance SFPs for performance measurements in substation WAN and LAN deployments.

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 can support more devices and handle 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 run on 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 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 (by 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 (for example, 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 (for example, 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 that follows.

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 secure firewalls Cisco Catalyst Center, Identity Services Engine and SDWAN Manager
CIP-005-5	Electronic Security Perimeter(s)	IR8300 Zone-based Firewall, Cisco Secure Firewalls, and Cisco Duo and Anyconnect
CIP-007-6	Systems Security Management	Cisco Catalyst Center, Identity Services Engine and SDWAN Manager FirePower Management Center, and FirePower firewall and SecureX security orchestration
CIP-008-5	Incident Reporting and Response Plan	Cyber Vision, Catalyst Center, ISE, SDWAN Manager, Firepower Management Center, Cisco Secure Firewall, xDR security orchestration

NERC CIP Requirement	Area	Technologies applied
CIP-010-2	Configuration Change Management and Vulnerability Assessments	Cisco Cyber Vision, Catalyst Center, ISE, SDWAN Manager, Firepower Management Center and xDR Cisco-Cybervision, Catalyst Center, ISE, and SDWAN Manager
CIP-011-2	Information Protection	Segmentation with firewalls and TrustSec, network infrastructure with encrypted communications (such as VPN and MacSec), Anyconnect, Catalyst Center, SDWAN Manager, 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 (such as. secure boot, secure store, anti-counterfeit mechanisms and so on) with Cisco TrustAnchor in the network infrastructure
- Visibility and security analysis of devices (such as. IEDs, RTUs, PLCs, and so on) 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 such as: 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:

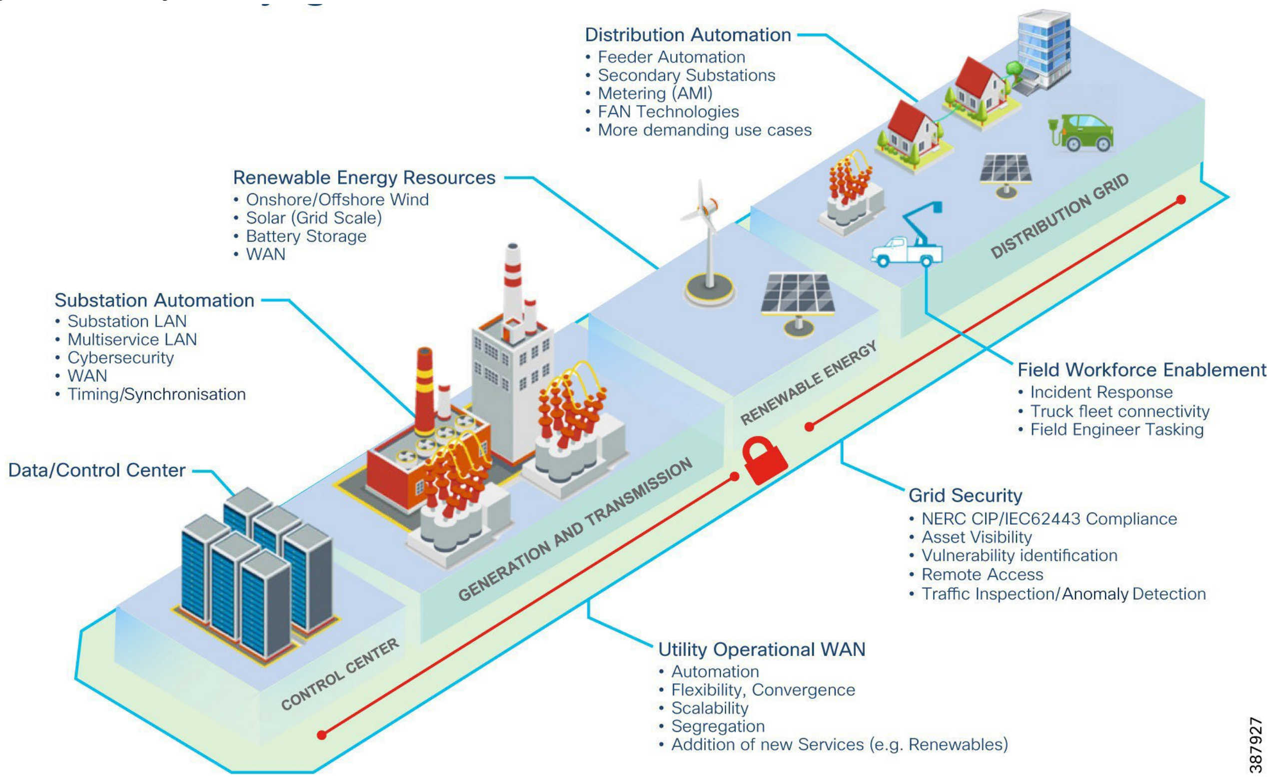
- Enabling further digitalization of the distribution system enabling more real-time control and management to handle the new energy sources and increased demands on the electrical system
- Faster deployment and upgrade to distribution systems with reliable, secure remote access
- Network infrastructure that is more energy efficient, supports Power over Ethernet to efficiently power a range of devices (for example, cameras, access points, and so on) and is designed for a circular economy
- Reducing the substation footprint. Collapsing more functions into less hardware. Security (Firewalls, IDS/IPS), timing and other external components can be collapsed into a single platform (IR8340). This reduces the pressure on substation infrastructure such as power, rack space and heat dissipation.

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 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

The Cisco Substation Automation Solution release 3.0 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 DNA-Center
- Substation Wide-Area Network (WAN) centralized network deployment and management via Cisco Software-Defined WAN (SD-WAN) technologies (for example, 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 platforms 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 SDWAN Manager for SD-WAN routing capabilities

What's new in Substation Automation

In this 3.3 version of Cisco Substation Automation, the New Features include:

- PTP Telecom profile over Utility WAN network
- PTP Telecom profile to PTP Power profile conversion on Cisco IR8340 Substation Router
- Serial Pseudowire extending serial data from substation router to the headend over Utility WAN
- UTD for IPS on IR8340
- Zone-based firewall on IR8340 with high availability

New products introduced to the Substation Automation 3.3 network and security architecture include:

- Microchip TP 4100 as substation automation WAN timing source (primary reference clock)
- The Cisco Catalyst® IE9300 Rugged Series mixed port switches for secure, reliable, low-latency station and process bus communication, IEC61850-3, and IEEE 1613 compliant
- The Cisco Catalyst® IE3500 multifunctional, modular, rugged substation switch as PRP Redbox, HSR-PRP Redbox, HSR Dual Attached node, and application hosting
- Provider connectivity assurance SFPs for measurements in the Substation WAN and LAN deployments

The products provide the following capabilities within the overall validated design:

- Layer 3 Scada substation to datacenter - Catalyst IR8340 - including security and timing (ZBFW, IDS/IPS, CyberVision sensor and IEEE1588 PTP, NTP timing)
- Layer 2 Ethernet based protection substation to substation - Catalyst IE9300 - Extending PRP between substations., HSR, PTP
- Teleprotection interfaces within the substation - SEL ICON
- Transport Network (WAN) substation edge - NCS540

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 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 3.2 focuses on enhancements to the ESP zone design.
- Refer to previous 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. Some of the documents require a signed non-disclosure agreement (NDA) with Cisco.

Other Relevant Documents

As stated previously, 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

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

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
- Additional relevant documents can be found in: https://www.cisco.com/c/en/us/solutions/design-zone/industries/power-utilities.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

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.

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

Technical Requirements Summary

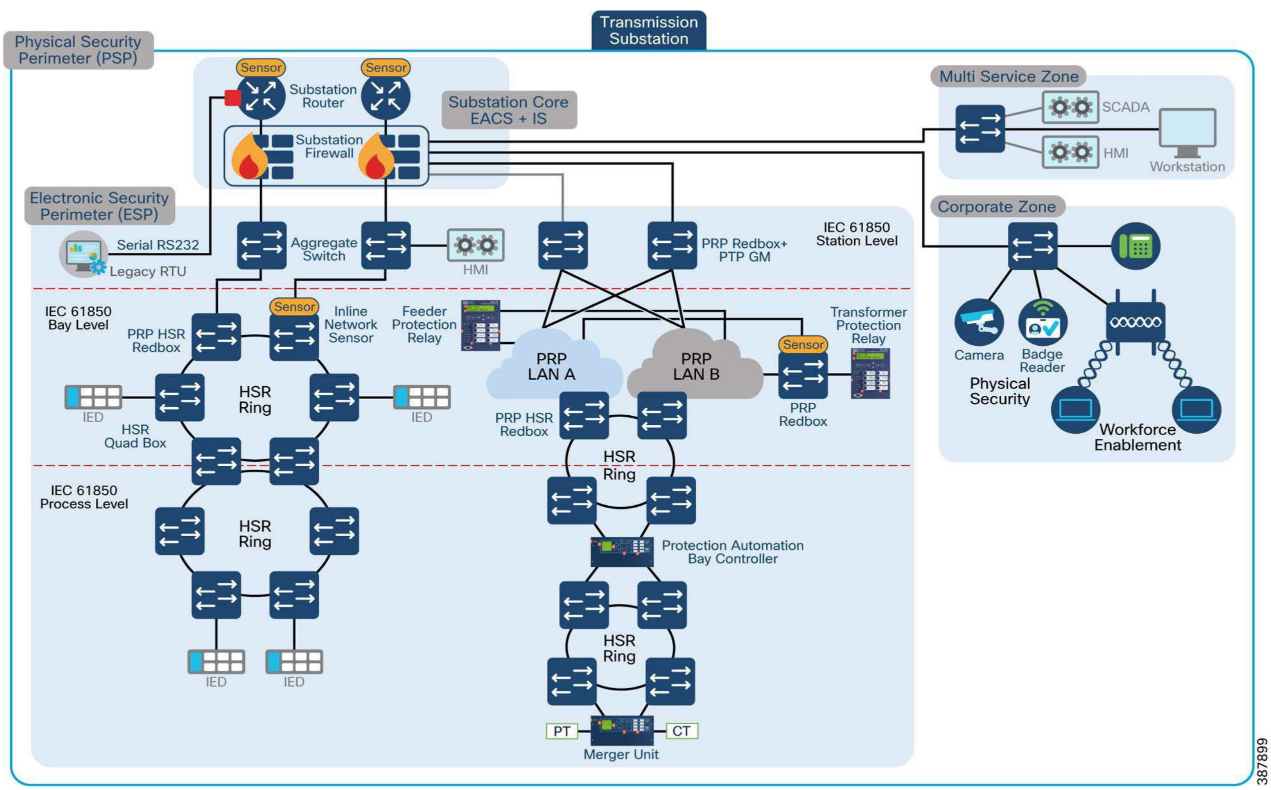
Key Technical Requirements the Substation Automation solution is designed to meet include:

- 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 (such as: 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



The new Cisco Digital Substation Architecture 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 is not 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 on supported devices.

Prior to segment routing, multi-protocol label switching (MPLS) packets were forwarded using label switching instead of IP-based routing, which means the routers forwarded traffic based on the label and not the destination address.

This required only the “edge” routers to perform an IP lookup, while intermediate “core” routers performed only a label lookup.

Unfortunately, MPLS did not remove the complexity from an existing network and added more complexity through additional protocols. Adding more complexity was that each MPLS node required the state to be synchronized across the entire network. As the size of networks grew, so did the state and complexity, making it more difficult to operate and manage.

Segment Routing relies on a small number of extensions to Cisco Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. It can operate with an MPLS (Multiprotocol Label Switching) or an IPv6 data plane, and it integrates with the rich multi-service capabilities of MPLS, including Layer 3 VPN (L3VPN), Virtual Private Wire Service (VPWS), Virtual Private LAN Service (VPLS), and Ethernet VPN (EVPN).

Segment routing can be directly applied to the Multiprotocol Label Switching (MPLS) architectures with no change in the forwarding plane. Segment routing uses the network bandwidth more effectively than traditional MPLS networks and offers lower latency.

Benefits of Segment Routing

- Ready for SDN: Segment routing was built for SDN and is the foundation for Application Engineered Routing (AER).
- SR prepares networks for business models, where applications can direct network behavior. SR provides the right balance between distributed intelligence and centralized optimization and programming.
- Minimal configuration: Segment routing for TE requires minimal configuration on the source router.
- Load balancing: Unlike RSVP-TE, load balancing for segment routing can take place in the presence of equal cost multiple paths (ECMPs).
- Supports Fast Reroute (FRR): Fast reroute enables the activation of a pre-configured backup path within 50 milliseconds of path failure.
- Plug-and-Play deployment: Segment routing tunnels are interoperable with existing MPLS control and data planes and can be implemented in an existing deployment.

SDWAN for WAN Router Management

SD-WAN is part of a broader technology of software-defined networking (SDN). SDN is a centralized approach to network management which abstracts the underlying network infrastructure apart from its applications. The de-coupling of data plane forwarding, and control plane allows SDN to centralize the intelligence of the network and allows for more network automation. Operations simplification, centralized provisioning, monitoring, and troubleshooting are all principles of SDN applied by SD-WAN to the WAN.

The Cisco SD-WAN solution is an enterprise-grade WAN architecture overlay that enables digital and cloud transformation for enterprises. It helps to integrate routing, security, centralized policy, and orchestration into large- scale networks. It is multi-tenant, cloud-delivered, highly automated, secure, scalable, and application-aware with rich analytics. This solution guide uses Cisco catalyst SDWAN for Substation WAN Router (Cisco IR8340) management.

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

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 several 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 DNAC, ISE, Wireless Lan Controllers (WLC), SDWAN Manager, and Firepower Management Center (FMC)
- Industrial cyber security tools such as Cyber Vison Center.

Electronic Security Perimeter Zone - Design Considerations

The ESP is the network that supports 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.

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 applications 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 3 for a depiction of a Cisco ESP zone reference architecture.

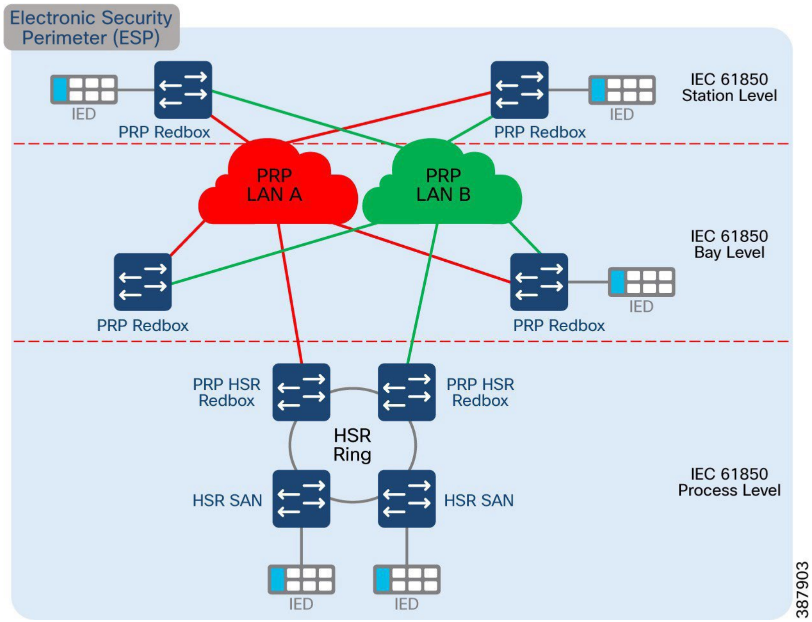
Deployment models are typically based on the size of the substation ESP zone. Substation IEDs can connect to Cisco IE switches built in one of a variety of topological options, namely hub and spoke, ring, or tree. Cisco offers high-availability redundancy mechanisms such as Resilient Ethernet Protocol (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 the 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 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 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

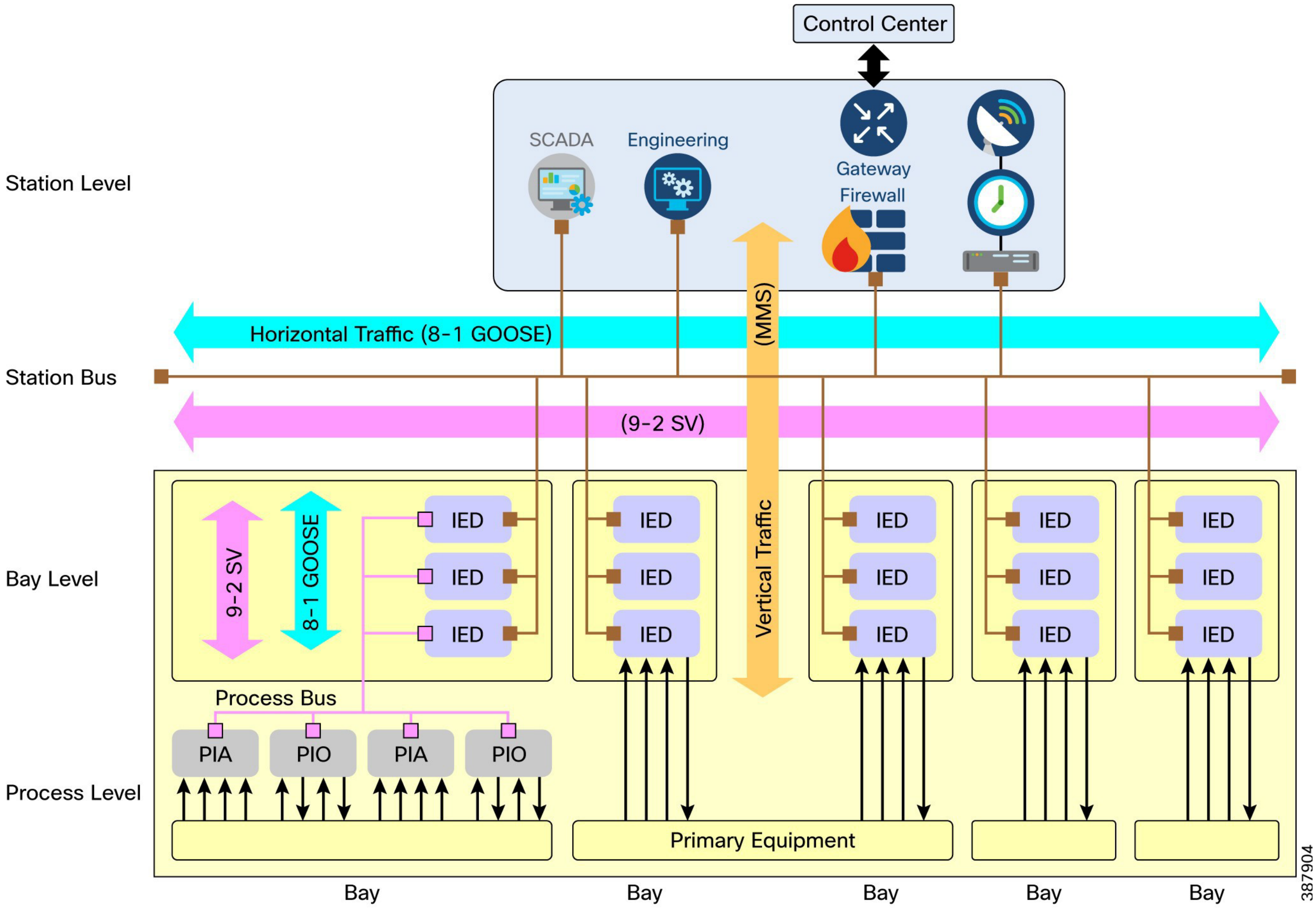
The protocols typically found on a station bus include GOOSE (Layer 2 multicast), MMS, SNTP, SNMP, FTP, and others (Transmission Control Protocol—TCP/IP or User Datagram Protocol—UDP/IP Layer 3 unicast).

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 process 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.

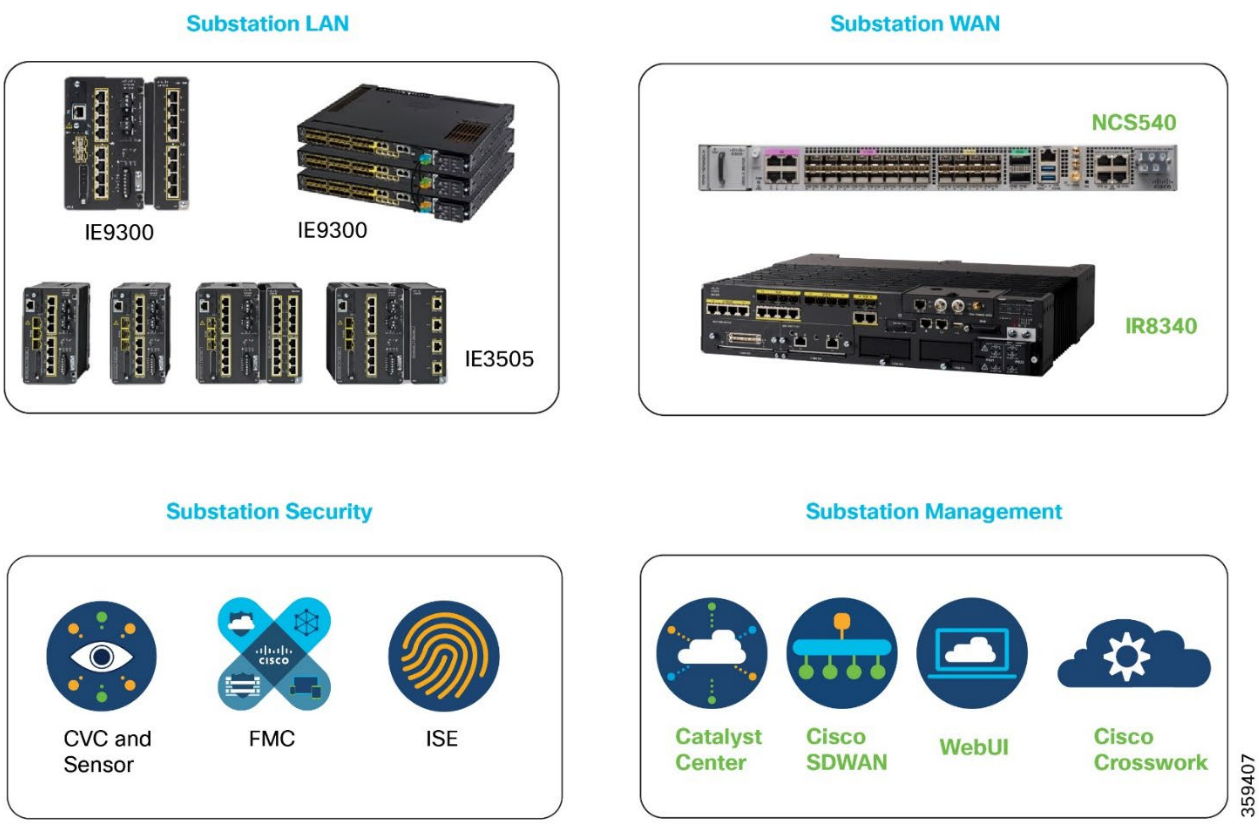
Figure 4 Where to Find MMS, GOOSE, and SV in Station and Process Bus



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 Networking Portfolio



There are several key roles played by various pieces of the network and cybersecurity portfolio. The table that follows 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
Substation WAN Segment Routing Provider Edge and Provider Nodes	NCS540
Station Bus Switches	IR8300, IE9300, IE3400, IE3505
Process Bus Switches with Power Profile support	IE9300, IE3400, IE3505
Substation Firewall	NA
Corp and CIP Zone Switches	IE3x00, IE9300
Wi-Fi Access Point in Corp zone	IW6300
Central Headend Router	C8500
Central Headend Firewall	FPR4150
OT Visibility Manager	Cyber Vision Center
OT Inline Sensors	Cyber Vision Sensor running on IE3400, IE9300, IR8300, IE3500
PRP RedBox	IE3400, IE3505, IE9300, IR8340
PRP HSR RedBox	IE3400, IE3505
HSR QuadBox	NA
PRP Infrastructure Switches	IE3400, IE9300

Role	Product
HSR SAN	IE3500, IE9300, IE3400, IE5000
PTP Grand Master	Cisco IE9320, Cisco IR8340, GT3000 from microchip
PTP Transparent Clock	IE3400, IE3505, IE9300, IR8340
PTP Boundary Clock	IE3505, IE3400, IE9300, IR8340
PTP over PRP	IE9300, IE3400, IE3505
Substation LAN Network Management	DN2-HW-APL (include L and XL)
Substation WAN Management	SDWAN WAN Manager

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) and IEC62850-9-3-PUP 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 the first industrial-grade fully integrated routing and switching platform from Cisco. 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 several roles in the architecture, include a resilient Transmission or Distribution Substation headend router into the Utility WAN, resilient Station-bus switch, zone-based Firewall, hosting a Cyber Vision sensor for flow visibility, PTP Grandmaster clock and providing serial-based connectivity for legacy devices. The product is managed by either Cisco Catalyst Center or SDWAN Manager.

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 information about the IR8340.

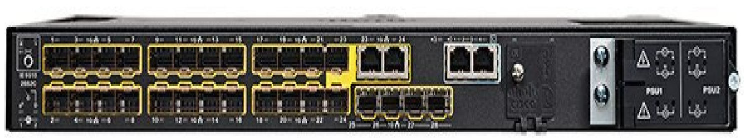
Cisco IE 9300

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 is 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 about IE9300 refer to:

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

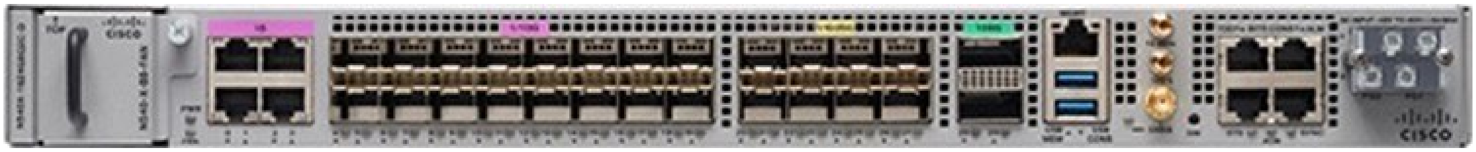
Figure 7 Cisco IE9300



Cisco NCS540

The Cisco Network Convergence System 540 Medium Density Routers (NCS 540) are designed for cost-effective delivery of next-generation services and applications. These routers are temperature-hardened, high-throughput, small form factor, low-power-consumption devices suitable for both outdoor and indoor deployments. With in-built trust anchor hardware infrastructure and anti-counterfeit protection along with software enabled security features, NCS 540 is most trusted and secured platform. They are powered by the industry-leading carrier-class version of Cisco IOS XR software designed for operational efficiency and service agility. Cisco IOS XR software offers advanced features such as programmability, application awareness, network visibility, and automation. The Cisco NCS 540 series of routers is an intelligent converged access platform which enables service providers to deliver next-level business and entertainment experiences.

Figure 8 Cisco NCS540



The Cisco NCS540 routers can be deployed as Provider Edge and Provider nodes as part of Segment Routing enabled WAN Backhaul. For more details, refer to:

https://www.cisco.com/c/en/us/products/collateral/routers/network-convergence-system-500-series-routers/datasheet- c78-740296.html

Cisco IE3500

The Cisco IE3500 Rugged Series switches deliver high bandwidth, higher power and feature rich switching performance in a rugged and modular form factor. The Cisco IE3500 Rugged Series are designed with features that enable the industrial network infrastructure to seamlessly accommodate machine vision use cases, AI-driven analysis, virtualization, large scale networks, robust security, and edge-to-cloud connectivity. Note that lossless redundancy protocols like High Availability Seamless Redundancy and Parallel Redundancy Protocols are supported only on IE3505 variants.

Figure 9. Cisco IE3505

359408

Refer to the latest datasheets for more information.

https://www.cisco.com/c/en/us/products/collateral/networking/industrial-switches/ie3500-rugged-series/ie3500-rugged-series-ds.html

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
IE3505	http://www.cisco.com/go/ie3505
Cyber Vision	https://www.cisco.com/c/en/us/support/security/cyber- vision/series.html
ASR1000	https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8500-series-edge-platforms/datasheet-c78-744089.html

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 service 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 (for example, 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, therefore 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, 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 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.

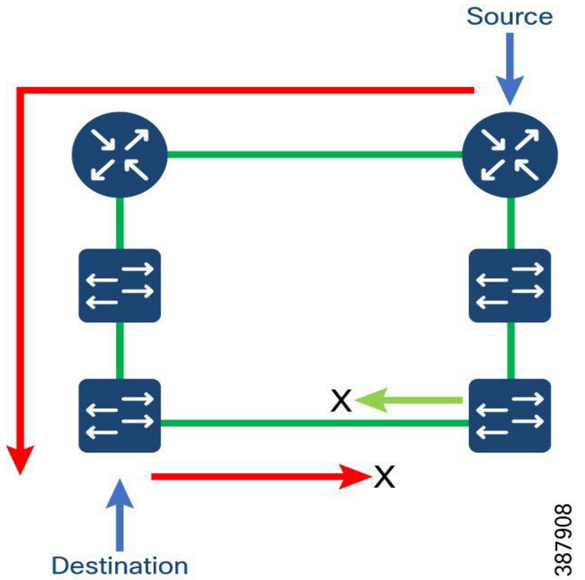
Spanning Tree Protocol

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 10 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 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.

Topology Examples

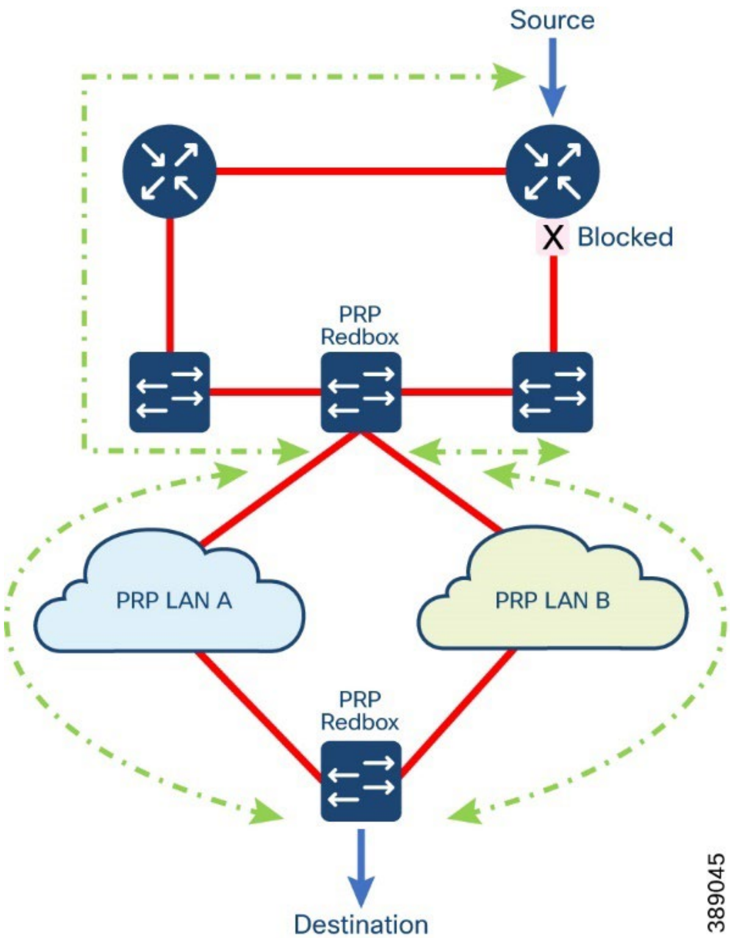
Station Bus using RSTP and PRP for Process Bus

This section recommends the deployment of Rapid Spanning Tree Protocol (RSTP) for station bus and Parallel Redundancy Protocol (PRP) for process bus in Substation Automation networks. Building on the previous section, which outlines the advantages and disadvantages of using RSTP for station bus deployments, this section advises positioning a Cisco Industrial Ethernet switch that supports both RSTP and PRP RedBox functionalities within the station bus. RSTP should be enabled for station bus integration, while PRP should be utilized to connect Intelligent Electronic Devices (IEDs) within the process bus. This recommendation is based on the stringent communication requirements of process bus deployments, where PRP is no-loss traffic resiliency is particularly beneficial.

The topology includes the Cisco IR8340 Substation Router in a Customer Edge (CE) role, acting as the gateway to the Substation LAN network. This router also aggregates station bus devices, which can be connected in a ring topology using RSTP. Additionally, the IR8340 supports Global Navigation Satellite System (GNSS) and can function as a Precision Time Protocol (PTP) Power Profile GrandMaster, distributing time to various critical substation automation devices.

Switches that are aware of both PRP and RSTP can be strategically positioned to manage communication between station bus and process bus devices efficiently. Trunk interfaces should be enabled among these devices in both the station bus and process bus, facilitating the transmission of different traffic types such as PTP, GOOSE, and MMS between the two buses. Process bus devices, like Merging Units, generate high-rate traffic such as Sampled Values, which can lead to bandwidth inefficiencies and impact other time-critical applications. To mitigate this, the design recommends employing VLANs, Quality of Service (QoS), and filtering mechanisms as discussed in other sections of this guide. These strategies ensure efficient traffic management and maintain the performance and reliability of the Substation Automation network.

Figure 11 RSTP for Station Bus and PRP for Process bus



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.
- It is 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 3ms to its directly connected ring neighbor. And it expects to receive a special beacon frame every 3ms 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 10ms. 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 (C378.238 2011 or 2017) over REP is supported on IE3400 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, require 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 require 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 3400, Cisco IE 3500, 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 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

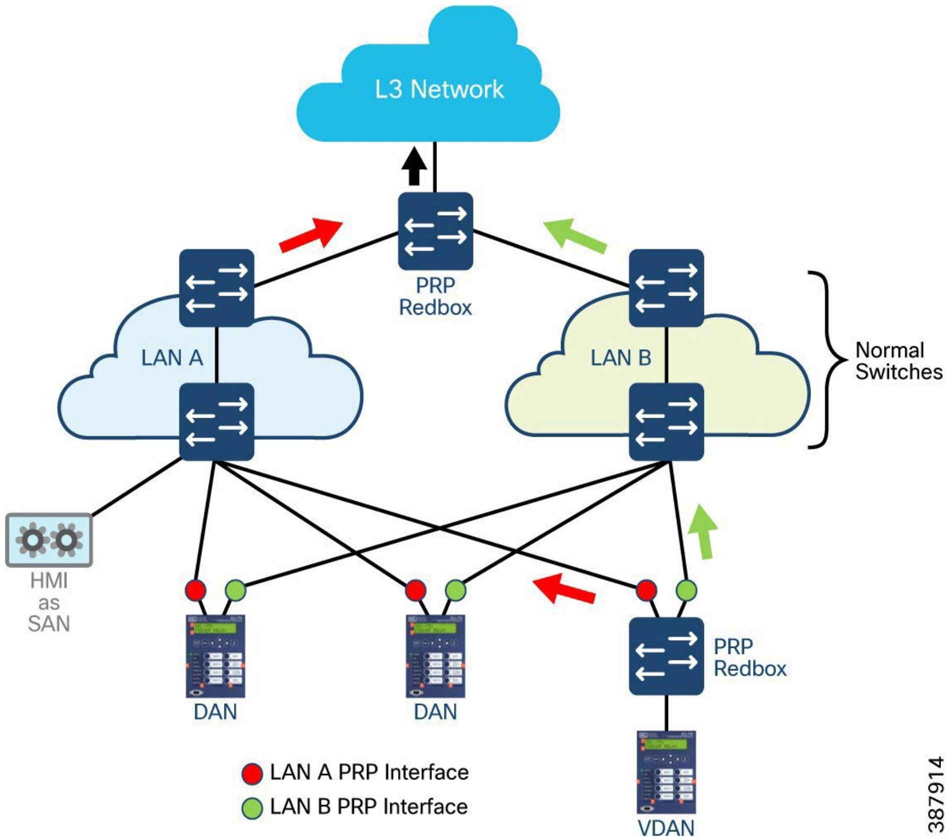
The following figure shows a PRP topology with two LANs each consisting of many switches as part of the LAN. The switches in each of the LAN can also be in the form of a Ring topology with Spanning Tree or REP configured to avoid loops in the ring. The switches in each of the LAN can provide connectivity 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 does not 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 12 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 if 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-3400, IE-3505, IE-9300, and IR8340
- Applications like Cyber Vision Sensor, Stealthwatch, DNAC work seamlessly. These applications use stateful Layer 3 connectivity. For example, the reachability and the stateful session between Cyber Vision Center and Sensor over PRP is not impacted as the keepalive for the Cyber Vision 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 the GridSecurity Guide and relevant sections in this guide.

PRP with redundant Layer-3 connectivity (combined station and process bus)

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 does not 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. 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 TSO control center network over WAN network and the devices connected in the Substation Automation PRP LAN network. For example, TCP traffic like MODBUS or DNP3 could be traffic flowing from the SCADA in the control center to one or many of the IEDs connected in the PRP LAN network.

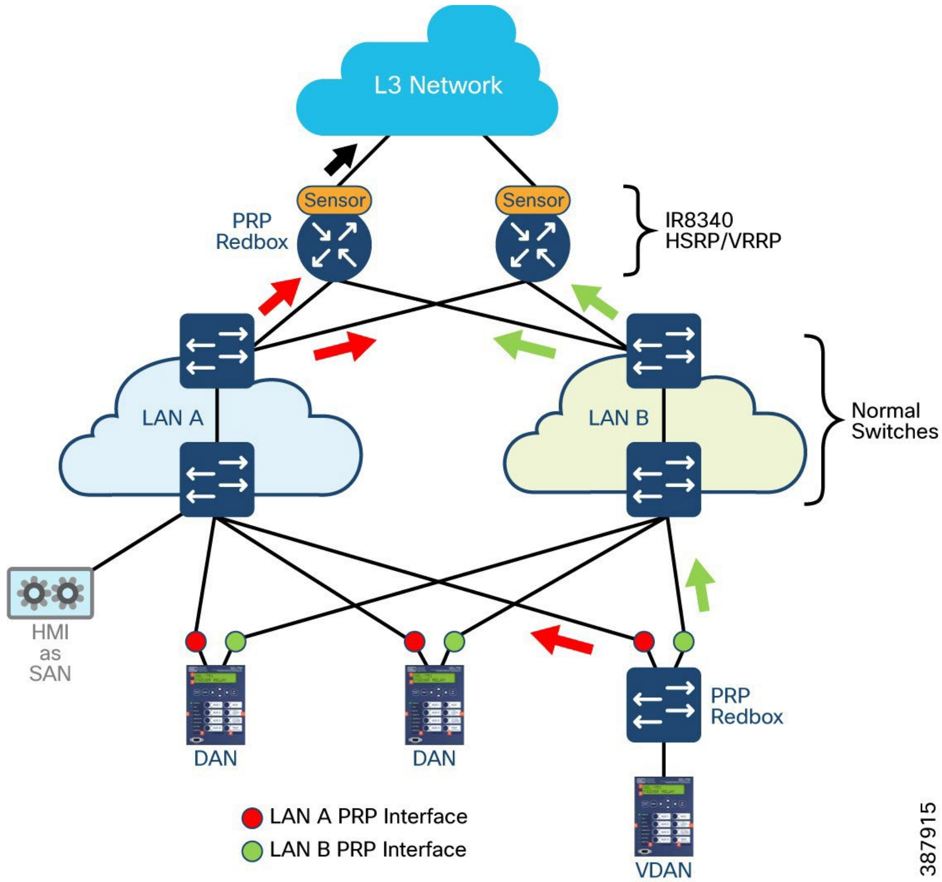
To optimize network redundancy, we need to design our network that aligns both Cisco Layer 3 HSRP and Layer 2 redundancy services with each other. HSRP will assign the active and the standby router based on priority. The highest priority will be the active HSRP router amongst the HSRP group. If the priority 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, causing 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 13 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 if 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-3400, IE-3505, IE-9300, and IR8340
- Resilient, but not lossless, connectivity to WAN and Layer 3 networks via the redundant routers
- Traffic of applications like Cyber Vision Sensor, Stealthwatch, and Catalyst Center through the PRP network work seamlessly. These applications use stateful Layer 3 connectivity. For example, the reachability and the stateful session between Cyber Vision Center and Sensor over PRP is not impacted as the keepalive for the Cyber Vision session timeout is higher, in the order of seconds. Similar were the observations for Stealthwatch and Catalyst Center. For more details refer to the GridSecurity Guide and relevant sections in this guide. Note that using Catalyst Center to set up the PRP network is not currently supported.

Design Considerations

- It is recommended to use fiber links because 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.

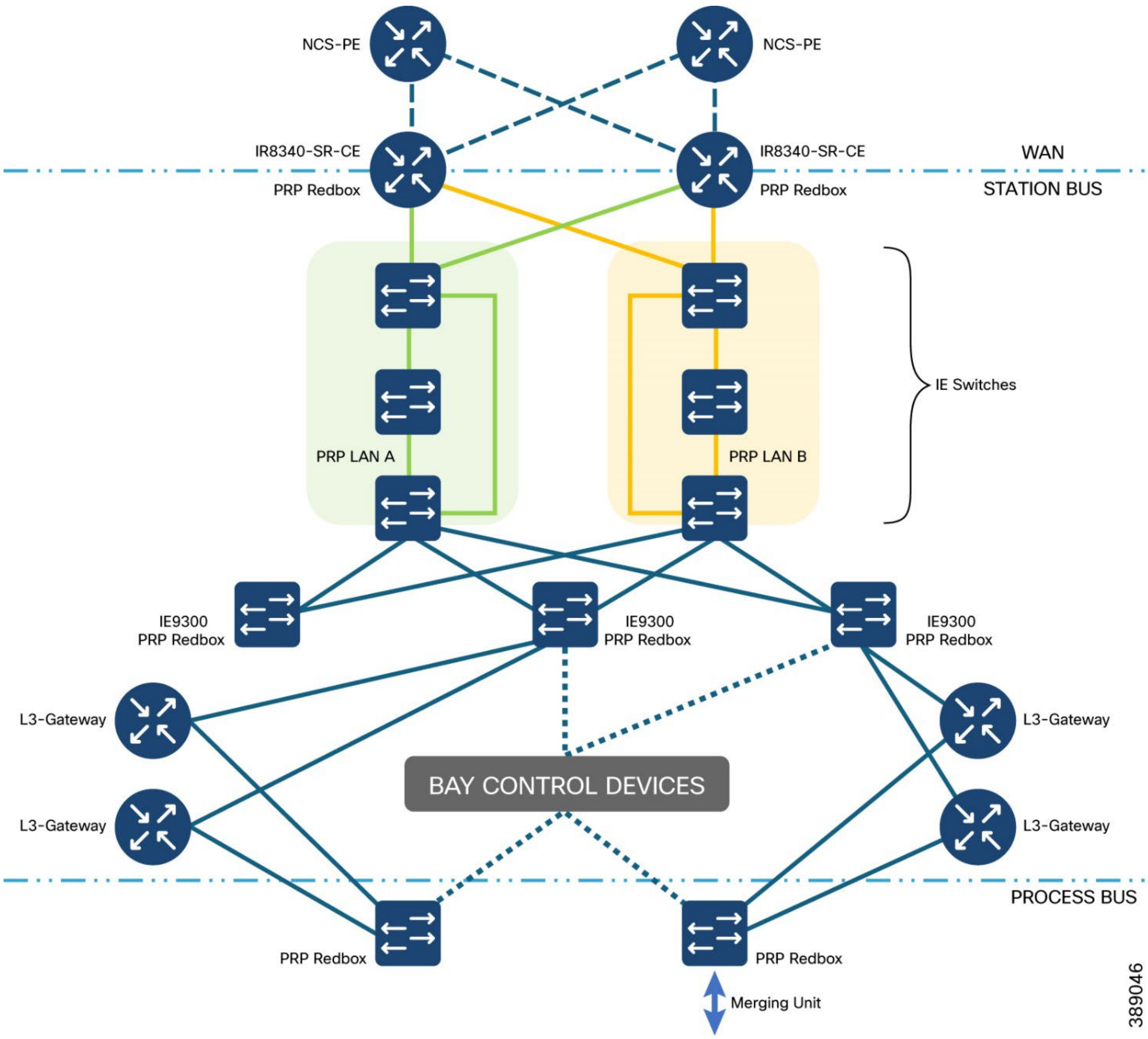
- Configure unique VLANs for each IED to avoid multicast flooding.
- Enable storm control on the access/IED facing interfaces.

- PRP Station Bus and PRP Process Bus

The design recommendation for a Substation Automation LAN network utilizing a PRP topology encompasses both the station bus and process bus to ensure high availability and resiliency. At the core of this design is the Cisco IR8340 router, which functions as both the Customer Edge (CE) router and a PRP Redbox, serving as the gateway for the substation LAN network. The Substation Automation Station bus is structured with two PRP LANs, PRP LAN A and PRP LAN B, each comprising multiple switches. These switches can be configured in a ring topology with Spanning Tree Protocol (STP) or Resilient Ethernet Protocol (REP) to prevent loops. Each switch within these LANs can connect to single attached nodes, while the topology also supports Dual Attached Nodes (DANs). These PRP-aware Intelligent Electronic Devices (IEDs) or network devices are equipped with two network interfaces, each linked to a different LAN, thereby ensuring redundancy and resiliency. DANs transmit duplicate packets through both interfaces, with a Redundancy Control Trailer (RCT) appended to each frame to help the destination node identify and discard duplicate packets. This mechanism ensures zero recovery time in the event of a path failure, as traffic seamlessly continues over the alternate path.

Additionally, the design incorporates PRP Redboxes to connect Bay Control devices at the bay level, facilitating communication between the Station BUS, Bay Control, and Process BUS. These PRP Redboxes leverage two PRP channels supported by Cisco Industrial Ethernet switches, enhancing communication resiliency across these segments. Furthermore, Cisco Industrial Ethernet switches are positioned as Layer 3 (L3) Gateways to enable L3 SCADA communication protocols such as MMS and DNP3 between the control center and the IEDs in the Process BUS. These gateways utilize trunk ports to manage VLANs between the Process BUS and Station BUS, allowing for the transfer of PTP Powerprofile if necessary. By restricting bandwidth-intensive traffic like Sampled Values to specific VLANs, the design effectively segments traffic, ensuring efficient network performance and management.

Figure 14 PRP for Station bus and Process bus



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 if 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-3400, IE-3505, IE-9300, and IR8340
- Resilient, but not lossless, connectivity to WAN and Layer 3 networks via the redundant routers
- Traffic of applications like Cyber Vision Sensor, Stealthwatch, DNAC through the PRP network work seamlessly. These applications use stateful Layer 3 connectivity. For example, the reachability and the

stateful session between Cyber Vision Center and Sensor over PRP is not impacted as the keepalive for the Cyber Vision session timeout is higher, in the order of seconds. Similar were the observations for Stealthwatch and DNAC. For more details refer to the GridSecurity Guide and relevant sections in this guide. Note that the use of DNAC to set up PRP network is not currently supported.

Design Considerations

- It is recommended to use fiber links because 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 that support the HSR protocol are called 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 3505, Cisco IE 3400 switches, Cisco IE9300 switches and Cisco IR8340 Substation Automation Router.

Design Considerations

The design considerations for HSR are broken 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 shown below.

- 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.

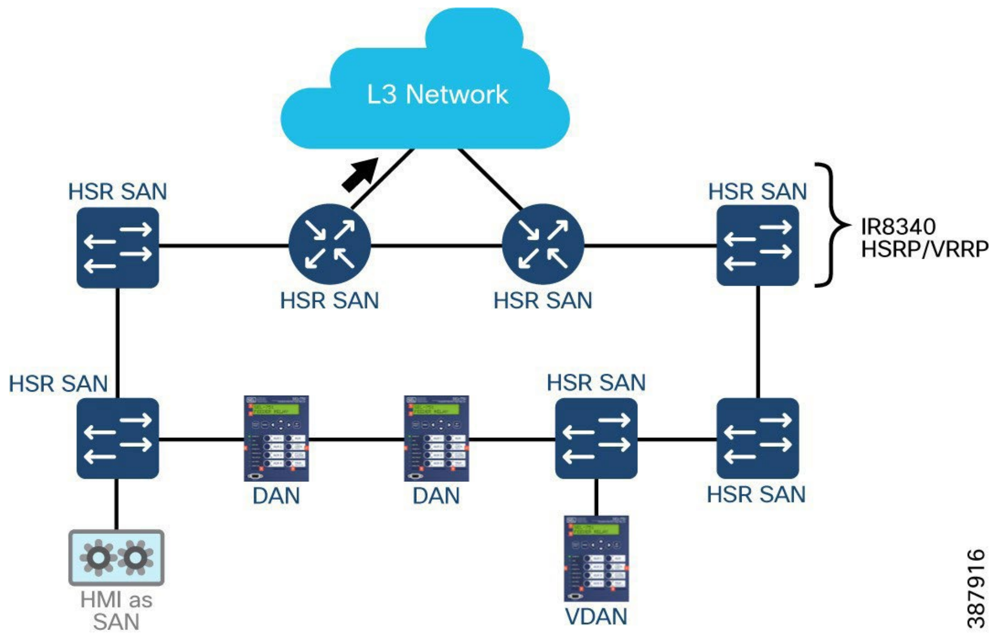
To optimize network redundancy, we need to design our network that aligns both Cisco Layer 3 HSRP and Layer 2 redundancy services with each other. HSRP will assign the active and the standby router based on priority. The highest priority will be the active HSRP router amongst the HSRP group. If the priority 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, causing 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 15 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 Cisco IE 4010, Cisco IE 3400, 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

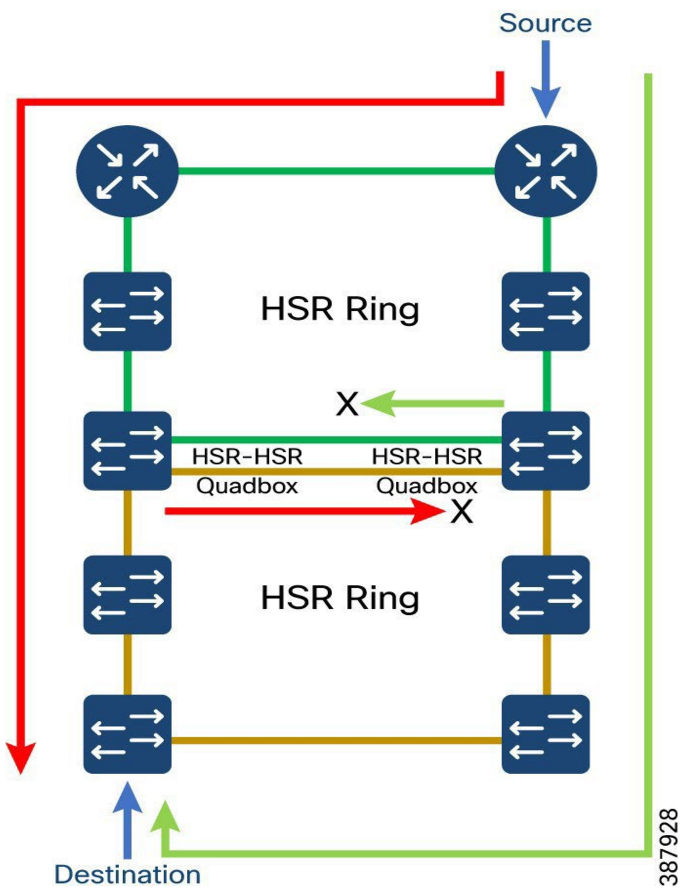
HSR rings can also be implemented in such a way that key switches are participating in two HSR rings, using four interfaces to connect the respective rings, which is known as HSR-HSR or QuadBox. When the HSR-HSR mode is licensed and enabled, the switch shuts all non-HSR ports to avoid traffic interference. 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 16 **HSR - HSR Ring**



Note: PTP over HSR QuadBox is not supported.

HSR-PRP Dual RedBox

Internetworking between HSR-PRP, also known as Dual RedBox, is used to connect PRP and HSR networks together. It is commonly deployed in utility substations, so323 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 RedBoxes, 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.

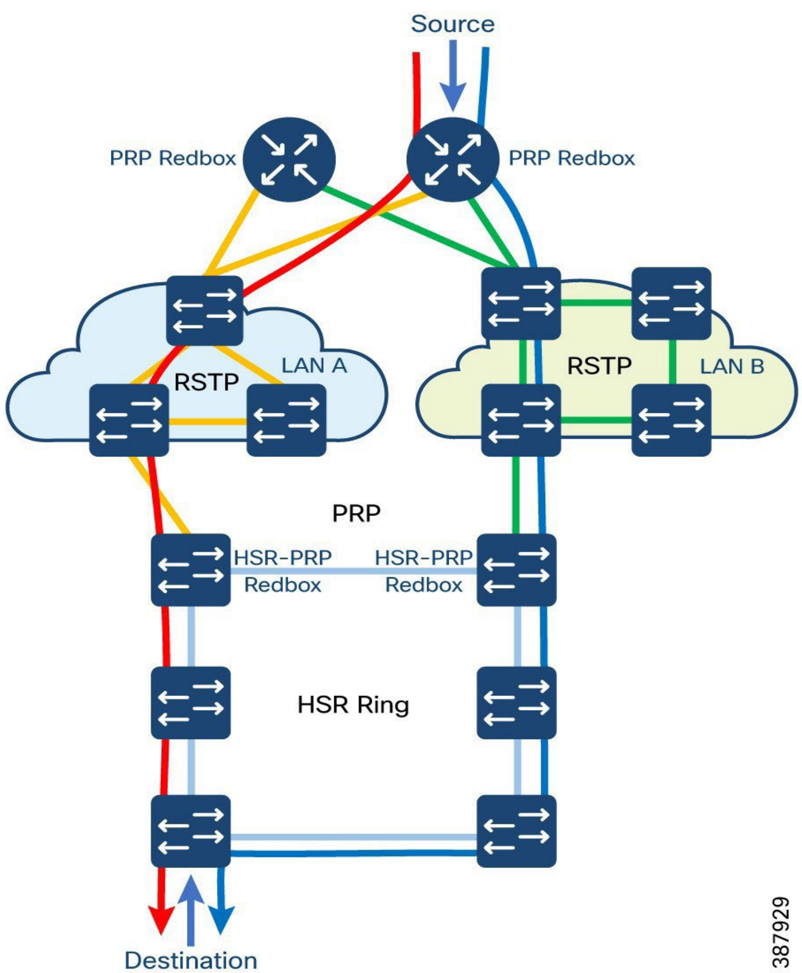
Design Considerations

- In HSR-PRP Dual RedBox mode (IE 4000 only), the device 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
- In HSR-PRP Dual Redbox mode on IE3400 only, the device doesn't have a restriction with respect to the number of ports that can be used. However, the following are predefined:
  - Only Gig1/1 and Gig1/2 as HSR ring interfaces, automatically assigned when the feature is enabled.
  - The port connected to the PRP network can be any other port from the base module or expansion module.

  - All remaining ports are available for normal use. However, they behave like any other PRP LAN port, either LAN A or LAN B and hence cannot be sent over to another PRP LAN depending on the PRP network the IE3400 node acting as PRP-HSR RedBox is connected to. Basically, ports operate like a SAN Port having access to only LAN A or B, whichever the RedBox is connected to.
  - HSR ring members and the port connecting to PRP LAN A or LAN B should be in the same VLAN.

- 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 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 17 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 tables list 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 + PTP GM	IE9320, IR8340
Station Bus Ring using HSR SAN+ Transparent Clock	IE3400, IE3505, IE9320, IR8340
Station Bus Ring using HSR SAN+ Boundary Clock	IE3505, IE3400, IE4000, IE9320
HSR PRP Redbox	IE3505, IE3400
HSR Quad Box	IE4000
HSR SAN	IE3505, IE3400, IE9340, IE3400, IR8340

Table 9 Resiliency Protocol - PRP and Roles

PRP Roles	IR and IE
PRP Redbox + PTP GM	IE9320, IR8340
Station Bus LAN Switch Non-PRP + Transparent Clock	IE9300, IE3400, IE3500
Process LAN Switch non-PRP + Transparent Clock	IE9300, IE3400
PRP Redbox + HSRP/VRRP	IR8340
PRP HSR Redbox	IE3505, IE3400

Timing and Synchronization

Digital vs Analog Substation Synchronization

The advent of IEC 61850 and the subsequent digitalization of power substations brings a paradigm shift. This is because of new synchronization of architectural and performance requirements not seen before by the protection or control engineer:

- Sampled Values need to be timestamped - on-site- with sub-microsecond accuracy
- Network Wide Phasor Measurements are to be correlated within 26 / 31 microseconds (60Hz / 50Hz network respectively)
- Redundant packet timing architecture (vs point to point wired analog timing)

Proliferation of multiple GPS receivers in the same substation synchronizing different sub-systems is a practice that will need to be abandoned.

In legacy analog substations, packet timing is used mainly to synchronize event logs, non-critical for day to day operations, commonly from multiple local and/or remote time sources from multiple vendors. In a digital substation, packet timing now synchronizes critical substation operations, from only one active substation master for all the devices.

Failure of the substation " master" is to be avoided by careful architectural planning, as it will now likely initiate cascading failures in the entire site that could also propagate to the electrical network.

Digital Substation Automation Timing

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 Protocol (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.

Per well-known IEEE paper: " Smarter Time Sync: Applying the IEEE PC37.238 Standard to Power System Applications" (Brunner/Antonova 2011 64th Annual Conference for Protective Relay Engineers):

One of the challenging topics is the accurate synchronization of the data sources providing the sampled values. The communication network used to transmit the sampled values does not support a constant or predictable transmission delay. Therefore, the mechanism chosen assumes a synchronized sampling at the source. All devices sample at the same time and add a reference to the sampling time. With the help of that reference, the application using the sampled data can correlate the samples received from multiple sources. Depending on the application and the requirements concerning acceptable phase errors, the required synchronization accuracy may be as accurate as 1 microsecond.

Again, the 1 microsecond error is at the end of the chain of TC switches (not to confuse with the 250ns requirement at the substation Grandmaster's synchronization interfaces). Time Synchronization over a Local Area Network synchronizes devices and can increase the number of devices driven through one Ethernet network. It reduces the cabling infrastructure and cost by transporting 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 or IEC61850-9-3 PUP 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 to 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. Peers are clients and servers to each other.

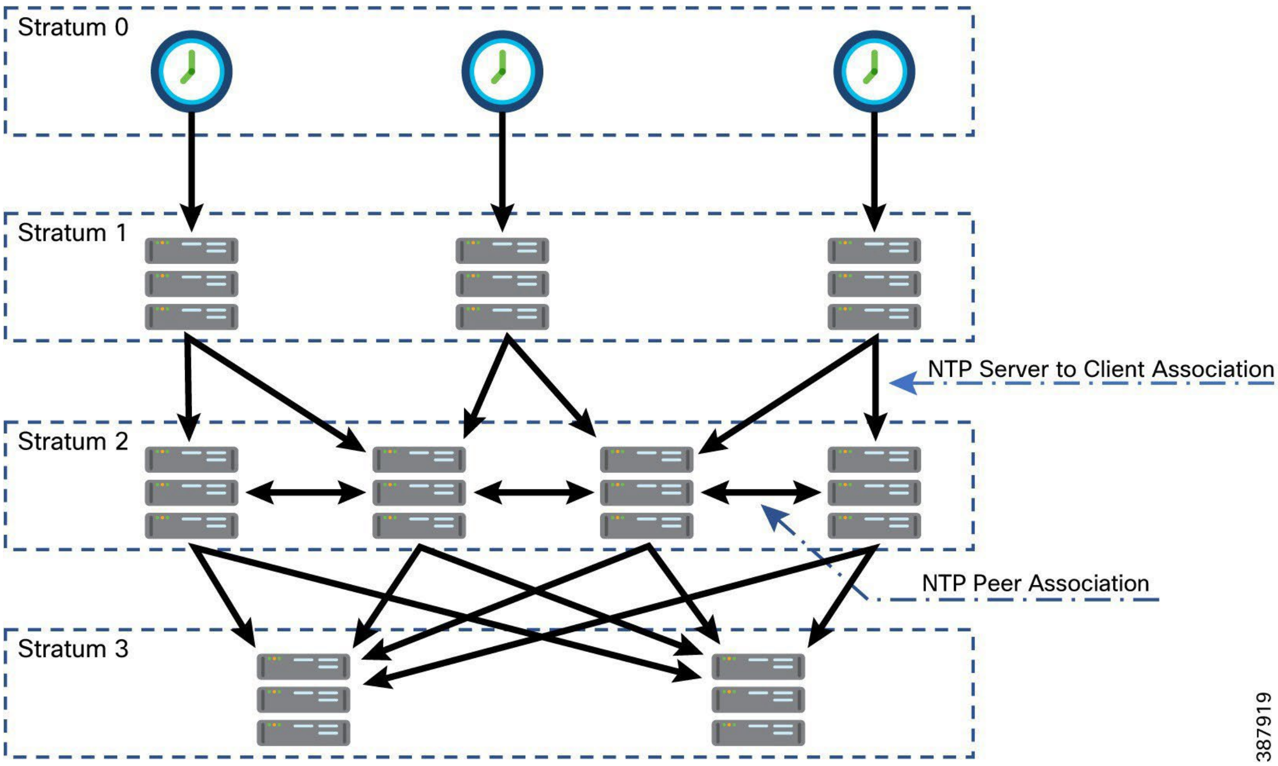
These roles are not exclusive and any device in the Substation Automation architecture can act as one or more of these roles. For example, an NTP server is generally a client to servers higher up in the NTP hierarchy. The network infrastructure is often both a client on the uplinks and a server on the 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 18 NTP Clock Hierarchy



The ability of a client (for example, 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 synchronizes 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 association with multiple servers. It will use multiple inputs to provide better time synchronization of the local clock. The clock algorithm 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 (for example, 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 secondary clocks various requests.

Boundary Clock

A boundary clock is a multiport device Industrial Ethernet Switch that becomes a secondary on one port. As a secondary clock, the boundary clock synchronizes its internal clock to the primary. The boundary clock then becomes a primary to IED devices connected to the other ports on the Industrial Ethernet Switch. Other clocks connected to these ports will become secondary 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 to offload the need of the Grandmaster to respond directly to many 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 primary nor secondary clocks. Transparent clocks sit in-line between the primary and secondary 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 to confirm this information.

Table 11 PTP roles and profiles on Cisco Industrial Ethernet products

PTP Role	Platform	Profiles supported
Grandmaster	IE9300, IR8340, Microchip GT3000	PTP Power profile
PTP Transparent Clock both e2e and p2p	IE9300, IE3400, IE3505	PTP Power profile 2011 PTP Power profile 2017
PTP Boundary Clock	IE9300, IE3400, IE3505	PTP Power profile 2011
PTP Over PRP Redbox	IE9300, IE3500, IE3400	
PTP over HSR	IE9300, IE3400, IE3505	

Design Considerations

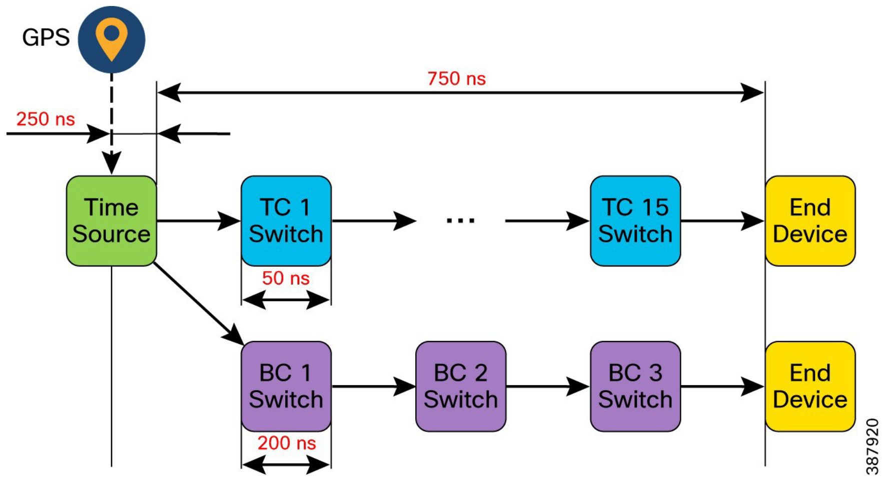
Substation Grandmaster Clock Design Options

When designing the timing architecture for a digital substation, the source and distribution of the Grandmaster (GM) clock are critical. Two primary design options are typically considered.

Option A: Local GNSS-Connected Grandmaster within Substation LAN

This design approach involves deploying a dedicated PTP Grandmaster device directly within the Substation LAN, which obtains its highly accurate time synchronization directly from Global Navigation Satellite Systems (GNSS) such as GPS, GLONASS, or BeiDou. An example device like the GridTime™ 3000 GNSS Time Server or a Cisco Industrial Router (e.g., IR8340) is installed within the substation, connected to an external GNSS antenna, acting as the primary PTP Grandmaster for the entire substation LAN and distributing precise time using the PTP Power Profile. The benefits include direct and accurate synchronization to Coordinated Universal Time (UTC) at the substation level and simplified local deployment by reducing reliance on the WAN for time distribution. However, considerations include the need for robust physical security for the GNSS antenna and Grandmaster device, susceptibility to local jamming, spoofing, or environmental disturbances affecting the GNSS signal, and the requirement for redundant local GNSS-connected GMs to ensure high availability.

Figure 19 PTP Clock and End to End Delay

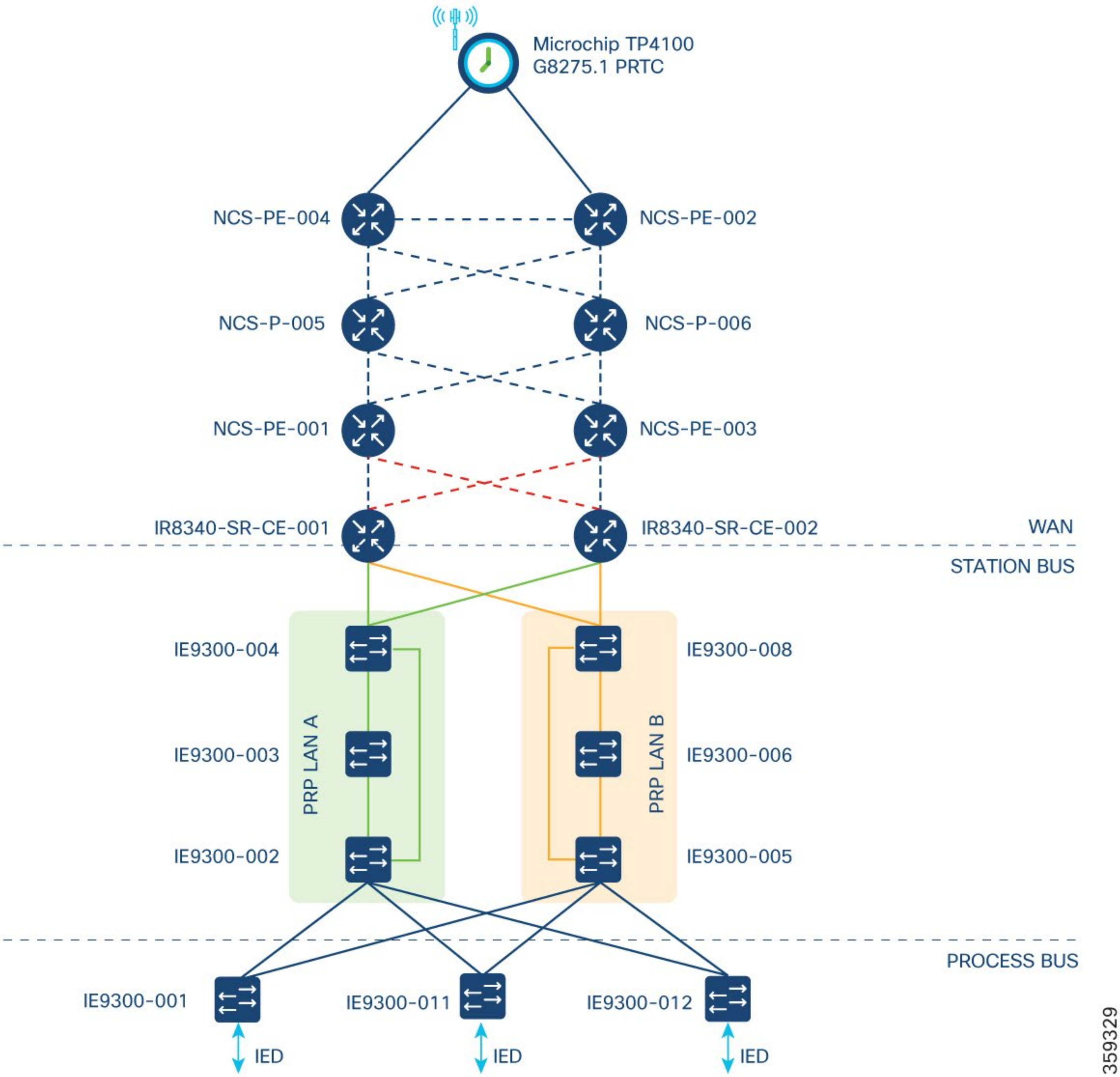


Option B: Centralized GNSS with PTP Telecom to Power Profile Conversion at Substation Boundary

This design centralizes highly secure and robust GNSS receivers at a more protected location, such as a Utility Operations Center or a hardened regional data center and distributes time to substations via the Wide Area Network (WAN). This approach aims to protect GNSS from being hacked or disturbed at individual substation sites, mitigating growing vulnerabilities associated with local GNSS exposure. In this architecture, a Centralized PTP Telecom Grandmaster, such as the Microchip TP4100, generates highly accurate time from GNSS-referenced Primary Reference Time Clocks (PRTCs) in a central, secure facility.

This time is then distributed across the utility's WAN using a PTP Telecom Profile (e.g., ITU-T G.8275.1), optimized for network synchronization over large geographical distances, often over a Segment Routing (SR)-enabled WAN. At each substation boundary (the interface between the WAN and the Substation LAN), a dedicated router like the Cisco Industrial Router IR8340 acts as a PTP Boundary Clock. It receives the highly accurate time synchronized via the PTP Telecom Profile (G.8275.1) from the WAN. When configured as a PTP Telecom profile slave, the IR8340 prioritizes the PTP Telecom profile as its clock source, even if a local GNSS signal is connected; the GNSS input is then automatically selected as the fallback source if the PTP Telecom profile becomes unavailable. The IR8340 then performs the critical function of converting this profile to the PTP Power Profile (IEEE 1588 2012). It then distributes this time to the local substation devices.

Figure 20 TP4100 as PTP Telecom GM over WAN



Benefits of using Microchip TP4100 as a G.8275.1 PRTC

The Microchip TP4100 offers high precision, reliability, scalability, interoperability, robust security, and monitoring.

Benefits of using Cisco IR8340 as Substation WAN Boundary Clock

The Cisco IR8340 provides crucial profile conversion, supports Parallel Redundancy Protocol (PRP) for resilient LAN distribution, and offers robust WAN connectivity. For critical deployments, dual IR8340 routers can be deployed for enhanced resiliency. The main considerations for this option are the substation timing's dependence on WAN reliability and performance, and the need for careful planning to ensure compatibility and accurate translation between different PTP profiles.

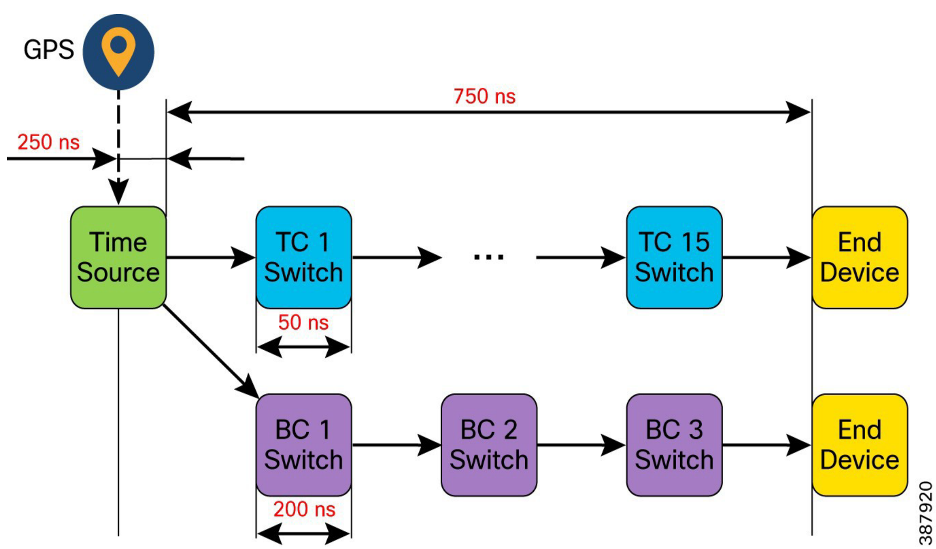
General PTP Power Profile Design Considerations

Regardless of the Grandmaster clock sourcing option chosen, several general design considerations apply to PTP Power Profile implementations within the substation.

The placement of the PTP Grandmaster (GM) is crucial for minimizing clock inaccuracy, ideally on the station bus for process bus applications. 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 primary role to the reference clock.

Managing the end-to-end delay budget is critical, as Substation Automation LAN applications typically require no more than 1000ns (1µs) from the PTP Grand Master to the IED. Each Cisco Industrial Ethernet device contributes to this delay: a Transparent Clock (TC) adds a maximum resident time delay of 50ns, a Boundary Clock (BC) introduces 250ns, and a Grandmaster connected to GPS adds up to 250ns. The cumulative sum of these delays across the entire device chain must remain within the 1µs budget. These facts are depicted in the following figure.

Figure 21 PTP Clock and End to End Delay



The selection of clock types is also important. Transparent Clocks are beneficial in networks with changing topologies (e.g., ring topologies) as they compensate for latency without becoming part of the PTP hierarchy, though they do not alleviate processing load from upstream master clocks. Boundary Clocks, conversely, can offload the Grandmaster in large PTP networks by acting as intermediaries.

Ensuring compliance with the chosen Power Profile (e.g., IEEE1588 2008 , IEEE 1588 2012, C37.238-2011 or C37.238-2017) is vital. When Power Profile mode is enabled, Cisco Industrial Ethernet switches or routers drop the PTP announce messages that do not include these two types of Length and 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.

Implementing a redundant star topology is recommended to reduce time error in substation automation applications, and utilizing the time properties persist command can help maintain time accuracy during temporary grandmaster outages. For PTP traffic, designing explicit Segment Routing (SR) paths can minimize delay, enforce path predictability, and improve resiliency.

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, that is, 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, for example, by using bays. Bays could be based on multiple rings or multiple stars as well as multiple point-to-point links.

Substation LAN Clock Options: Dedicated Grandmasters and Cisco Industrial Devices

Several hardware options are available for implementing PTP Grandmaster and other PTP roles within the Substation LAN, each with specific capabilities.

GridTime™ 3000 GNSS Time Server

The GridTime™ 3000 GNSS Time Server functions as a dedicated PTP Grandmaster, delivering high accuracy (within 250ns at the Ethernet port). It features advanced holdover with a rubidium atomic MAC oscillator, guaranteeing 1µs for 24 hours, and supports multiple GNSS constellations (GPS, GLONASS, BeiDou, Galileo) as well as various timing protocols including PTP, NTP, and IRIG-B. For resiliency, it supports PRP for PTP timing flows, and it includes robust cybersecurity features such as secure boot and anti-jamming/spoofing detection.

The GridTime 3000's rubidium atomic MAC (Miniature Atomic Clock) oscillator uses compact state of the art laser interrogation with proprietary fanless passive cooling technology, not requiring forced ventilation or mechanical fans, much less prone to challenging environments vs heat-generating legacy lamp-based versions. This guarantees holdover operation within 1 microsecond in a wide temperature operation range, for at least 24 hours.

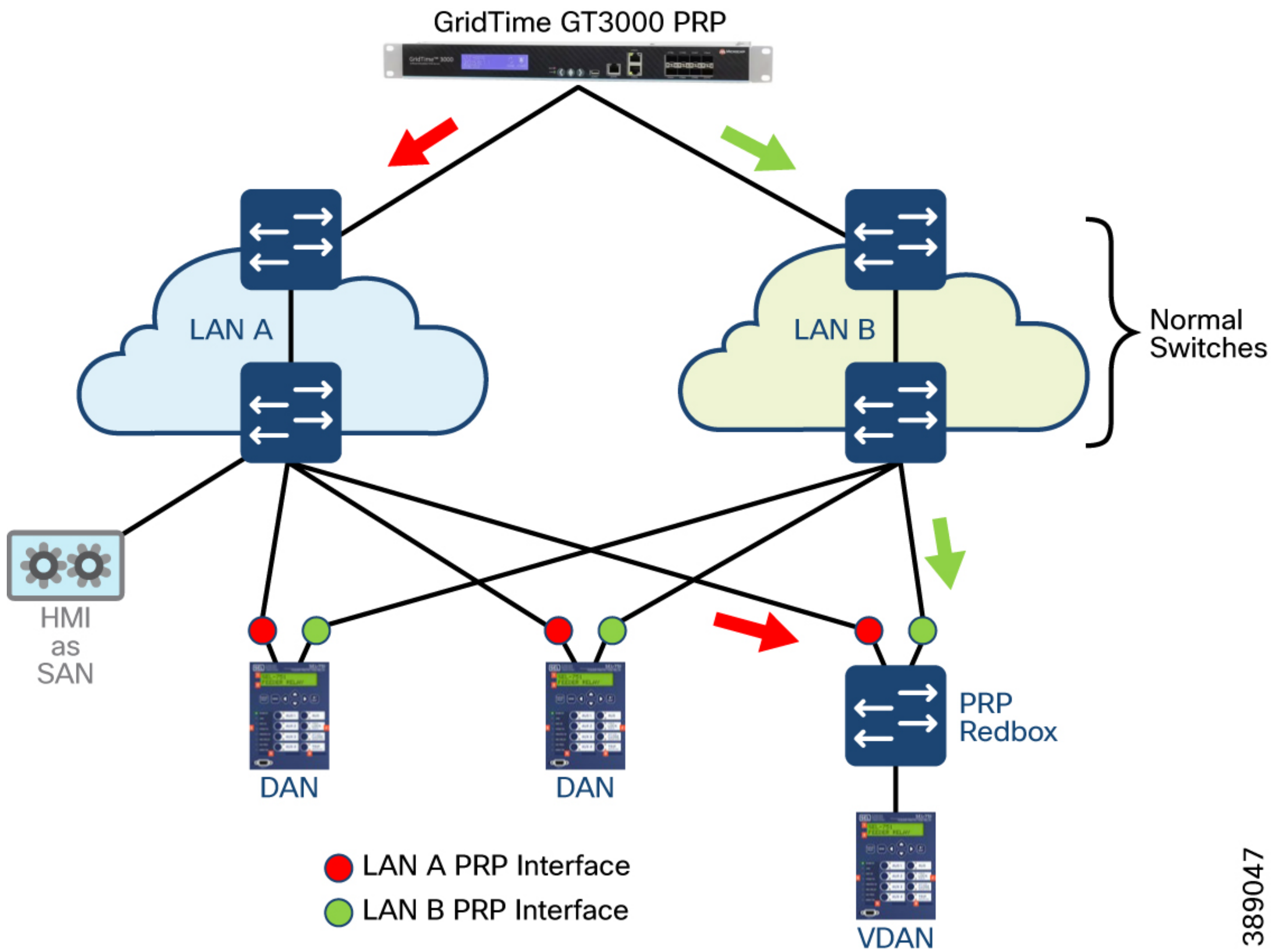
The GridTime 3000 supports a wide range of industry profiles for IEEE 1588 Precision Time Protocol (PTP), up to 10 independently configured Ethernet ports, and multiple GNSS constellations including GPS, GLONASS, Galileo, and BeiDou. It features SNMP management and monitoring, external authentication via RADIUS and LDAP, TLS certificate installation, and comprehensive system and GNSS commissioning logs. The server is designed to synchronize station and bay-level equipment, support digital substation time synchronization with sampled values, and enhance industrial automation and SCADA systems.

In response to evolving substation design philosophies, the GridTime 3000 offers flexible licensing options, allowing utilities to enable features as needed. Its ports are electrically isolated up to 2.5 kV (IEC 61000-4-18:2006) to ensure continued operation during power surges. The server's resilient timing capabilities include malicious software checking, anti-jamming and spoofing detection algorithms, and compliance with IEC 61850-3:2013 standards. Redundant power supplies, optional additional oscillators, firmware verification, and PRP support further enhance network reliability.

Cybersecurity is a priority, with secure boot and industry-standard access control ensuring only authorized personnel can access the system. The GridTime 3000 supports multiple timing protocols, including PTP, NTP, PRP, IRIG-B, serial time strings, T1/E1/J1, and programmable pulses. It features 10 dedicated 1 Gb Ethernet ports with simultaneous NTP and PTP capabilities, and the option to upgrade two SFP Ethernet interfaces to 10 Gb.

The server's GNSS commissioning log verifies proper installation and antenna performance, while advanced system logging provides a detailed audit trail for enhanced security and diagnostics. The modern web interface allows for easy configuration and management via any modern browser. Time quality-based output suppression ensures the accuracy of time provided to end devices, preventing false trips by suppressing output if the clock deviates past the configured threshold.

Figure 22 GridTime 3000 as PTP GM using PRP3409



Cisco Industrial Router IR8340

The Cisco Industrial Router IR8340 can function as a PTP Grandmaster (GMC-BC mode) for local GNSS synchronization (Option A) or as a critical WAN Boundary Clock for PTP Telecom to Power Profile conversion (Option B). It supports a GNSS receiver for synchronization to UTC. It also supports NTP to PTP feature (using an NTP server as reference). Its timing module includes support for IRIG-B (in/out), TOD/1PPS, and SyncE, with GNSS support for Stratum 3 NTP redistribution. For resiliency, it supports PRP for LAN distribution to IEDs, though the document notes it does not support PTP over PRP RedBox, REP, and HSR resiliency protocols for WAN links. As a router, the IR8340 provides robust WAN connectivity for transporting timing information, including over MPLS or Segment Routing networks.

Cisco Industrial Ethernet Switch IE9300

The Cisco Industrial Ethernet Switch IE9300 primarily functions as a PTP Transparent Clock (both E2E and P2P) and a PTP Boundary Clock. It supports PTP Power Profile 2011 and PTP Power Profile 2017 when in Transparent Clock mode. It is crucial to consult the latest platform-specific documentation for definitive support and detailed configuration guidelines for any Cisco Industrial Ethernet product.

Clock Class Changes

The following table, shows the values of “ClockClass” and “SmpSynch Value” that change in the GM messages depending on its state; these messages will indicate the Clock Quality and Accuracy to the PTP devices:

State	GM Clock Accuracy	GM ClockClass	SmpSynch Value
In Sync	The time is accurate to within 250 ns	6	2
Previously in sync, now In Holdover	The time is accurate to within 250 ns	7	2
Previously in sync, now In Holdover	The time is accurate to within 1 µs	52	1
Previously in sync, now In Holdover	The time is equal to or greater than 1 µs	187	1
Returned to sync	The time is accurate to within 250 ns	6	2

MUs, IEDs, and other devices are Slave-Only PTP ordinary clocks. These devices stay in "listening" mode until they receive an Announce message from a Master Clock. The Announce message is the one containing the ClockClass values.

If the ClockClass value indicates an inaccuracy greater than 1 microsecond, the slave device will lose connection to the Clock source.

When these units lose the Clock Source (Master Clock), they immediately go to a Free-running state, which would mean an inaccuracy of 1-10 microseconds (µs) over 1-10 seconds depending on the local oscillator. Considering that the required accuracy allows a maximum error of 1 microsecond, this means that in one second all the devices within the substation will be non-compliant.

Having the PTP slaves in free running mode, will likely start a potentially cascading effect in the substation leading to a service affecting event.

Slave capable units (OCs or BCs) can use BMCA (Best Master Clock Algorithm) to select the best Clock depending on its quality, meaning they can switch to another time source should they lose the original one.

The BMCA will only be useful if there are at least two Masters. If there is only one Master in the Substation, the devices will not have any protection and will go directly into Free Running state.

Time Source

The GMC-BC mode allows an Industrial Ethernet Switch like IE9300 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 supports the NTP to PTP feature. The Cisco Router IR8340 and Cisco IE 9300 Industrial Ethernet Switch also support the GNSS receiver.

The Cisco IR8340 Timing Module supports a comprehensive set of timing features including:

- IRIG-B (in/out): Supports both analog (AM) and digital (TTL) IRIG-B time code formats compliant with IRIG standard 200-04. It can receive (input) or transmit (output) multiple IRIG-B formats such as B002, B003, B006, B007 (digital TTL) and B122, B123, B126, B127 (analog AM). These formats provide time-of-year and year information in BCD and binary formats. The module has separate physical interfaces for analog and digital signals with input/output capabilities.
- GNSS Receiver: The timing module includes a GNSS receiver that supports GPS and other satellite systems, enabling precise time synchronization and Stratum 3 NTP redistribution.
- ToD (Time of Day) and 1PPS (One Pulse Per Second): Provides output of ToD messages or 1PPS signals for synchronization purposes.
- IEEE 1588 v2 (PTP) and SyncE: Supports Precision Time Protocol (PTP) profiles including telecom profiles (G.8265.1, G.8275.1) and SyncE for frequency synchronization.
- Stratum 3 NTP Redistribution: GNSS support enables the IR8340 to redistribute NTP with Stratum 3 accuracy.

The IR8340 timing module is pluggable (Cisco PID: IRM-TIMING-MOD) and must be installed when the router is powered down. It requires the Network-Advantage license to enable all timing features including GNSS, IRIG-B, and PTP profiles.

Regarding the Cisco IE9300 Rugged Series Switches, they support IRIG-B input and output interfaces with multiple analog (AM) and digital (TTL) IRIG-B time code formats compliant with IRIG standard 200-04. The IE9320 models have two mini-BNC connectors on the front panel for digital and analog IRIG-B time code, each configurable as input or output. Supported IRIG-B formats include AM-B122, AM-B123, AM-B126, AM-B127 (analog) and TTL-B002, TTL-B003, TTL-B006, TTL-B007 (digital).

The IE9300 also supports GNSS for precise timing synchronization, and IEEE 1588v2 PTP is supported on the platform. The IE9300 offers enhanced features including higher PoE power budgets, vertical stacking, and advanced software capabilities with Cisco IOS XE. It supports PTP with feedforward boundary clock and PDV filter features and meets industrial standards such as IEEE 1613 and IEC 61850-3.

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 Router synchronizes its clock to one or more NTP servers. How well the router synchronizes to UTC will depend on the quality of the NTP implementation.

Need for Resiliency of PTP GM Clock in Substation LAN Network

The Grandmaster clock serves as the sole primary source of time in the PTP domain, making its resiliency absolutely critical to prevent cascading failures throughout the substation. It is strongly recommended to deploy at least two PTP Grandmaster clocks within the Substation Automation LAN network, regardless of the chosen design option for the GM source.

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 primary 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 primary 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 primary clocks or no primary clocks, as a result of the primary 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.

To enhance robustness, each master should receive an external time reference, such as a PTP Telecom Profile (for Option B) or a redundant GNSS source (for Option A), in addition to its primary source. Implementing Parallel Redundancy Protocol (PRP) connections for the masters is crucial for protecting PTP timing flows to the IEDs, facilitating seamless switchover in the event of a master failure. While dedicated GM devices like the GridTime 3000 support PRP, specific Cisco Industrial devices may have varying levels of support for PTP over PRP/HSR. It is imperative to avoid single points of failure by strategically locating redundant clocks to mitigate common mode failures (e.g., power outages, environmental issues).

If a slave device loses its clock source and no other master is available, it will transition into a " Free-running" state. This can lead to significant timing inaccuracies (1-10 μs over 1-10 seconds), rendering devices non-compliant and potentially triggering service-affecting events. The presence of at least two masters allows slave-capable units to leverage the BMCA to switch to an alternate source, thereby preventing devices from entering a free-running state.

Following recommendations and best practices, the best way to avoid having different devices in a Free-running state is to have dual Masters in the Substation, each of them receiving an external reference from the transport network (typically PTP Telecom Profile) besides just the GNSS reference. Each Master runs at least one PRP connection (depending on the number of switches). With this topology, if a Master fails and needs to be removed/replaced, all the devices will remain locked to a Time reference and will continue to perform with a max time inaccuracy of 1 microsecond.

Additional recommendations:

- Under the premise that in the longest possible chain of 15 LAN switches, all behaving as Transparent Clocks, there is no significant time error accumulation, and the Substation Master is allowed to have a maximum time error of 1 microsecond in the event of a loss of references (GNSS/external inputs). The usual minimum acceptable holdover time for the Master would be not to exceed 1 microsecond of time error for at least 24 hours. This typically allows maintenance crews to arrive on site overnight for most scenarios.
- Withstand harsh environments under challenging operational situations (temporary loss of station's climate control).

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 secondary and passive-secondary ports (see below)

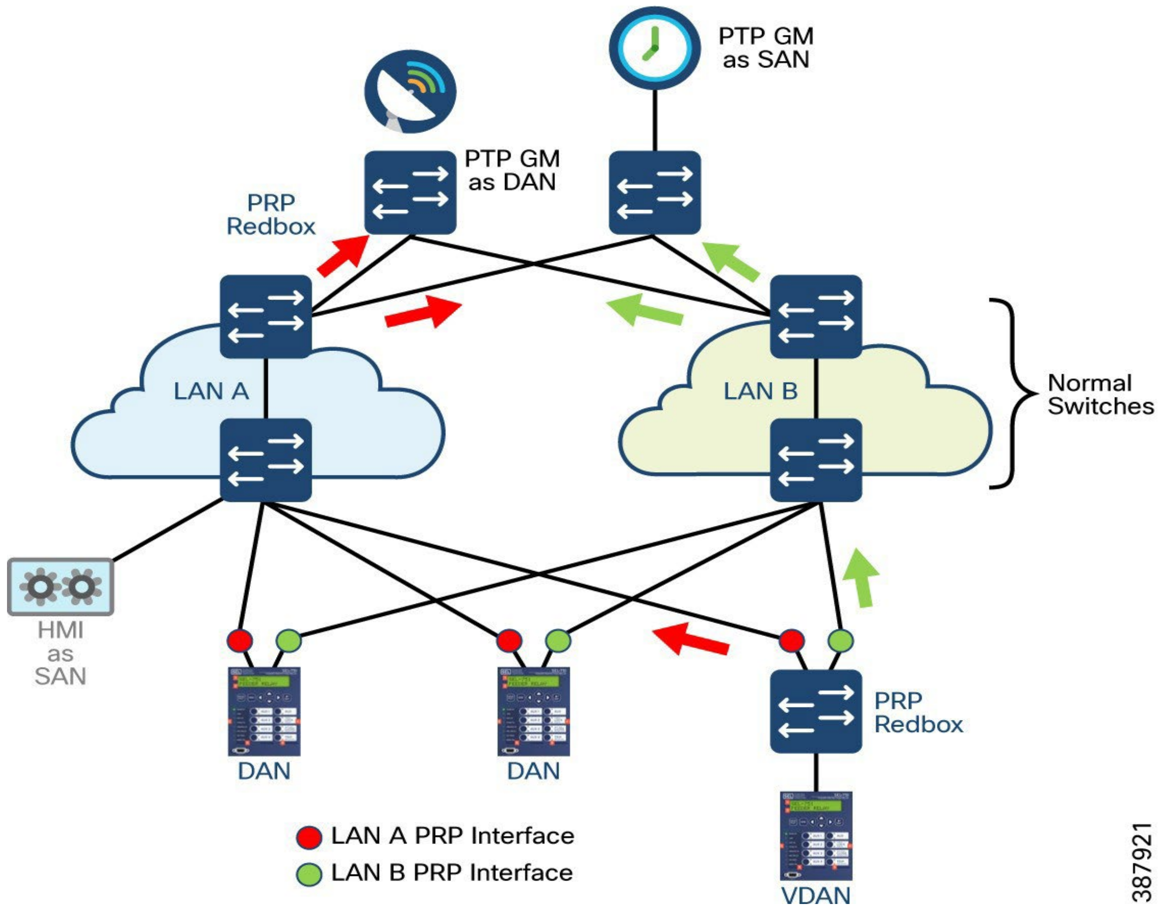
The following are possible ways that the PTP GM can be positioned in a PRP topology:

- 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 23 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 SECONDARY) is used to synchronize the local clock (VDAN in the figure). While the LAN-A port is the SECONDARY, the LAN-A port virtual clock is used to synchronize VDAN. The other PRP port, LAN-B, is referred to as PASSIVE_SECONDARY. The LAN-B port virtual clock is still synchronized to the same PTP GrandMaster but is not used to synchronize VDAN, unless the LAN-A goes down. Then LAN-B port takes over as the SECONDARY 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 virtual clock and the LAN-B port 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 SECONDARY and the LAN-B port becomes PASSIVE_SECONDARY.

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

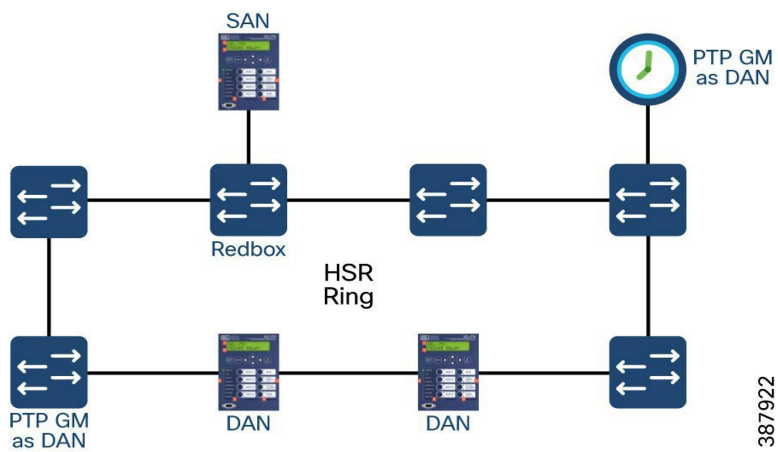
Platform	IE3500	IE3400	IE9300
PTP Power Profile over PRP	Yes	Yes	Yes

PTP Over HSR

The HSR duplicate/discard logic is not used for PTP packets to provide high availability for PTP through redundancy. PTP packets will have an HSR tag inserted, however each node in the ring does not deduplicate the packets and treats each HSR lane as a separate timing source for clock selection.

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 SECONDARY) 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 SECONDARY and port-B as PASSIVE. If port-A goes down, then port-B port takes over as the secondary device and is used to continue synchronizing the local clock on RedBox.

Figure 24 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 HSR. For the most accurate and latest information refer to the platform guide.

Table 13 Cisco Industrial Ethernet Platforms and PTP over HSR

Platform	IE3400	IE3505	IE9300
PTP Power Profile over HSR	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 several 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 traffic, they 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 serve 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 because 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 uses 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.

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 Manageme nt	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.

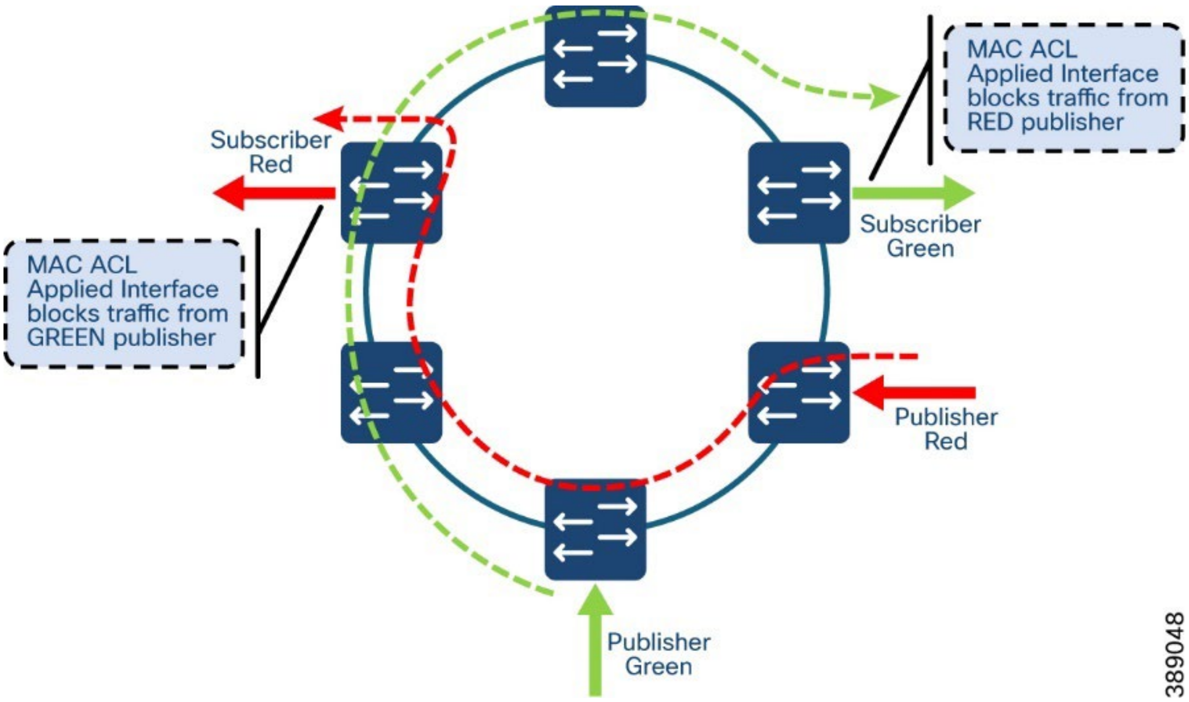
Multicast Filtering

In a Substation Automation network, GOOSE and Sampled Values represent significant traffic types, operating on a Layer 2 multicast Subscriber/Publisher model. Sampled Values are generated at a very high rate, and GOOSE messages, triggered by certain events, can also be produced at elevated rates. This high-frequency traffic can lead to latency and jitter issues, potentially affecting the performance of various applications within the Substation Automation network. To mitigate these challenges, this design guide recommends employing mechanisms such as MAC Access Control Lists (ACLs), Quality of Service (QoS), and traffic segmentation.

Filtering traffic using MAC ACLs is a key strategy discussed in this section of the guide. MAC ACLs filter traffic based on information in the Layer 2 header of each packet, allowing control over which hosts can access different network segments and determining which types of traffic are forwarded or blocked at interfaces. However, it is important to note that MAC ACLs cannot be applied universally to all interfaces. For instance, in ring topologies, such as those using RSTP or HSR, and in parallel networks like PRP, multicast filtering on trunk ports is not feasible. This is because a multicast publisher cannot identify the block in the ring topology or the location of the device requiring the multicast traffic.

To address this, the design guide suggests applying MAC ACLs in the egress direction on interfaces that connect to subscribers, rather than on trunk interfaces. This approach allows for the filtering of multicast traffic based on the specific interests of the subscribers, while ensuring that the traffic continues to flow through the trunk interfaces unimpeded. Additionally, VLANs can be used for traffic segregation, as detailed in the relevant sections of this document. By implementing these strategies, the design ensures efficient traffic management, reducing latency and jitter, and enhancing the overall performance of the Substation Automation network.

Figure 25 Filtering using MAC ACL in Substation LAN networks



Platform	IR8340	IE9300	IE3400
MAC ACL - Egress direction	No	Yes	Yes

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

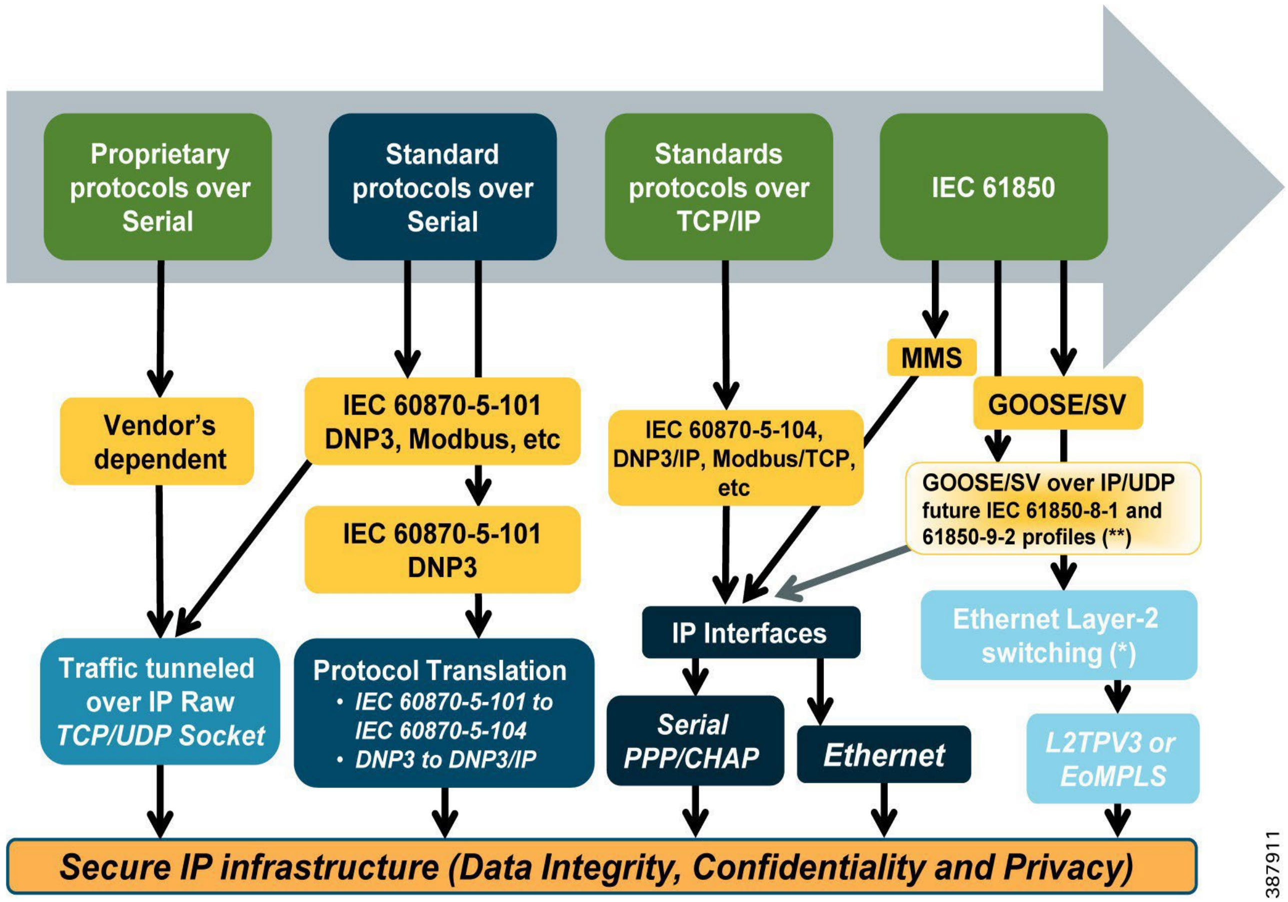
Substation Core and Utility WAN Networking - Requirements

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 several 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 26 SCADA Protocols



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-5GS6-R16SA-GL(=)	5G (SA/NSA) Sub 6 GHZ module for North America, LATAM, Europe and Asia Pacific
P-LTEA7-NA(=)	Category 7 LTE module for North America
P-LTEA7-EAL(=)	Category 7 LTE module for Europe, LATAM, Australia, New Zealand, India, Singapore, Malaysia, Thailand and United Arab Emirates

P-LTEA7-JP(=)	Category 7 LTE module for Japan
P-LTE-MNA(=)	Category 4 LTE module for AT&T, FirstNet™ Capable and Verizon, US
P-LTE-US(=)	Category 4 LTE module for AT&T, U.S
P-LTE-VZ(=)	Category 4 LTE module for Verizon, U.S
P-LTE-GB(=)	Category 4 LTE module for Europe
P-LTE-IN(=)	Category 4 LTE module for India
P-LTE-JN(=)	Category 4 LTE module for Japan

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 and the multi-service
- 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 the 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

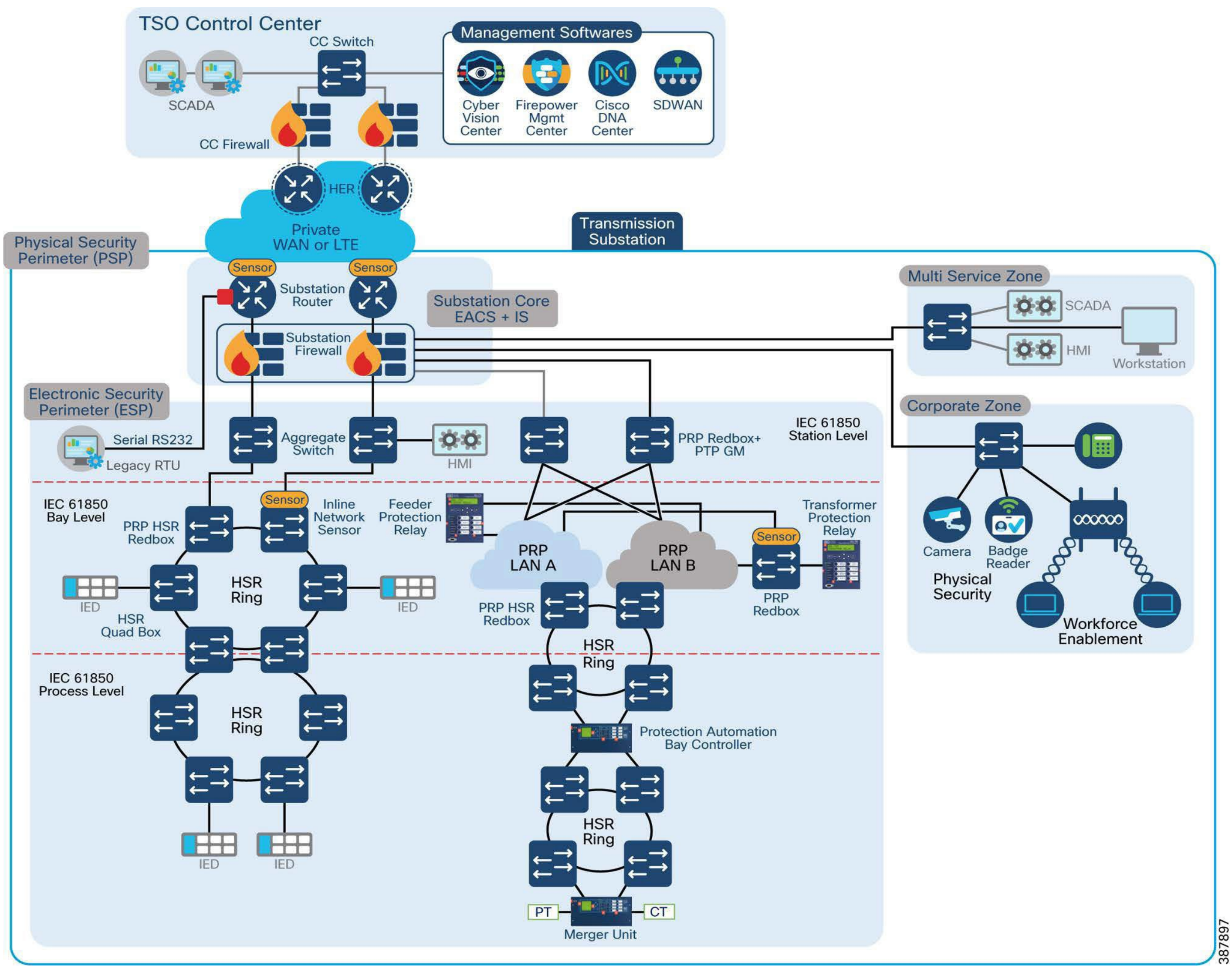
EACS Design Considerations

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 that follows.

Figure 27 **L3 Routing between ESP Zone and Substation Core Zone**



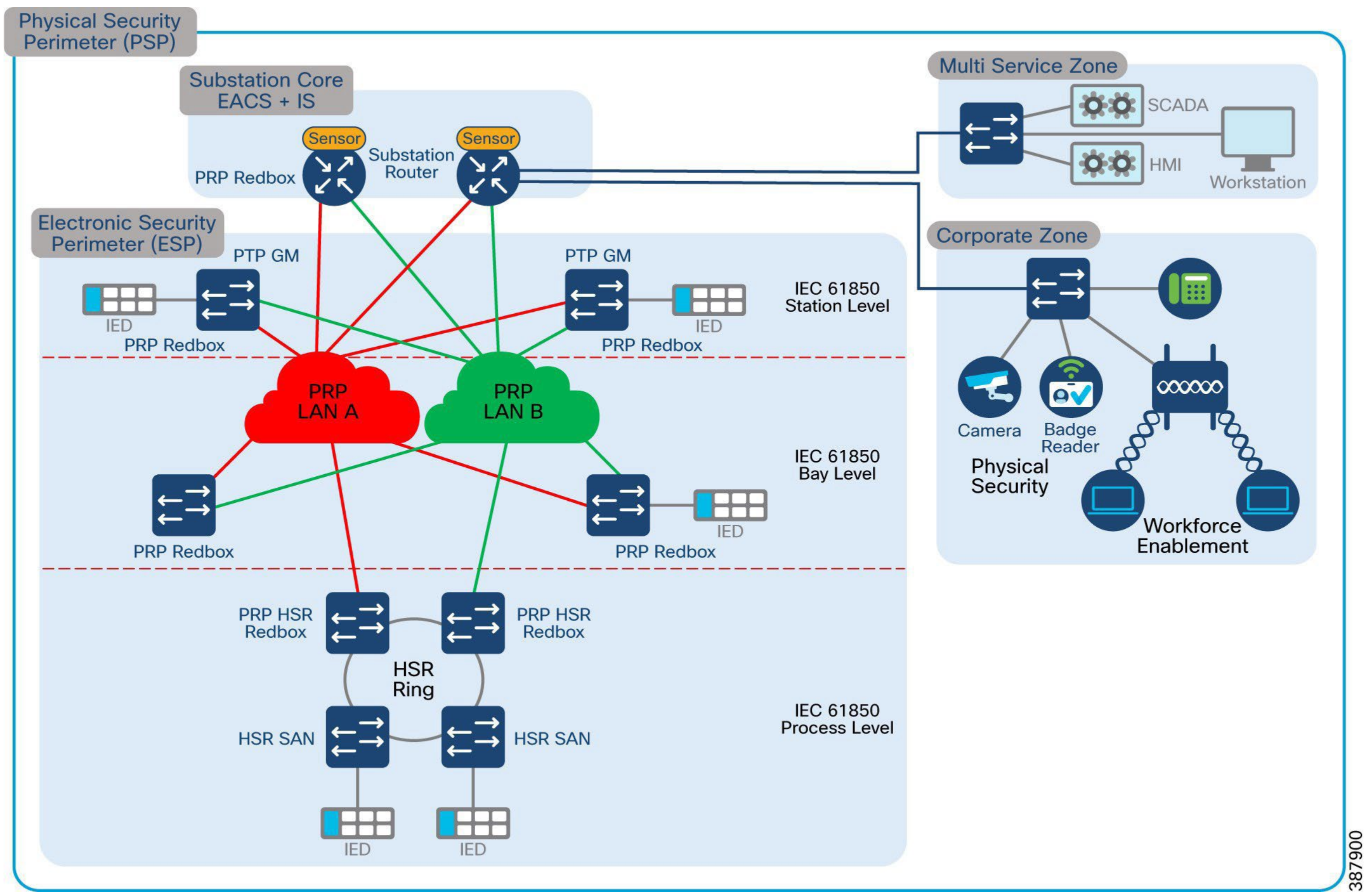
Design Option 2

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.

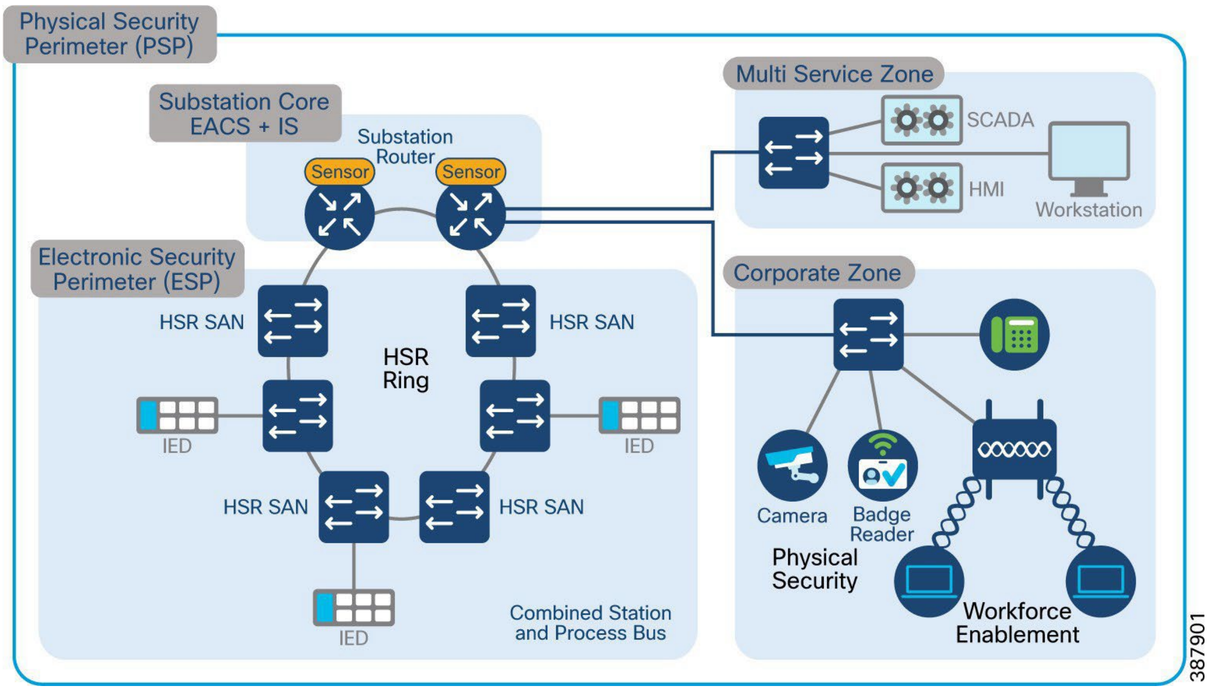
- Option A - Substation Router as PRP Redbox as part of IEC 61850 Station BUS as depicted in the figure that follows. Multi Service and CORP Zones can be connected as star to Substation Router, or we can run L2 Ring protocol like REP or RSTP based on application requirements.

Figure 28 Substation Router aggregating ESP and Multiservice Zones



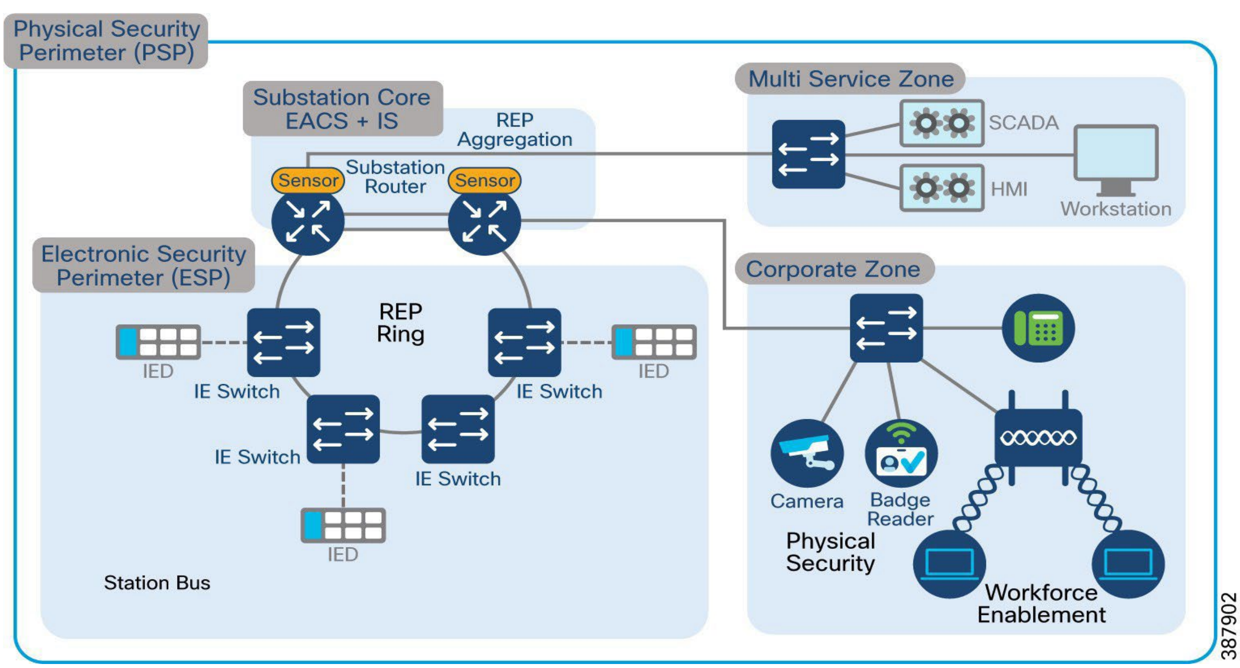
- Option B - Substation Router used as HSR SAN as part of IEC 61850 Station BUS as depicted in the figure that follows and design for other zones like the option above.

Figure 29 Substation Router as HSR SAN



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

Figure 30 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 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.

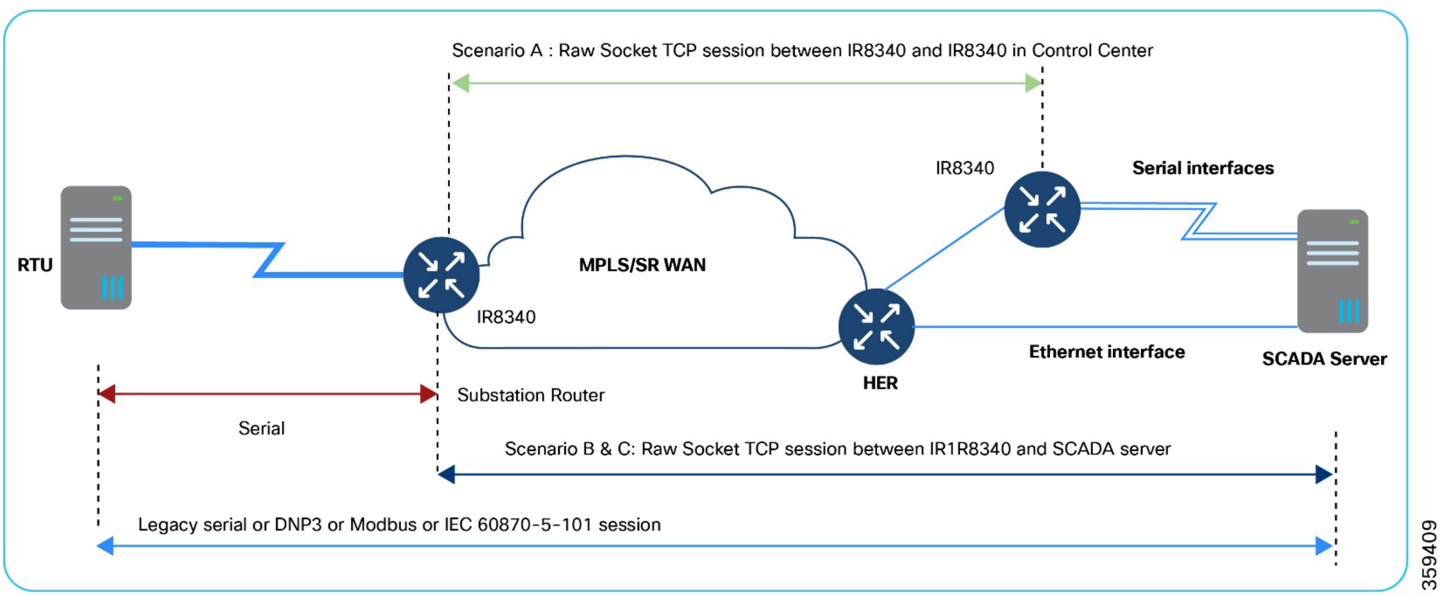
Raw Socket transports Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). Raw Socket supports point-to-point and point-to-multipoint connections over an asynchronous serial line and has a built-in auto TCP connection retry mechanism. Packetization and sending data 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 31 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, a migration strategy is needed 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.

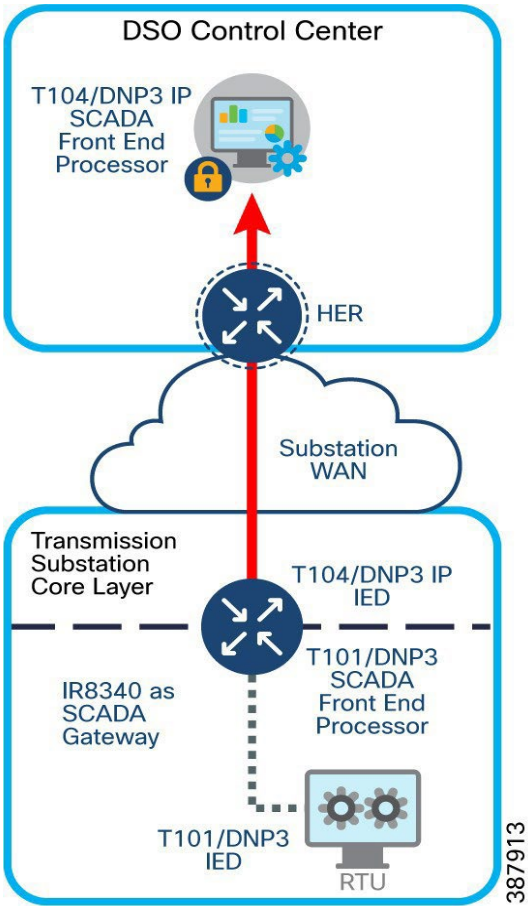
The SCADA Gateway function allows for the following translations between:

- 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 32 SCADA Protocol Translation



In the diagram above the IR8340 acts as SCADA gateway to implement T101 Primary and T104 Secondary functionalities. One RTU per serial interface is connected. DA Gateway/ Secondary Substation router act as T101 Primary for T101 Secondary RTU. In turn DA Gateway/Secondary Substation router acts as T104 Secondary to SCADA T104 Primary 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 (like dnp3 unsolicited response) unbalanced mode is suitable for multi drop links where only primary 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 receiving 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

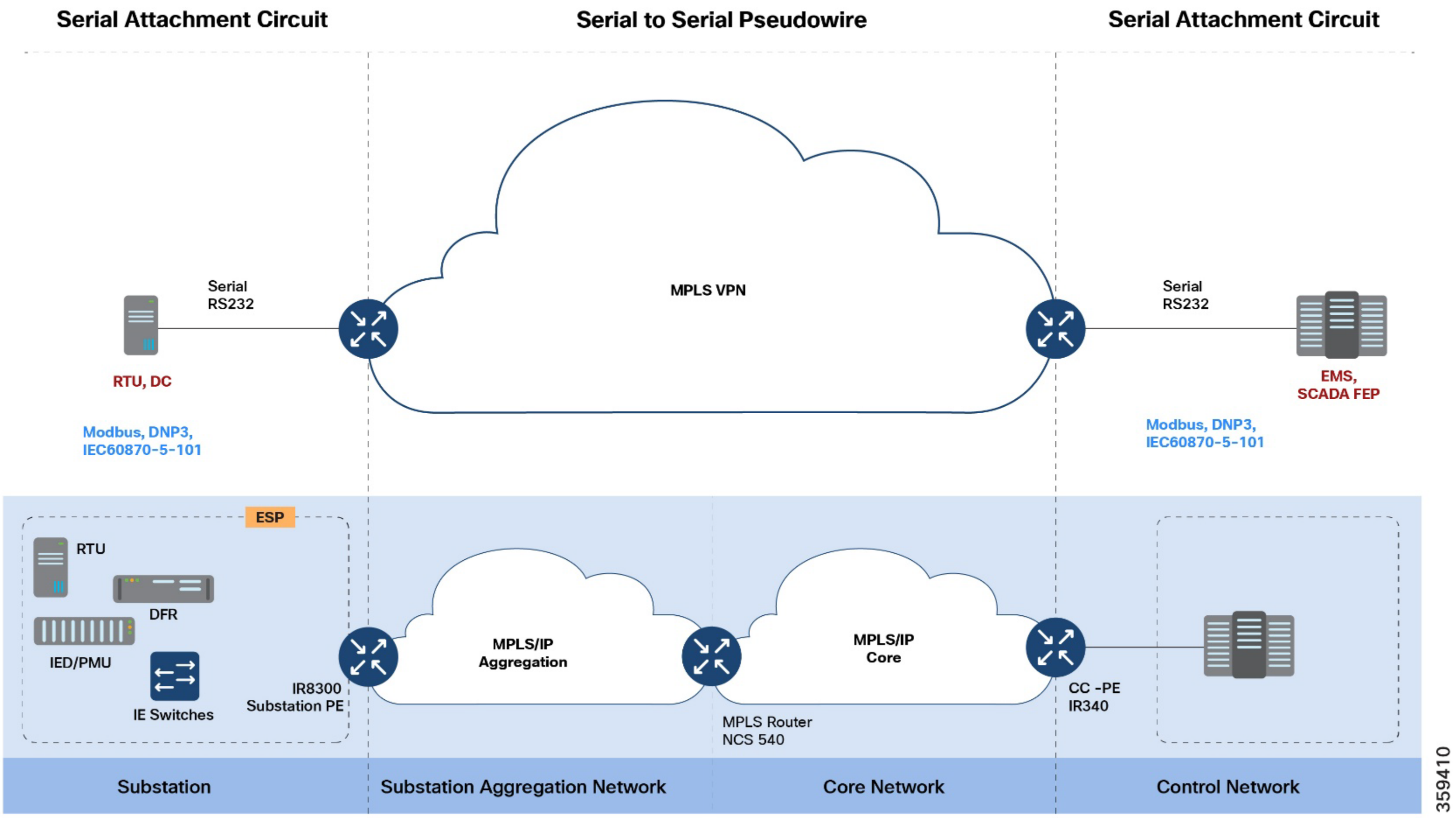
Serial over Pseudowire for SCADA Data Transport:

One highly effective option for transporting legacy serial data from Remote Terminal Units (RTUs) at substations to the SCADA Front End Processor (FEP) at the control center is Serial over Pseudowire using Cisco MPLS technology. This approach leverages the utility's existing MPLS backhaul network to encapsulate and transport serial traffic, offering a streamlined and cost-effective solution. It notably eliminates the need for deploying and managing firewalls at individual transmission substations, simplifying the network architecture and centralizing traffic inspection at the control center. This can be achieved either through a direct serial-to-serial pseudowire connection, where both ends terminate on serial interfaces, or via a serial-to-Ethernet interworking pseudowire, which converts the serial data to Ethernet frames for IP transport to the FEP.

When designing a Serial over Pseudowire solution, several key considerations must be taken into account. The deployment relies on a utility-owned MPLS backhaul network, with Cisco Catalyst IR8340 Rugged series routers recommended to function as the Provider Edge (PE) devices at both the substation and the control center. The TSO Control Center PE router should be a dedicated device for aggregating legacy SCADA connections, capable of handling up to 1000 pseudowires, especially in a Serial to Ethernet Interworking scenario. It's imperative to use Cisco IOSXE software releases 17.17.1 or later for full functionality.

A critical design limitation is that pseudowire redundancy is not supported, necessitating alternative strategies for high availability. For serial-to-serial deployments, scalability is inherently limited by the number of physical serial interfaces on the Control Center PE. In contrast, serial-to-Ethernet interworking, while offering greater scalability, uses raw socket TCP clients on the Control Center PE's loopback interface, which do not support advanced packetization sub-options like packet length or timers, although TCP and UDP servers are supported. The primary architectural benefit remains the ability to eliminate firewall inspection at the substation, simplifying security enforcement to the control center.

Figure 33 Serial to Serial Pseudowire

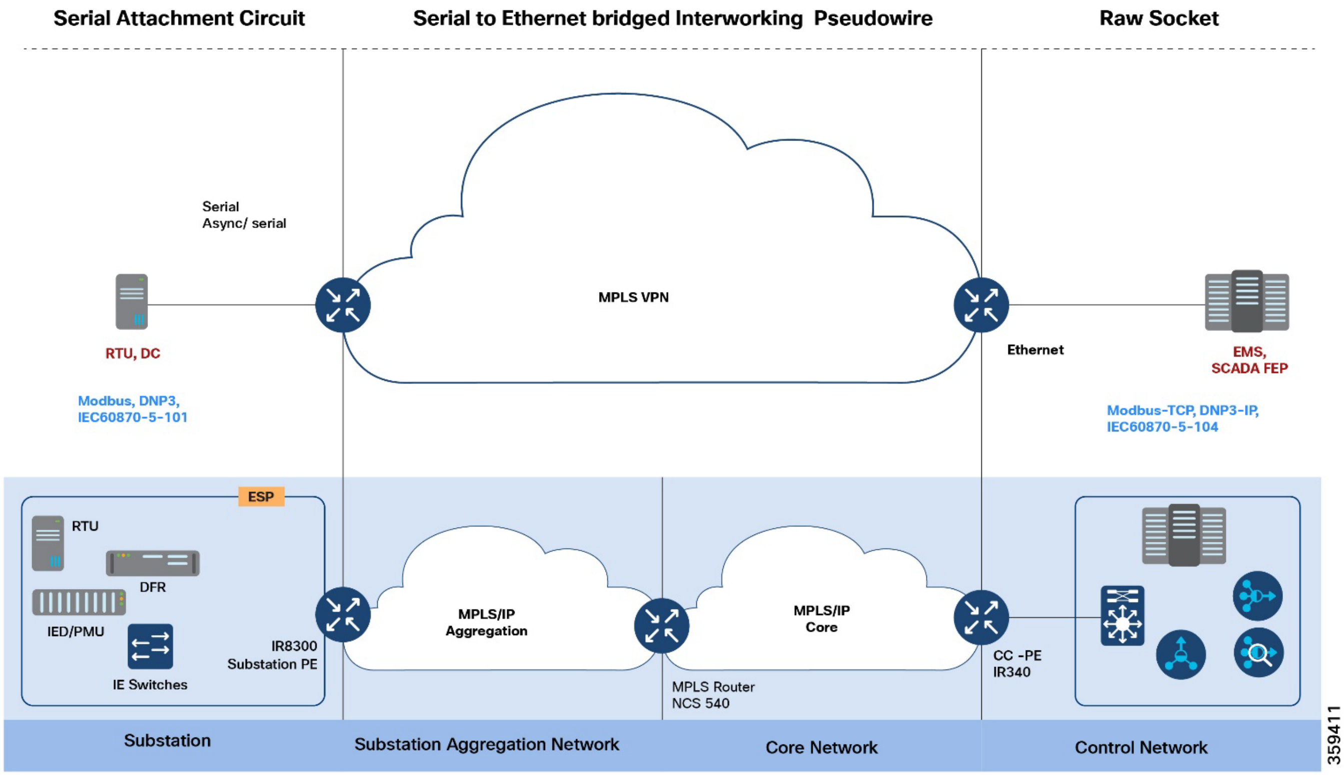


The figure above illustrates a deployment scenario in which legacy SCADA traffic is transported between a Remote Terminal Unit (RTU) at a substation and a SCADA Front End Processor (FEP) at a control center using a serial-to-serial pseudowire over an MPLS network.

The figure depicts the following key components and connections:

- Substation Side: A " Legacy RTU" is connected via an RS232 serial interface to a " Substation Router" (specifically, a Cisco Catalyst IR8340 Rugged router). This serial interface acts as the attachment circuit for the pseudowire.
- MPLS Network: The Substation Router is connected to an " MPLS Network" (represented as a cloud), which serves as the transport medium for the pseudowire.
- Control Center Side: On the other end of the MPLS network, a " Control Center PE Router" (also a Cisco Catalyst IR8340 Rugged router) receives the pseudowire. The SCADA FEP is connected to this Control Center PE Router via its own RS232 serial interface, which serves as the attachment circuit on the headend side.

Figure 34 Serial to Ethernet Bridged Internetworking Pseudowire



The figure above illustrates a deployment scenario where legacy SCADA traffic is transported between a Remote Terminal Unit (RTU) at a substation and a SCADA Front End Processor (FEP) at a control center using a serial-to-serial pseudowire over an MPLS network.

The figure depicts the following key components and connections:

- Substation Side: A " Legacy RTU" is connected via an RS232 serial interface to a " Substation Router" (specifically, a Cisco Catalyst IR8340 Rugged router). This serial interface acts as the attachment circuit for the pseudowire.
- MPLS Network: The Substation Router is connected to an " MPLS Network" (represented as a cloud), which serves as the transport medium for the pseudowire.
- Control Center Side: On the other end of the MPLS network, a " Control Center PE Router" (also a Cisco Catalyst IR8340 Rugged router) receives the pseudowire. A raw socket TCP client is provisioned on this loopback interface to forward the RTU traffic to the SCADA Front End Processor (FEP) application. The FEP application is connected to the LAN side of the control center PE router through a firewall.

Utility WAN design considerations

As explained in the 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 35 On Net Substation

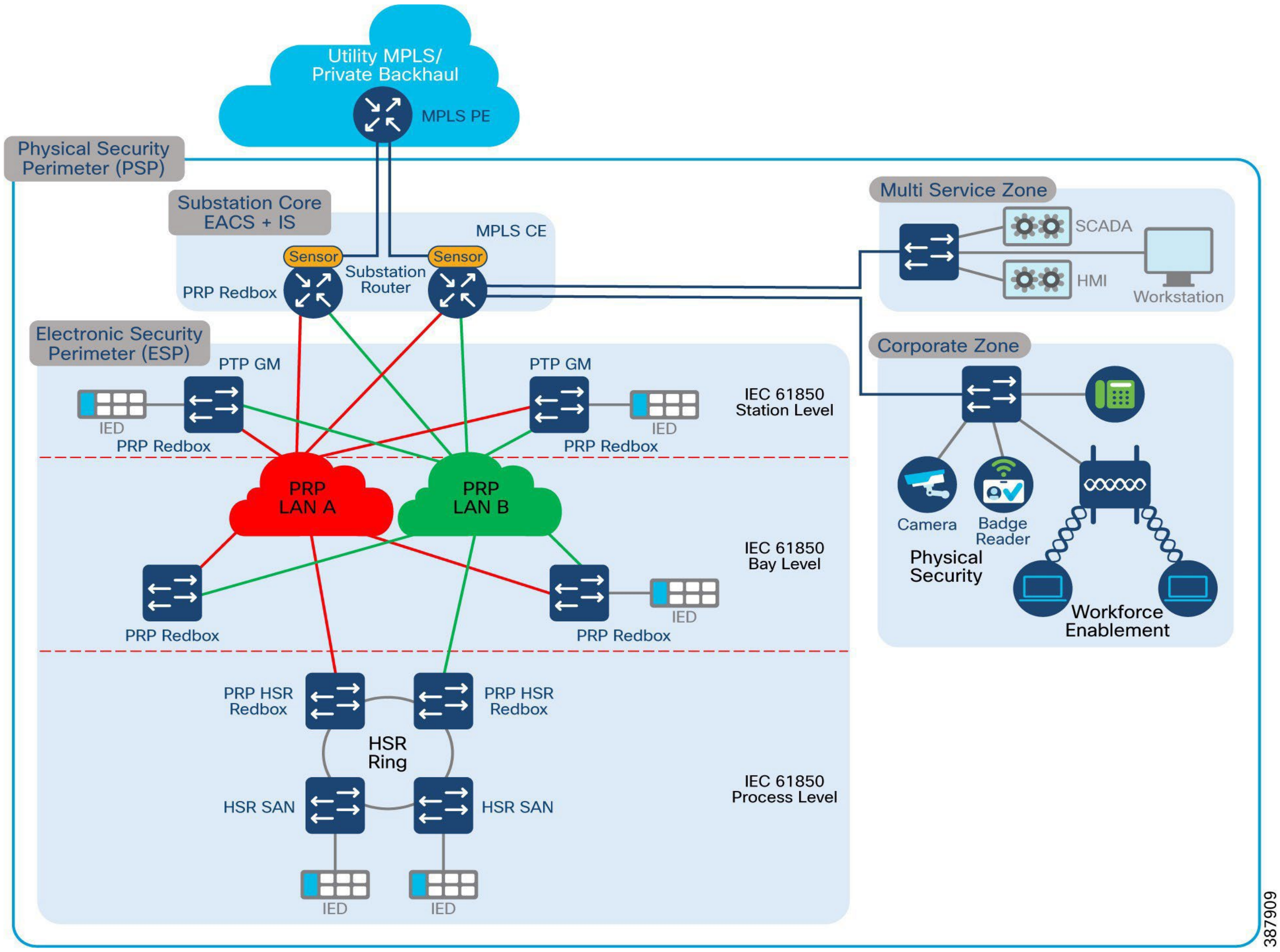
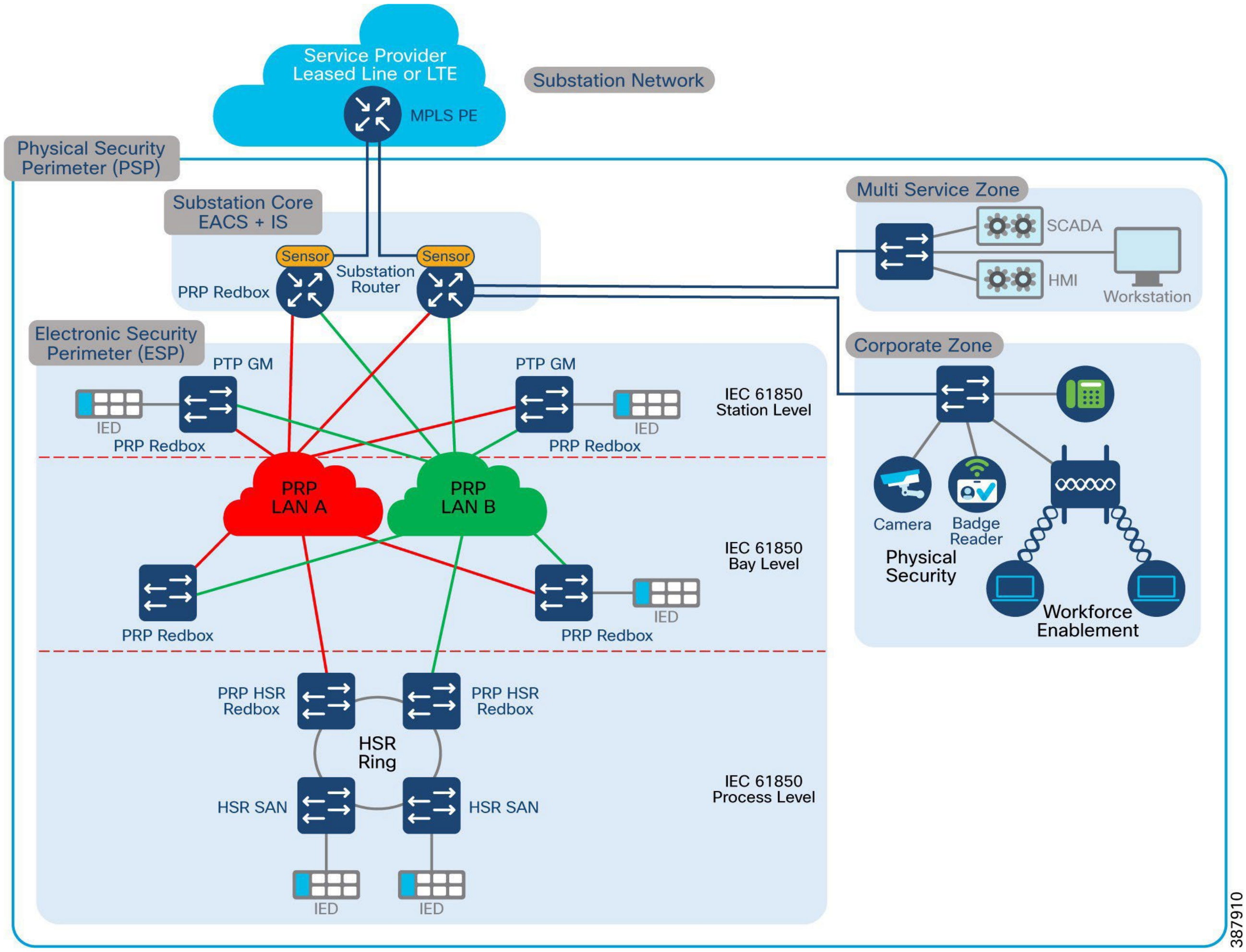


Figure 36 Off Net Substation



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 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

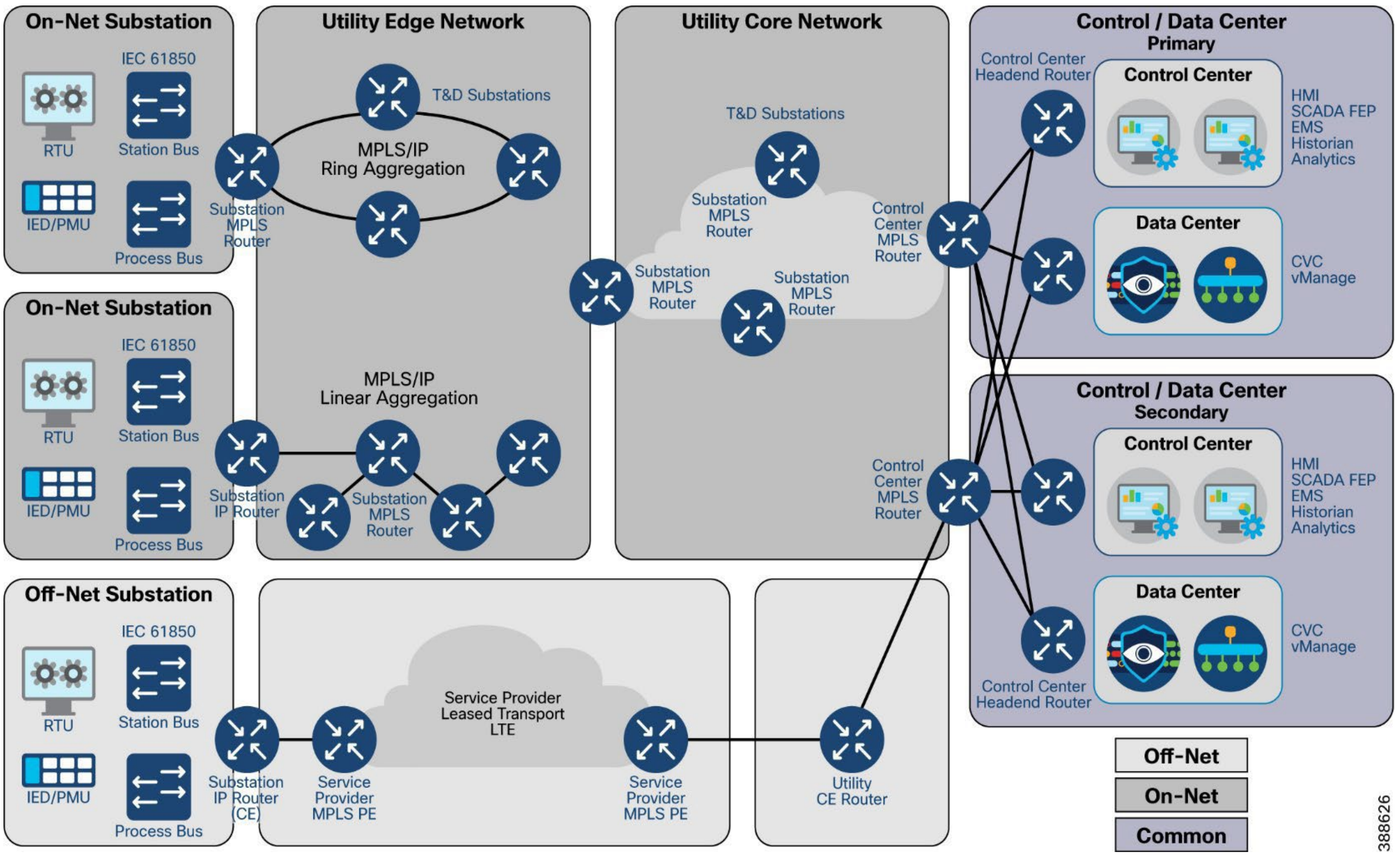
Substation Automation Router WAN Backhaul Redundancy is like Distribution Automation/Secondary Substation Gateway Design. Refer to the following DA CVD for more details on WAN Backhaul Redundancy design:

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

Next Generation Utility WAN Architecture

Segment Routing for Utility WAN

Figure 37 Substation WAN MPLS



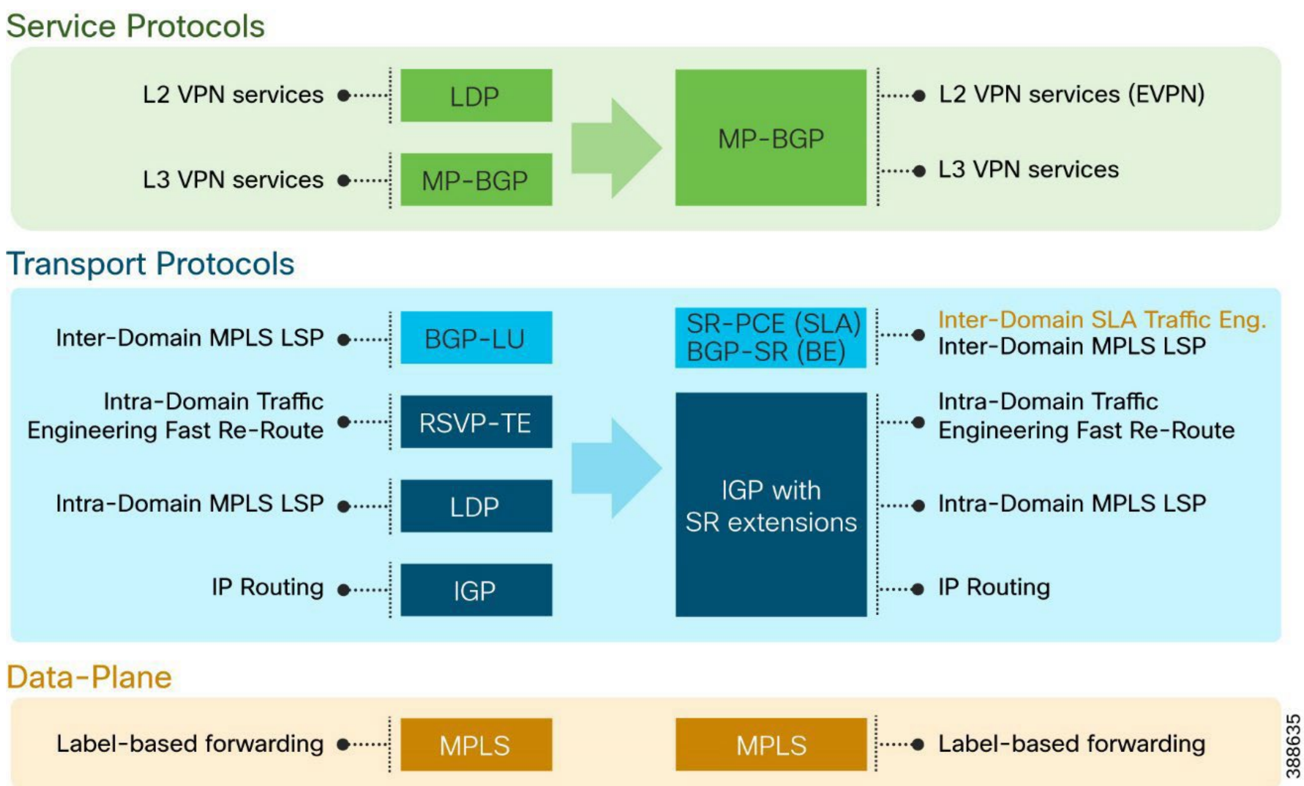
As depicted in the figure above, earlier versions of Substation Automation Wide Area Network designs utilized MPLS for its core. The solution provided different roles for Substation router viz a customer edge router or a provider edge router in an ON-NET Substation model and as a Customer Edge router in an OFF-NET Substation model that utilized cellular backhaul. Various services were enabled from these routers in different roles.

In IP MPLS based WAN networks, L3VPN and L2VPN services, Traffic Engineering (TE) / Fast Reroute (FRR) capabilities are offered over the MPLS backbone. At transport protocol layer, Label Switched Path (LSP) signaling is required for both MPLS Label Distribution Protocol (LDP) & Resource Reservation Protocol (RSVP)-TE, and BGP-LU is leveraged for inter- domain MPLS LSP. At the service protocol layer, separate service protocols are leveraged, LDP for L2VPN services and MP-BGP for L3VPN services. This results in a complex protocol stack, complex troubleshooting and operational challenges.

Therefore, while data plane in MPLS has rarely been challenged, various control plane protocols for label signaling have added operational complexity as well as scalability challenges. Segment Routing is a technology focused on addressing the pain points of existing IP and MPLS networks in terms of simplicity, scalability, and ease of operation.

Segment routing is a source-based routing architecture. A node chooses a path and steers a packet through the network via that path by inserting an ordered list of the segments, instructing how subsequent nodes in the path, that receive the packet, should process it.

Figure 38: Network Evolution with Segment Routing



Segment Routing relies on a small number of extensions to Cisco Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. It can operate with an MPLS (Multiprotocol Label Switching) or an IPv6 data plane, and it integrates with the rich multi service capabilities of MPLS, including Layer 3 VPN (L3VPN), Virtual Private Wire Service (VPWS), Virtual Private LAN Service (VPLS), and Ethernet VPN (EVPN). This solution guide is based on validation with SR over MPLS data plane.

Segment routing can be directly applied to the Multiprotocol Label Switching (MPLS) architectures with no change in the forwarding plane. Segment routing utilizes the network bandwidth more effectively than traditional MPLS networks and offers lower latency.

Segment Routing therefore simplifies the transport by removing the need for multiple protocols: LDP, RSVP and BGP-LU (in inter-domain scenarios). No RSVP state is to be maintained on the routers, resulting in scalable solutions. Segment routing for traffic engineering (SR-TE) enforces a policy between a source and destination pair by leveraging source routing. Routers in the core network are instructed to follow a path based on the specified constraint instead of the shortest path calculated by the IGP. Segment Routing Path Computation Element (SR-PCE) is Cisco Path Computation Engine (PCE) coupled with Segment Routing to program simple and scalable inter-domain transport connectivity, Traffic Engineering, and advanced Path control with constraints, adhering to network SLAs.

Benefits of Segment Routing

- Ready for SDN: Segment routing was built for SDN and is the foundation for Application Engineered Routing (AER). SR prepares networks for business models, where applications can direct network behavior. SR provides the right balance between distributed intelligence and centralized optimization and programming.
- Minimal configuration: Segment routing for TE requires minimal configuration on the source router.
- Load balancing: Unlike in RSVP-TE, load balancing for segment routing can take place in the presence of equal cost multiple paths (ECMPs).
- Supports Topology-Independent Loop-Free Alternate (TI-LFA) Fast Reroute (FRR): TI-LFA FRR enables the activation of a pre-configured backup path within 50 milliseconds of path failure.

- Plug-and-Play deployment: Segment routing tunnels are interoperable with existing MPLS control and data planes and can be implemented in an existing deployment.

For more information about segment routing, refer to the documents below.

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/segment-routing/710x/configuration/guide/b-segment-routing-cg-710x- ncs540/about-segment-routing.html

https://xrdocs.io/design/blogs/latest-converged-sdn-transport-hld

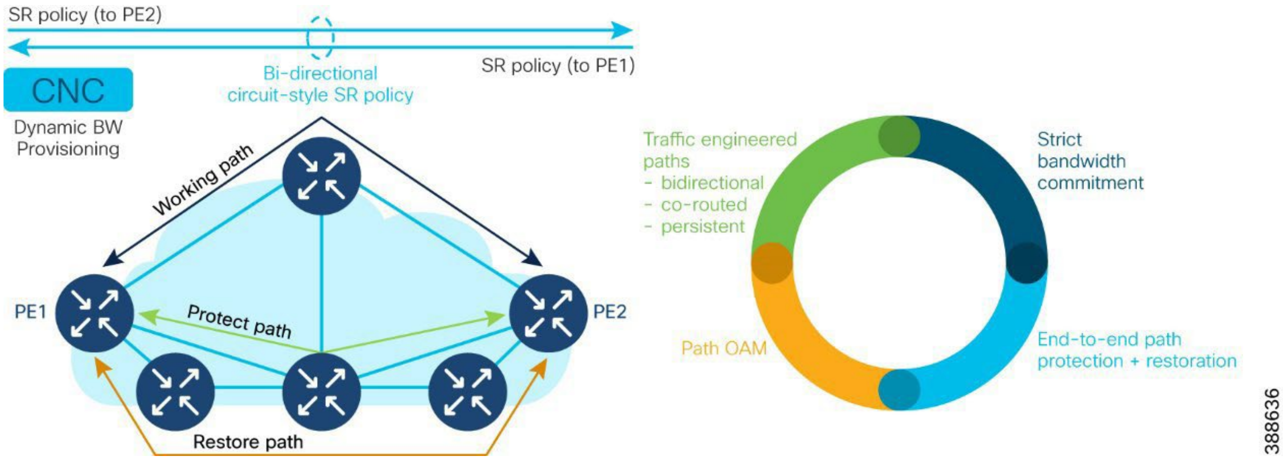
Circuit-Style Routing

A key requirement of utility transport networks is path predictability for latency sensitive applications such as Teleprotection. Utilities require the ability to co-route traffic, which means map upstream and downstream traffic over a bi-directional, well-defined path in the network. This applies to both the active and protection paths, and is the way synchronous optical network (SONET) and synchronous digital hierarchy (SDH) networks operated with unidirectional path switched ring (UPSR) and subnetwork connection protection (SNC-P).

In traditional IP MPLS based networks, Flex LSP is leveraged to meet Utilities' Teleprotection requirements. Flex LSP facilitates the establishment of bidirectional label-switched paths (LSPs) dynamically through the Resource Reservation Protocol-Traffic Engineering (RSVP-TE). Call Admission Control (CAC) ensures that the LSP has sufficient bandwidth to accommodate the Layer 2 circuit.

With the transition to modern transport, SR-TE offers path predictability required for Utility WAN Layer 2 Teleprotection services by leveraging the latest circuit-style segment routing (CS SR-TE) capabilities. CS SR leverages network controllers to configure bi- directional co-routed active & protection paths with sub-50-ms switching times. When CS SR is used the network behavior is fully predictable to meet utility network requirements.

Figure 39: Network Modernization with Circuit-Style Segment Routing



The following are some properties of CS SR-TE services relevant to Utility-Layer-to-Tele protection:

- Co-routed bidirectional: Both forward and return paths are routed over the same path between a source and destination pair, guaranteeing the asymmetry delay bound mandated for Teleprotection services
- Persistence: The working and protect paths, once calculated, are persistent throughout the lifecycle of the circuit-style SR-TE service. Path re-optimization is disabled and is only performed when explicitly requested by the user.
- Guaranteed Bandwidth and Latency: Strict bandwidth and latency commitment to ensure zero impact on SLA because of network load from other services, a requirement essential to delivering mission-critical applications such as Teleprotection.
- End-to-end path protection + restoration: 1:1 working path: protect path + restore path ensures that

bandwidth constraints can always be met, even in the event of link/node failure. The working and protect paths are configured with a disjointedness constraint. The working path has a higher preference than the protect path, thereby enforcing the working path to be the active path. When both working and protect paths are down, the restore path becomes active, and remains so until the working or protect path recovers.

There are two types of provisioning CS SR-TE:

- Manual CS SR: Explicit working & protect path definition that requires humans to always track the consumed bandwidth.
- Dynamic CS SR: Dynamic path provisioning via Crosswork Network Controller (CNC) that offers the capability for dynamic bandwidth allocation & tracking. CNC offers CS SR-TE Feature Pack that provides a bandwidth-aware Path Computation Element (PCE) for computing CS SR-TE policy, as explained later in the Network Management section.

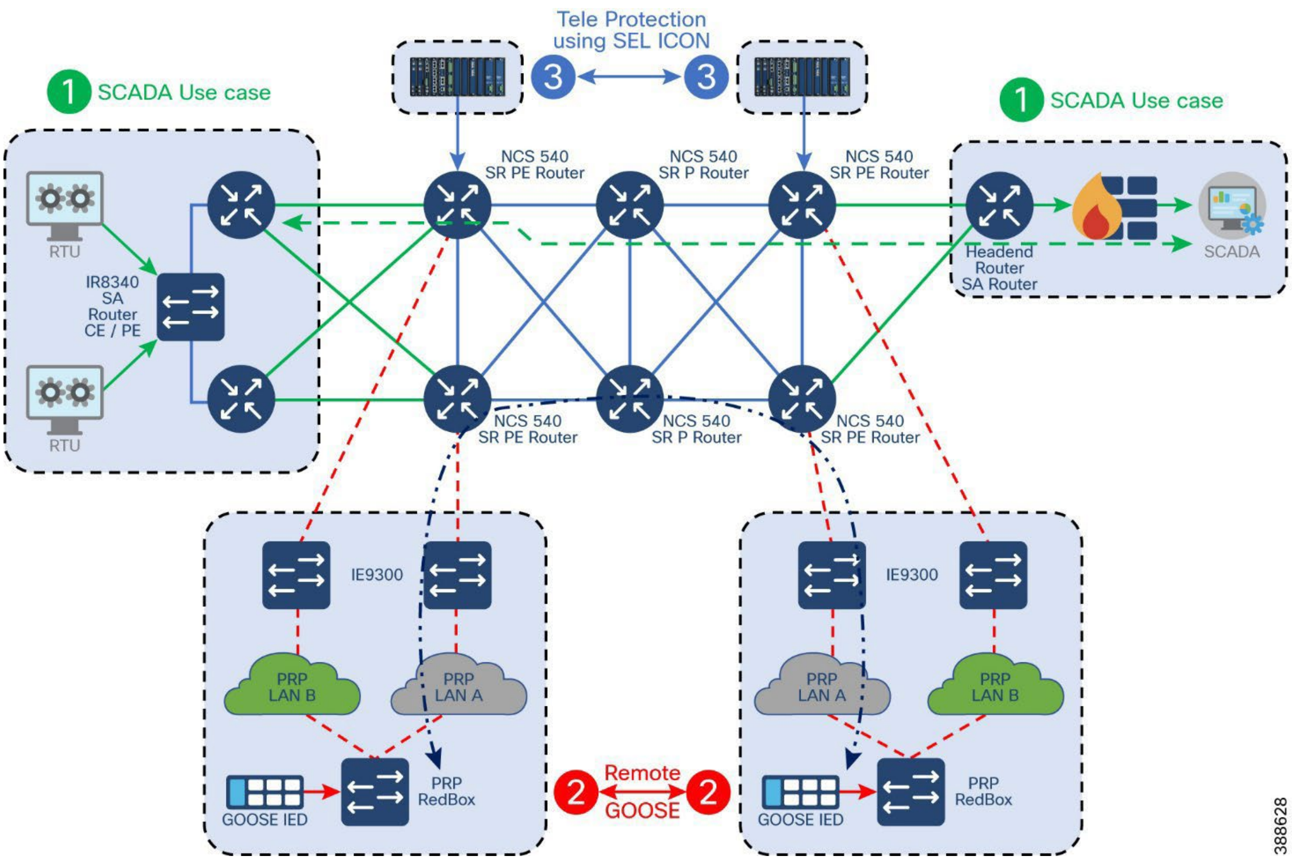
The recommendation is to automate the policy provisioning with CNC to avoid human error in BW tracking.

Latest CS SR enhancements guarantee sub-50-ms switching times in the event of failures, a crucial requirement for Utility WAN Teleprotection. Segment Routing Performance Measurement (SR-PM) offers the functionality of path liveness check and upon failure detection in the active working path, the path switch to the protect/restore path occurs. With the latest CS SR enhancement of offloading this liveness-check functionality from software to hardware, failure detection can be guaranteed at ~10ms, thereby enforcing the sub-50ms path switching time. CS SR-TE therefore provides deterministic path behavior aligning with utility WAN network requirements.

https://www.cisco.com/c/en/us/products/cloud-systems-management/crosswork-network-automation/circuit-style-sr-te-wp.html
https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/segment-routing/710x/configuration/guide/b-segment-routing-cg-710x-ncs540/configure-sr-te-policies.html#Cisco_Concept.dita_07c49a77-4092-486e-adc6-8be6eaf4f1f1

As discussed in the previous text of this document, this section continues to propose the following design options for different services in a Substation network over segment routing enabled core network. The following topology depicts the logical segment routing enabled core and various services over the network from a substation.

Figure 40 Substation WAN - Segment Routing Enabled



The following table lists the different products used in this validated design and their respective roles and services.

Table 16 SR WAN design devices and roles

Platform	Role	Segment Routing	Services
IE8340	Substation Layer 3 Aggregation • Customer Edge • Provider Edge	Enabled on Provider Edge and positioned as a spur	L3VPN • SCADA • IP Telephony • CCTV
IE9300	Substation Layer 2 Aggregation • PRP RedBox	Not Applicable	Layer 2 Aggregation
IE3505, IE5000, IE3400	Substation Layer 2 Switches	Not Applicable	Layer 2 switches
NCS540	Substation Core Devices • Provider Edge • Provider Nodes	Enabled	Segment Routing Transport • Layer 3 Services • Layer 2 Services

L3VPN Services

IR8340 as a Customer Edge Router

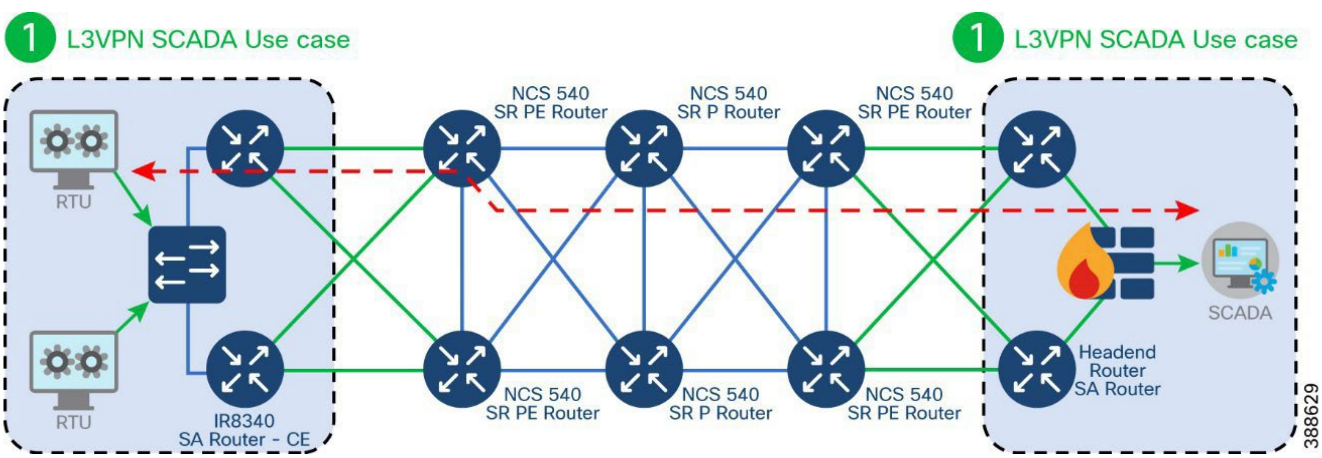
The Cisco Substation Router IR8340 is used as a Customer Edge (CE) router to provide IP based services like SCADA, IP Telephony, CCTV, Network management, etc. using separate VRFs in a Substation LAN network deployment. A Customer Edge router can advertise an IP prefix using any of the following sources:

- **Static configuration**
  Static routing provides the most stable and controlled scenario for the PE-CE interconnect. With static route definitions, there are no opportunities for errant routes to be introduced other than by typing them directly into the configurations. Also, there is less CPU impact with static routes because there is no dynamic routing process to run.

- **A dynamic routing protocol between CE and PE**
  Using a dynamic routing protocol reduces the amount of configuration effort on both the PE and CE routers. Also, changes within the customer's network addressing are readily accommodated and alternate pathing is more easily deployed.

The design guide recommends using routing protocol like eBGP as CE - PE route distribution protocol due to its inherent stability, scalability, and control features. It would also be desirable to use the built-in authentication mechanisms between the neighbors.

Figure 41 IR8340 Substation Router as CE over SR



The network design must accommodate high availability, and the following requirements must be considered:

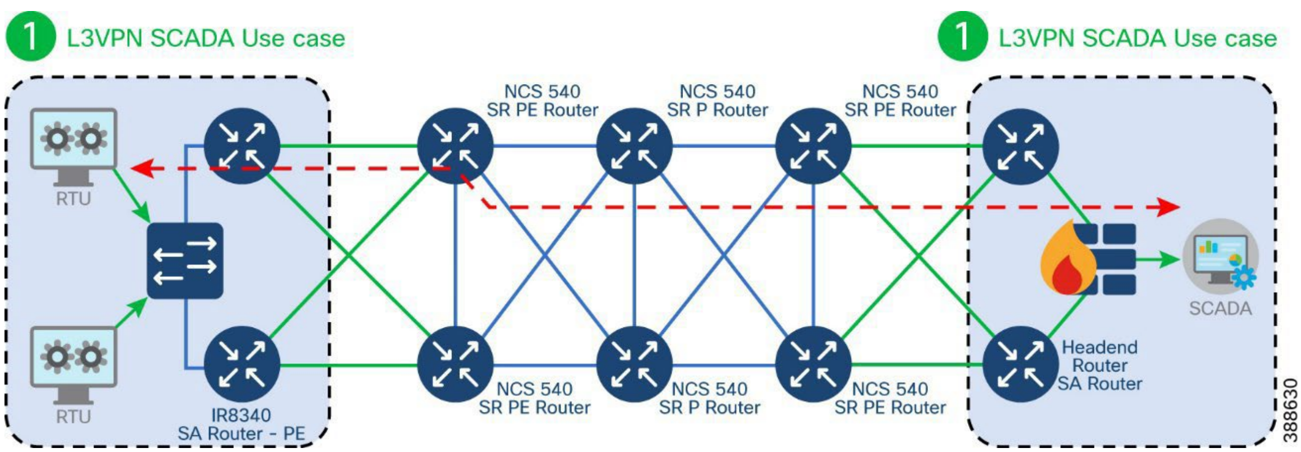
- WAN link redundancy between the substation and the energy control center. Automatic failover is assumed and sub-second convergence is desirable.
- WAN router redundancy if required by the utility customer for critical substations. Automatic failover is assumed and sub-second convergence is desirable.

The guidance is to use appropriate mechanisms provided by BGP for multihoming and load balancing if required. The following links point to some of the options that can be enabled.
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13762-40.html#toc-hld--255936387
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

IR8340 as Segment Routing Enabled Provider Edge

Cisco Substation Router IR8340 supports basic segment routing capability required for it to act as a provider edge node. These capabilities on IR8340 are leveraged to provide Layer 3 services. It is recommended to segment different types of Layer 3 services in a substation using L3VPN. The L3VPN services could be SCADA, Network Management, IPTV for physical security, and so on. It is also recommended to not use IR8340 as part of the segment routing core. The device should be a spur as shown in the following topology. IR8340 does not support segment routing capabilities for Layer2 services like BGP EVPN. The design guide recommends HSRP for first hop resiliency between IR8340 devices.

Figure 42 IR8340 Substation Router as PE over SR



NCS540 as SR enabled PE Router and P Router

The Cisco NCS540, running IOS XR, offers complete feature-rich Segment Routing (SR) by leveraging the MPLS data plane or an IPv6 data plane to forward network packets based on source routing paradigm. SR seamlessly integrates with the rich multi-service capabilities of MPLS, including Layer 3 VPN (L3VPN), Virtual Private Wire Service (VPWS), Virtual Private LAN Service (VPLS), and Ethernet VPN (EVPN). SR requires simple extensions to IGP protocols, for example, IGP or OSPF to provide full intra-domain routing and forwarding over the label switched infrastructure across the core. SR supports Fast Reroute (FRR) capability that enables the activation of a pre-configured backup path within 50 milliseconds of path failure. The validation has been done with SR over MPLS data plane.

The design guide recommends Cisco NCS50 in PE and P roles, leveraging SR transport for technological simplicity and flexibility. TI-LFA FRR can be enabled under IGP for L3VPN services requiring fast convergence to minimize service disruption. To address specific L3VPN services that demand bounds on asymmetry delay, circuit-style segment routing policies can be provisioned to enforce co-routed bidirectional path behavior.

The BGP control plane is leveraged with VPNv4 address family exchange between PE nodes. The design guide suggests integrating a BGP route reflector within the core to enhance simplicity and scalability, as opposed to establishing direct peering among the PEs.

L2 EVPN Service

Ethernet VPN (EVPN) is a solution that provides Ethernet multipoint services over MPLS networks. EVPN contrasts with the existing Virtual Private LAN Service (VPLS) by enabling control-plane based MAC learning in the core. In EVPN, PEs participating in the EVPN instances learn customer MAC routes in control-plane using MP-BGP protocol, as shown in Figure 33. Control-plane MAC learning brings several benefits that allow EVPN to address the VPLS shortcomings, including support for multihoming with per-flow load balancing.

The EVPN-VPWS (E-LINE service) is a BGP control plane solution for establishing an EVPN instance between a pair of PEs for point-to-point layer 2 services. EVPN-VPWS enables forwarding traffic from one network to another without MAC lookup. The PEs run MP-BGP in control plane. EVPN provides the following benefits:

- Integrated Services: Integrated L2 and L3 VPN services, L3VPN-like principles and operational experience for scalability and control, all-active multihoming and PE load-balancing using ECMP, and enables load balancing of traffic to and from CEs that are multihomed to multiple PEs.

- Network Efficiency: Eliminates flood and learn mechanism, fast-reroute, resiliency, and faster reconvergence when the link to dual-homed server fails, optimized Broadcast, Unknown-unicast, Multicast (BUM) traffic delivery.
- Service Flexibility: MPLS data plane encapsulation, support existing and new service types (E-LAN, E-Line), peer PE auto-discovery, and redundancy group auto-sensing.

The following EVPN modes are supported:

- Single-homing - Enables you to connect a customer edge (CE) device to one provider edge (PE) device.
- Multihoming - Enables you to connect a customer edge (CE) device to more than one provider edge (PE) device. Multihoming ensures redundant connectivity. The redundant PE device ensures that there is no traffic disruption when there is a network failure. Following are the types of multihoming:
  - Single-Active - In single-active mode only one PE among a group of PEs attached to the Ethernet-Segment can forward traffic to and from that Ethernet Segment.
  - All-Active - In all-active mode all the PEs attached to the particular Ethernet-Segment is allowed to forward traffic to and from that Ethernet Segment.
  - Port-Active - In this mode, only the PE which is in the active mode sends and receives the traffic. This mode supports single-active redundancy load balancing at the port-level or the interface-level.

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/l2vpn/710x/b-l2vpn-cg-710x-ncs540/evpn-features.html

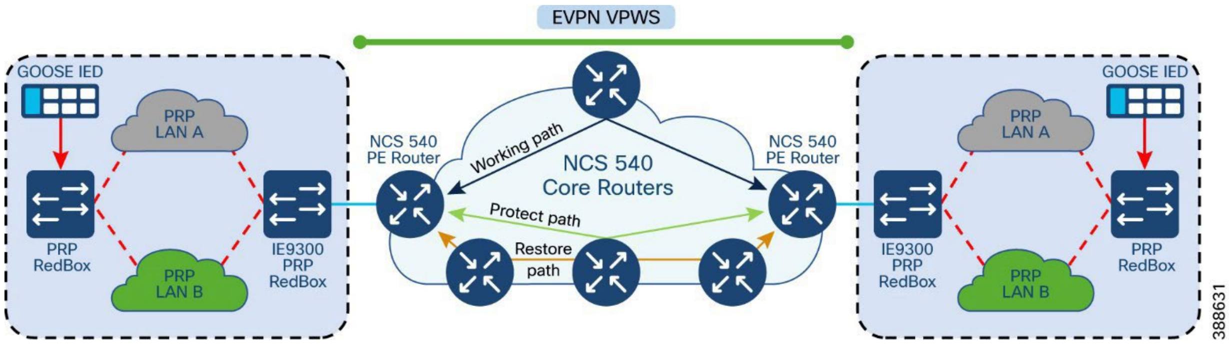
IE9300 as Customer Edge

This document recommends positioning the Cisco IE9300 as Layer 2 Substation LAN aggregation Edge device in BGP L2 EVPN deployment scenarios. IE9300 supports PRP RedBox capability, thus providing an option to connect and aggregate Substation LAN network. IE9300 can be connected as a single home Customer Edge device to the PE.

To address L2 Teleprotection use cases, the design guide recommends provisioning EVPN VPWS service wherein IE9300 is single homed to PE NCS540 at each substation end. Both PRP LAN A and LAN B depict a collection of infrastructure switches either in a star or ring topology deployed to help scale the number of end devices and also transport packets generated by PRP Redbox connected to these LANs thus providing lossless resiliency in case of network failure in any of the PRP LANs.

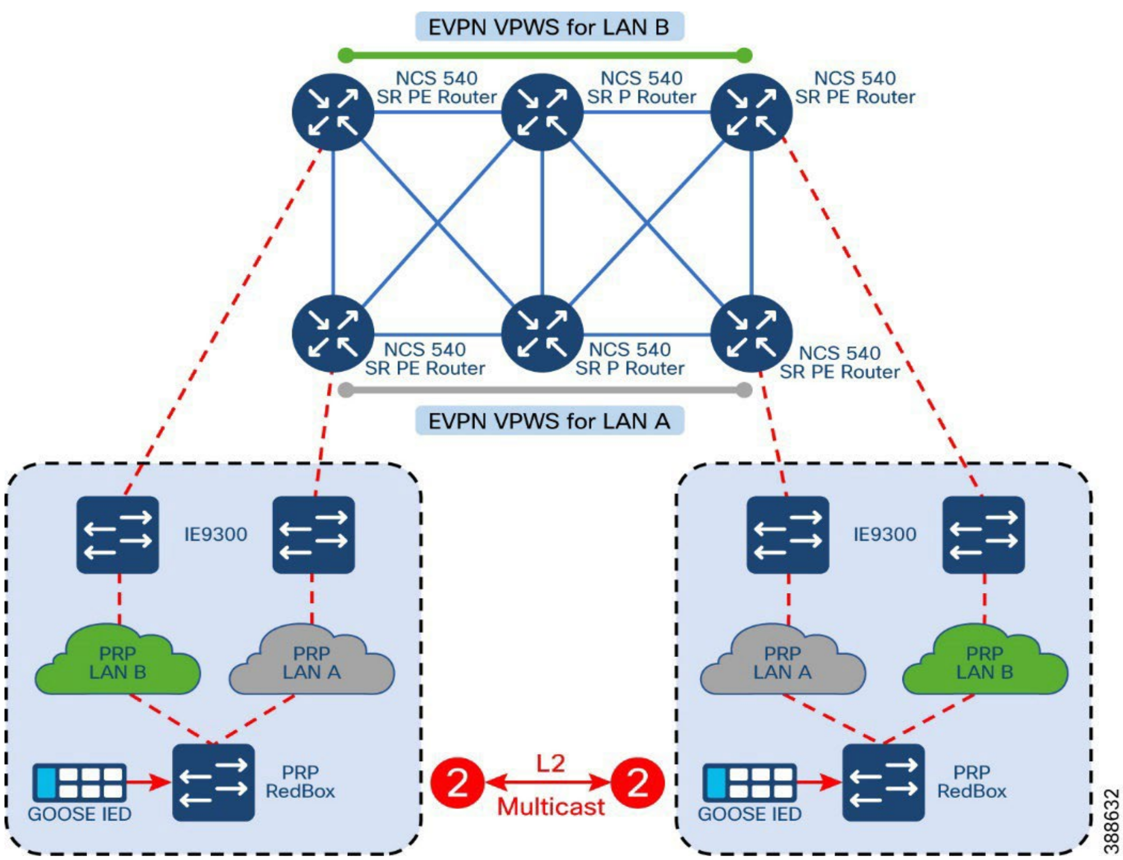
EVPN VPWS Preferred Path steering to an SR-TE Policy feature allows to set the preferred path between the two endpoints for EVPN VPWS pseudowire (PW) as dictated by the SR-TE policy. Utility Teleprotection requirement of co-routed bidirectional path behavior demands the use of CS SR-TE stitched to a single-homed EVPN VPWS service with Preferred Path only. Path predictability is therefore guaranteed with a deterministic next hop PE at the remote end, thereby validating this design.

Figure 43 Standalone IE9300 as L2 Gateway for L2 Teleprotection services with CS - SR



The design guide recommends the following architecture as illustrated in the topology below, to cater to the L2 Teleprotection use case with CE Resiliency, particularly highlighting redundancy for Customer Edge (CE) when needed. In line with the recommendation from the previous design, single homed EVPN VPWS service with Preferred Path steering to a CS SR-TE Policy is the building block for the CE Resiliency architecture design. Each CE is connected to one PRP LAN (LAN A or LAN B, not both). The CE IE9300s are not enabled with PRP redundancy and therefore each CE acts as a plain switch. One EVPN VPWS service extends PRP LAN A between the two substations, while the second EVPN VPWS service extends the PRP LAN B between the two.

Figure 44 Dual IE9300 as L2 Gateway for L2 Teleprotection services with CS - SR



In addition to the L2 Teleprotection use case, the design recommends enabling manageability and reachability to applications such as Cybervision on the IE9300, which is single-homed to the PE NCS540 at each substation end, by utilizing Integrated Routing and Bridging (IRB) on the NCS540. This approach ensures seamless integration and efficient communication between the substation devices and the network.

IRB requires two essential components: a Bridge Virtual Interface (BVI) and a Layer 2 Attachment Circuit (AC) interface. The BVI is a virtual interface within the router that operates like a standard routed interface, providing a gateway for the corresponding bridge-domain to a routed interface within the router. Although the BVI itself does not support bridging, it plays a crucial role in connecting the bridge-domain to the routed network.

To implement this design, the BVI interface should be associated as the Routed Interface on a Bridge Domain on the NCS540. This configuration allows the BVI to act as a gateway, facilitating communication between the Layer 2 and Layer 3 domains. The design further recommends using BGP (L3VPN) protocols to advertise the routes from the BVI to routers present in the WAN or to the Head-End Router (HER). This ensures that the routes are efficiently propagated throughout the network, enabling robust and scalable connectivity.

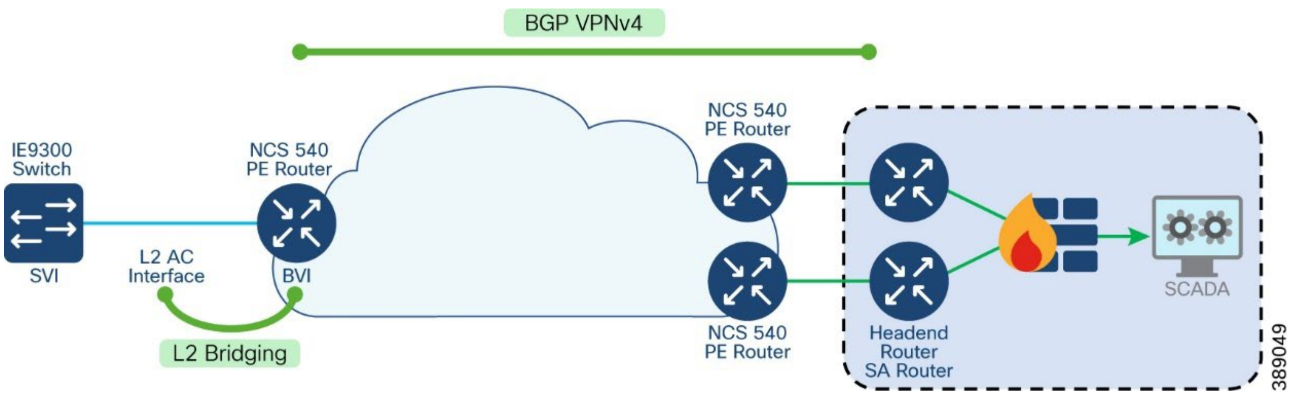
By leveraging IRB on the NCS540, the design achieves a flexible and manageable network architecture that supports both Layer 2 and Layer 3 functionalities. This approach enhances the overall network performance and reliability, ensuring that applications like Cybervision can operate effectively within the substation environment.

For detailed configuration guidance on implementing IRB, please refer to the following configuration guide:

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/interfaces/24xx/b-interfaces-hardware-component-cg-24xx-ncs540/int-routing-bridging.html

This resource provides comprehensive instructions and examples to assist in the successful deployment of IRB on the NCS540.This resource provides comprehensive instructions and examples to help successfully deploy IRB on the NCS540.

Figure: 45 Substation LAN to Control Centre Reachability(L3) via NCS540 WAN using IRB



Layer 2 WAN Substation to Substation for Teleprotection

The solution calls for a re-validation of the SEL ICON Virtual Synchronous Network (VSN) platform over the new Segment Routing enabled WAN.

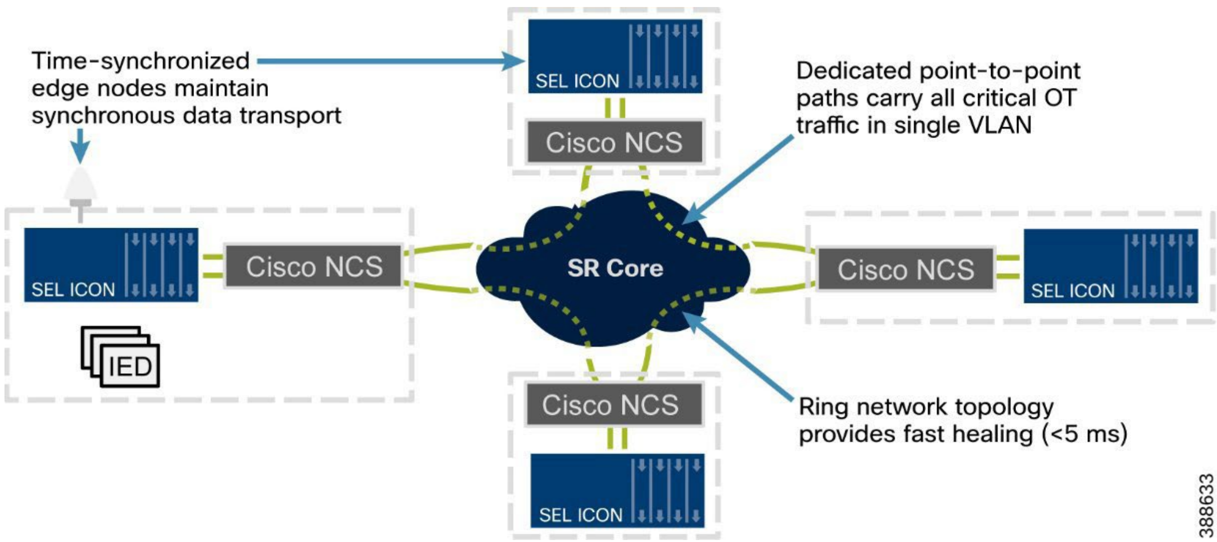
ICON packet transport delivers mission-critical traffic with low and deterministic latency over an Ethernet transport network.

SEL is the Cisco chosen partner to support the low bit rate Teleprotection interfaces. Wide range of interfaces. In the converged mode of operation, the ICON operates as an edge multiplexer with support for all substation circuits (EIA-232, EIA-422, EIA- 485, G.703, 2-wire FXO/FXS, 4-wire voice frequency, direct transfer trip [DTT], IEEE C37.94, and DS1).

ICON deterministic transport uses bidirectional point-to-point links provisioned through Segment Routing enabled core networks combined with an innovative, ultraefficient approach of packetizing TDM data to achieve <1 msec latency, <0.5 msec asymmetry, and <5 msec healing.

The ICON serves as an edge device that interfaces with the core transport routers or switches at 1 GigE. In this converged mode of operation, the ICON network is deployed in traditional ring topologies overlaid on top of the core network, as shown in the following figure.

Figure 46 SEL ICON overlay architecture



Point-to-point bidirectional Ethernet services (E-LINE), traversing static paths are provisioned in the core network between adjacent ICON node line ports. This core requirement allows the ICON network to maintain determinism for both the primary and backup circuit paths, and it alleviates concerns that a core router may arbitrarily reroute ICON traffic onto a path not qualified for maintaining reliable protective relaying communications. When connecting through the core network, a packet delay variation (PDV) setting on the ICON can be adjusted based on the jitter measured through the core network. The PDV setting is a bidirectional link setting. Adjusting the PDV at one end of the VSN link automatically adjusts it at the other end. Such an adjustment eliminates any data communication asymmetry in one direction of the link versus the other.

The following are some motivators for a joint Cisco + SEL ICON solution. SEL ICON provides:

- Demarcation between IT and OT.
- Build core connectivity once (traffic engineering simplified).
- High-speed path restoration (< 5msec).
- Eliminate circuit path asymmetry.
- Time distribution gateway function.
- Real-time circuit latency monitoring.
- Firmware upgrades per card.
- Single C37.94 / 4W / 422 Sync circuit per sub-module (minimizing service interruptions upon firmware upgrades).
- Interoperate and/or replace current channel bank.
- Fully redundant power supplies and line cards.
- ICON edge equipment >20-year life cycle.

The ICON employs a switch-on far-end failure indication (FEFI) mechanism to ensure that the primary or backup path of a circuit remains symmetrical in the event of a unidirectional path failure. That, coupled with a bidirectional PDV link setting, eliminates asymmetry for circuits communicating over the ICON VSN. A bidirectional static path in the core also allows the ICON to perform the healing functionality at the edge. Protection failover (switching performance) of the ICON is less than 5 msec in the event of a path failure.

The core network must offer ICON VSN the highest-priority traffic treatment possible (typically one below the core network NMS) and use strict scheduling rather than round-robin. Strict scheduling minimizes latency fluctuation for VSN traffic in the core, so overall path latency improves by setting a lower PDV value within the ICON. All other Ethernet traffic traversing the core network must have a lower priority treatment than the ICON VSN traffic.

A bidirectional static path (that is, the same path through the core is used for both ingress and egress traffic) is crucial for the ICON VSN to maintain the elimination of asymmetry and to provide high-speed failover.

To preserve the high performance and path determinism of the ICON through a core network of SR enabled routers, the following are provisioning requirements for the services carrying the ICON VSN traffic:

- Bidirectional point-to-point Ethernet static path (tunnel)
- Ethernet access services
  - EVPL support for 10 Mb - 1 Gb throughput for ICON VSN.
  - SM/MM fiber transceiver support
  - Choose appropriate bandwidth interface viz 1G, 10G, 25G, and so on based on the traffic and required priority for different flows. For example, a VSN session requires about 205Mbps of high priority forwarding. The number of such sessions and other traffic decides the type of core interface that is warranted.
  - Services built on top of SR (+ controller)
  - Needed for SEL ICON VSN point-to-point line port connectivity.
  - VSN traffic is L2 Ethernet multicast traffic (like GOOSE) that is sensitive to packet loss, latency, latency variation (PDV)
- Low latency
  - End to end teleprotection applications require no more than 5 msec one-way delay. This includes relay application communication interface (serialization / packetization), ICON VSN, Cisco transport, and fiber propagation delays.
  - The network size will dictate latency experienced by the end customer, but latency budget for lab testing should not exceed 2 msec with the most hops.
- Ultra-fast path failover
  - Needed for TDM and SONET/SDH services.
  - End to end teleprotection applications require no more than 5 msec path recovery on link or node failure.
  - Path failover shall be provided by ICON (unless Cisco transport can offer better than 5 msec path recovery guaranteed, for example a hitless switchover)
- Low path asymmetry
  - End to end teleprotection applications require no more than 0.5 msec path asymmetry. This is the cumulative difference of sum total (relay application communication interface, ICON VSN, Cisco transport, and fiber propagation) one-way forward vs return end-to-end delays.
- HW based QoS implementation
  - Highest-priority traffic treatment
  - Strict scheduling (priority queue)
  - Guaranteed Committed Information Rate (CIR)
  - Ability to cope with traffic congestion.

SEL ICON terminates non-Ethernet connections and interfaces to NCS540 over Ethernet. NCS540s provides Ethernet point-to-point service across the core, interconnecting the SEL ICONs in a ring. EVPN-VPWS service with Preferred Path configuration is steered to an SR-TE policy between each pair of endpoints NCS540 PEs. Teleprotection application specific critical traffic is transported over the dedicated point-to-point path dictated by the SR-TE policy in a single VLAN between the endpoint NCS540s. Because SEL ICON is a synchronous application, it requires a high accuracy time source. GPS and IRIG-B receivers are on the server module and are valid sources for all line module types. The newest line module, EPLM, supports 1588 PTP Telecom Profile G.8275.1. It is recommended to use one of the available timing receivers as a time source.

Network Management

Substation LAN and Cisco Catalyst Center

Cisco Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco Catalyst Center GUI provides network visibility and uses network insights to optimize network performance and deliver an 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 Catalyst 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:

- Catalyst 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 Catalyst 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 Catalyst Center:

- Cisco Catalyst 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 Catalyst Center requires Internet connectivity for licensing information and updates. We recommend 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 Catalyst Center. 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst Center:

- Cisco Catalyst 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 Catalyst Center, nevertheless devices connected behind an industrial firewall can be provisioned and managed by Cisco Catalyst Center.
- Cisco Catalyst Center does not support automated workflows or assurance for resiliency protocols such as PRP, HSR, REP, DLR. Switches can be still discovered by Cisco Catalyst Center and benefit from features such as software upgrades, compliance, and device assurance.
- Cisco Catalyst Center cannot manage products by third-party vendors.

The following list is some of the key features of the Cisco Catalyst Center:

- 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 Catalyst Center
- Monitoring of network devices and endpoint network status, including IACS devices
- Troubleshooting and remediation tools provided by Cisco Catalyst Center
- Network insights
- Security analytics

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

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

- Establish role-based access control in Cisco Catalyst Center, which is required to create users with the right privileges to perform Cisco Catalyst Center tasks introduced in the guide.
- Cisco Catalyst 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 Catalyst 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 Catalyst 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 that 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst SD-WAN Manager

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

- Centralized network and policy management, and operational simplicity, reduce 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.

Cisco Catalyst SD-WAN Solution Overview

This section provides an overview of the Cisco Catalyst 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 SDWAN Manger version 20.8.1.

- The Cisco Catalyst 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 Catalyst SD-WAN solution consist of the Cisco Catalyst SD-WAN Manager network management system (management plane), the Cisco Catalyst SD-WAN controller (control plane), the Cisco Catalyst SD-WAN Validator orchestrator (orchestration plane), and the WAN Edge router (data plane).

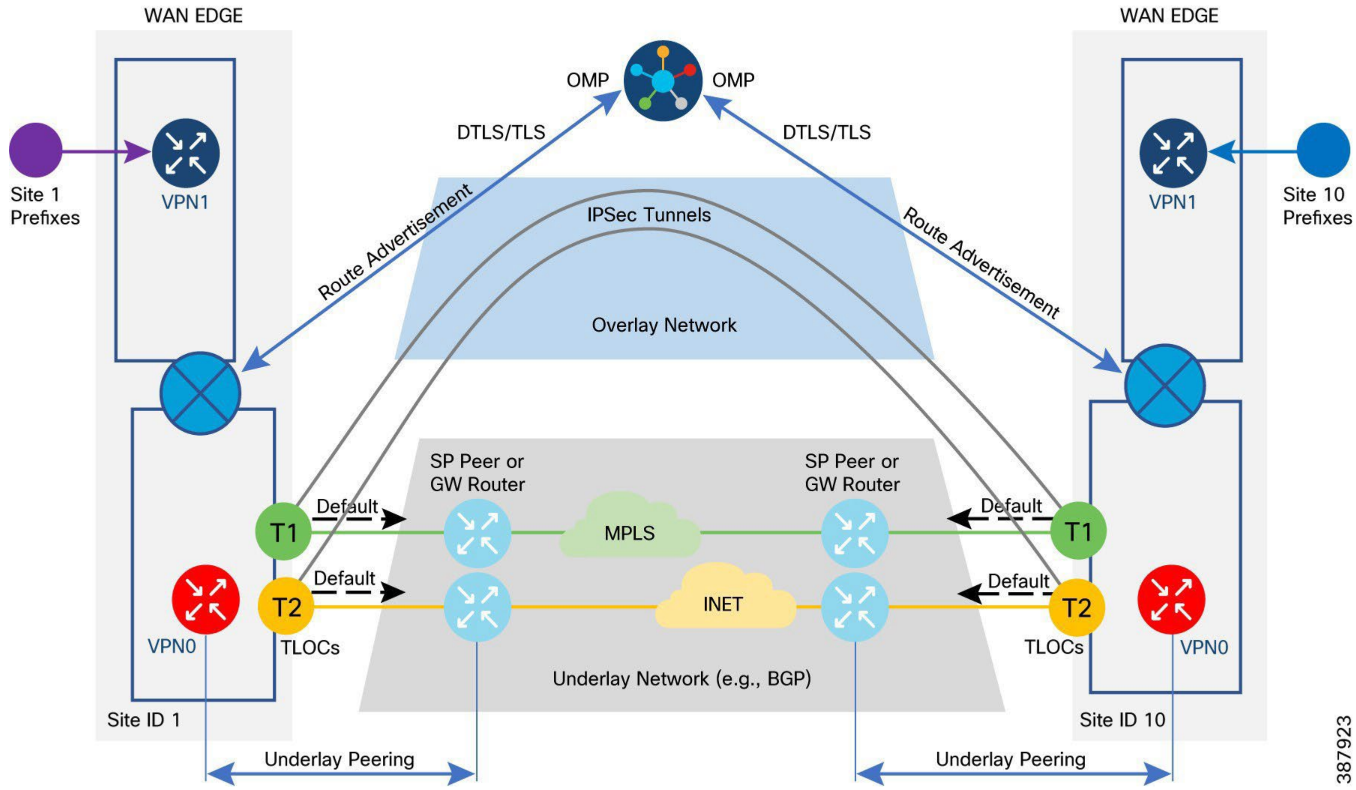
- Cisco Catalyst SD-WAN Manager - This centralized network management system is software-based and provides a GUI interface to easily monitor, configure, and maintain all Cisco SD-WAN devices and their connected links in the underlay and overlay network. It provides a single pane of glass for Day 0, Day 1, and Day 2 operations.
- Cisco Catalyst SD-WAN 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.
- Cisco Catalyst SD-WAN Validator orchestrator - This software-based component performs the initial authentication of WAN Edge devices and orchestrates Cisco Catalyst SD-WAN Controller, Cisco Catalyst SDWAN Manager, and WAN Edge connectivity. It also has an important role in enabling 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 Catalyst 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 47 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 SDWAN Manager 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 Cisco 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.

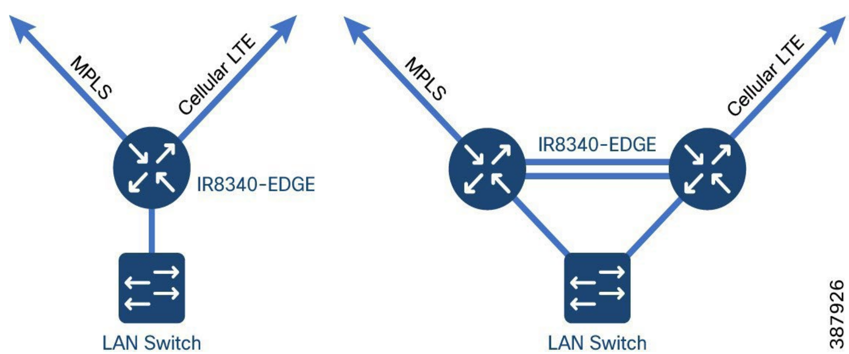
IPsec-encapsulated tunnels encrypt data traffic to other WAN Edge router locations, and BFD sessions are also formed over these tunnels. User traffic originating from the service VPNs is directed to the tunnels. When a transport or link to a transport goes down, BFD times out and the tunnels are brought 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 48 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 Cisco SD-WAN related information.
  - Cisco IR8340 Substation router contacts Cisco Catalyst SD-WAN Validator over a secure tunnel.
  - After authentication, Cisco Catalyst SD-WAN Validator sends the Cisco Catalyst SD-WAN Manager IP and Cisco Catalyst SD-WAN Controller IP address to the Cisco IR8340 Substation Router.

- Cisco Catalyst SD-WAN Manager sends the full configuration to the Cisco IR8340 Substation router.
  - Cisco IR8340 Substation router contacts Cisco Catalyst SD-WAN Controller over a secure tunnel. After authentication, it will join the Cisco 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.

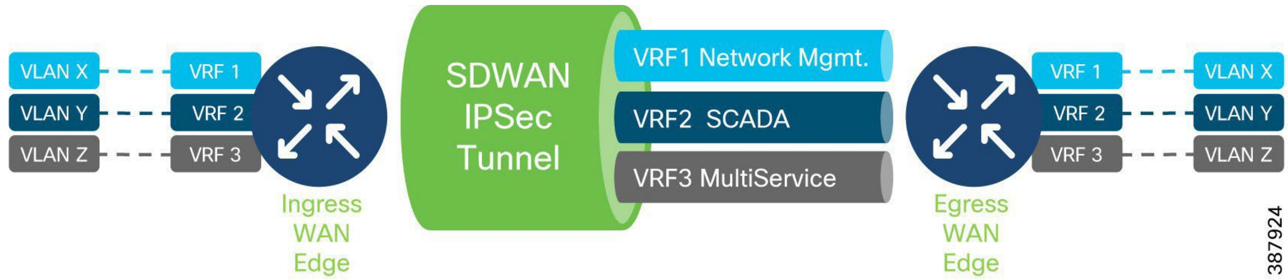
- Onsite BootStrap process
  - Supported on Cisco SD-WAN Cisco IOS XE only. IR8340 runs IOS-XE image. The device can also be onboarded using onsite bootstrap process.
  - Use Cisco Catalyst SD-WAN Manager to generate a configuration file.
  - Copy the configuration file to a bootable USB drive and plug the drive into a device, or copy the configuration to the bootflash of a device.
  - Boot the device.
  - After bootup, Cisco SD-WAN 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 Cisco SDWAN Substation Edge Router and asr1000 series would act as Head End WAN Edge router.
- Traffic should be flowing between substations 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 center. The traffic from the SA LAN can be of different services like SCADA, Network Management, VOIP, Video, and so on forwarded to the control center 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 49 SDWAN WAN Edge VRF Deployments



- WAN Edge routers should exhibit resiliency when one of the WAN backhauls fail. For example, 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 SDWAN Manager.
- 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, and so on, as supported on IR8340 WAN Edge router.

Cisco Crosswork Network Controller

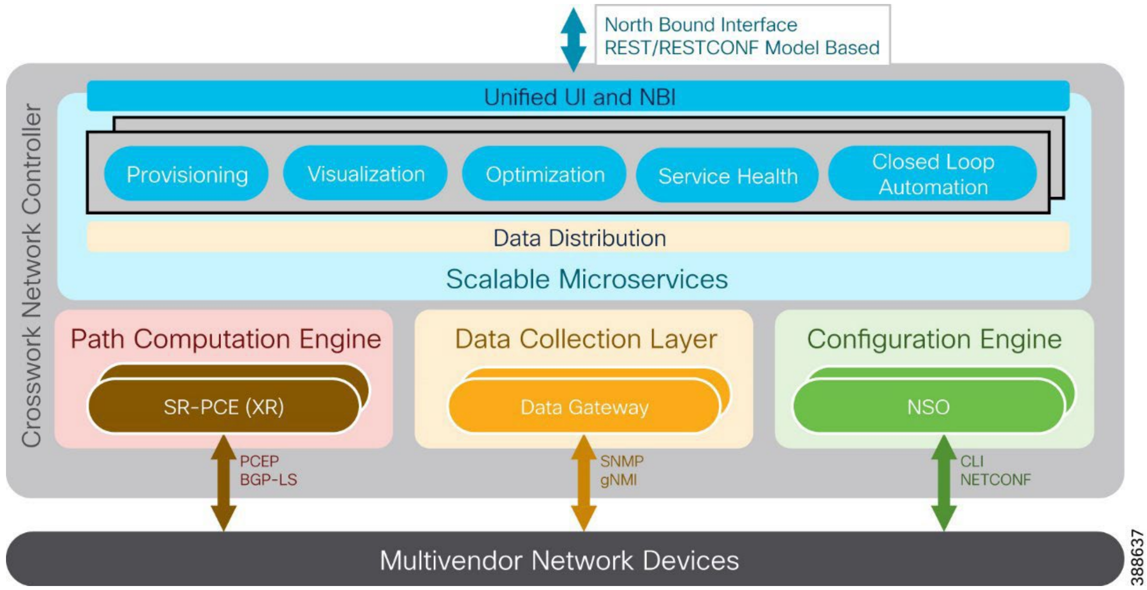
Cisco Crosswork Network Controller (CNC) automation suite offers a unified platform for seamlessly deploying, managing, and monitoring end-to-end transport networks with real-time visibility and control. Crosswork enhances customer experience by enabling real-time visualization of networks, and GUI-driven deployment of policies, VPN services, and traffic engineering with advanced SLAs over multi-vendor & multi-domain transport networks.

The Crosswork Infrastructure is a microservices-based platform, leveraging a cluster architecture to provide scalability and high availability (HA). Cisco Crosswork Data Gateway (CDG) is a foundational component of Crosswork. CDG is responsible for collecting device and interface statistics from the deployed network devices managed by Crosswork. This data is then analyzed and processed by the Crosswork applications, enabling efficient management of the network and adaptation to changes. The number of CDGs required to be deployed in the network is contingent on factors, for example, the number of devices, amount of collected data, network topology, and redundancy requirements.

CNC is Cisco's integrated automation product to effectively manage and operate end-to-end networks that includes key external components, such as Cisco Network Services Orchestrator (NSO), Segment Routing Path Computation Element (SR-PCE):

- **SR-PCE**: The Cisco IOS XR SR-PCE functionality enables real-time reactive feed via BGP-LS/ISIS/OSPF from the deployed topology headend nodes across multiple domains. SR-PCE computes inter-area/domain/AS paths and enforces the computed SR-TE policies.
- **NSO**: NSO facilitates provisioning of services using service packages for VPN - L2VPN, L3VPN and Traffic Engineering Tunnels - SR-TE, SRv6-TE, RSVP-TE, and CS SR. NSO service packages use Network Element Drivers to provision device-level config across various vendors. A comprehensive ecosystem of NEDs is available supporting Cisco and other vendors, allowing for enhanced capabilities in multivendor service provisioning.

Figure 50 Crosswork Network Controller Overview



The essential native Crosswork applications bundled as part of the Essentials package include:

- Crosswork Active Topology: CAT enables topology & service visualization via logical and geographical maps.
- Crosswork Optimization Engine: COE communicates with SR-PCE and NSO providers and makes the information available to Crosswork applications. COE offers real-time network optimization by leveraging SR-PCE and provides a graphical user interface for real-time visualization. The COE solution facilitates SR/SRv6 automation, congestion mitigation, traffic engineering through the user-friendly GUI.

In addition, Crosswork offers advanced applications bundled as the Advantage package:

- Crosswork Service Health: This component overlays a service level view and enables the customer to monitor the health of the services (for example, L2/L3 VPN) based on the rules established.
- Crosswork Health Insights: It performs KPI monitoring, alerting, and troubleshooting. Health Insights facilitates programmable monitoring and analytics by constructing dynamic detection and analytics modules. These modules enable operators to monitor network events and issue alerts based on user-defined logic.
- Crosswork Change Automation: This application automates the process of deploying changes in the network. Orchestration is defined via an embedded Ansible Playbook, followed by configuration changes being pushed to NSO for network deployment.
- Crosswork Zero Touch Provisioning: ZTP streamlines onboarding and provisioning of Day 0 configuration resulting in faster deployment of network devices.
- Element Management Functions: This includes deep inventory collection, alarm management and image management using Inventory, Fault, and Software Image Management (SWIM) functions.

Crosswork Automation solution for deploying and operating transport networks encompasses the following:

- Intent-based Automated Provisioning: Services VPNs (L2 and L3VPN) & Transport SR-TE/SRv6/RSVP-TE
- Dynamic Traffic Engineering: Path Calculation for fine-grained path control and automated real-time optimization, BW aware path control, BW Congestion Detection & Mitigation, Scalable Telemetry collection for BW aware path calc, service and performance monitoring
- Integrated service lifecycle management: visualization demonstrating topology, overlay services & underlay p2p TE paths, automated Service Health Monitoring, Secure Zero Touch Provisioning, Monitoring performance and close loop automation to push changes.

Design Considerations

- When designing a deployment strategy for Crosswork Network Controller (CNC), several key considerations must be addressed to ensure optimal performance, security, and reliability. First, it is essential to choose the applications to be deployed and determine the resources as detailed in the Crosswork Installation Guide.
- Identifying the appropriate topology model for deploying CNC is another critical step, also covered in Crosswork Installation Guide.
- It is vital to have secure firewalls between Crosswork Network Controller and the network devices. However, the firewalls are not provided by Crosswork Network Controller and must be set up separately by the user.
- In terms of network management, devices can be reached either in-band or via out-of-band management interfaces, depending on local security policies.

  In-band management leverages the same IGP/BGP network paths used for regular data traffic, making it cost-effective and simpler to implement as it does not require additional infrastructure. However, this approach can be less reliable since management access is lost if the primary network fails. Additionally, it can introduce potential security risks if management traffic is not properly segmented and secured.

  Conversely, out-of-band management uses a dedicated network separate from the primary data network, offering enhanced reliability and security. This isolation ensures that management access remains available even during network failures and allows for more stringent security measures, protecting management interfaces from potential threats originating from the data network. The trade-off includes higher costs and increased complexity due to the need for additional hardware, such as dedicated management interfaces and separate network infrastructure.

  Ultimately, the decision should be guided by the specific needs of the organization, including network size, security requirements, budget constraints, and the criticality of maintaining uninterrupted management access
- It is crucial to identify the Function Packs to be installed in Network Services Orchestrator (NSO) to meet specific requirements. For example, for Utility WAN L2 Teleprotection use cases, CNC offers the Circuit-Style Manager (CSM) - the Circuit-Style SR-TE Feature Pack, which provides a bandwidth-aware Path Computation Element (PCE) for computing circuit-style SR-TE policy paths. By leveraging centralized bookkeeping of bandwidth resources, CSM enforces computed paths to meet strict bandwidth requirements while ensuring persistent bidirectional co-routed paths with predictable latency. These CS SR-TE policies, including Working/Protect paths and operational statuses, can be visualized on the CNC GUI geographical/logical map, enabling users to monitor bandwidth resource usage and path failover behavior.

For more information, see the following guide: Crosswork Installation Guide

Cisco Provider Connectivity Assurance (PCA) for Utility Networks

The ongoing digital transformation within the utilities sector necessitates a fundamental shift towards highly reliable, secure, and high-performance IP-based connectivity for critical infrastructure points. Traditional network monitoring tools often prove insufficient for this transition, as they lack the capabilities required to meet the stringent network demands of mission-critical Operational Technology (OT) systems such as SCADA, Teleprotection, and inter-substation communications.

The Utility Wide Area Network (WAN) typically comprises a dedicated infrastructure connecting the Transmission Service Operator (TSO) Control Center with various Substations and other field assets. This WAN transports critical services that demand deterministic and predictable network performance to ensure operational continuity and reliability. The consequences of network issues in these environments can range from operational inefficiencies to grid instability and significant safety hazards. Traditional monitoring tools frequently lack the granularity and accuracy required for utility WANs, especially where high reliability and low latency are paramount, making it difficult to detect transient issues or microevents that can impact critical services.

Cisco Provider Connectivity Assurance (PCA) Overview

Cisco Provider Connectivity Assurance (PCA) is a comprehensive solution engineered to address these sophisticated challenges by transforming network management from reactive troubleshooting to proactive optimization. PCA provides continuous verification that the network consistently meets the stringent performance and reliability criteria required by OT services. This continuous assurance is essential for maintaining high availability and low latency, both critical in utility environments where downtime or increased latency can have significant consequences.

PCA offers highly detailed, service-centric visibility with microsecond accuracy and millisecond sampling intervals. This fine granularity enables the detection of short-lived issues that other assurance methods may miss. By continuously monitoring transport services, PCA plays a key role in meeting Service Level Agreements (SLAs) for various OT services, allowing for proactive detection of potential issues before they affect operations, thereby reducing downtime and improving overall network health.

PCA Components and Architecture

PCA architecture is composed of PCA Sensors and PCA Analytics, designed to provide not just raw data, but actionable intelligence.

PCA Sensors

PCA Sensors are designed to generate and collect high-quality service measurements over the transport network using synthetic traffic for continuous service assurance. These sensors can also collect telemetry or time-series data from network devices via the Sensor Collector. The primary sensors used in utility deployments are Sensor SFP modules, available in 1G or 10G form factors. These modules function as standard SFPs but incorporate an internal FPGA that adds a measurement layer to their capabilities.

Sensor SFP Deployment Modes:

- **In-line:** Installed directly in the traffic path (e.g., in a trunk port), replacing another SFP. This mode is suitable for capturing granular throughput measurements.
- **Out-of-line:** Installed in an unused port of a device, with measurements sent via the host side.

Key Sensor SFP Features:

- Hardware Timestamping: Delivers microsecond-level accuracy for precise low-latency measurements.
- Continuous, High-Frequency Synthetic Packet Generation: Enables millisecond-level sampling without overloading the CPU or impacting measurements.
- One-way Metric Support: Accurately detects directional performance issues, unlike round-trip measurements that may mask such problems.
- Measurement of the Real Service Path: Synthetic measurement packets travel alongside actual user traffic using the same CoS, DSCP, or VLAN tags to accurately reflect real network behavior.
- Granular Throughput Measurements: Provides ultra-granular real-time throughput measurement based on L2/L3 user-defined parameters (e.g., VLANs, IPs, DSCP, ports).

PCA Platform

The PCA Platform is typically installed in a centralized location with computing resources (for example., the Control Center). It manages and configures the Assurance Sensors and collects measurement data for streaming to the Analytics platform.

Key PCA Platform Elements:

- Sensor Control: Configures, manages, and collects data from Sensor SFP/Modules.
- PCA Sensor Management UI: Part of the PCA platform, used to configure PCA devices, create and manage performance sessions, and process KPIs.
- Sensor Collector: Acts as a proxy between sensors and PCA Analytics to facilitate split domains (on-prem sensors, cloud analytics) or as a gateway in full on-prem solutions.
- Other Software (Docker Container) Sensor Agents: (Not detailed in this design, but available) Include Actuate TWAMP/ICMP Echo, Telemetry Collector, Transfer (DNS, HTTP, port), Trace (traceroute), and TCP Throughput (RFC 6349).

PCA Analytics

PCA Analytics transforms raw data from the sensors into meaningful information to assist in day-to-day operations. It provides near real-time visibility, correlating performance assurance information from PCA Sensors with contextual metadata to provide insights for reporting, analysis, and troubleshooting. Ingested data is enriched with contextual information relevant to utility needs, such as service type (SCADA, GOOSE, Teleprotection), substation information (geo-coordinates, region, city, site), equipment information (model, type, vendor), connectivity details (fiber, leased line), and other business or operational related information (site maintenance company, business criticality).

This metadata is extensively used for filtering, grouping, aggregation, and correlation to identify commonalities for root cause analysis and troubleshooting. It also adds flexibility for multiple reporting scenarios and personalized dashboards for different personas (for example, engineering, operations). The PCA Analytics platform is available as a SaaS offering hosted in the cloud or as an on-premise deployment.

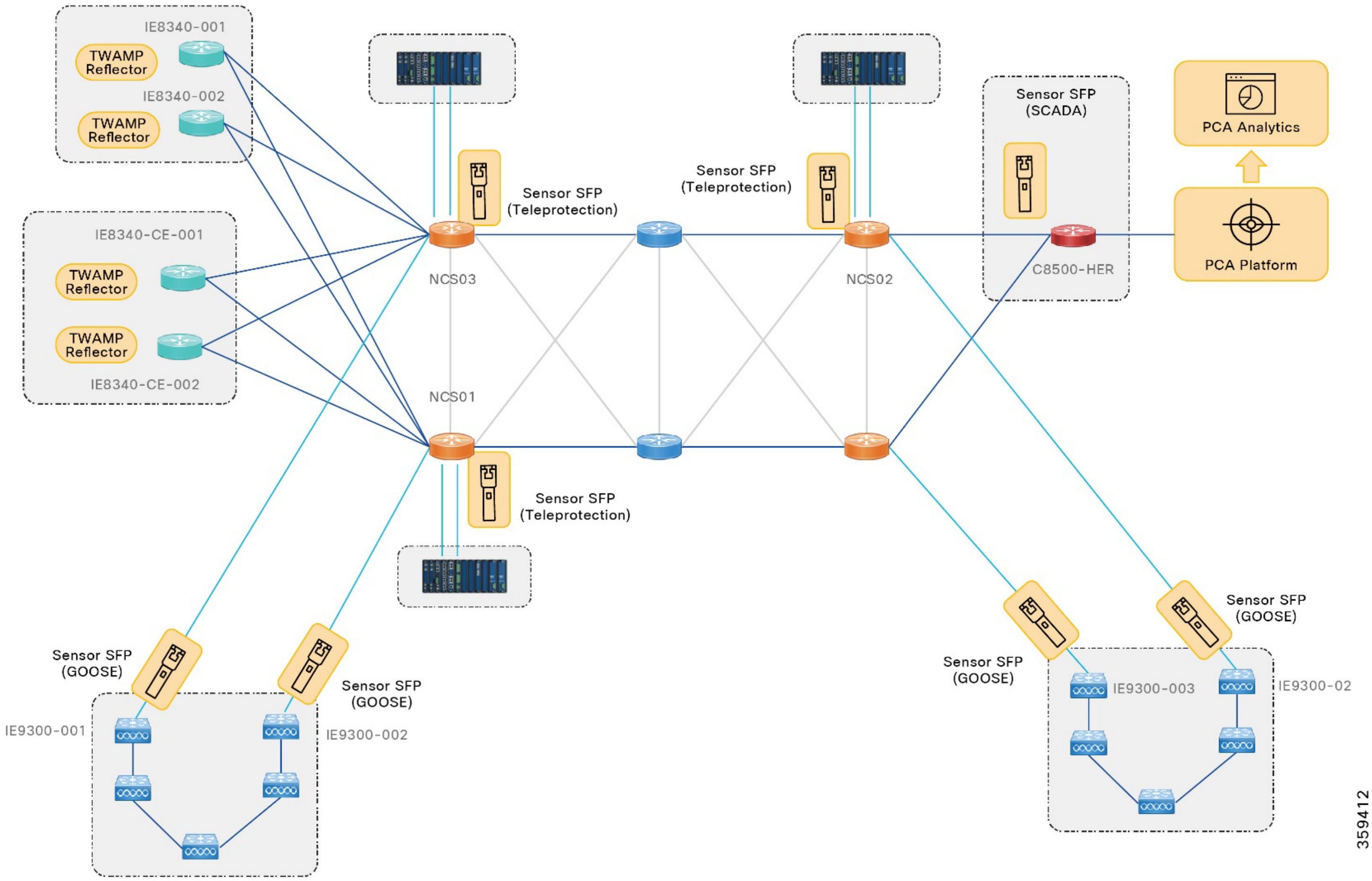
Supported Protocols and Capabilities

PCA leverages well-known and widely used standard protocols for network assurance:

- TWAMP (RFC 5257): Used for Layer-3 measurements.
- Y.1731: Used for Layer-2 measurements (ETH-DM).

PCA extends beyond standard implementations by providing a broader set of Key Performance Indicators (KPIs) and deeper insights. This enables utilities to benefit from granular assurance while leveraging existing capabilities in their own infrastructure (for example, using TWAMP reflector capabilities already present in most routers like Cisco Catalyst IR8340 or NCS540).

Figure 51 PCA Components and Usecases



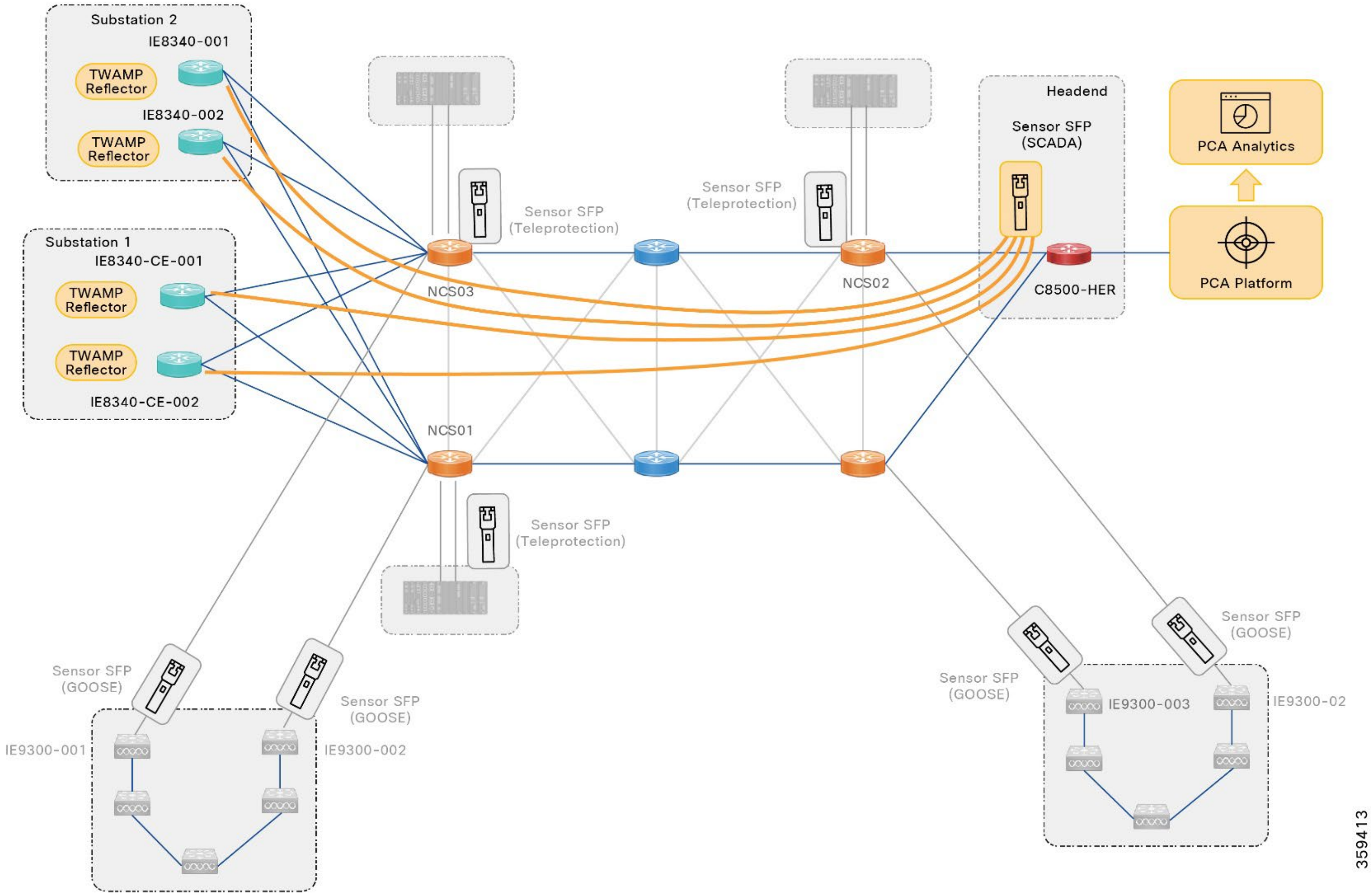
Key Use Cases and Deployment Examples

PCA is used to monitor transport paths connecting the TSO Control Center and Transmission Substations, regardless of whether the service connectivity is on-net (utility-owned MPLS/IP network) or off-net (public backhaul, leased line, cellular backhaul), and irrespective of the service protocol (L2 or L3 VPN). This design focuses on the assurance of three critical and low-latency services transported across the network:

SCADA Use Case

- Service Type: Hub-and-spoke connectivity over Layer-3 from the Control Center to all substation RTU locations across the MPLS backbone.
- Assurance Method: Layer-3 TWAMP performance sessions are deployed.
- Sensor Placement: Sensor SFPs are installed in an out-of-line mode in a Headend router at the Control Center.
- Measurement Target: TWAMP sessions are configured towards TWAMP reflectors in the SCADA routers of each substation.
- Configuration: TWAMP sessions can be configured to travel with the SCADA traffic using the same VLAN and DSCP or TOS marking to accurately reflect real service performance.

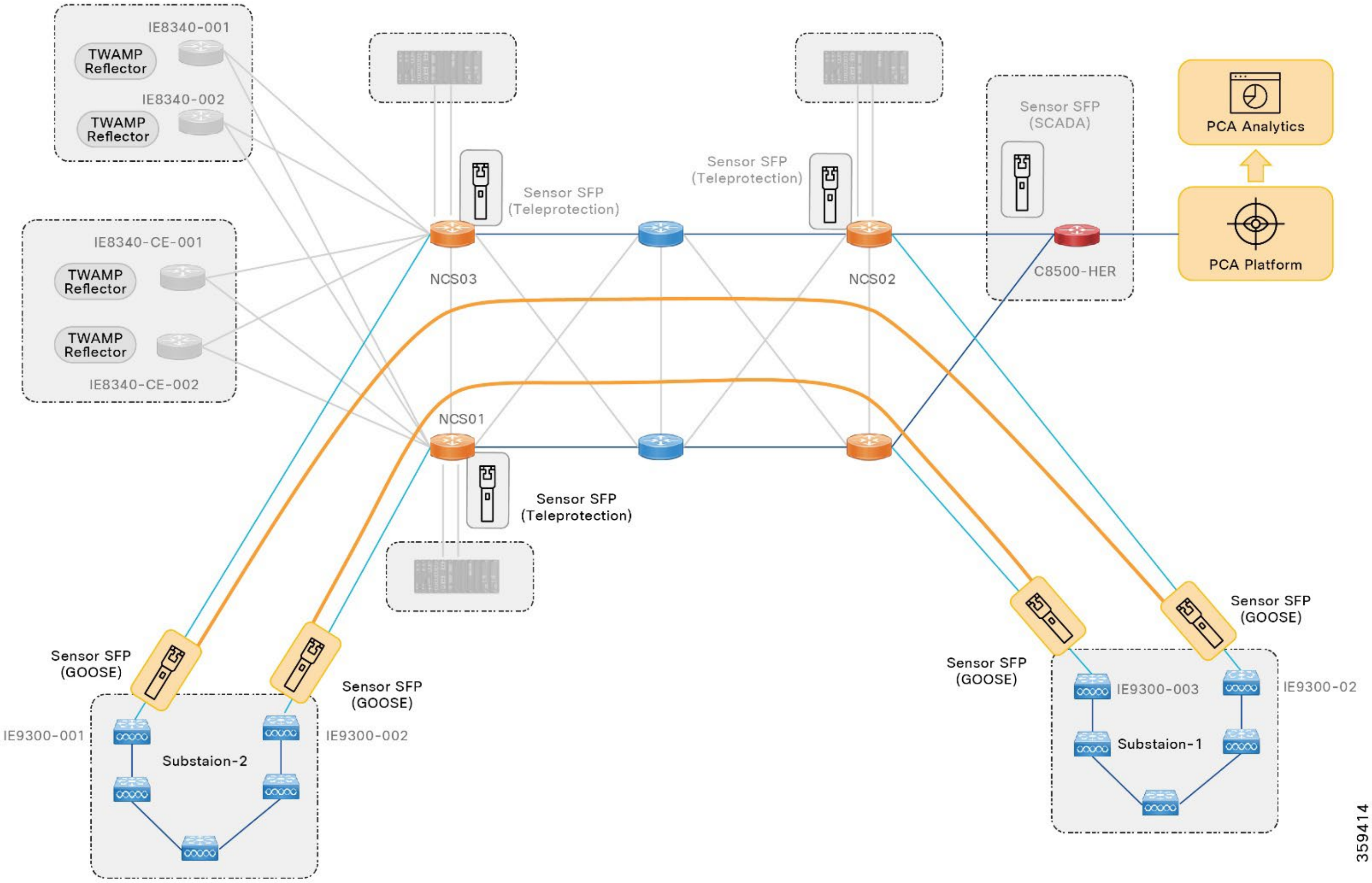
Figure 52 PCA SCADA L3VPN



GOOSE Use Case

- Service Type: Assurance of Layer-2 low-latency traffic between Substations.
- Assurance Method: Layer-2 ETH-DM Y.1731 sessions are configured to monitor the connectivity of L2VPNs between substations, providing latency, jitter, and packet loss KPIs.
- Sensor Placement: Sensor SFPs are placed in-line in a trunk port connecting the substation switch with the WAN router (e.g., NCS).
- Additional Capability: In-line placement allows for granular per-flow throughput measurements of the links.

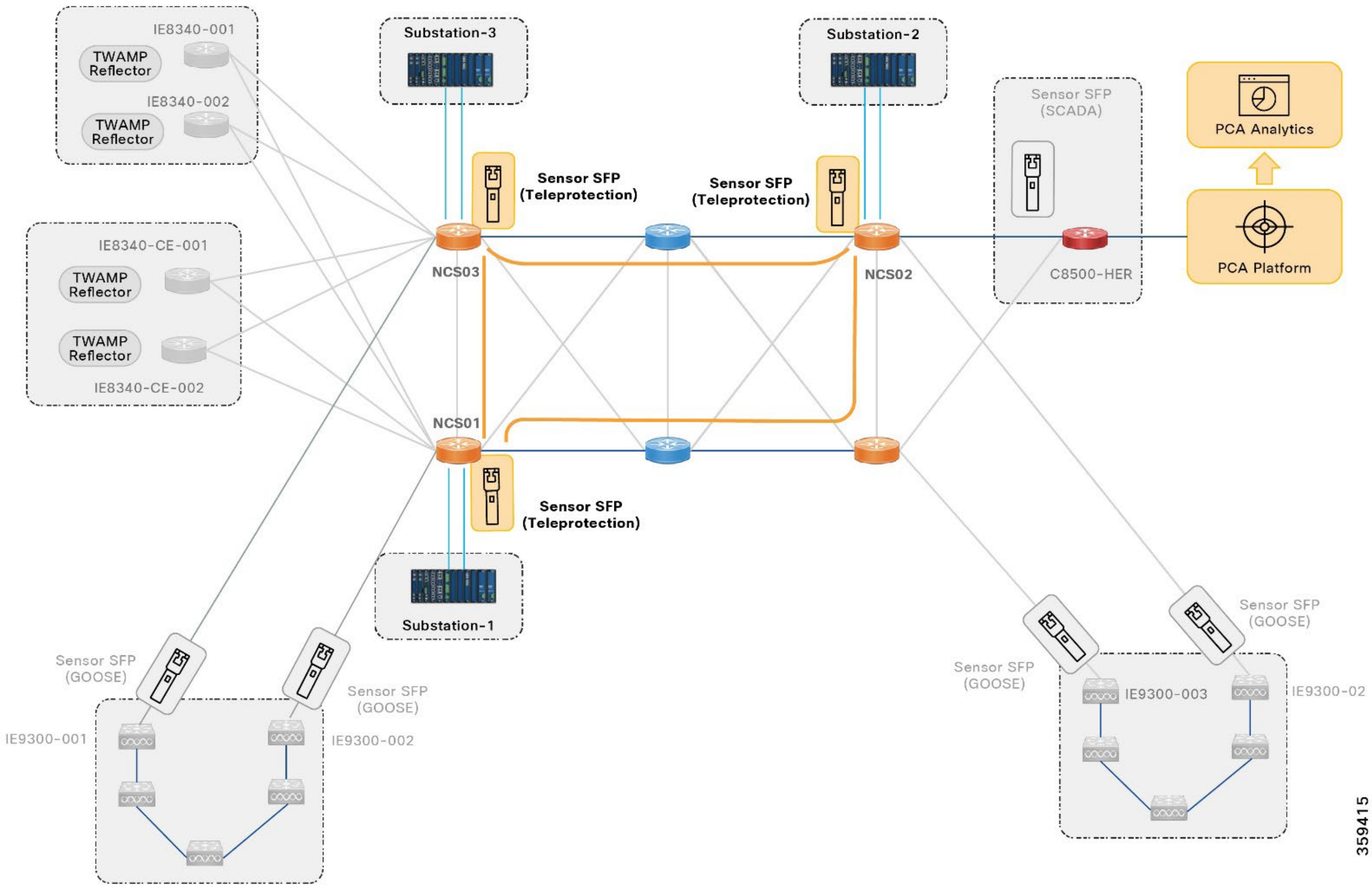
Figure 53 PCA GOOSE



Teleprotection Use Case

- Service Type: Hop-by-hop monitoring of the Layer-2 Ring topology used by Teleprotection traffic, requiring strict low-latency and high availability.
- Assurance Method: Layer-2 ETH-DM sessions are used for monitoring.
- Sensor Placement: Sensor SFPs are placed in an out-of-line mode in a port of the NCS routers that connect the SEL ICON with the WAN.

Figure 54 PCA Teleprotection



Optional Service Extensions

Assurance can also be extended to new emerging services or other services that, while not critical, fall under the transport team's responsibility. Extending assurance to these services can help the transport team improve quality and increase operational efficiency. Examples include:

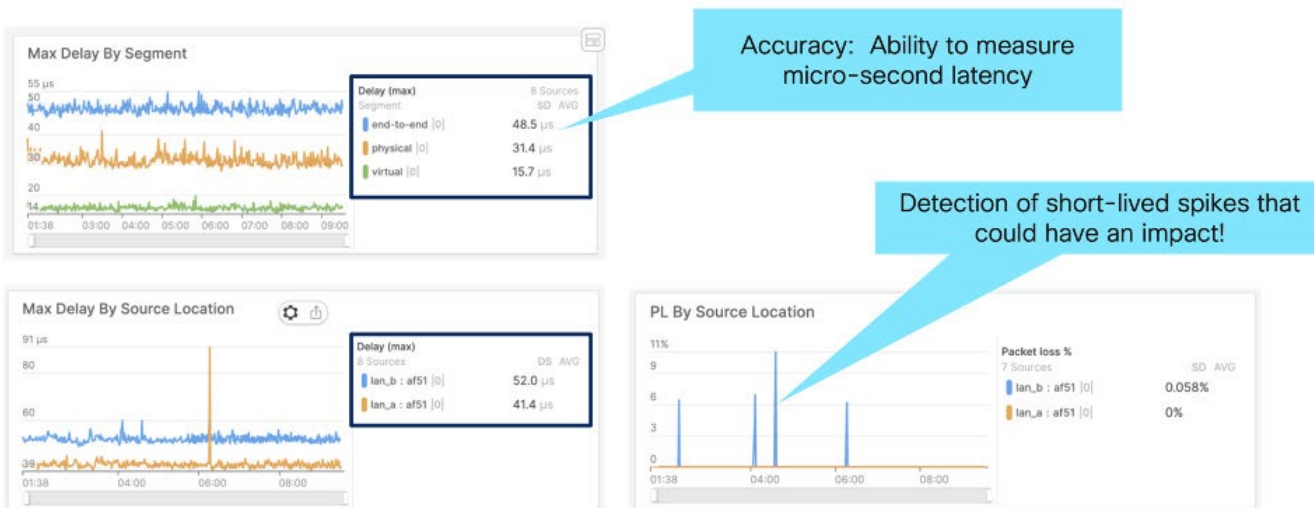
- Corporate traffic (data, video, IP voice)
- AMI (Smart metering data from aggregation point to a datacenter)
- IP CCTV

Critical Design Considerations for Cisco PCA in Utility Networks

- Sensor SFP Placement and Mode:
  - **In-line vs. Out-of-line:** Determine the appropriate deployment mode for Sensor SFPs based on the specific use case and desired measurements.
    1. **In-line:** Required for granular per-flow throughput measurements and direct traffic path monitoring (e.g., GOOSE use case for L2VPNs). This replaces an existing SFP.
    2. **Out-of-line:** Suitable for monitoring services without interrupting the primary traffic path, utilizing an unused port (e.g., SCADA, Teleprotection use cases).
  - **Location:** Strategically place Sensor SFPs at critical points in the network, such as Headend routers (for SCADA), substation switches connecting to the WAN (for GOOSE), or routers connecting OT equipment to the WAN (for Teleprotection).
  - **Form Factor:** Ensure compatibility with existing network equipment (1G or 10G Sensor SFP form factors).

- Service-Specific Measurement Requirements:
  - **Protocol Selection:** Choose the appropriate standard protocol (TWAMP for Layer-3, Y.1731 for Layer-2) based on the service being monitored.
  - **Traffic Path Emulation:** Configure synthetic measurement packets to travel with the actual user traffic using the same CoS, DSCP, or VLAN tags to accurately reflect real network behavior and performance.
  - **One-way vs. Round-trip:** Leverage one-way metric support for accurate detection of directional performance issues, which round-trip measurements might mask.
  - **Granularity and Accuracy:** Design for microsecond-level accuracy and millisecond sampling intervals to detect short-lived issues critical for OT environments.

Figure 55 **PCA Granular Assurance capabilities**



- Integration with Existing Network Infrastructure:
  - **TWAMP Reflector Capabilities:** Utilize existing TWAMP reflector capabilities in routers (e.g., Cisco IR or NCS family) to minimize the need for additional hardware at remote sites for Layer-3 measurements.
  - **Network Device Compatibility:** Ensure Sensor SFP compatibility with the host devices (routers, switches) where they will be installed.

- PCA Platform and Analytics Deployment:
  - Centralized PCA Platform Location: The PCA platform (Sensor Control, Sensor Management UI) requires a centralized location with adequate computing resources, typically in the Control Center.
  - Analytics Deployment Model: Decide between SaaS (cloud-hosted) or on-premise deployment for PCA Analytics based on organizational preference, security policies, and connectivity requirements.
  - Sensor Collector Role: If Analytics is cloud-based and sensors are on-premise, deploy the Sensor Collector as a proxy/gateway to facilitate data streaming.

- Metadata Strategy for Actionable Intelligence:
  - Contextual Enrichment: Plan for comprehensive metadata enrichment (e.g., service type, substation info, equipment info, business criticality) to enable effective filtering, grouping, aggregation, correlation, and personalized dashboards for different operational personas.
  - Data Ingestion and Management: Consider how metadata will be ingested and managed within the PCA Analytics platform to maximize its value for reporting, analysis, and troubleshooting.

- Network Impact and Resource Management:
    - Synthetic Traffic Overhead: While designed to be lightweight, consider the cumulative overhead of continuous synthetic packet generation on network links, especially in highly constrained environments.
    - CPU/Resource Impact: Ensure that the synthetic traffic generation does not overload device CPUs or impact the performance of critical services. Sensor SFPs are designed to offload this, but overall system impact should be considered.

- Scalability and Future-Proofing:
    - Service Expansion: Design the PCA deployment to be extensible, allowing for easy addition of assurance for new emerging services or other non-critical services as organizational needs evolve.
    - Network Growth: Consider the future growth of the utility network and ensure the PCA architecture can scale to accommodate additional substations, field assets, and services.

Benefits and Value Proposition

Implementing a robust and reliable assurance mechanism like Cisco PCA provides significant benefits for utility networks:

- Proactive Issue Detection: Detects potential issues before they impact operations, reducing downtime.
- Enhanced Grid Stability: Ensures operational continuity and reliability for critical OT services.
- SLA Compliance: Continuously verifies network performance against stringent SLAs.
- Actionable Intelligence: Transforms raw data into meaningful insights for reporting, analysis, and troubleshooting.
- Improved Operational Efficiency: Streamlines network management and reduces reactive troubleshooting efforts.
- Protection of Critical Infrastructure: Safeguards vital utility assets and services.
- Uninterrupted Service Delivery: Contributes to reliable service delivery to customers.

Network Management Summary

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

- Centralized network and policy management, and operational simplicity, reduce 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 bullets describe Cisco Catalyst 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.

Cisco CNC automation suite offers a simplified network management platform for seamlessly managing end-to-end transport networks with real-time visibility and control. Aligned with Utility WAN transport networks, CNC encompasses the following:

- Centralized network management with Intent-based Automated Provisioning for Services VPNs (L2VPN and L3VPN) and Transport SR-TE/SRv6/RSVP-TE. CNC offers dynamic traffic engineering with path calculation for fine-grained path control and automated real-time optimization.
- Integrated service lifecycle management with visualization demonstrating topology, overlay services & underlay p2p TE paths, automated service health monitoring.
- In line with requirements for Utility WAN Teleprotection applications, CNC offers the capability to compute CS SR-TE policy paths with sub-50ms convergence. Herein, the COE provides the Segment Routing Path Computation Element (SR-PCE) that is bandwidth-aware to compute and provision CS SR-TE policy paths.

Cisco PCA is a comprehensive solution designed to ensure the reliability and performance of critical IP-based connectivity for Operational Technology (OT) systems in utility networks.

- Core Purpose: Proactively assures network performance for mission-critical OT services (SCADA, GOOSE, Teleprotection) by transforming reactive monitoring into predictive optimization.
- Addresses Key Challenges: Overcomes limitations of traditional monitoring tools by providing ultra-granular, high-accuracy visibility (microsecond precision, millisecond sampling) crucial for detecting transient issues in utility WANs.
- Key Components:
  - **PCA Sensors (Sensor SFPs):** Hardware-based modules (1G/10G) for precise synthetic traffic generation and measurement, deployable in-line or out-of-line.
  - **PCA Platform:** Centralized management for sensor configuration and data collection.
  - **PCA Analytics:** Transforms raw data into actionable intelligence through contextual enrichment (metadata) for advanced visualization, reporting, and troubleshooting.
- Measurement Capabilities: Leverages standard protocols (TWAMP for L3, Y.1731 for L2) with enhanced features like hardware timestamping, one-way metric support, and real service path emulation.

- Primary Benefits:
  - Proactive issue detection and reduced downtime.
  - Enhanced grid stability and operational continuity.
  - Guaranteed SLA compliance for critical services.
  - Improved operational efficiency and informed decision-making.
  - Protection of critical infrastructure and uninterrupted service delivery.

Conclusions

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

- Ethernet in the electronic security perimeter (ESP) zone
- Substation Primary Reference Timing Clock Design.
- Cisco Provider Connectivity Assurance
- The new Cisco IE 9300 and IR8340.
- Evolution of Utility owned WAN network design using segment routing.
- NCS540 as segment routing capable routers.
- Cisco Crosswork Network Controller for managing utility owned segment routing enabled WAN network.
- 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 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 17 lists the acronyms and initialisms that may have been used in this SA CVD version 3.3:

Table 17 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 17 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
PCA	Provider Connectivity Assurance
PCP	Priority Code Point
PI	(Cisco) Prime Infrastructure

Table 17 Acronyms (continued)

Acronym	Definition
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PoE	Power Over Ethernet
PRP	Parallel Redundancy Protocol
PRTC	Primacy Reference Time Clock
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
SR	Segment Routing
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