Cisco Substation Automation Utility WAN

Cisco Solution Guide

November, 2023

Contents

Substation Automation Architecture 3

New Infrastructure: More Capability, Higher Performance, Smaller Footprint 4

Evolution to Segment Routing and EVPN 5

Benefits of Segment Routing 5

Circuit-Style Routing 6

EVPN 7

IEC61850 8

Teleprotection Overview 9

Network Requirements 12

Path Symmetry 12

What Contributes to Delays in Network Communications? 13

Architecture 14

Substation Automation Validated Design 17

Cisco Substation Automation Reference Architecture 19

SDN Converged Transport Network 19

Summary 21

Use Cases 22

Layer 3 Substation to Datacenter 22

Layer 2 substation to substation 23

Layer 2 substation to substation for Teleprotection 23

Transport Network Considerations 24

SEL ICON Timing 25

Summary of Substation Use Cases 26

Layer 3 Use Cases 26

Layer 2 Use Cases 27

Conclusion 29

References 29

Substation Automation Architecture

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. With this solution, the network infrastructure can support more devices and handle more bandwidth with more resiliency and capabilities, supporting advanced services such as time synchronization and hosting virtualized 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 Substation Automation solution helps utilities overcome the following challenges:

- A growing number of process and station bus devices with higher bandwidth requirements
- Limited space in substations for equipment
- The 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
- The need to scale to support more substations

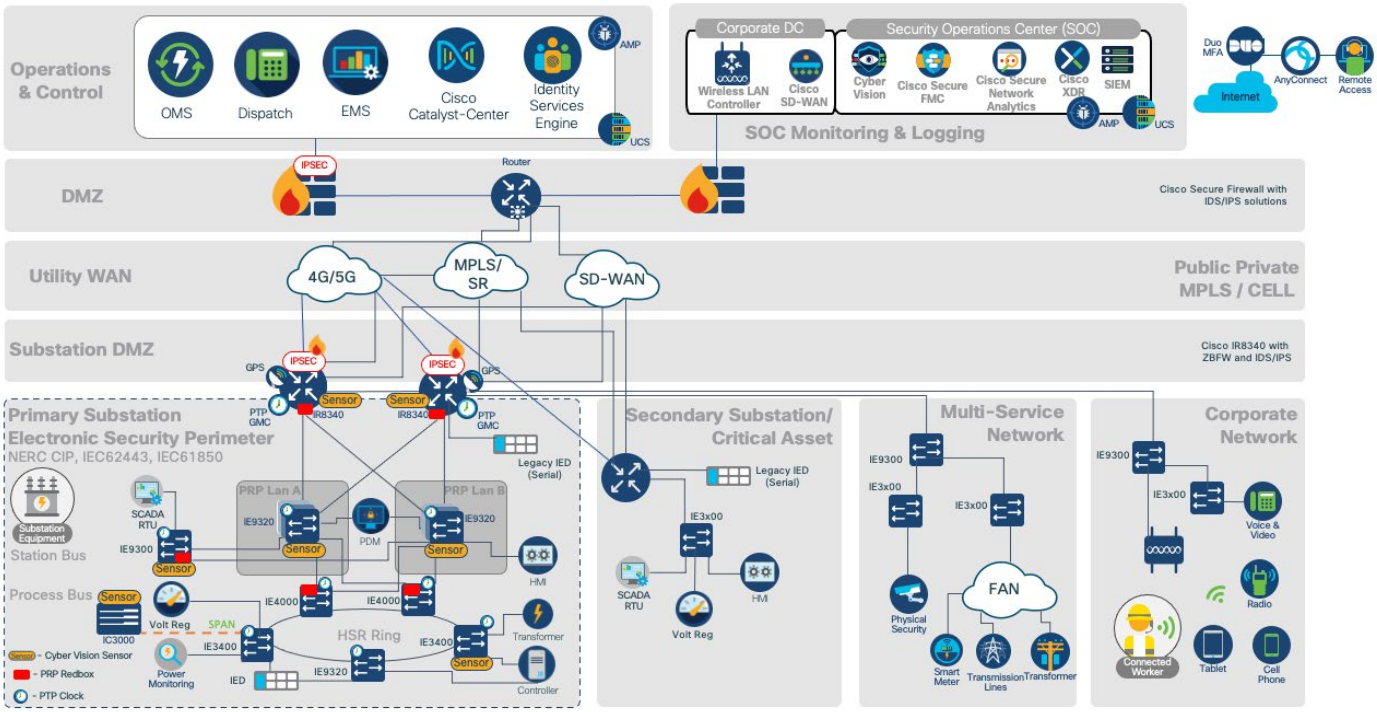
The Substation Automation solution helps utilities overcome these challenges and lays the foundation for more reliable, sustainable, and efficient grid operations at a lower cost. Key features of this solution include:

- More ports and faster speeds: Introduction of the IEC 61850-3 and IEEE 1613 compliant Cisco Catalyst IE9300 Rugged Series switches with 28 Gigabit Ethernet fiber ports for secure, reliable, low-latency station and process bus communication
- Higher density: Backplane is stackable up to eight units
- Greater reliability: Support for a range of resiliency and synchronization protocols
- Multifunctional router: Introduction of IEC 61850-3 and IEEE 1613 certified Cisco Catalyst IR8340 and IR1101 rugged routers for a combination of scalable WAN connectivity, firewall security, and application hosting in a variety of substations
- Reliability: Support for a range of resiliency and synchronization protocols
- Greater security: Support for a range of features, including zone-based firewall and IPS/IDS, Cisco Trustsec, IEEE 802.1x Network Access Control, Cisco Trustworthy features (secure boot, signed firmware and SUDI), visibility of Substation Automation devices and traffic flows with Cisco Cybervision, and MACsec for local link encryption
- Flexibility: Highly modular platforms to support switching, routing, synchronization, and edge compute needs
- Availability: Support for lossless network topologies and protocols, such as High-Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP)
- Precision: Support for substation-wide time synchronization, for example, the 2017 IEEE Precision Time Protocol-Power Profile
- Critical functions: Support for substation communications, such as IEC 61850, Modbus, IEC 60870-5-104 (IEC 104), and Distributed Network Protocol 3 (DNP3)

- Simplicity: A range of management options, including Cisco DNA Center for switching and Cisco Catalyst SD-WAN Manager for SD-WAN routing capabilities

The following sections provide an overview of the key additions to the solution: the new infrastructure, new network management options (Cisco Catalyst Center, and Cisco SD-WAN Manager for Cisco Catalyst SD-WAN), cybersecurity updates, and a review of the new Substation Automation reference architecture.

Figure 1. Substation Automation Architecture



New Infrastructure: More Capability, Higher Performance, Smaller Footprint

The Substation Automation solution includes an enhanced network infrastructure for modern grid and substation automation. The addition of new industrial routers and switches helps utilities improve grid operations and security and reduce costs. The new infrastructure supports more features, more connectivity, higher performance, and more management options than the previous network infrastructure in a similar or smaller footprint and with fewer boxes. This solution enables utilities to connect more devices with higher bandwidth requirements, support more resilient topologies, improve cybersecurity, and more easily deploy and manage their networks at scale and with lower operating costs.

The key additions to the network infrastructure include the Cisco Catalyst IE9300 Rugged Series Switches and Cisco Catalyst IR8340 Rugged Series Router for primary substation networks. Each device supports utility-specific features, including:

- IEC 61850-3, IEEE 1613, and IEC 62443 certifications
- IEEE1588 Precision Time Protocol—Power Profile (2017)
- IEC62439-3 HSR and PRP lossless resiliency protocols

The solution also now supports the Cisco IR1100 Rugged Series router to interconnect secondary substations and monitor distributed critical assets in the field.

Evolution to Segment Routing and EVPN

Before segment routing, multiprotocol label switching (MPLS) packets were forwarded by using label switching instead of IP-based routing, which means that the routers forwarded traffic based on the label and not the destination IP address. This approach required the "edge" PE routers to perform only an IP lookup, while intermediate "core" routers performed only a label lookup, which is faster.

Unfortunately, MPLS didn't remove complexity from an existing network. In fact, it added more complexity through additional protocols and each MPLS node requiring the state to be synchronized across the entire network. As the size of networks grew, so did the state and complexity, making the network more difficult to operate and manage.

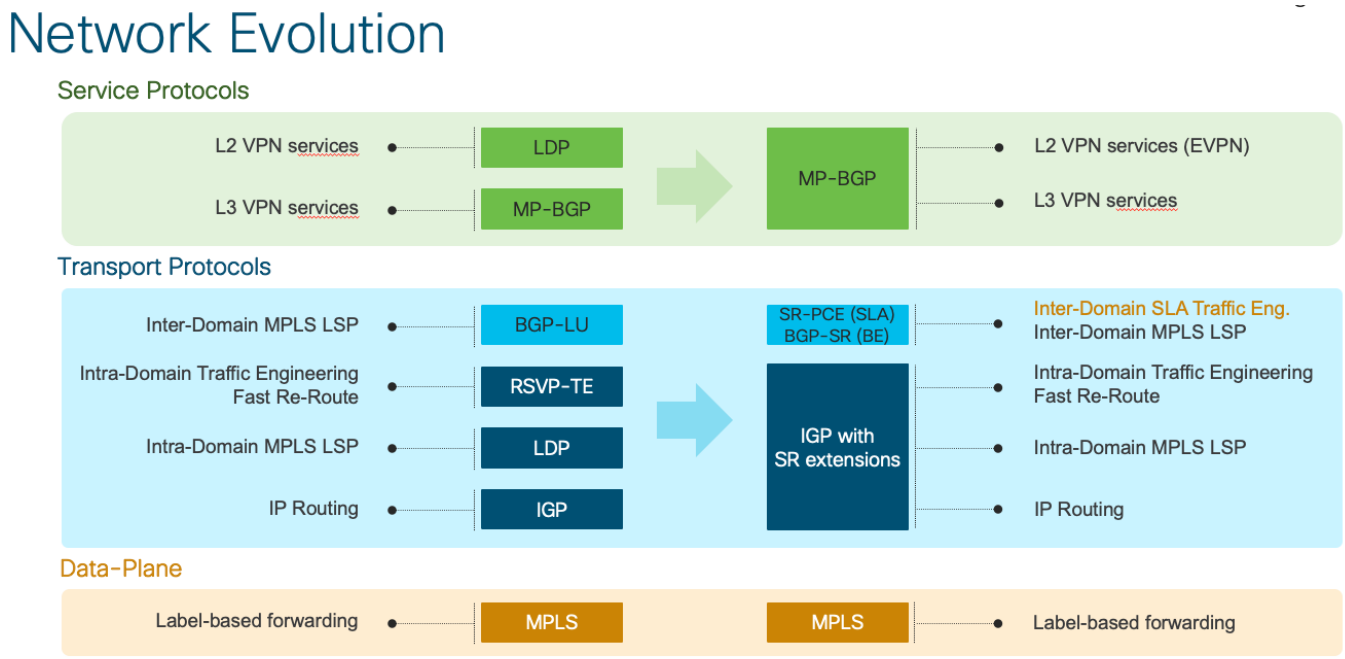
Segment routing relies on a small number of extensions to Cisco Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. It can operate with an MPLS or an IPv6 data plane, and it integrates with the rich multiservice capabilities of MPLS, including layer 3 VPN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

Segment routing can be directly applied to the 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.

Benefits of Segment Routing

- Ready for SDN: Segment routing was built for SDN and is the foundation for Application Engineered Routing (AER)
- Segment routing prepares networks for business models in which applications can direct network behavior, and provides the right balance between distributed intelligence and centralized optimization and programming
- Minimal configuration: Segment routing for traffic engineering requires minimal configuration on the source route
- Load balancing: Unlike in 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 preconfigured backup path within 50 ms of a 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

Figure 2. Segment Routing Service Protocols



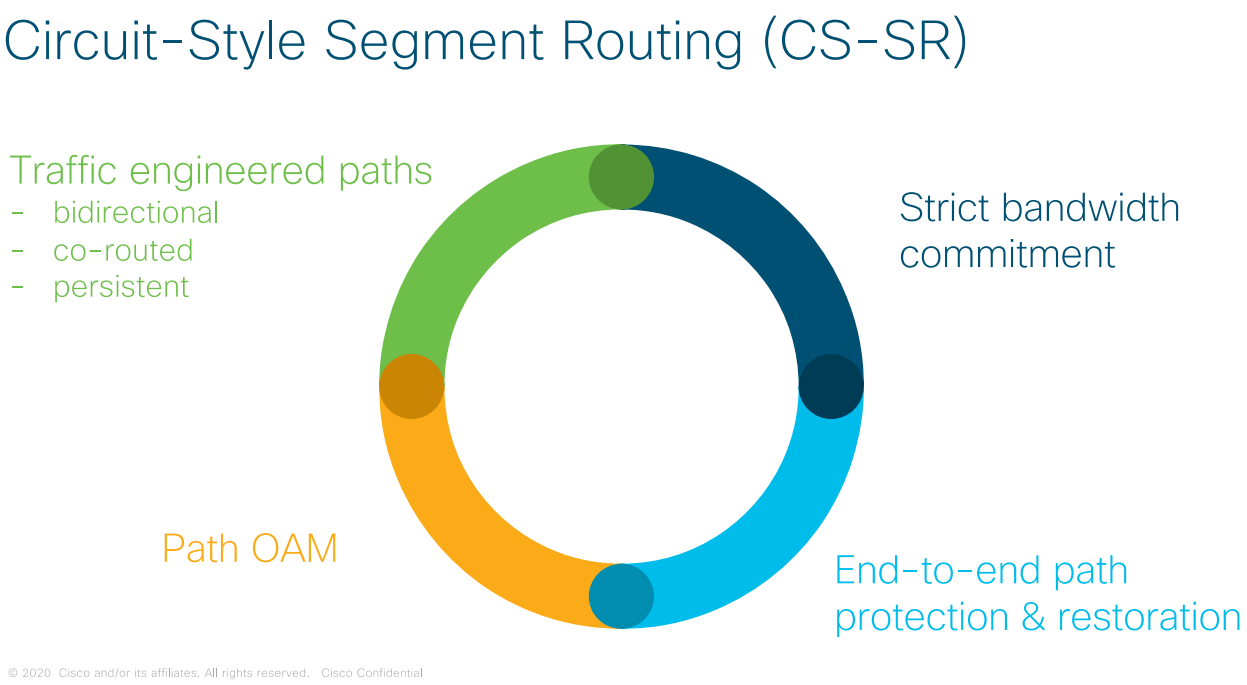
LDP: Label Distribution Protocol, **MP-BGP**: Multi-protocol BGP, **BGP-LU**: BGP Labeled-Unicast, **PCE**: Path Computation Element, **RSVP-TE**: Reservation Protocol Traffic Engineering, **BE**: Best-Effort

Circuit-Style Routing

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

Segment routing networks provide those transport capabilities by leveraging the new circuit-style segment routing (CS-SR) capabilities. CS-SR leverages network controllers to configure bidirectional co-routed active and 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 3. Circuit-Style Segment Routing Capabilities



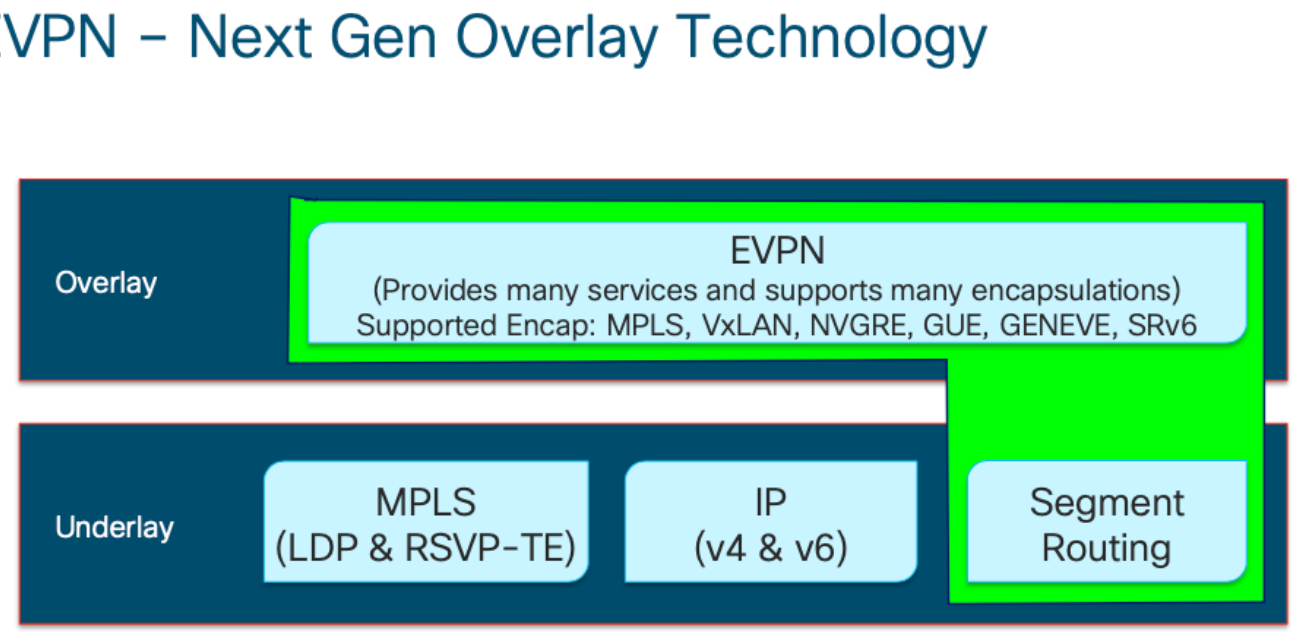
EVPN

EVPN is the next generation L2VPN technology. It provides layer 2 and layer 3 VPN services in a scalable and simplified manner. The evolution of EVPN started due to the need of a scalable solution to bridge various layer 2 domains and overcome the limitations that are faced by VPLS, such as scalability, multihoming, and per-flow load balancing.

EVPN uses MAC addresses as routable addresses and distributes them to all participating PEs via the MP-BGP EVPN control plane. EVPN is used for E-LAN, E-LINE, and E-TREE services and provides data plane and control plane separation. This approach allows the use of different encapsulation mechanisms in the data plane while maintaining the same control plane. In addition, EVPN offers many advantages over existing technologies, including more efficient load balancing of VPN traffic. Key advantages include:

- Multihoming and redundancy
- Per flow-based load balancing
- Scalability
- Provisioning simplicity
- Reduced operational complexity

Figure 4. EVPN Capabilities



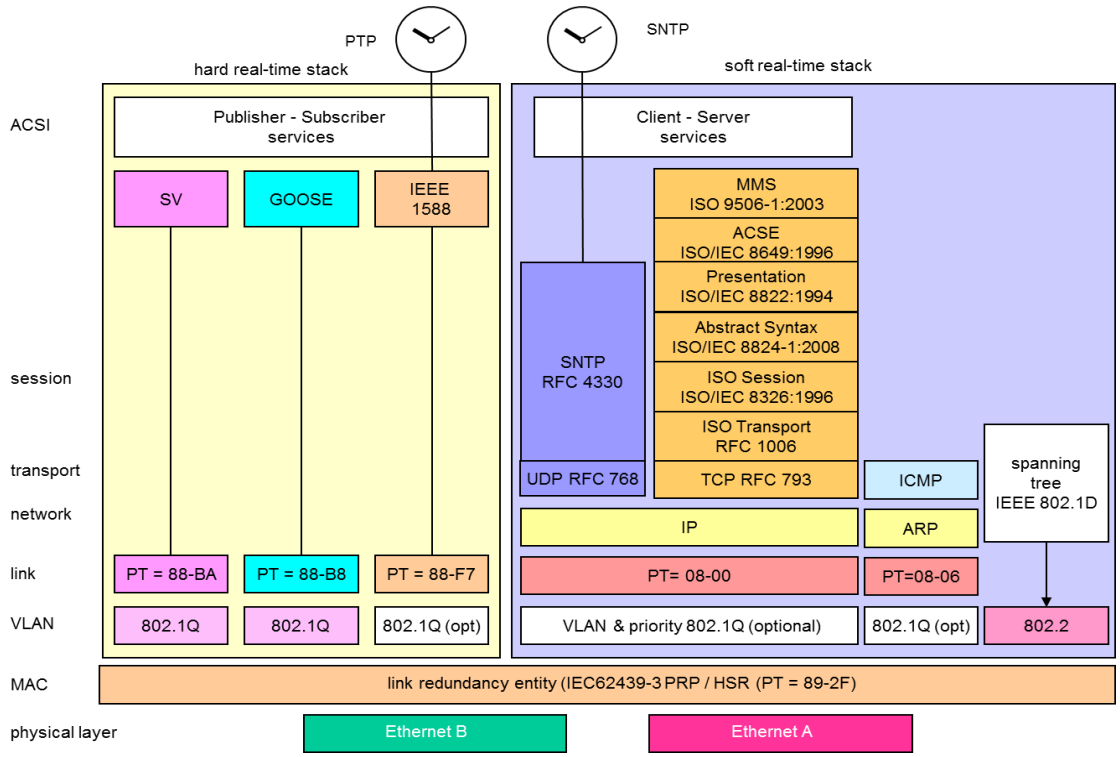
IEC61850

The IEC61850 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 part of these digital transformations. The standard establishes or references a number of concepts, including:

- 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 (4 ms) using multicast Ethernet mechanisms
  - Sample Values (SV), a mechanism for publishing sampled analog measurements from measurement devices over Ethernet
- Construction, design and conditions in which substation equipment, including network infrastructure, must operate
- Conformance and interoperability testing for substation equipment

Figure 5. IEC61850 Protocol Stack



Source: IEC TC57

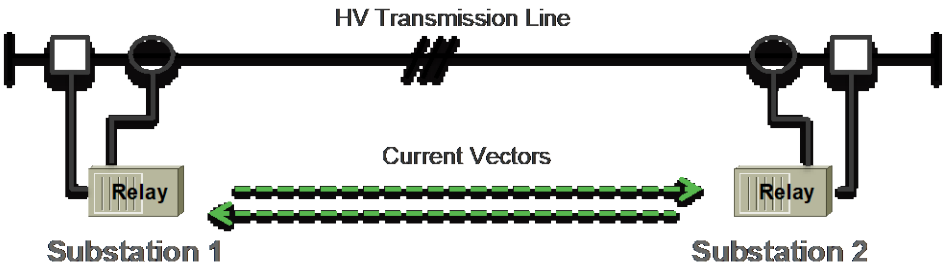
Teleprotection Overview

Teleprotection is a protection system that is in charge of monitoring the condition of the power grid, isolating faults, and preventing damage to critical parts of the power grid.

For background, some common teleprotection schemes are discussed below. The WAN solution has to support these most challenging requirements to support this use case.

Current Differential (87L) Protection

Figure 6. Current Differential Protection



Key characteristics of current differential protection:

- Differential protection: A function that operates on a percentage, phase angle, or other quantitative difference between two or more currents or other electrical quantities.
- Current differential protection: Operates on the principle of comparing current samples across the two ends of a protected line.

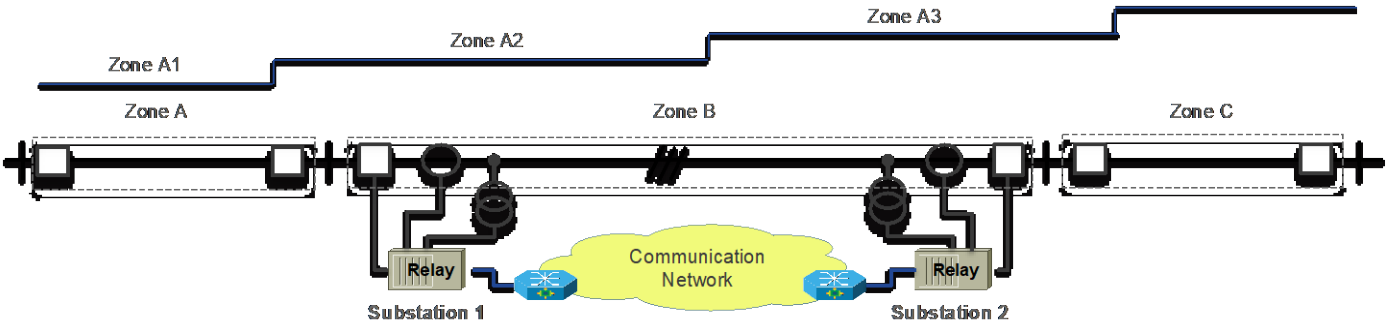
- Non-zero differential current (under ideal conditions) implies fault on the line causing the protection devices to trip.
- Current samples are transmitted to the remote end using a direct fiber or a communication network.

  Current samples for comparison must be taken at the same time across the two line ends. Otherwise, the phase angle shift that is produced by comparing currents from different time instances creates a false differential current, leading to a false tripping of the protection devices.
- Two mechanisms are available to synchronize relays to ensure current samples are aligned:
  - GPS-based synchronization
  - Proprietary echo (or ping-pong) mechanism based on round trip delay over the communication channel

Current differential teleprotection has the most stringent requirements in the network.

Distance Protection

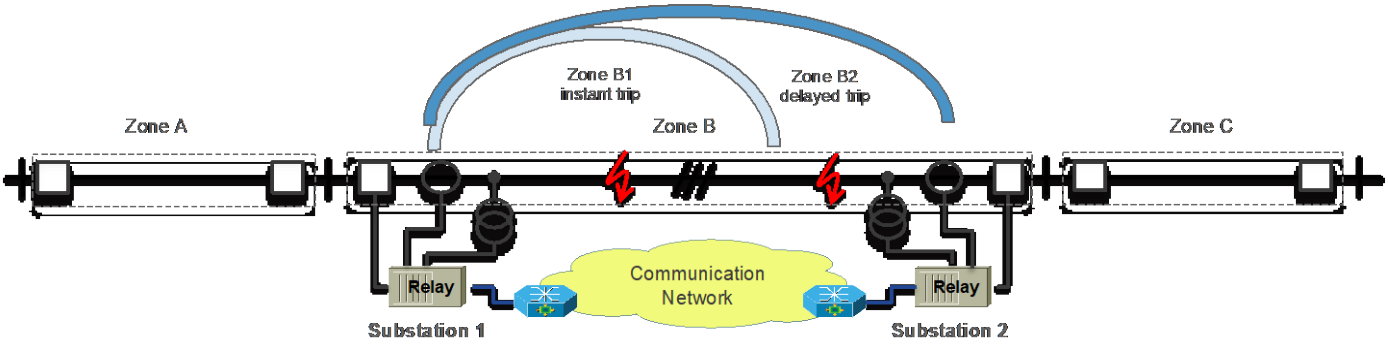
Figure 7. Distance Protection



Key characteristics of distance protection:

- Distance protection, a function that operates when the circuit admittance, impedance, or reactance increases or decreases beyond a predetermined value. The change of the impedance seen by the relay is caused by a fault.
- Distance relays, also known as impedance relays, are relays that use the measured voltage and current to calculate the line impedance.
- Teleprotection refers to the use of communication between relays to improve the performance of protection schemes, allowing for faster fault location and clearing at the relays, with higher selectivity.

Figure 8. Distance Protection Zones



- For distance protection purposes, the power system is divided into zones.
- The “real world” measured impedance depends on the distance to the fault, but also on many other variables such as temperature, wind, measurement accuracy, and so on. These differences may add up to 30%!
- Most protection relays trip instantaneously inside their zone 1 (usually 70% to 90% of the line).
- A zone 2 is included so that the relay trips when the fault is in the last part of the line (bellow 100% impedance) but with a delay to wait for any potential relay trip from a fault in an adjacent line.
- Things are usually a bit more complex in the real world with directional and overlap relays and zones.

Network Requirements

Path Symmetry

Path symmetry (congruency) is validated by comparing the difference in time delay of the transmit path and the receive path between two relay devices. The transmit and receive times are taken into consideration by line protection relays for differential calculations.

The transmit and receive times can sometimes be reported by the teleprotection relays.

Path symmetry requirements from customers or standards typically range between 500 µs and 1 ms.

IEC61850-5 introduced some WAN performance classes to clarify the WAN requirements within the various latency classes specified in IEC61850-90-1.

Table 1 shows the latency requirements for certain classes of application when traversing the WAN.

Table 1. WAN Latency Classes per IEC61850-90-12

Class	Latency	Use
TL1000	≤ 1,000 ms	All other messages*
TL10	≤ 10 ms	Telecontrol and teleprotection data
TL3	≤ 3 ms	Differential protection

* “All other messages” refers to noncritical traffic that does not fall under the more stringent classes.

Table 2 shows the requirements for teleprotection (current differential), which includes the 200 µs asymmetry delay maximum and 50 ms fault convergence:

Table 2. Communication Requirements for Teleprotection from IEC61850-90-12

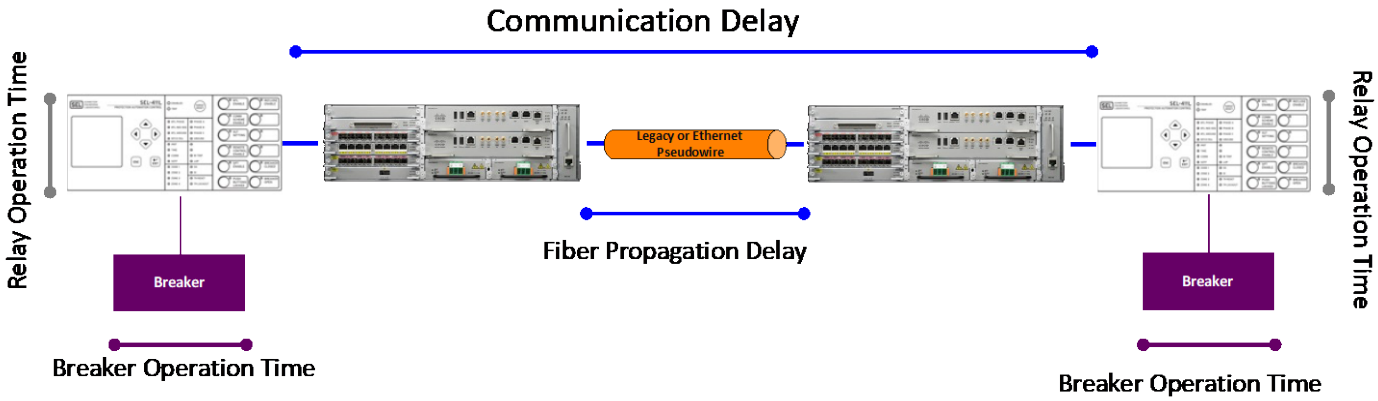
	Analog comparison (Current differential)	Command	Transfer tripping
Direction	Bidirectional	Bidirectional	Unidirectional
Message (useful) size	50 bits to 100 bits[1)]	Few bits (On/off)	Few bits (On/off)
Message (frame) periodicity	3 to 12 times per cycle	Sporadic	Sporadic
Bit rate (Bandwidth)	9,6 to 64 kbit/s	< 10 kbit/s	< 10 kbit/s
Latency	< 2,5 ms to 10 ms[4)]	< 10 ms	< 10 ms
Jitter[2)]	< 100 µs	Not required	Not required
Latency Asymmetry	< 200 µs[3)]	Not critical	Not critical
Time accuracy (relative)	< 100 µs	Not critical	Not critical
Error rate (BER, FER or PER)	$< 10^{-6}$ to 10^{-8}	$< 10^{-6}$	$< 10^{-6}$
Recovery delay	< 50 ms	< 50 ms	< 50 ms
Unavailability	$< 10^{-4}$ for single system (HV) $< 10^{-7}$ for double redundant system (EHV)	$< 10^{-2}$ to 10^{-3} (order of 1−dependability)	$< 10^{-4}$ (order of 1−dependability)
NOTE 1 One phase or segregated (three-phase) current differential protection NOTE 2 0,25 to 0.05 × Unit Interval (ITU-T G.823] NOTE 3 Some legacy standards required only an asymmetry of 750 µs for teleprotection equipment; this value sometimes still appears depending on the voltage level Source: IEC TC57 WG10			

What Contributes to Delays in Network Communications?

The following attributes contribute to the delay in communications across any IP based network:

- Path latency: Includes processing, queuing, serialization, and transmission delays
- Propagation delay: Every 124.3 miles (200 km) of fiber adds 1 ms
- ± PDV: Path delay variation or jitter due to network congestion
- Compensation for jitter (de-jitter buffer)

Figure 9. Network Delay



Architecture

Two types of critical services are required to be transported across the transport network from the substation:

- Layer 2: Substation to substation traffic. Typically, IED to IED protection traffic using IEC61850 GOOSE packets.
- Layer 3: SCADA traffic from a substation to a data center and multicast WAMs traffic from substation PMUs to regional PDCs.

However, new emerging services also exist and are required to be supported in any new architecture. For example, to support the move toward virtualized components in the substation, migration of virtual machines or containers for virtualized applications (virtualized RTU or protection devices) needs to be possible between substations for resiliency.

Other noncritical Layer 3 services:

- Corporate: Enterprise traffic (data), video, and IP voice
- Physical security: Substation perimeter monitoring devices, CCTV, and access control devices
- AMI: Smart metering data from an aggregation point to a data center
- FAN: External field area network data to a data center (IoT sensors, Wi-SUN wireless mesh, LoRaWAN and other wireless technologies used in the field area network)

Figure 10. Layer 2 Service Architecture

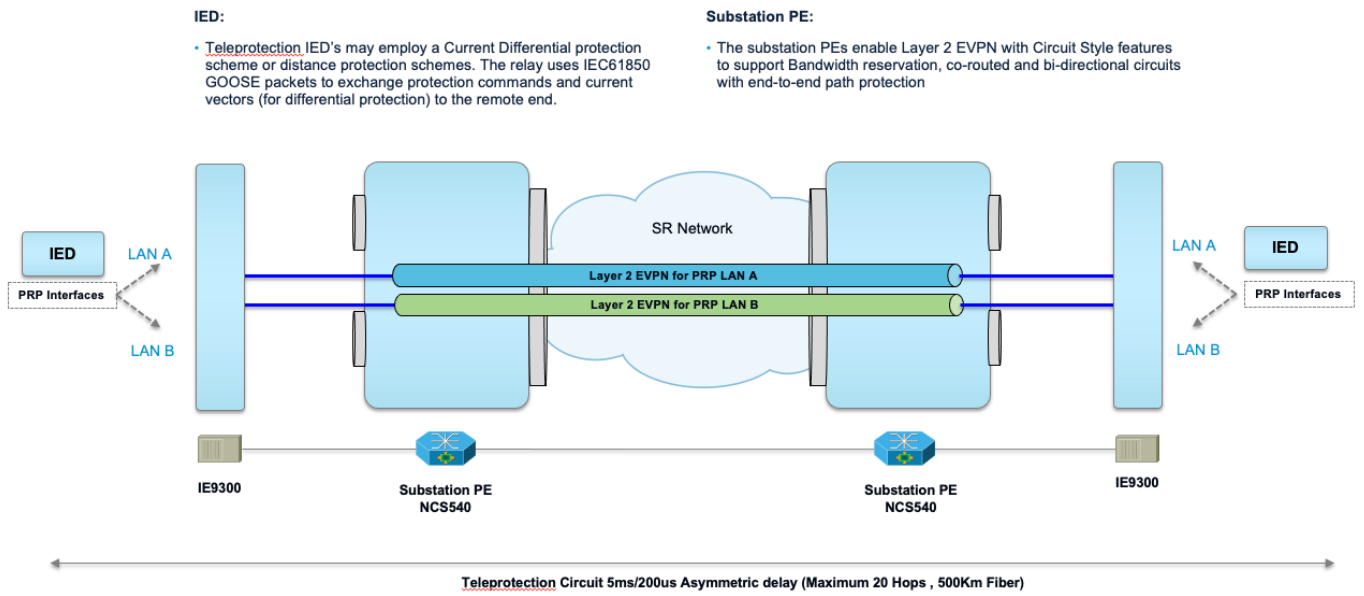
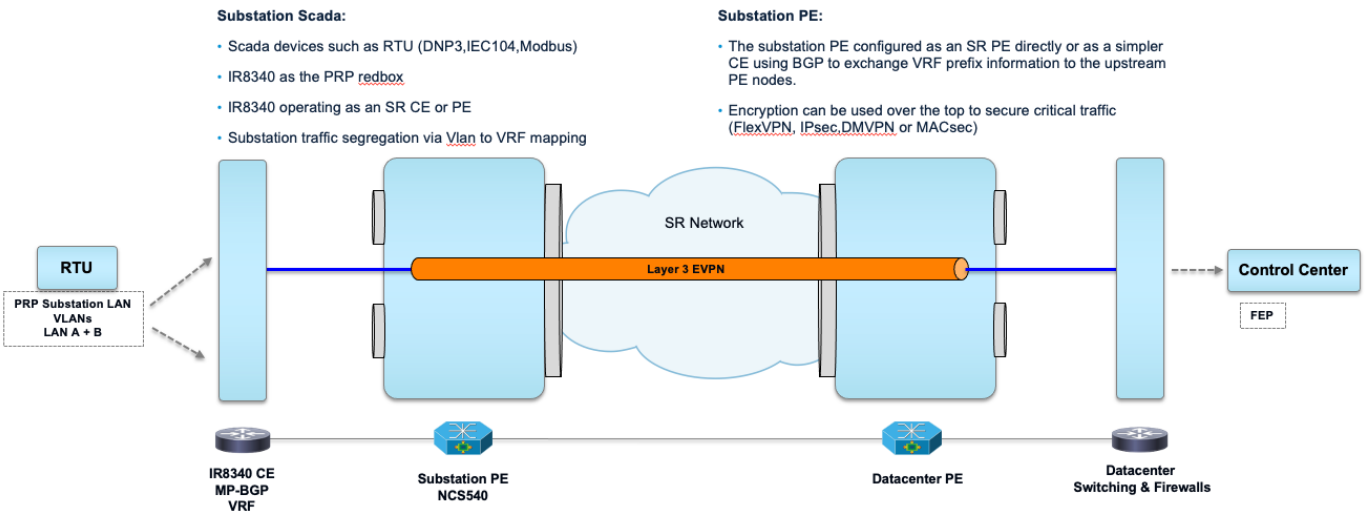


Figure 11. Layer 3 Service Architecture

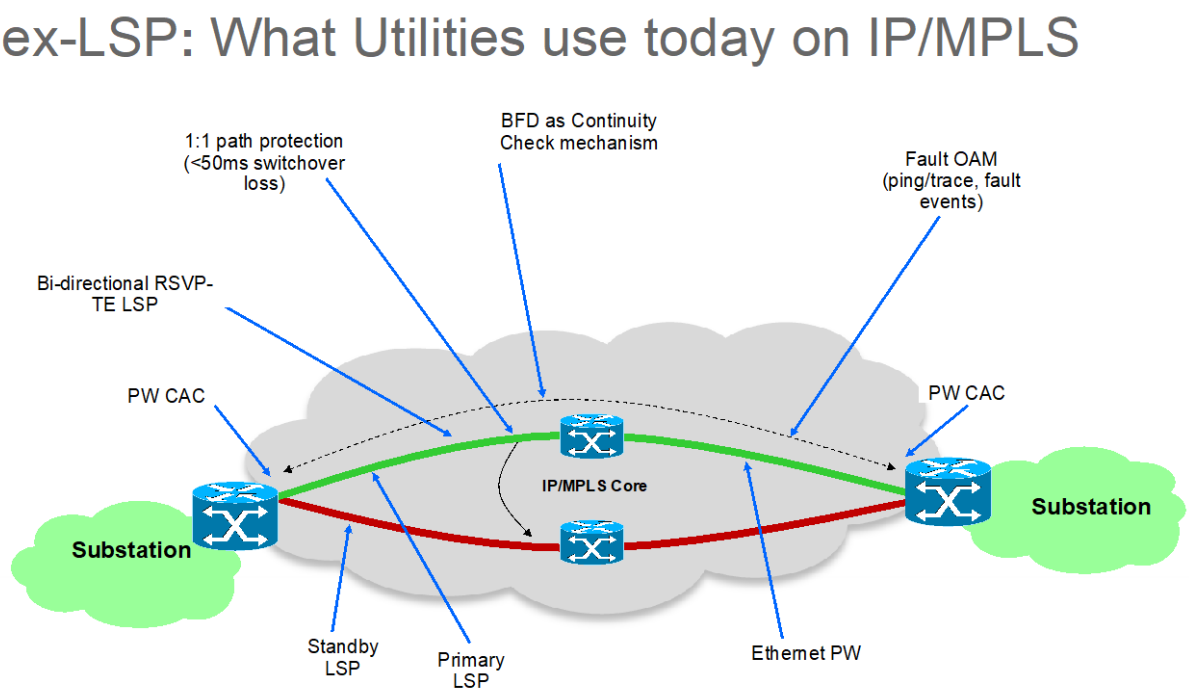


Previously on IP/MPLS networks, Cisco validated designs used Flex LSP features to provide a deterministic path behavior across the packet network. The critical requirements for MPLS based Label Switched Paths (LSP) are:

- Bidirectional co-routed path: Each LSP must support traffic in both directions and the forward and reverse paths must follow the same engineered route.
- End to end path protection: The complete LSP should be protected with a backup path from PE to PE. This backup path should be presignaled and bandwidth should be reserved for a fast switchover if an error occurs on the primary path.

Therefore, any solution on a segment touted network must deliver these capabilities as a minimum.

Figure 12. IP/MPLS LSP Requirements



Substation Automation Validated Design

The new updated Cisco Substation Automation validated design describes the Cisco validated substation automation solution architectures. The purpose of the solution 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 is intended to introduce software-defined network management capabilities with Cisco Catalyst Center for the substation LAN and Cisco Catalyst SD-WAN for WAN management.

The Cisco Substation Automation validated 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:

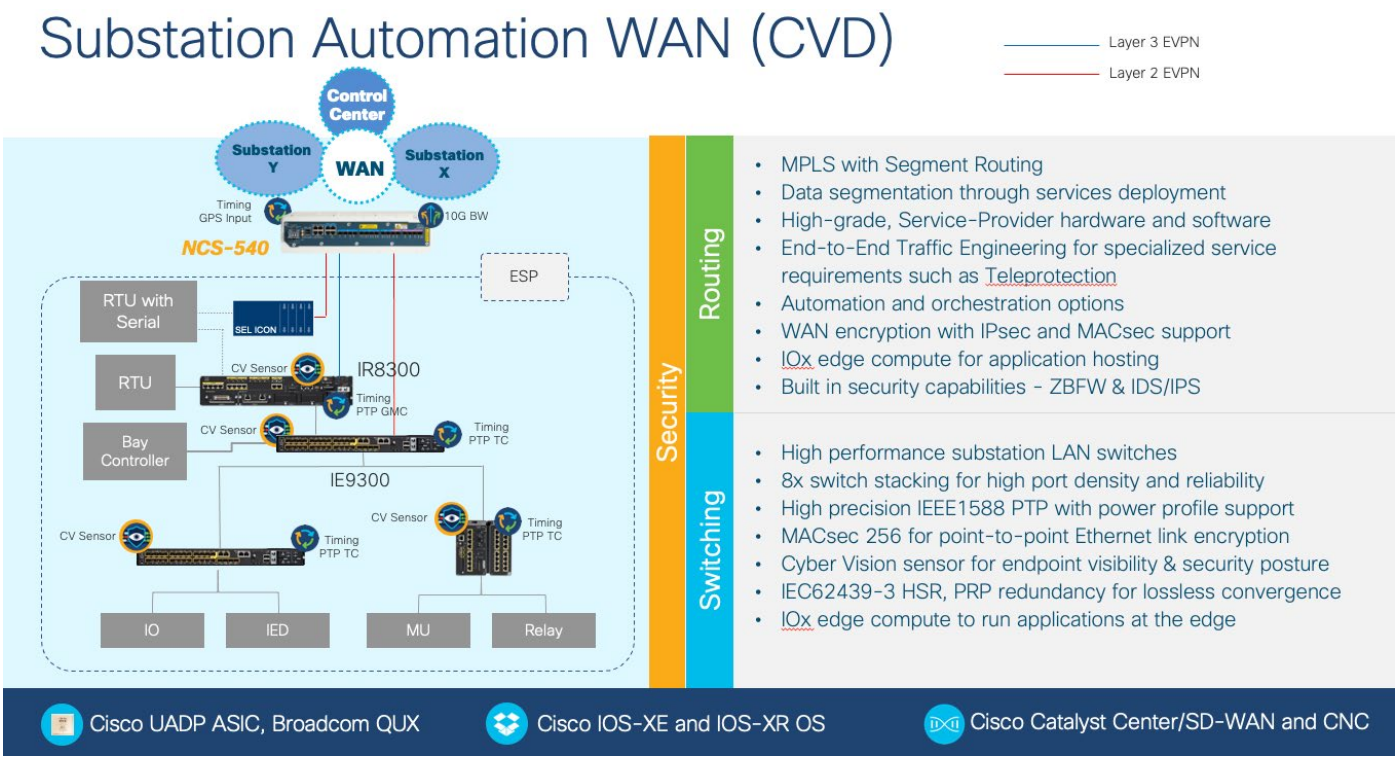
- High availability in the ESP zone topology with PRP and REP
- GOOSE validation
- Dying gasp in the network infrastructure to provide smoother outages
- PTP in the Substation LAN based upon the 2014 IEEE Precision Time Protocol–Power Profile
- Firewall redundancy

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 monitoring of traffic flow anomalies
- QoS to predictably service a variety of network applications and traffic types
- Validation of a recently introduced Industrial Ethernet switch, Cisco IE 4010, for use in a substation LAN

The major addition to the updated Cisco substation automation solution is the new Utility WAN architecture. This update provides solution details for the integration of the Cisco substation automation solution with the Cisco SDN converged transport Cisco Validated Design. It supports substation to control center use cases and intersubstation services such as teleprotection.

Figure 13. Cisco Substation Automation WAN Architecture



The Cisco Validated Substation Automation Solution supports and enhances many of the features and use cases that are listed above. The key new aspects covered in this 3.0 version include new products and features.

New features supported in this version include:

- Substation LAN centralized and automated network deployment and management via Cisco DNA Center
- Substation WAN centralized network deployment and management via Cisco SD-WAN technologies (for example, Cisco Catalyst SD-WAN Manager)

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

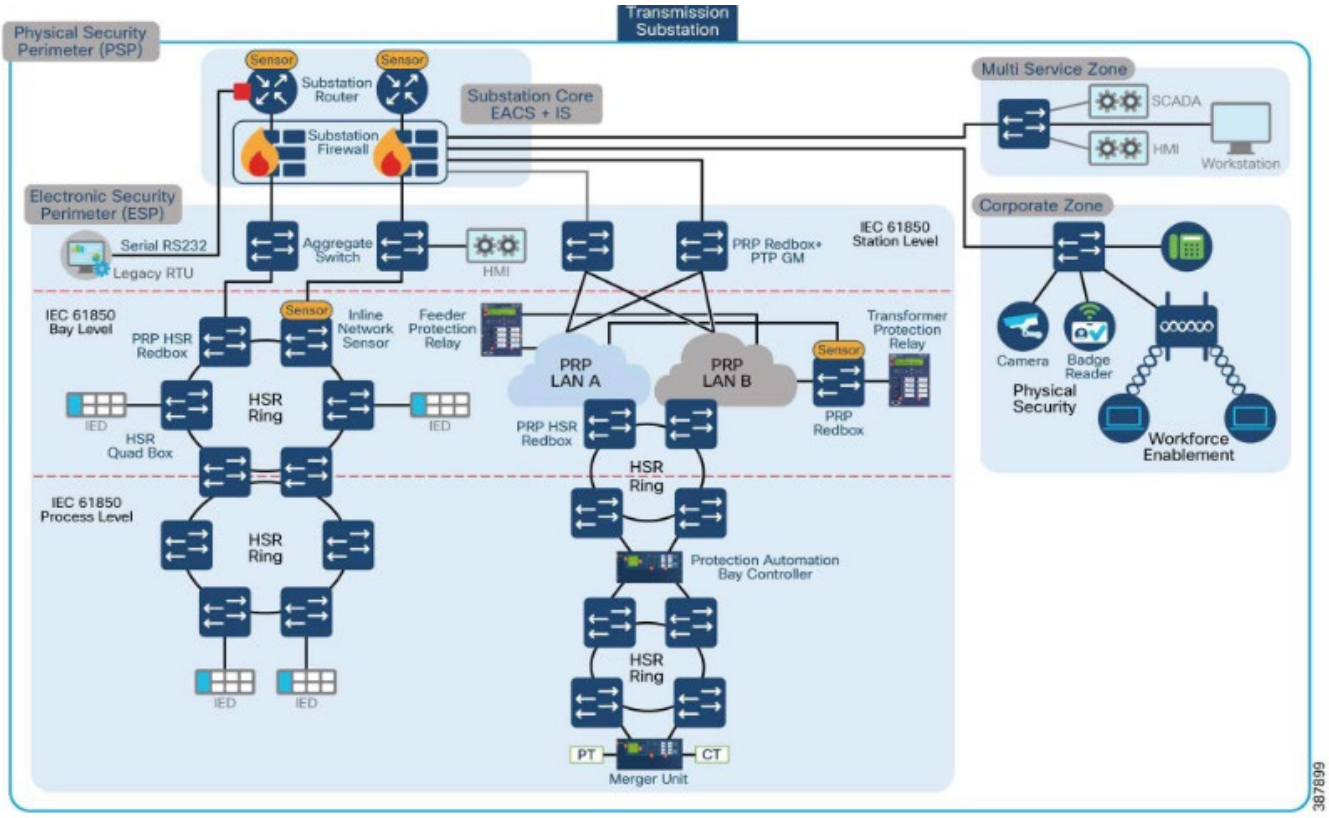
- The Cisco Catalyst IE9300 Rugged Series switches with 28 gigabit Ethernet fiber ports for secure, reliable, low-latency station and process bus communication, compliance with IEC 61850-3 and IEEE 1613, and stackable up to three units
- The Cisco Catalyst IR8340 multifunctional, modular, rugged substation router with scalable WAN connectivity, firewall security, and 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, including 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: A range of management options, including Cisco Catalyst Center for switching and Cisco Catalyst SD-WAN Manager for SD-WAN routing capabilities

Cisco Substation Automation Reference Architecture

Figure 14. Cisco Substation Automation Validated Design Architecture



The Cisco new digital substation architecture comprises an operations and control center, demilitarized zone, WAN tier, transmission Substation Physical Security Perimeter (PSP) and WAN connectivity for other secondary substations, and local multiservice and corporate networks. The PSP is divided into substation core, Electronic Security Perimeter (ESP), and Multiservice and Corporate (CORP) zones. Based on the IEC 61850 standard, ESP is further subdivided into station, bay, and process Levels.

SDN Converged Transport Network

The Cisco Converged SDN Transport design satisfies the following criteria for scalable next-generation networks. For more information, see *Converged SDN Transport High Level Design v5.0* at https://xrdocs.io/design/blogs/latest-converged-sdn-transport-hld.

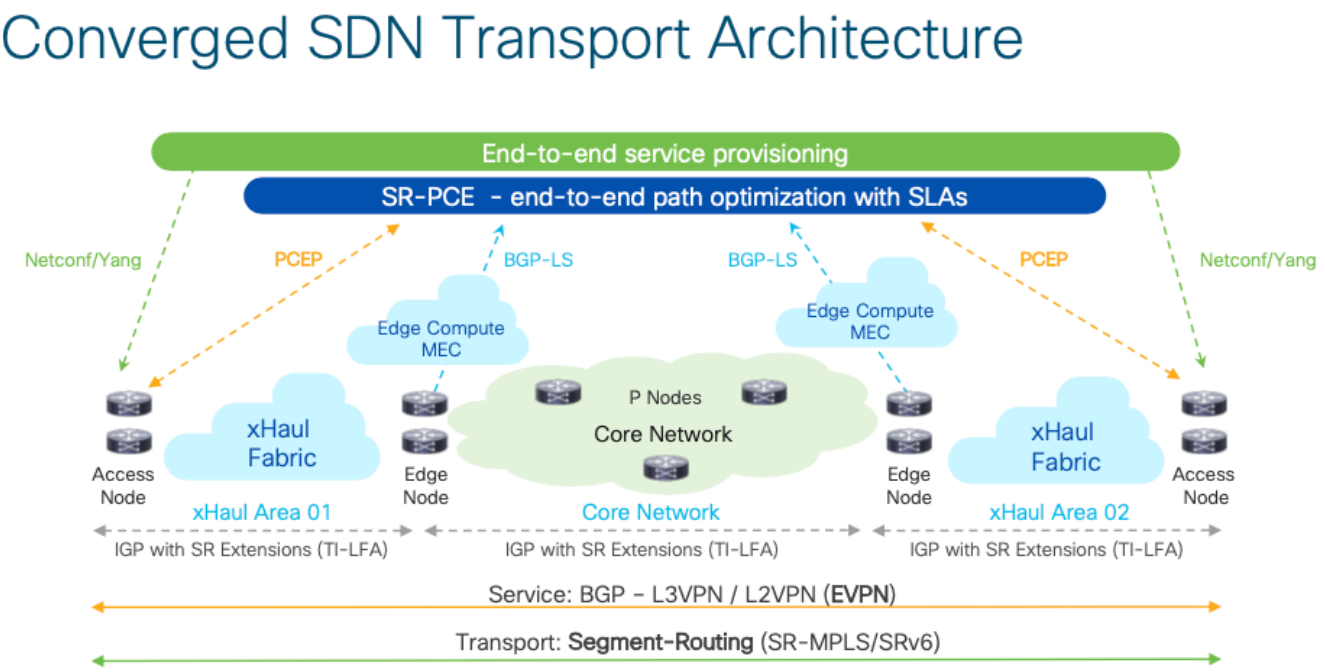
- Simple: Based on segment routing as a unified forwarding plane and EVPN and L3VPN as a common BGP based services control plane
- Programmable: Uses SR-PCE to program end-to-end multidomain paths across the network with guaranteed SLAs
- Automated: Service provisioning is fully automated using NSO and YANG models with the Cisco Crosswork Network Controller to enhance operations and network visibility

The Converged SDN Transport is made of the following main building blocks:

- IOS-XR as a common operating system that is proven in service provider networks
- Transport layer based on segment routing as a unified forwarding plane

- SDN: Segment Routing Path Computation Element (SR-PCE) as the Cisco Path Computation Engine (PCE) coupled with segment routing to provide simple and scalable interdomain transport connectivity, traffic engineering, and advanced path control with constraints
- Service layer for layer 2 (EVPN) and layer 3 VPN services based on BGP as the unified control plane
- Automation and analytics:
  - NSO for service provisioning
  - Netconf and YANG data models
  - Telemetry to enhance and simplify operations
  - Zero touch provisioning and zero touch deployment (ZTP/ZTD)

Figure 15. Converged SDN Transport Architecture



The Cisco Converged SDN Transport Design aims to enable simplification across all layers of a WAN network. Thus, the converged SDN transport services layer focuses on a converged control plane based on BGP.

BGP based services include EVPNs and traditional L3VPNs (VPNv4 and VPNv6).

EVPN is a technology that was initially designed for Ethernet multipoint services to provide advanced multihoming capabilities. By using BGP for distributing MAC address reachability information over the MPLS network, EVPN brought the same operational and scale characteristics of IP based VPNs to L2VPNs. Today, beyond DCI and E-LAN applications, the EVPN solution family provides a common foundation for all Ethernet service types, including E-LINE, E-TREE, and data center routing and bridging scenarios. EVPN also provides options to combine L2 and L3 services into the same instance.

To simplify service deployment, provisioning of all services is fully automated by Cisco Network Services Orchestrator (NSO) using (YANG) models and NETCONF.

There are two types of services: end-to-end and hierarchical.

For more information about the Cisco converged SDN transport validated design, see the documentation here: https://xrdocs.io/design/.

Ethernet VPN

An EVPN solves two longstanding limitations for Ethernet services in service provider networks:

- Multihomed and all-active Ethernet access
- Service provider network: Integration with a central office or data center

NCS 540 Small, Medium, Large Density Routers for the Substation edge

The NCS 540 family of routers supports mobile and business services across a wide variety of service provider and enterprise applications, including support for routed optical networking in the QSFP-DD that is enabled NCS-540 Large Density router.

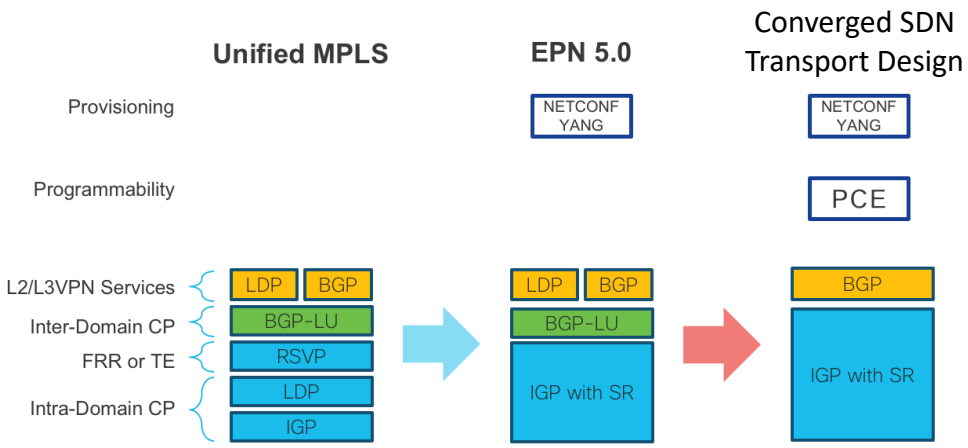
For more information about the NCS 540 router line, *see Cisco Network Convergence System (NCS) 540 Series*: https://www.cisco.com/c/en/us/products/routers/network-convergence-system-540-series-routers/index.html.

Summary

The Converged SDN Transport brings significant simplification at the transport and services layers of a service provider network. Simplification is a key factor for real software-defined networking (SDN). Cisco continually improves service provider network designs to satisfy market needs for scalability and flexibility.

From a very well established and robust Unified MPLS design, Cisco has embarked on a journey toward transport simplification and programmability. This journey started with the transport control plane unification in Evolved Programmable Network 5.0 (EPN5.0). The Cisco Converged SDN Transport provides another leap forward in simplification and programmability by adding services control plane unification and centralized path computation.

Figure 16. Evolution of Converged SDN Transport



The transport layer requires only IGP protocols with segment routing extensions for intradomain and interdomain forwarding. Fast recovery for node and link failures leverages Fast Reroute (FRR) by Topology Independent Loop Free Alternate (TI-LFA), which is a built-in function of segment routing. End-to-end LSPs are built using traffic engineering by segment routing, which does not require additional signaling protocols. Instead, it relies solely on SDN controllers, thus increasing overall network scalability. The controller layer is based on standard industry protocols, such as BGP-LS, PCEP, BGP-SR-TE, and so on for path computation, and on NETCONF/YANG for service provisioning, thus providing a on open standards-based solution.

With these features and functions, the Cisco Converged SDN Transport design brings an exciting evolution to wide-area networking.

Use Cases

The Cisco substation automation solution has to support various types of services. Both substation to control center and substation to substation services are required

There are three categories of traffic that the solution supports:

- Layer 3 Substation to data center: Traffic types, such as IP based SCADA data, IP based CCTV, enterprise data traffic, and IP telephony
- Layer 2 substation to substation: Layer 2 non-routable protocols (for example, IEC61850 GOOSE and sampled values), virtual machine migrations and third-party SCADA traffic
- Layer 2 substation to substation for teleprotection: Power protection services, which are low latency peer-to-peer communications using layer 2 non routable protocols with strict engineered paths across the network

The following sections provide additional information about these categories of traffic.

Layer 3 Substation to Datacenter

Layer 3 IP based services are supported by the Cisco Catalyst IR8340 substation gateway.

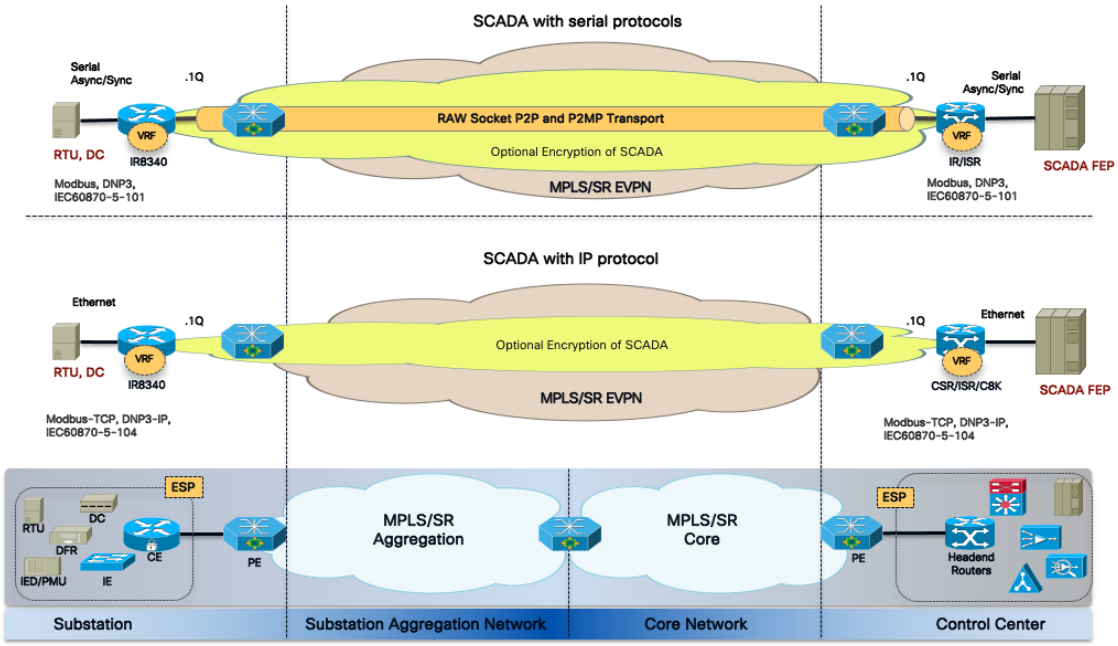
IP Based SCADA Traffic

The Cisco Catalyst IR8340 rugged router provides the transport for IP based SCADA protocols, such as Modbus-TCP, DNP3-IP, IEC 60870-5-104, and so on, that are supported over Ethernet interfaces. The IP SCADA traffic is transported between the substation and the control center using a L3 MPLS VPN.

IP Based SCADA Traffic Supporting Serial Transport via Raw Sockets

The Cisco Catalyst IR8340 provides the transport for legacy SCADA protocols, such as Modbus, DNP3, and IEC 60870-5-101, that are supported over legacy asynchronous serial interfaces. The SCADA traffic is tunneled between the substation and the control center using TCP raw socket. The raw-socket feature is VRF aware and allows for the isolation of the traffic using an L3 MPLS VPN.

Figure 17. SCADA with Ethernet and Serial Interface Connectivity



Layer 2 Substation to Substation

The Cisco Catalyst IE9300 rugged switch provides the transport for IP based teleprotection protocols, such as IEC61850 GOOSE, that are supported over Ethernet interfaces. The GOOSE traffic is transported between the substations using a circuit style policy to define the path characteristics (bandwidth reservation, path asymmetry, bidirectional and co-routed circuits).

Layer 2 Substation to Substation for Teleprotection

Teleprotection services are supported via the SEL ICON platform. This platform provides the interfaces that are required for substation protection devices while providing an Ethernet based uplink to the Converged Transport network (NCS).

Typical interfaces required within the substation for protection devices include the following:

- C37.94 Nx64K
- G703 codirectional
- 4 Wire E&M
- Sync/Async serial
- T1/E1Voice FXS/FXO

The Substation Automation validated design provides a revalidation of the SEL ICON Virtual Synchronous Network (VSN) platform over the new segment routed based WAN.

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

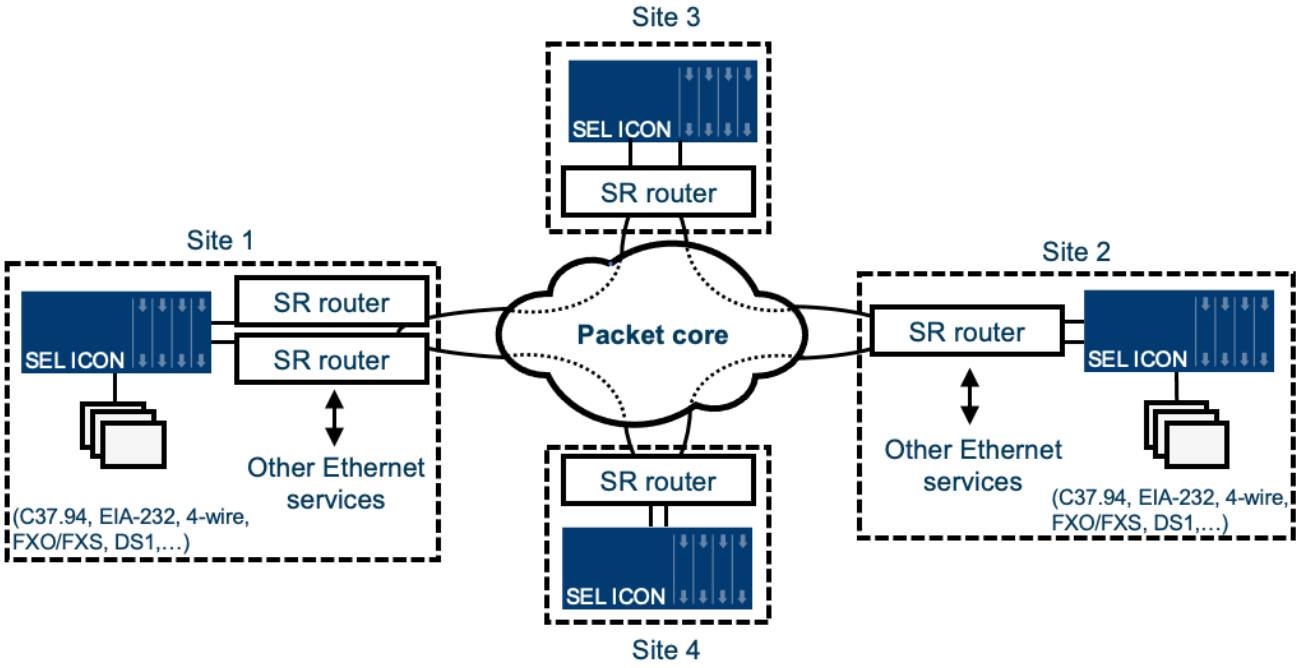
SEL is a Cisco partner that provides support for low bit rate teleprotection interfaces. SEL Integrated Communications Optical Network (ICON) is purpose-built for mission-critical communications, providing either SONET or Ethernet transport. The ICON is a WAN multiplexer optimized for industrial and utility applications. 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 that are provisioned through MPLS based core networks combined with an innovative, ultraefficient approach of packetizing TDM data to achieve <1 ms latency, <0.1 ms asymmetry, and <5 ms 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 transport network, as shown in the following figure.

Figure 18. SEL ICON Architecture



Point-to-point bidirectional Ethernet services, 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 that is 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 that is 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.

Transport Network Considerations

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

- Bidirectional point-to-point Ethernet static path (tunnel) highest-priority traffic treatment
- Strict scheduling (priority queue)
- Guaranteed Committed Information Rate (CIR)

A bidirectional static path (that is, the same path through the core 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.

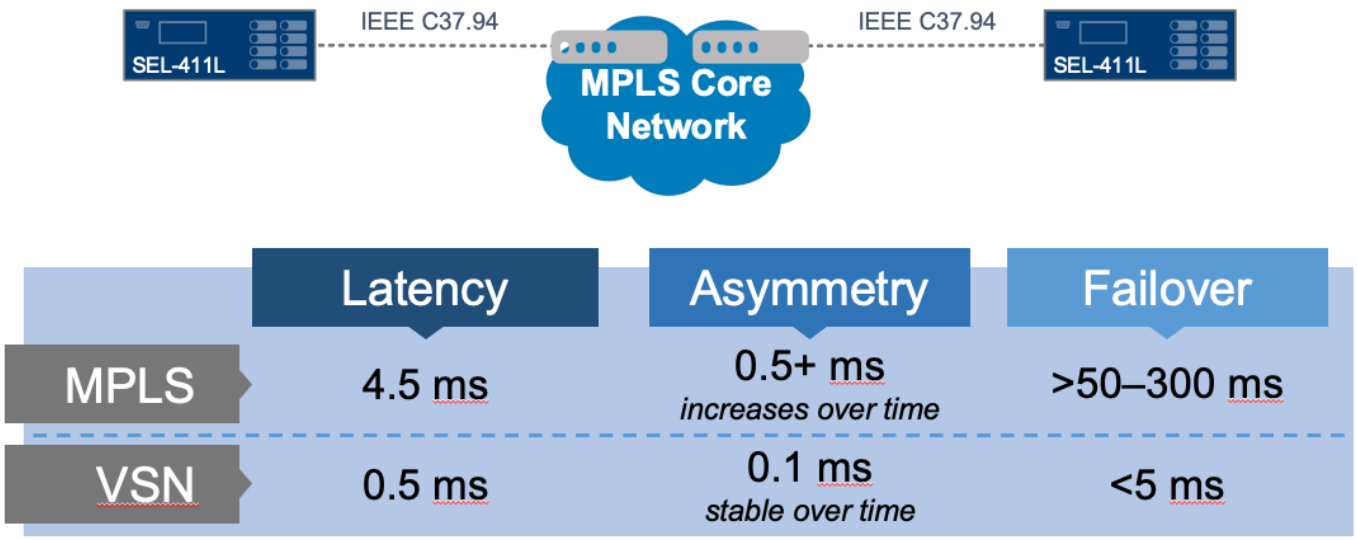
The ICON employs a switch-on far-end failure indication (FEFI) mechanism to ensure that the primary or backup path of a circuit remains symmetrical if a unidirectional path failure occurs. This approach, coupled with a

bidirectional PDV link setting, eliminates asymmetry for circuits that communicate 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 ms if a path failure occurs.

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 scheduling. Strict scheduling minimizes latency fluctuation for VSN traffic in the core. As a result, the overall path latency improves by setting a lower PDV value within the ICON. All other Ethernet traffic that traverses the core network must have a lower priority treatment than the ICON VSN traffic.

SEL ICON built-in features provide fast failover and minimal path latency compared to traditional technologies. Therefore, the underlying segment routing network provides layer 2 point-to-point paths for the ICON connections and does not provide any path protection. Fast failover is performed by the ICON platform.

Figure 19. SEL ICON VSN Advantages



SEL ICON Timing

Every node has a server module with a built-in GPS receiver that can input GPS time. Alternatively, the server module can receive an IRIG-B time signal from an external clock. This capability enables an ICON to provide time distribution via IRIG-B with 1 µs accuracy. ICON VSN transport can be operated in either of the following modes:

- ICON-to-ICON through a third-party Ethernet network (tunnel mode): Tunnel mode is used when transporting VSN packets through third-party network devices, such as an MPLS or CE core network. When operating in tunnel mode, the following methods are supported:
  - Dual-ended time synchronization (preferred method). The ICON nodes at each side of the tunnel connection are synchronized locally to a GPS or IRIG-B time signal (typically available in substations).
  - Single-ended time synchronization. One ICON is synchronized to a local time source (GPS or IRIG-B) and timing is passed to the other ICON across the tunnel connection. Do not use this mode unless the core network PDV can be guaranteed and the latency and asymmetry performance meet the specifications of ICON applications using the network.
- The ICON includes support for IEEE 1588 Precision Time Protocol (PTP) telecom profile (ITU-T G.8275), which supports a third-party network synchronization option. ICON can synchronize to a network provided PTP primary reference clock.

Summary of Substation Use Cases

Layer 3 Use Cases

Table 3. Typical Substation Layer 3 Use cases

Use Case	Interface	A End	B End	Unicast/ Multicast	Protocols	Notes
SCADA (RTU)	Ethernet	Substation	Control center	U	IEC61850 MMS IEC104, DNP3	–
SCADA (RTU)	Serial	Substation	Control center	U	Raw sockets UDP/TCP	–
PMU (WAMS)	Ethernet	Substation	Control center	M	C37.118	Can be to a regional concentrator
CCTV	Ethernet	Substation	Control center	U/M	Video, control	Local vs remote video storage
Access control	Ethernet	Substation	Control center	U	–	–
Management	Ethernet	Substation	Control center	U	SNMP, Netconf, Restconf, web sockets, HTTP, HTTPS, FTP, Telnet, SSH, RADIUS, TACACS, LDAP	–
IED (breaker, transformer, line, bus, and so on)	Ethernet	Substation	Control center	U	IEC61850 MMS, DNP3, IEC104	Protection and control
IoT Sensors	Ethernet	Substation	Control center	U	–	Temperature, humidity, light, weather, soil, and so on.
Fault recorder	Ethernet	Substation	Control center	U	–	–
Teleprotection	Ethernet	Substation X	Substation Y	M	IEC61850 R-GOOSE	UDP Encapsulated GOOSE

Sampled values	Ethernet	Substation X	Substation Y	M	IEC61850 R-SV	UDP Encapsulated SV
IP Telephony	Ethernet	Substation	Control center	U	SIP	–
Enterprise data	Ethernet	Substation	Control center	U	IP	–
Timing	Ethernet	Substation	Control center	M	IEEE1588, SyncE	WAN timing distribution
Power quality	Ethernet	Substation	Control center	M	–	–
SCADA translation	Serial to Ethernet	Substation	Control center	U	IEC 60870-5-101 and DNP3	–
Radio	Ethernet	Substation	Control center	U/M	pLTE, LMR, Tetra	Base stations at substations
System Integrity Protection Schemes (SIPS)	Ethernet	Substation	Control center	M	IEC61850 GOOSE	Hub and spoke scheme

Layer 2 Use Cases

Table 4. Typical Substation Layer 2 Use cases

Use Case	Interface	A End	B End	Unicast/ Multicast	Protocols	Notes
Teleprotection	Ethernet	Substation X	Substation Y	M	IEC61850 GOO	–
Teleprotection	Ethernet	Substation X	Substation Y	U	Proprietary	P2P Ethernet circuit
App migration	Ethernet	Substation X	Substation Y	U	VMware vMotion	Moving of virtualized applications between compute resources (vRTU)
Third-party traffic	Ethernet	Substation X	Substation Y	U	IP, Ethernet	Transparent transport of third-party traffic

Legacy TP (external Mux)	Ethernet	Substation X	Substation Y	U	IP, Ethernet	Encapsulated TDM relay protocols (C37.94, E&M, G703 bidirectional, serial)
Sampled values	Ethernet	Substation X	Substation Y	M	IEC61850 SV	–

Conclusion

Packet-based networks reliably support the most stringent teleprotection schemes with guaranteed SLAs that are well below the required latency budget.

The main factors consuming delay budget are relay protection interface types and speeds, and overlay transport if used (packet over TDM), and not the packet network itself.

Segment routing can ensure that LSPs are co-routed when echo-based IED synchronization is used for differential schemes.

SyncE or PTP ensures efficient synchronization distribution to SR PEs for circuit-style circuits.

Efficient QoS mechanisms ensure that teleprotection traffic is subject to minimum latency (for faster detection) and jitter (for accurate IED synchronization) as it traverses the packet network.

References

- Cisco utility validated designs: https://www.cisco.com/c/en/us/solutions/design-zone/industries/power-utilities.html#~validated-designs
- Converged SDN Transport Network Validated design: https://xrdocs.io/design/
- Datasheets
  - Cisco Catalyst IR8300 Rugged Series Router: 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 Catalyst IE9300 Rugged Series: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie9300-rugged-series/catalyst-ie9300-rugged-series-ds.html
  - Cisco NCS 540 Series: https://www.cisco.com/c/en/us/products/routers/network-convergence-system-540-series-routers/index.html#~products
  - SEL ICON: https://selinc.com/api/download/9326/

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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