The New Digital Substation

More efficient, more secure and ready for demanding modern Grid applications

Marcus Smith
IIoT Utilities Solution Manager

Dan Madey
IIoT Lead Utilities Architect

Agenda

01 Digital Substation Automation Solution
02 Substation WAN
03 Timing and Synchronization
04 DNP3 Deployment Architectures
05 Substation Visibility & Zero Trust
06 Conclusion

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Webex App

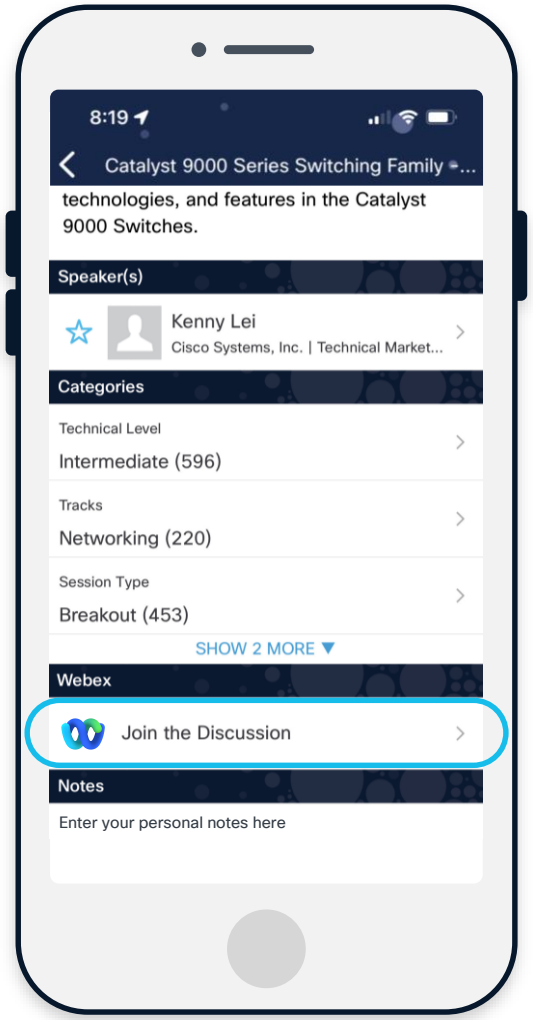
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKIOT-2015**

© 2025 Cisco and/or its affiliates. All rights reserved.

The New Digital Substation

Substation Automation Cisco Validated Design

cisco Live !

New demands on the network

Substations becoming more digitized and automated

- Physical and cyber security threats
- Increased bandwidth requirements (More connected devices)
- Need for reduced footprint and future proof technologies to keep up with evolving requirements
- High degree of timing synchronization required
- Need for simplicity and efficiency (e.g.Automation)

But digitization isn’t easy

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Utility Grid Solutions

Substation automation

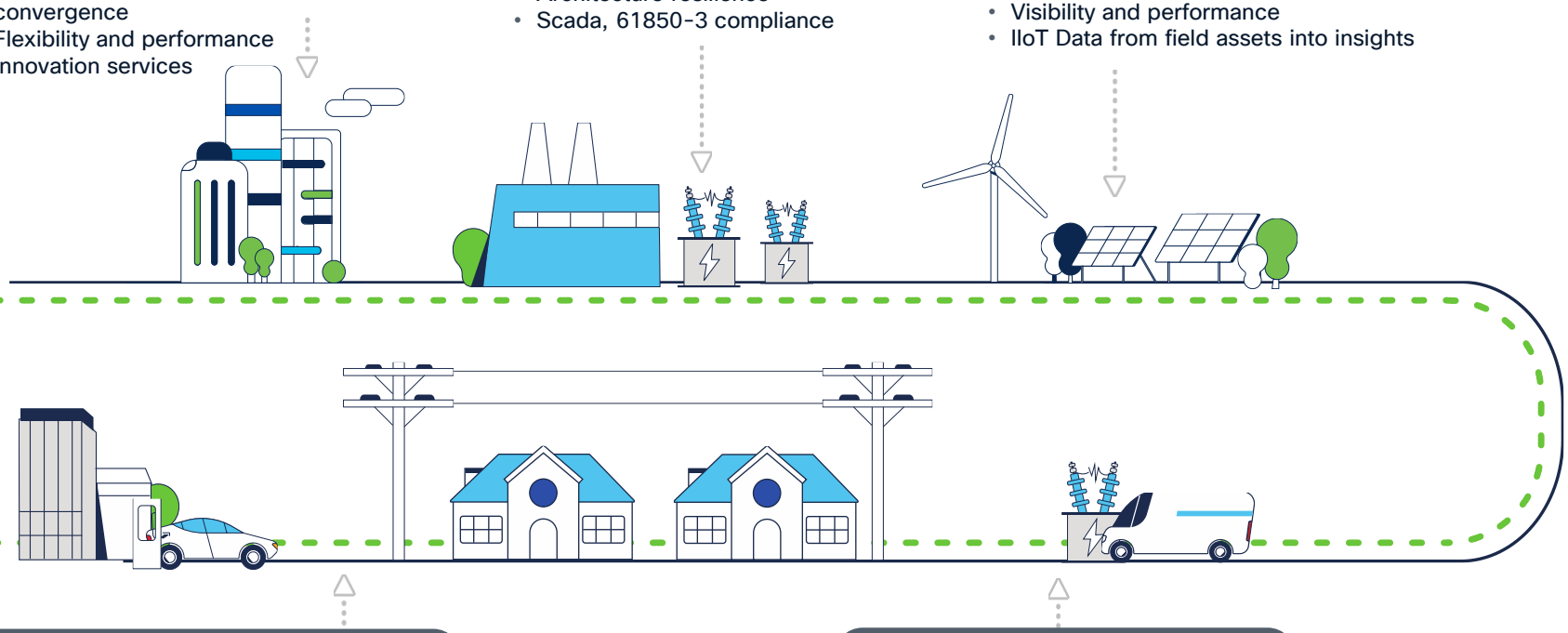
- New power needs such as AI datacenter and EV charging)
- Interoperability
- Architecture resilience
- Scada, 61850-3 compliance

Utility operational WAN

- Reduced OPEX through convergence
- Flexibility and performance
- Innovation services

Renewable energy resources

- Secure remote access and connectivity
- Visibility and performance
- IIoT Data from field assets into insights



Grid security

- NERC CIP/IEC62443
- Reduce risk to business
- Front workers safety

Advanced metering infrastructure

- Multi-service scalability
- Demand response, remote disconnect
- Open standard communications (Wi-SUN)

Distribution grid automation

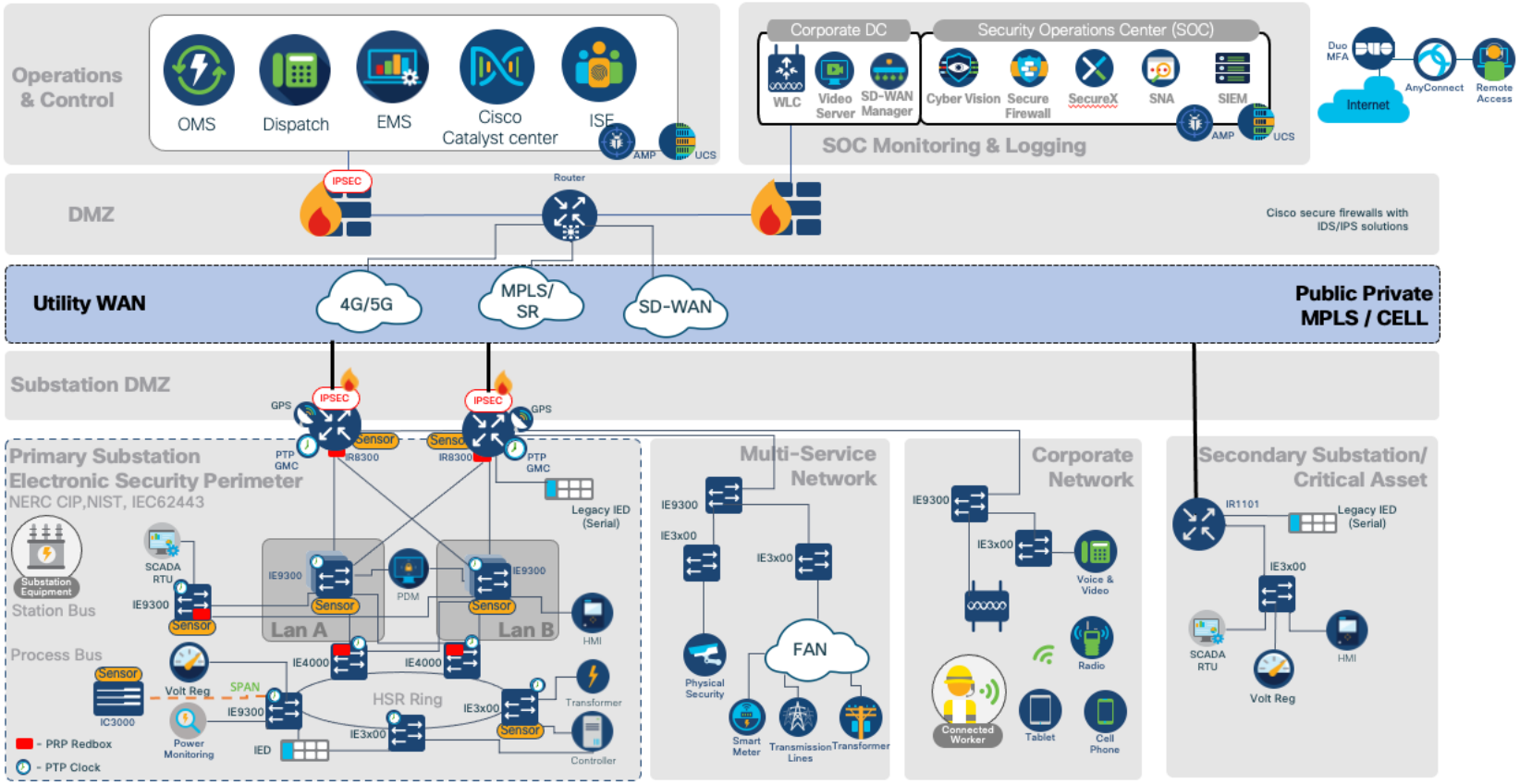
- Moving to the two way grid
- Demand Response
- Reliability, quality of service
- Grid efficiency and stability
- Energy efficiency, OPEX reduction

OT Network management and automation that delivers massive scale, OpEx efficiency, and operational visibility

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Validated Design: Substation Automation

Foundation for advanced protection and control, remote diagnostics and predictive maintenance capabilities.



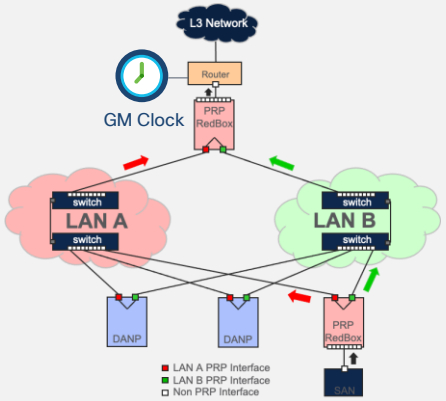
Features/Functions:

- Support **SCADA Services**
  - Serial/TDM to IP transition
  - Station & Process bus architectures – (IEC 61850 MMS,GOOSE & SV)
  - Support IEC104/DNP3 Architectures
- Support for **power management devices** (e.g. Syncro Phasor/PMU, Volt/Var) applications
- **Cybersecurity**
  - NERC CIP compliance
  - IEC62443 (Zones & Conduits)
- Visibility of connected substation devices and communications (**Asset Visibility**)
- Support lossless **Network resiliency and Precise timing**
  - HSR and PRP
  - IEEE1588 PTP Power profile
- **Management and Automation** to proactively identify WAN/LAN network issues and receive remediation suggestions and consistently configure and maintain network infrastructure
- **WAN Connectivity** – SD-WAN, IP/MPLS, Segment Routing, LTE, 5G and 450Mhz

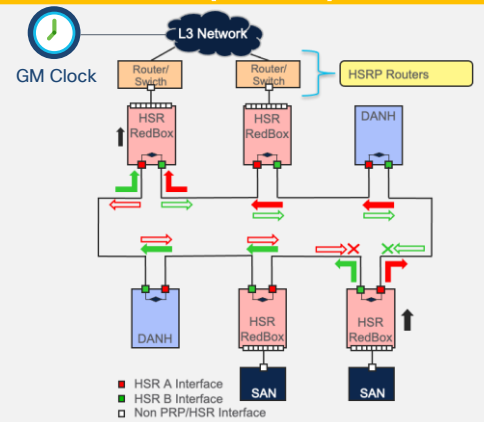
© 2025 Cisco and/or its affiliates. All rights reserved.

Support for IEC61850 Architectures

Parallel Redundancy Protocol (PRP)



High-Speed Resiliency (HSR)



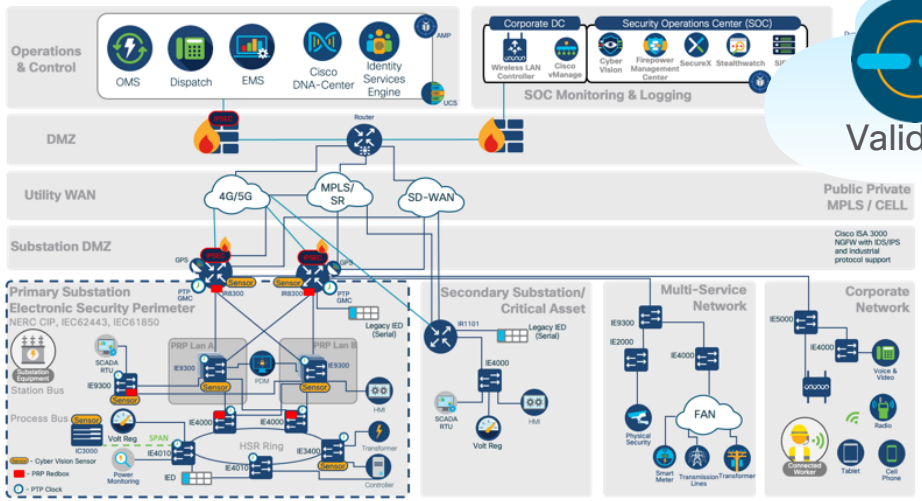
- Loss-less resiliency protocols and no single-point-of-failure topologies for maximum up-time (PRP & HSR)
- Station bus & Process bus topologies
- Substation Synchronization with support for
  - Power-Profile Precision Time protocol (Grandmaster, Transparent Clocks) C37.238/IEC61850-9-3
  - Wide-range of timing inputs and conversions (IRIG B)
- Low-latency communications with Quality-of-Service settings to prioritize IEC61850 critical traffic (GOOSE,SV)
- IEC 61850-3 certifications for substation hardware
- Validated Design topologies and product choices
- IEC62351 security profiles (TLS ,HMAC & MACsec)
- Platform for future evolution (e.g. Edge data, Virtualization, 5G, SDN)

© 2025 Cisco and/or its affiliates. All rights reserved.

Key Platforms in the SA Validated Design

Cisco Catalyst Center & ISE

Substation Automation CVD



Cisco SD-WAN

Manager

Validator

Analytics

Controllers

Catalyst IE9300 Rugged Series Switch

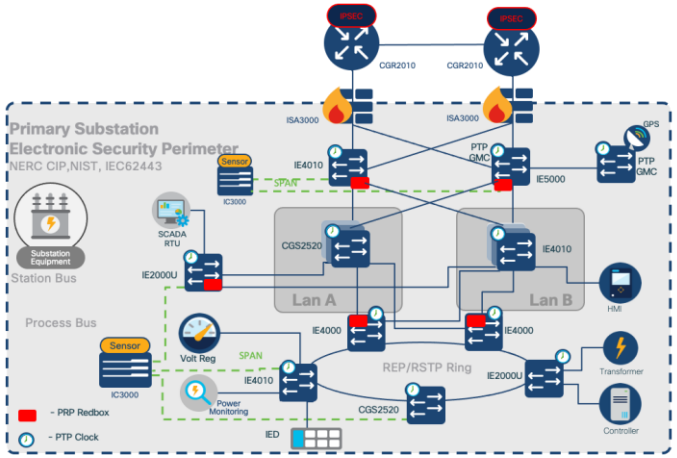
Catalyst IR8300 Rugged Series Router

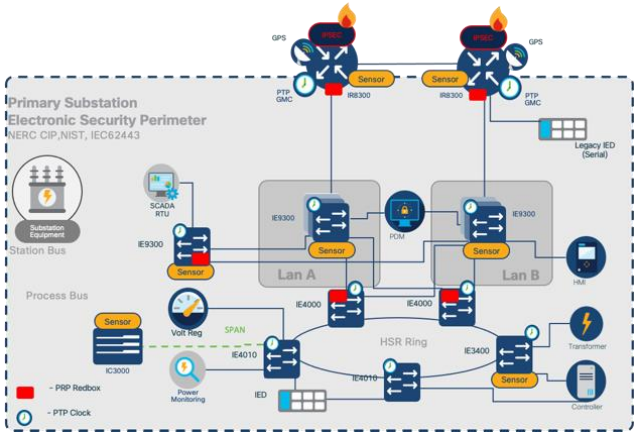
Blogs :
https://blogs.cisco.com/internet-of-things/four-must-haves-in-the-new-digital-substation

© 2025 Cisco and/or its affiliates. All rights reserved.

Digital Substation Architecture enables new capabilities, while being simpler to manage, more redundant and secure

Before





After

- Complex Redundant WAN design
- Separate boxes for:
  - WAN connections
  - Redbox Layer for PRP to WAN
  - PTP Grandmaster (IE5K or 3rd Party)
  - Firewalls
- Limited BW/Thruput:
  - Very limited WAN throughput (<50Mbps)
  - Limited MPLS support – CE only recommended
  - Limited WAN connections WAN Port count limited
  - Lack of Fiber SFP ports
  - No stacking possible (port count)
  - FE Downlink ports (e.g. CGS)
- No network consolidated network management
- Standalone CV sensors with SPAN ports
- Challenging to deploy TrustSec

- Simple redundant WAN design
- 4 box consolidation: WAN, PRP/HSR SAN Redbox, PTP GM and ZBFW Firewall (IDS/IPS with UTD), Reduced footprint/power/heat

- Dramatically higher BW/Thruput:
  - Higher WAN (950 Mbps LAN-WAN L3 IMIX) & switch throughput (950 Mbps LAN-LAN L2 IMIX)
  - MPLS CE and P/PE with TE, L3VPN
  - High bandwidth and fiber-density SFP and stacking to increase port count

- Common Network management with Catalyst Center and SD-WAN Manager for Automation
- Integrated CV sensors
- More secure infrastructure (TrustSec, Trust Features, MACsec)

© 2025 Cisco and/or its affiliates. All rights reserved.

Blog: https://blogs.cisco.com/internet-of-things/deliver-next-generation-substation-automation-with-the-cisco-catalyst-ir8340-rugged-router

Automated deployment and management

Automated Management for The Digital Substation

Cisco Catalyst Center

Reduce Downtime

Improve network visibility and performance with AI/ML and machine reasoning

Increase Efficiency

Automation and workflows simplify, empower, and streamline network management

Stay Compliant

Track updates, ensure SW images comply, and remain aware of security updates

Redefine the experience

Platform built on intent-based networking principles and driven by advanced AI, insights and security

Spend less time managing your operational network

© 2025 Cisco and/or its affiliates. All rights reserved.

Predictive Maintenance for your industrial network - proactively identify and mitigate connectivity issues

Network Assurance

Before → After

Hours spent fixing network faults	Resolve issues with a single module click

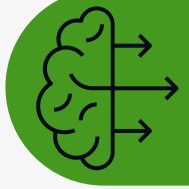
Automatically detect and prioritize issues

AI/ML-driven remediation for quick resolution

Improve network performance

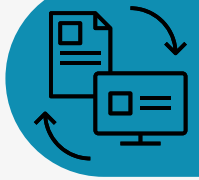
Cisco Catalyst Center **Assurance**

Constant monitor of network and devices for up-to-date visibility



AI/ML and machine reasoning for root cause analysis, to find anomalies instantly

Correlated insights, with telemetry data to accurately pinpoint root cause



Guided remediation allows for single-click resolution, allowing machine reasoning automation to close the loop

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst Center Network Automation to drive operational efficiency and streamline maintenance

Base Automation

Before → After

Manual device configuration	Simple automated workflows

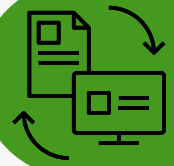
Workflows to do in seconds what used to take hours / days

Lower cost of network operations

Bridge the IT skill gap and save time

Cisco Catalyst Center Base **Automation**

Zero-touch provisioning speeds and simplifies adding new devices (PNP, RMA)



Software image management (SWIM) provides consistency for better network performance

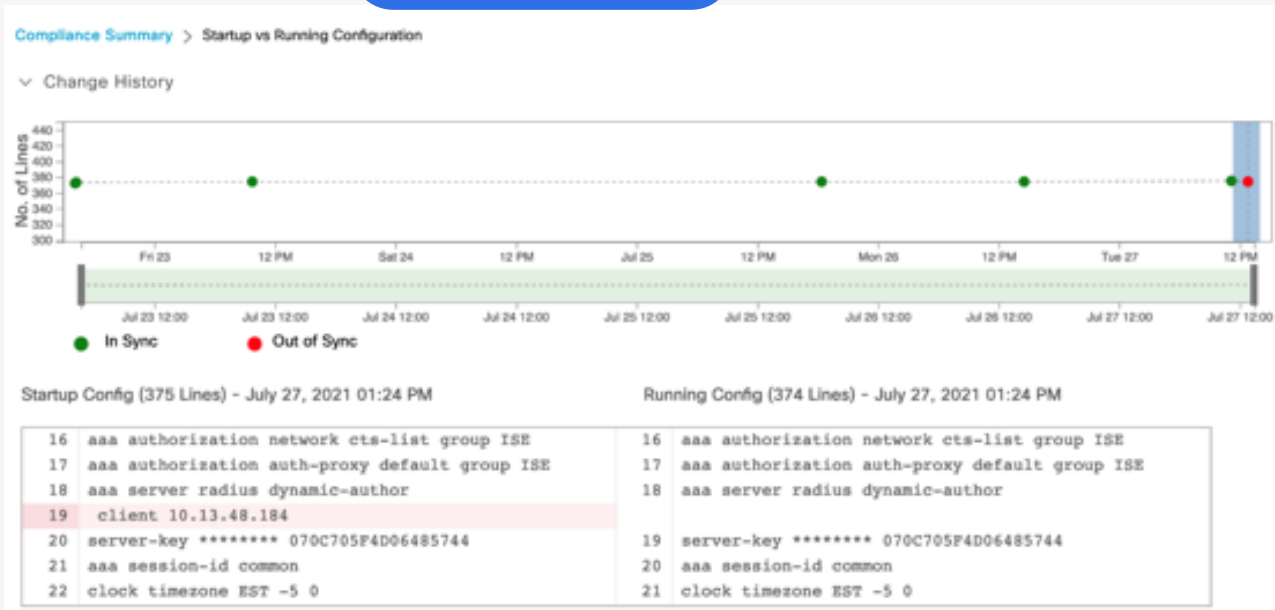
Machine reasoning (MR/ML) workflows automate complex tasks into the simple push of a button

© 2025 Cisco and/or its affiliates. All rights reserved.

Compliance Checks to ensure changes made to the network are consistent with your standards

Network Compliance

Configuration Drifts



Before → **After**

Discrepancy between As-Built vs As-Is network	Insights on deviations to ensure compliance

Continuous monitoring for network changes

Audit logging to track who (and what/when) made changes

Cisco Product Security Incident Response Team Alerts

“Golden Image” confirmation for all network devices

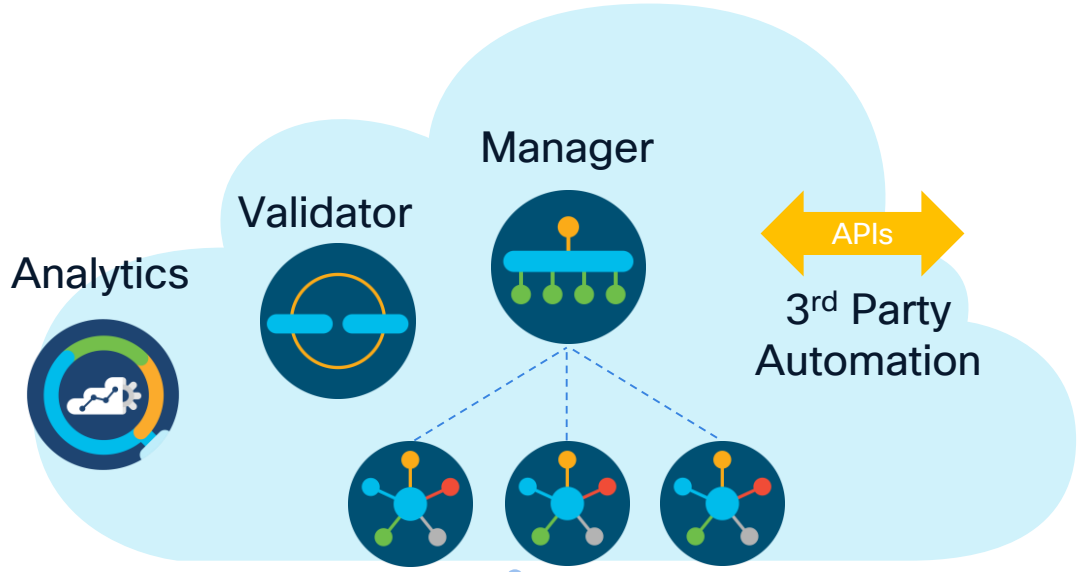
Critical Security Advisories – “Psirts”

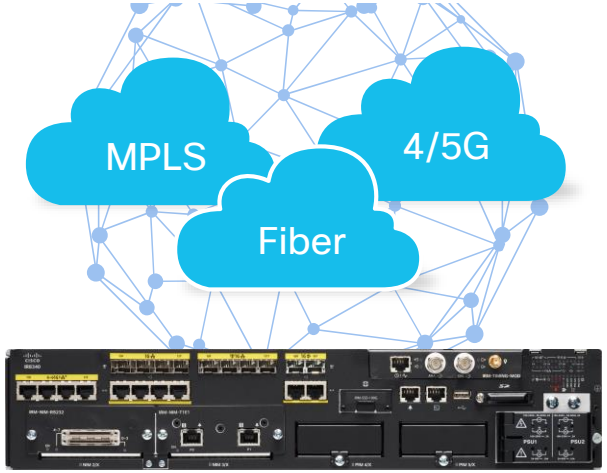
Cisco Catalyst Center **Compliance**

© 2025 Cisco and/or its affiliates. All rights reserved.

SD-WAN for Substation Automation

- Centralized provisioning & monitoring
- Implement centralized security policies
  - **ZBFW, IDS/IPS, URL Filtering, Cisco Umbrella DNS**
- Configuration templates
- Troubleshooting and monitoring
- Software upgrades
- IOS XE operating system
  - open interfaces: NETCONF,RESTCONF,YANG etc
- Validated for Substation use cases
  - Ethernet and Serial based SCADA use cases
- *NEW !* - Cyber Vision integration
  - Sensor deployment from SD-WAN Manager 20.15.1
- *NEW !* - 3rd party application deployment (e.g. vRTU) 20.16.1





IR 8340 Substation Gateway

© 2025 Cisco and/or its affiliates. All rights reserved.

More Capability, Smaller Footprint

Cisco Catalyst IR8340 Rugged Series Router

Built for the Substation edge

20x Services Throughput improvement
1G in access and edge
Switching ports (REP, HSR, PRP)

SD-WAN supported
GNSS Timing Module (NTP/PTP/IRIG B/SyncE)
ICS Visibility with Cyber Vision
256-bit WAN MACSec & IPsec

Built-in edge compute resources
MPLS & Segment Routing
Group Based Security Policy (Trustsec)

Cisco multi-layer security

- SSL acceleration
- Application firewall
- IPS/IDS and URL filtering
- AMP, ThreatGrid
- Umbrella SIG

WAN port density

Default 8G DRAM

1G w/ MACsec

Pluggable NVMe storage

5G

© 2025 Cisco and/or its affiliates. All rights reserved.

Industrial Routers with Next-Gen Firewall (NGFW)

+ Cisco Security

Ethernet | Cellular | MPLS | 5G | Starlink | Fiber

Multi-transport Agnostic

IOS-XE

Application Firewall
>5000 layer 7 apps classified (1500 on box)

Network Segmentation
Virtual Isolation between network segments

DoS Protection
Protection against denial-of-service attacks

NGFW Add-On

URL Filtering
Custom Domains & Web Reputation Score

Advanced Malware Protection
File Reputation & Sandboxing

Snort IDS/IPS
Most widely deployed IPS engine in the world

SSL Decryption
Detect Threats in Encrypted Traffic
IR8340 Only

Direct Internet Access

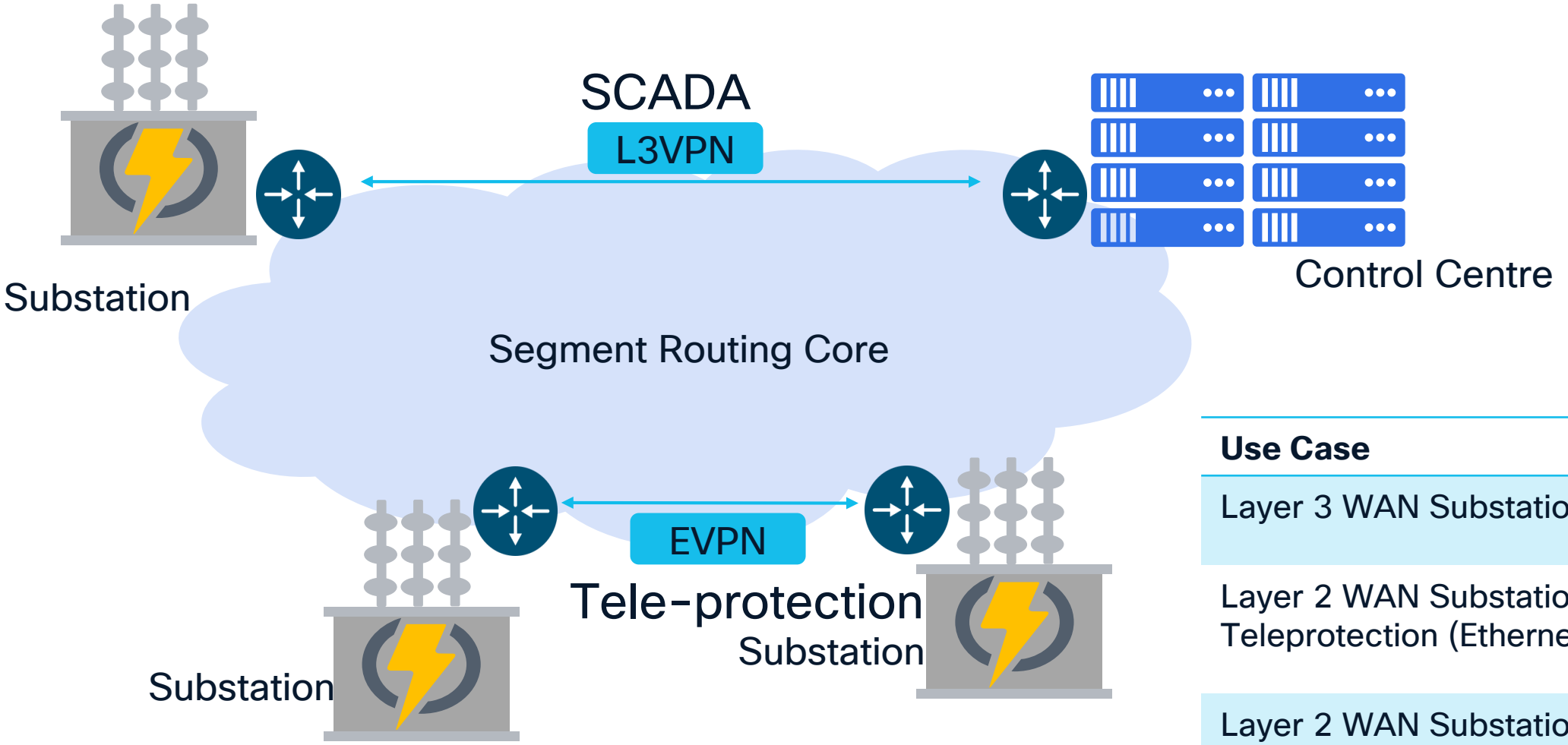
Secure Internet Gateway
DNS / Web Security with Cisco Umbrella

© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Wide Area Networking

CISCO Live !

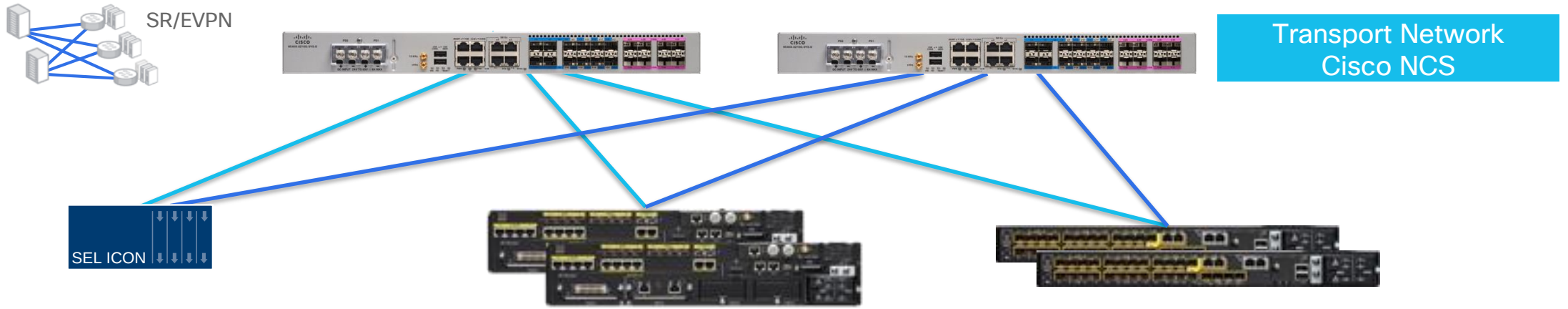
Utility WAN high level view



Use Case
Layer 3 WAN Substation to Datacentre
Layer 2 WAN Substation to Substation for Teleprotection (Ethernet based)
Layer 2 WAN Substation to Substation for Teleprotection (non-Ethernet based)

© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Automation WAN



SEL ICON – Non-Ethernet based Teleprotection	IR8340 - Layer 3 Gateway for Ip based services (e.g SCADA)	IE9320 - Layer 2 Gateway for Ethernet based teleprotection
• C37.94 (Nx64) • E&M 4W VF • G703 Codir • E1 • DS1 (Sync/Aysnc) • FXO/FXS • PTP Timing • IRIG-B • Ethernet • Serial (Aysnc/Sync) • Transfer Trip	• Scada Traffic • Cybervision (App hosting) • Timing (GPS/PTP/IRG-B) • PRP/HSR Redbox • ZBFW • SD-WAN • Cellular • MPLS/Segment Routing PE • IPsec & WAN MACsec	• PRP/HSR • GOOSE (Ethernet) based tele-protection • Trustsec • Cybervision (App hosting) • PTP C37.238/IEC61850-9-3 • MACsec

© 2025 Cisco and/or its affiliates. All rights reserved.

Layer 3 Services – SCADA Traffic

- eBGP peering between CE Substation Router and NCS PE router
- BGP control plane is leveraged with VPNv4 address family exchange between PE nodes
- SR TI-LFA FRR configured under IGP for sub-50ms convergence

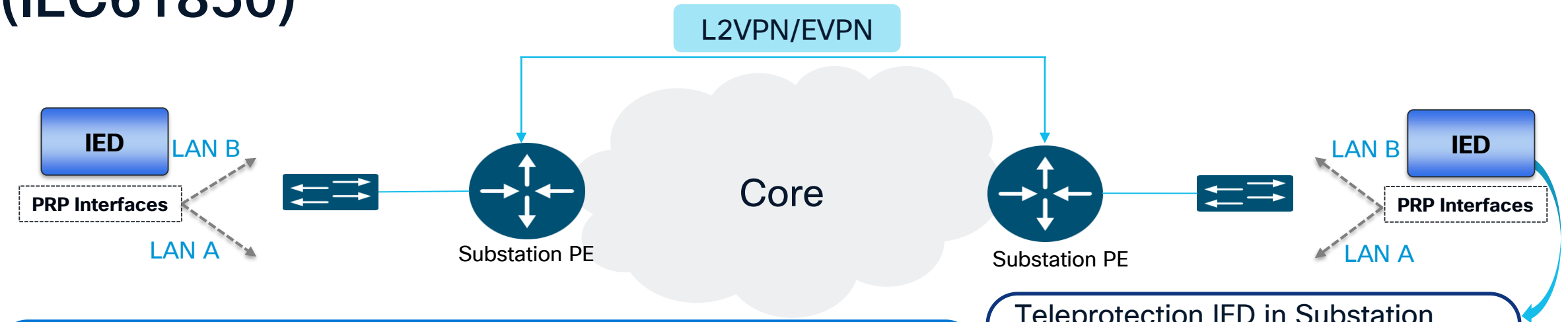
Requirements

- Over a design parameter of <=***500 km fiber length*** :
  - End-to-end maximum delay time of ***5ms***

Design and Requirements validated

© 2025 Cisco and/or its affiliates. All rights reserved.

Ethernet Based Teleprotection over Packet based Networks (IEC61850)



Path Predictability key requirement for Teleprotection services

- bounds on *asymmetry delay* & *end-to-end delay*
- *sub-50ms* convergence

Teleprotection IED in Substation

- may employ Current Differential, Distance protection schemes
- uses IEC 61850 GOOSE packets

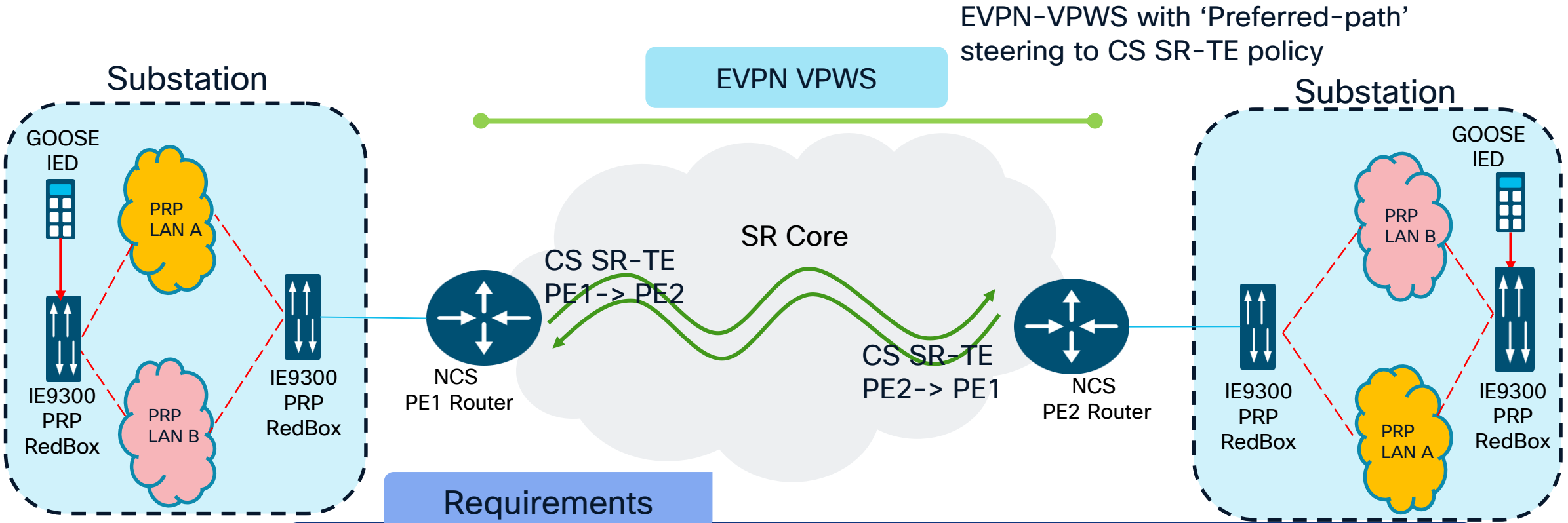
Transport necessary with *Circuit-style* features

- Flex-LSP used traditionally in IP/MPLS based networks (supported in XE based platforms)

GOOSE: Generic Object Oriented Substation Event
PRP: Parallel Redundancy Protocol

© 2025 Cisco and/or its affiliates. All rights reserved.

Layer 2 Services with Circuit-style SR



Requirements

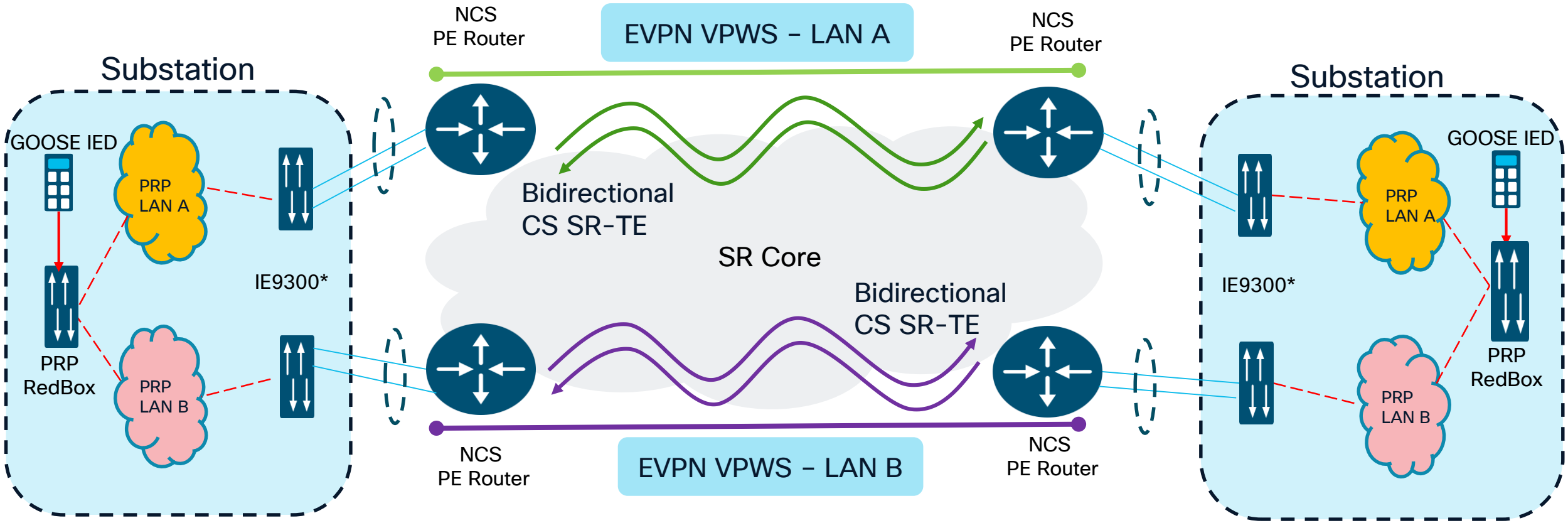
- Switching time from primary to backup path and vice versa < ***50ms***
- Over a design parameter of <=***500 km fiber length*** :
  - End-to-end maximum delay time of ***5ms***
  - Max. asymmetry delay of ***200µs***

Design and Requirements validated

RedBox: Redundancy Box

© 2025 Cisco and/or its affiliates. All rights reserved.

Layer 2 Services with Circuit-style SR:



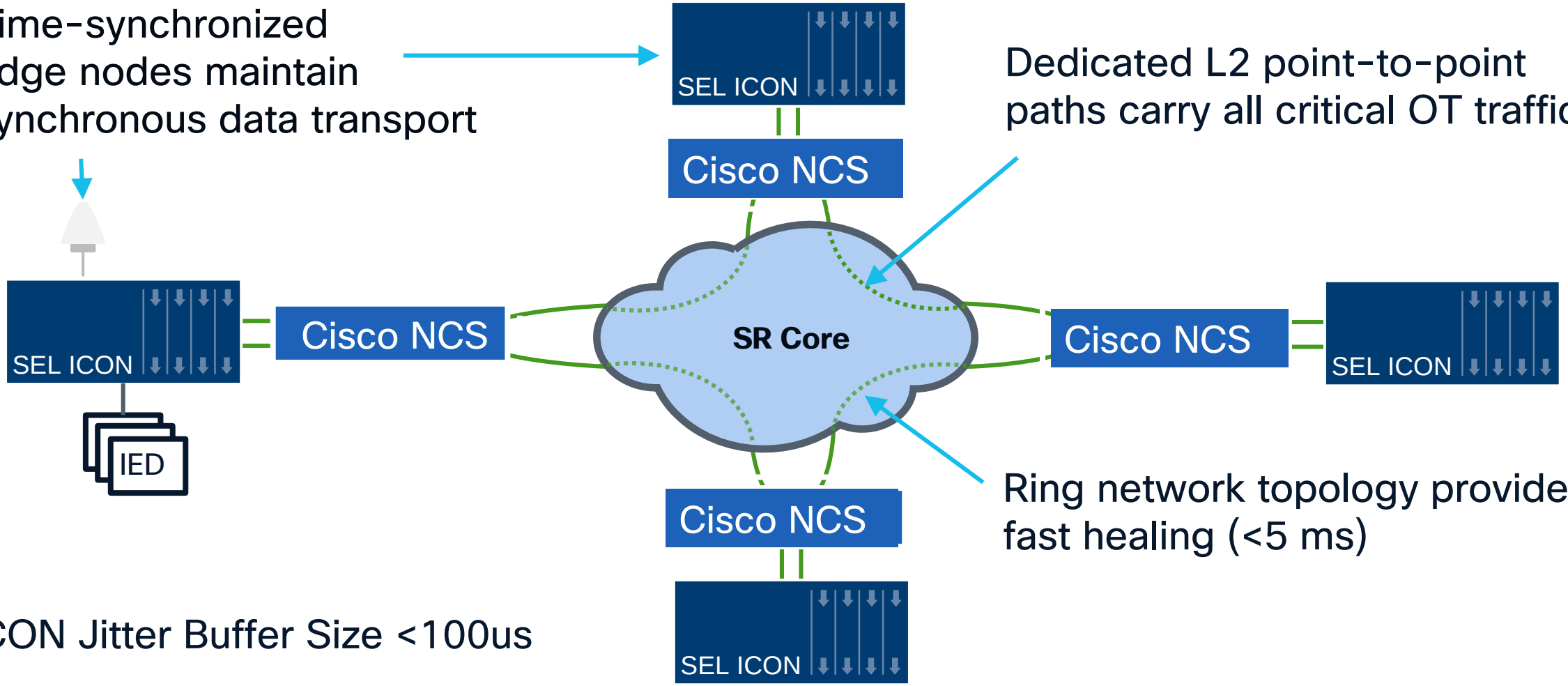
(*) CE = IE9300 with PRP Redundancy == OFF

- CE connected to one PRP LAN (LAN A OR LAN B) and acts as plain switch
- EVPN VPWS extends PRP LAN A and LAN B respectively between Substations

© 2025 Cisco and/or its affiliates. All rights reserved.

SEL ICON Overlay Architecture for Non-Ethernet based Teleprotection

Time-synchronized edge nodes maintain synchronous data transport



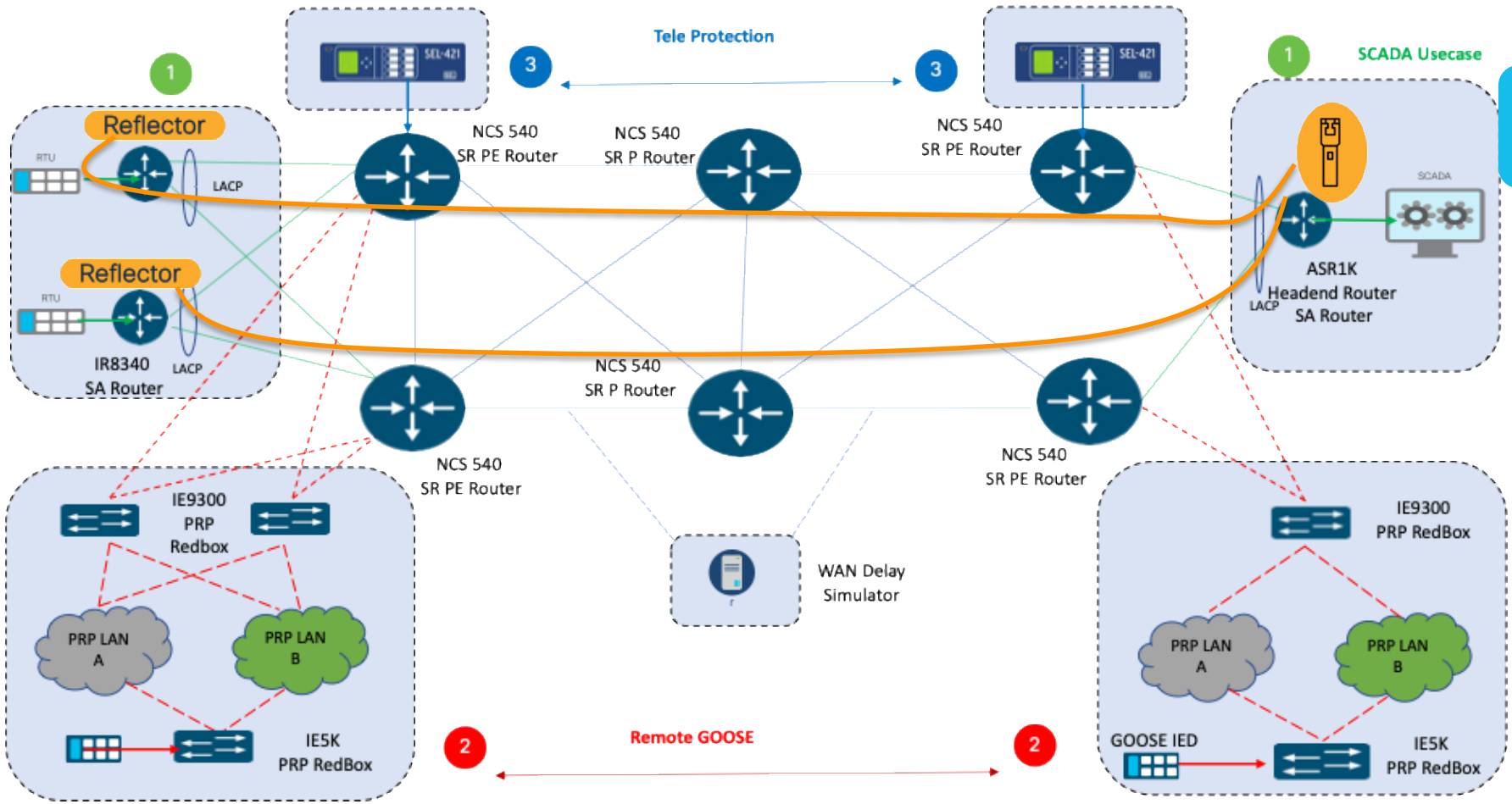
Dedicated L2 point-to-point paths carry all critical OT traffic

Ring network topology provides fast healing (<5 ms)

ICON Jitter Buffer Size <100us

© 2025 Cisco and/or its affiliates. All rights reserved.

Performance Assurance – L3 SCADA use case



PCA Analytics

PCA Platform

WAN substation to Control Center

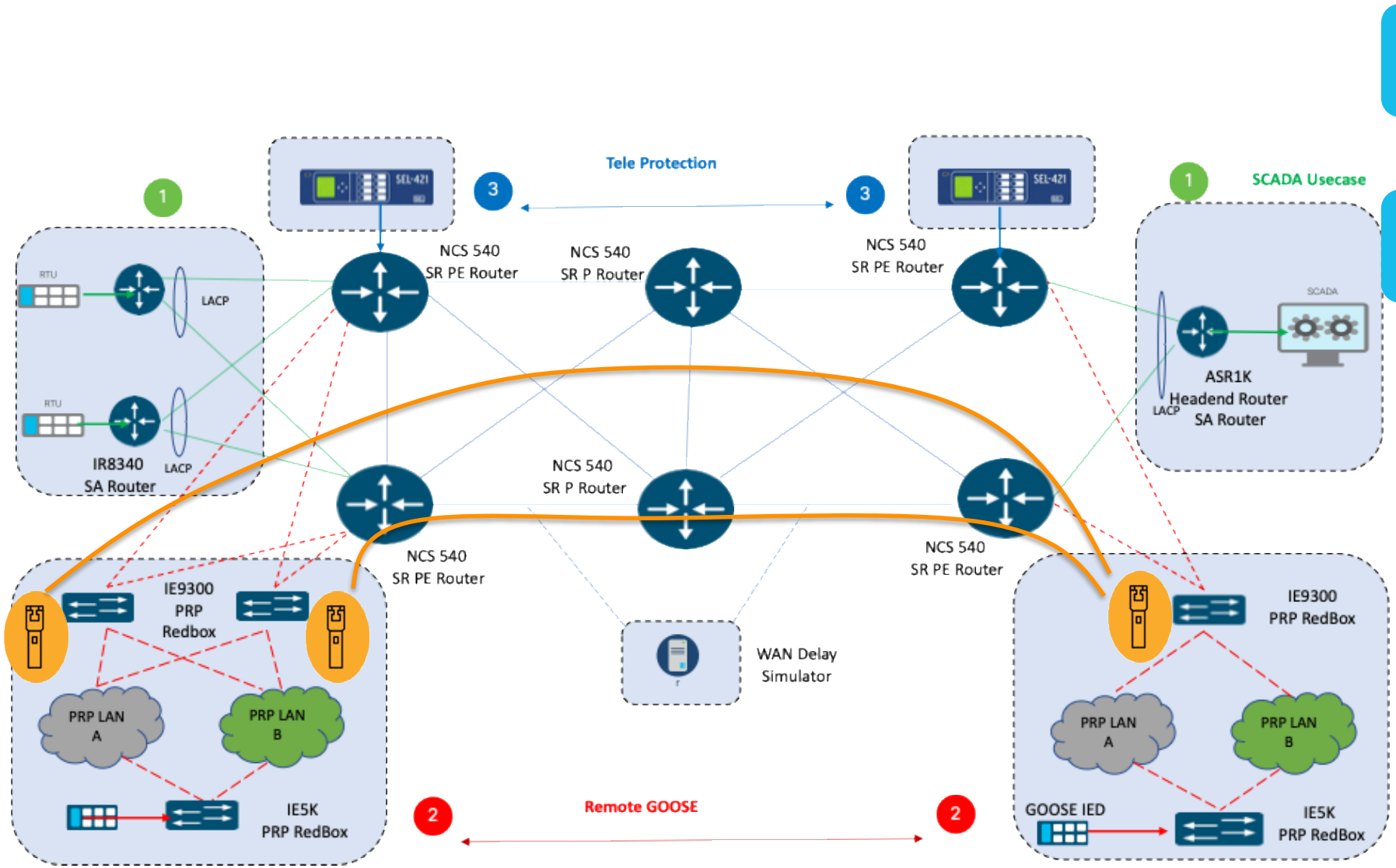
- L3VPN Control Center/Headend to Substation
- Scada: Critical traffic but no latency sensitivity
- Other IP traffic

→TWAMP+:

- Monitoring different VRFs carrying traffic from different services
- Packet Loss focus

© 2025 Cisco and/or its affiliates. All rights reserved.

Performance Assurance – L2 GOOSE



Inter-substation

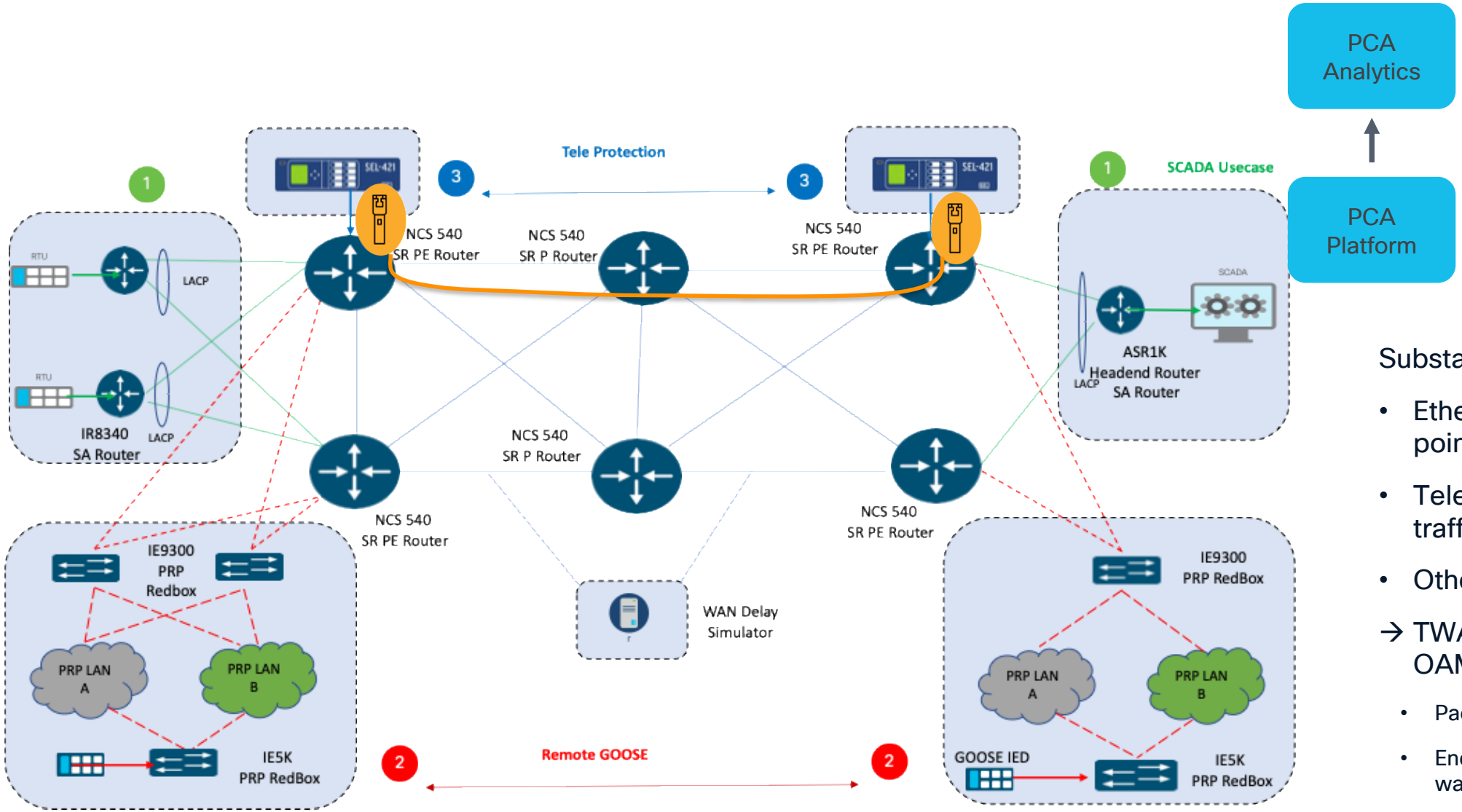
- Ethernet L2VPN
- GOOSE: : Latency < 5ms
- Other traffic

→TWAMP or ETH-OAM+:

- End-to-End Latency one-way metrics

© 2025 Cisco and/or its affiliates. All rights reserved.

Performance Assurance - L2 Teleprotection



Substation to substation

- Ethernet L2 point-to-point
- Teleprotection: critical traffic, low latency
- Other traffic

→ TWAMP or ETH-OAM+:

- Packet loss focus
- End-to-End Latency one-way metrics

© 2025 Cisco and/or its affiliates. All rights reserved.

Timing and Synchronization

Challenges by using GPS as the only clock source in the Substation

- GPS timing sources might be challenged by Spoofing or Jamming
- GPS antennas might be covered in meters of snow
- Substations sometimes are in mountains or tunnels
    - Long antenna cables might be required, are costly and will introduce loss
- Directives , regulations and Executive Orders to reduce the dependency of GPS for timing services are being discussed and implemented.
    - Both in US, Europe and the Middle east
    - Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services
    - NIST Tech Note: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2187.pdf

© 2025 Cisco and/or its affiliates. All rights reserved.

Sunday
November 17, 2024

dictionary + A - A

North Korea's GPS jamming continues for 10th day

Published: 17 Nov. 2024, 14:30

America is at risk of high impact GPS jamming and spoofing from space

Dana A. Goward October 24, 2024

BY MORGAN MEAKER BUSINESS OCT 17, 2024 6:32 AM

GPS Jamming Is Screwing With Norwegian Planes

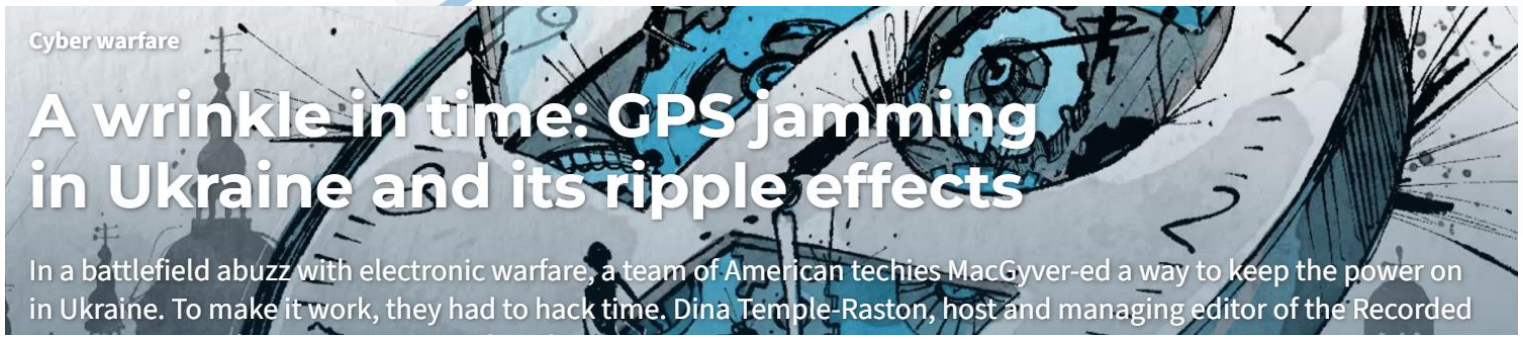
So much jamming is taking place in northeastern Norway, regulators no longer want to know.

SHARE ARTICLE

Russian Jamming Is Wreaking Havoc on GPS in Eastern Europe. But Is It Hybrid Warfare?

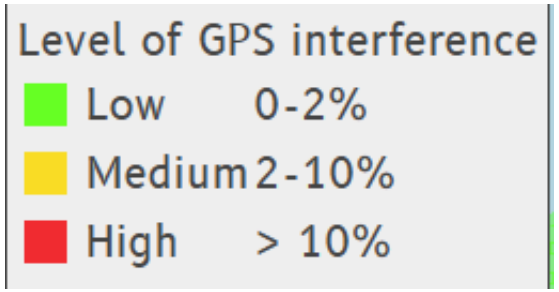
July 10, 2024 | By Shaun Waterman

Amid unprecedented amounts of electronic warfare in Russia's war on Ukraine, there is no doubt that the Russians are jamming GPS and other satellite-based navigation systems around the Baltic Sea. Earlier this year, the interference forced a temporary halt of

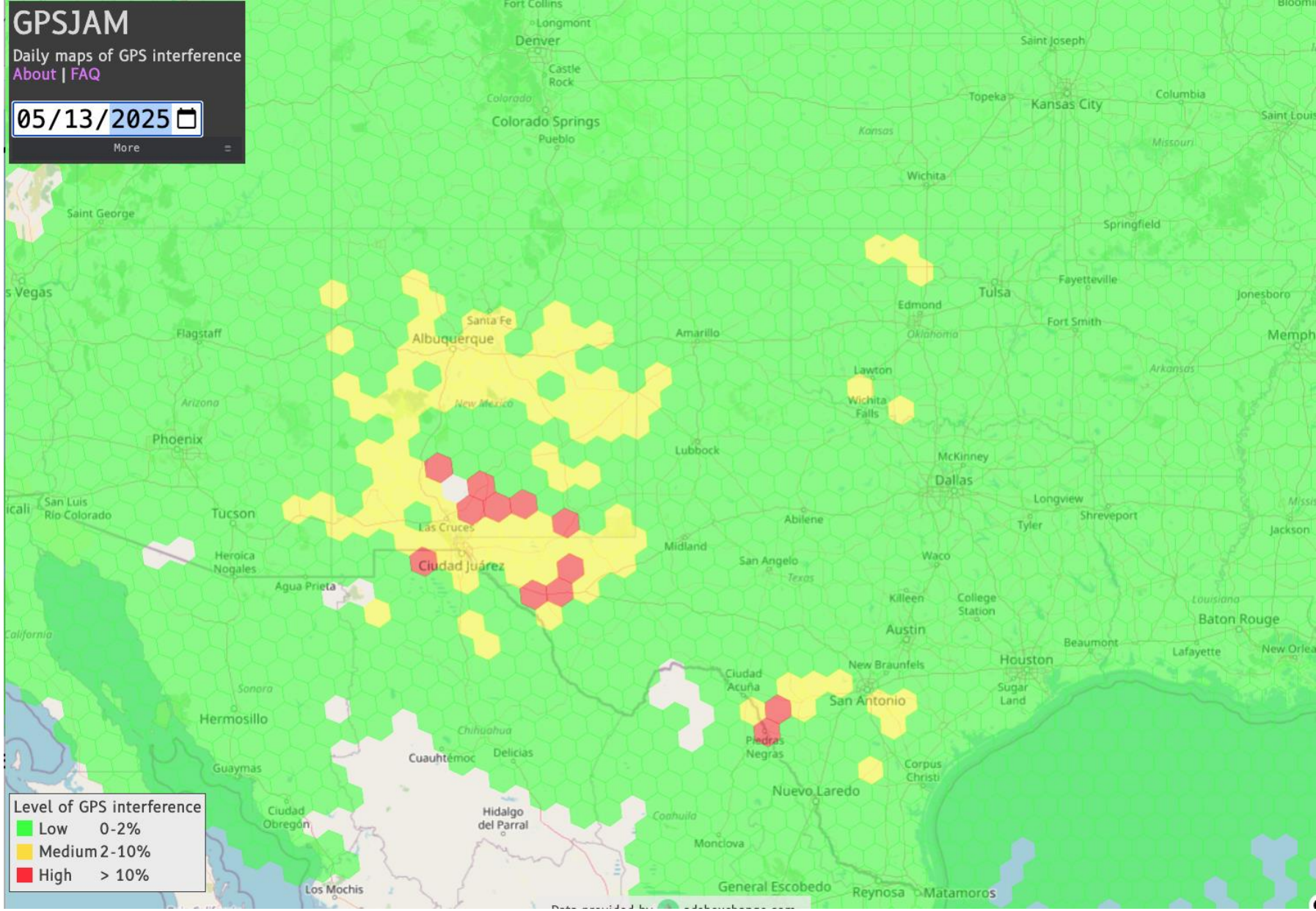


© 2025 Cisco and/or its affiliates. All rights reserved.

GPS Jamming in United States



Source: gpsjam.org



© 2025 Cisco and/or its affiliates. All rights reserved.

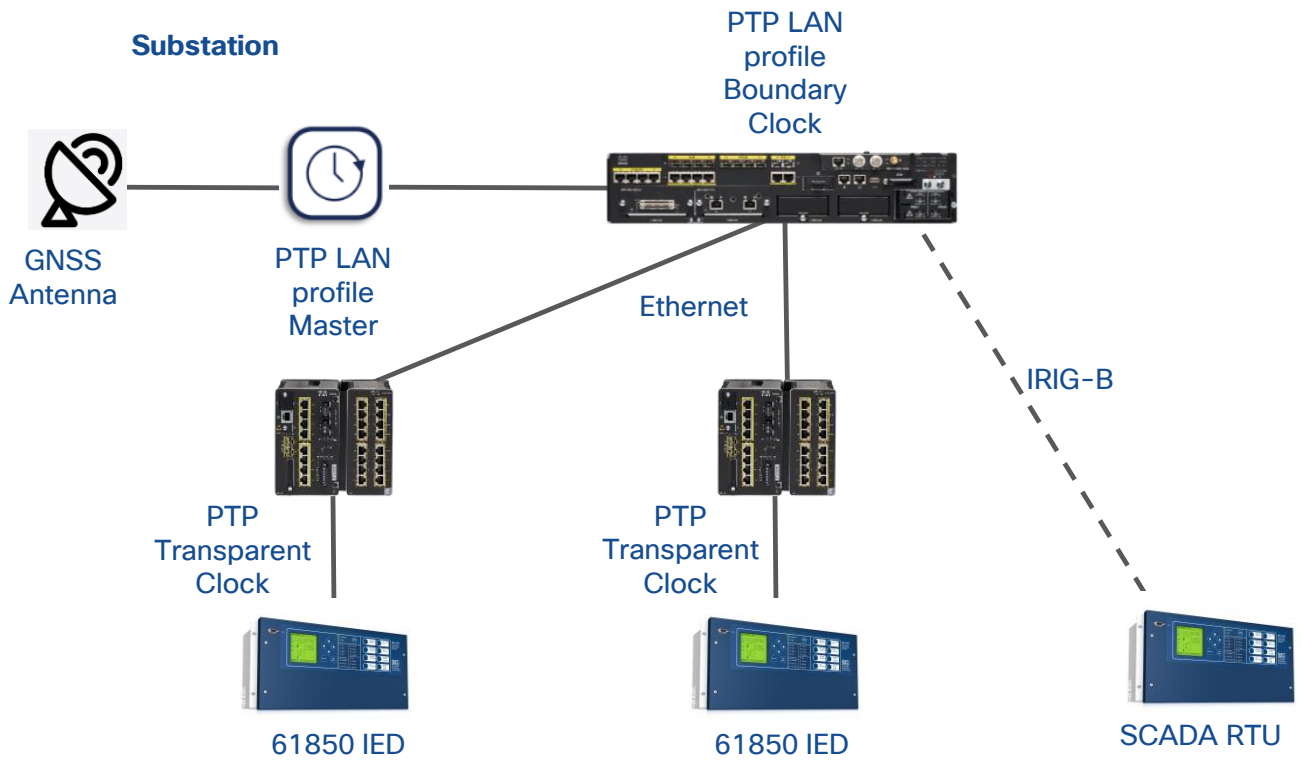
What's Strategies are Available ?

- Local substation-based GPS timing sources (situation today)
- Primary reference clocks (PRC) centrally located in the WAN
  - Provide timing to substation edge via the WAN (PTP/SyncE).
  - Conversion to power profile at substation edge for substation use
  - High quality (Cesium or Rubidium), Highly accurate and with jamming/Spoofing protection
- **PTP and network clocks used together to provide more robustness (PTP & SyncE)**
- PTP Telecom Profile for Frequency (G.8265.1)
- PTP Telecom Profiles for Time and Phase
  - **"Full on path Timing Support" (G.8275.1)**
  - "Partial Timing Support" (G.8275.2) also with GPS assist at the edge

© 2025 Cisco and/or its affiliates. All rights reserved.

Evolution of PTP Timing in Substations

Typical substation timing today with local GNSS

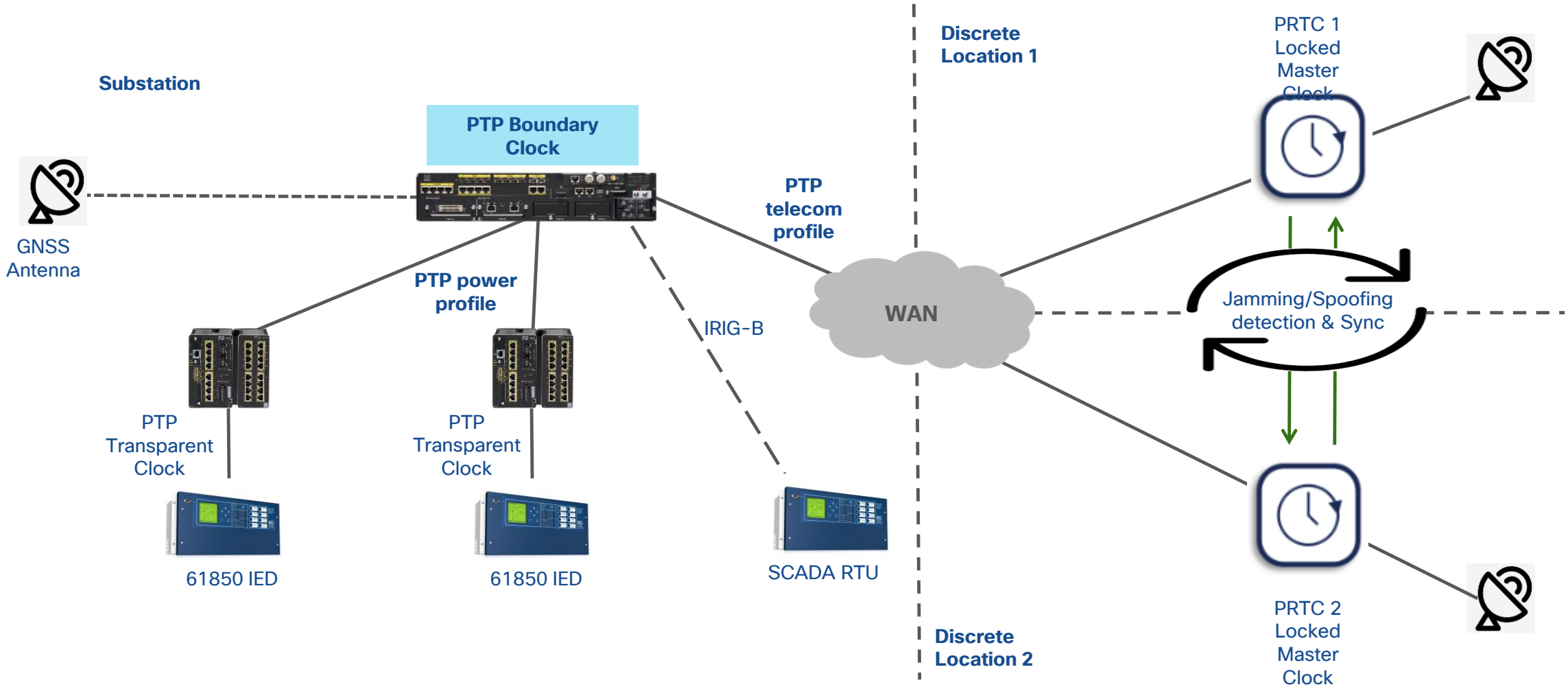


- Architecture Disadvantages:
  - Additional management domain for external PTP master at each substation.
  - Primary reference clock needed at each substation
  - Clock holdover not as good as higher quality master clocks. Quality vs quantity doesn't scale well over many substations. Higher quality clocks more sensitive to industrial temperature ranges, not suitable for substation deployment.
  - Failure domains at each substation. Equipment failure, jamming, spoofing. During failure, each substation will drift independently.
  - Weather or other environmental factors may impact reception each substation independently.
  - Little or no redundancy outside of substation.

© 2025 Cisco and/or its affiliates. All rights reserved.

Evolution of PTP Timing in Substations

Terrestrial based timing solution

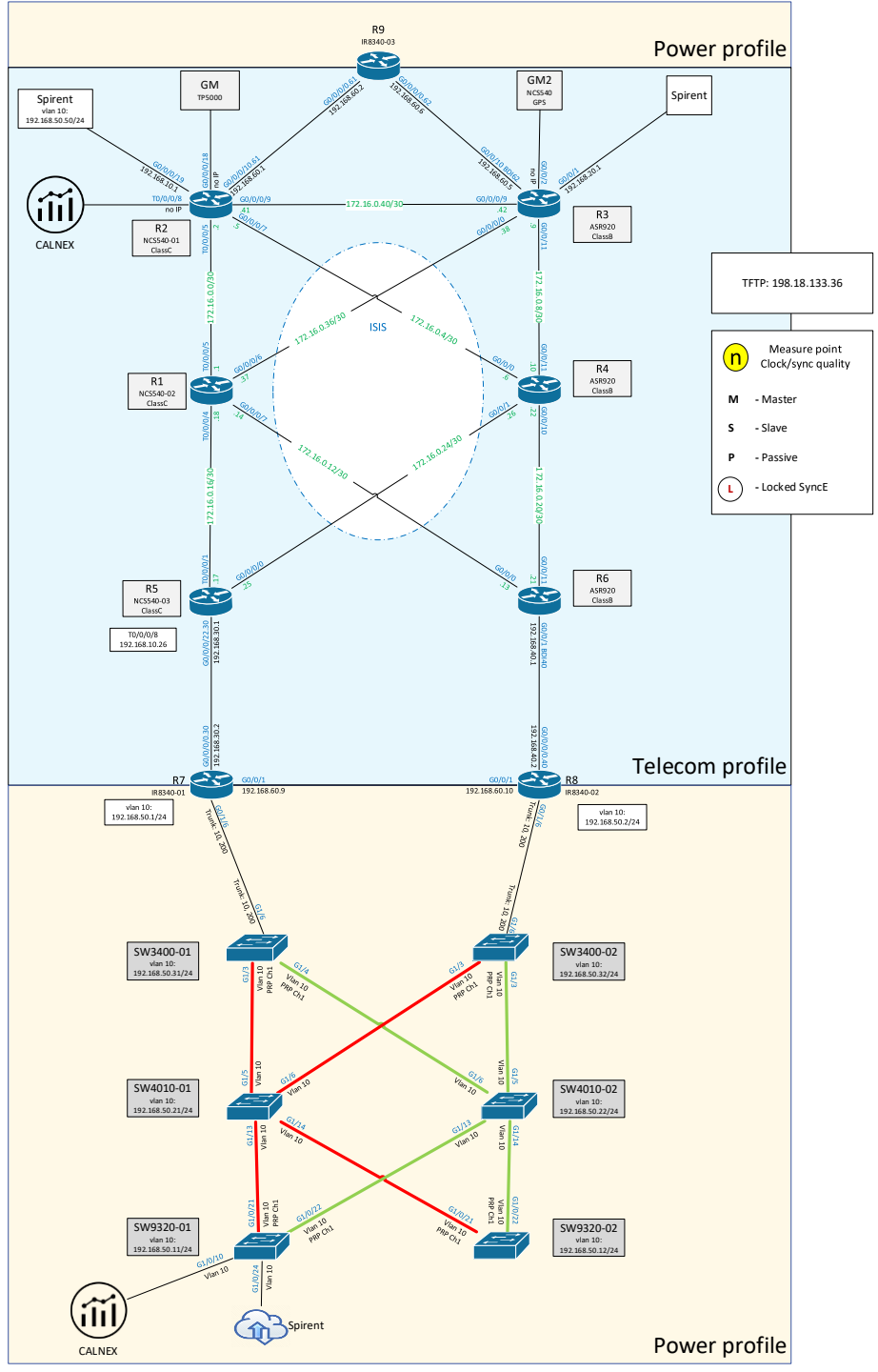


© 2025 Cisco and/or its affiliates. All rights reserved.

PTP CPOC testing

Customer CPOC in Cisco Lab

- Two Grand Master clocks (Microchip Timemaster)
- WAN with NCS540 and ASR920
  - Telecom Profile (8275.1) in the WAN
- IR8340 Substation Router with Timing Module
  - Power profile and PRP in the substation
  - PTP interworking Telecom to Power Profile
  - IR8340 acting as Boundary Clock
- Siemens Energy Protection IED's
  - Current differential scheme between IEDs



© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst IR8340 Substation Timing

IR8340 Timing Module

- GNSS
- IRIG-B
- TOD

Multi Band & Constellation Support

- GPS
- GLONASS
- BEIDOU
- GALILEO

Time Pulse Accuracy

- Clear sky – 20ns
- Indoor – 500 ns

Built-in Oscillator

- Stratum 3e
- More accurate hold-over in case of GNSS loss

Enabling Precision Timing for IEC61850 substation-based Applications

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Validated Design Update

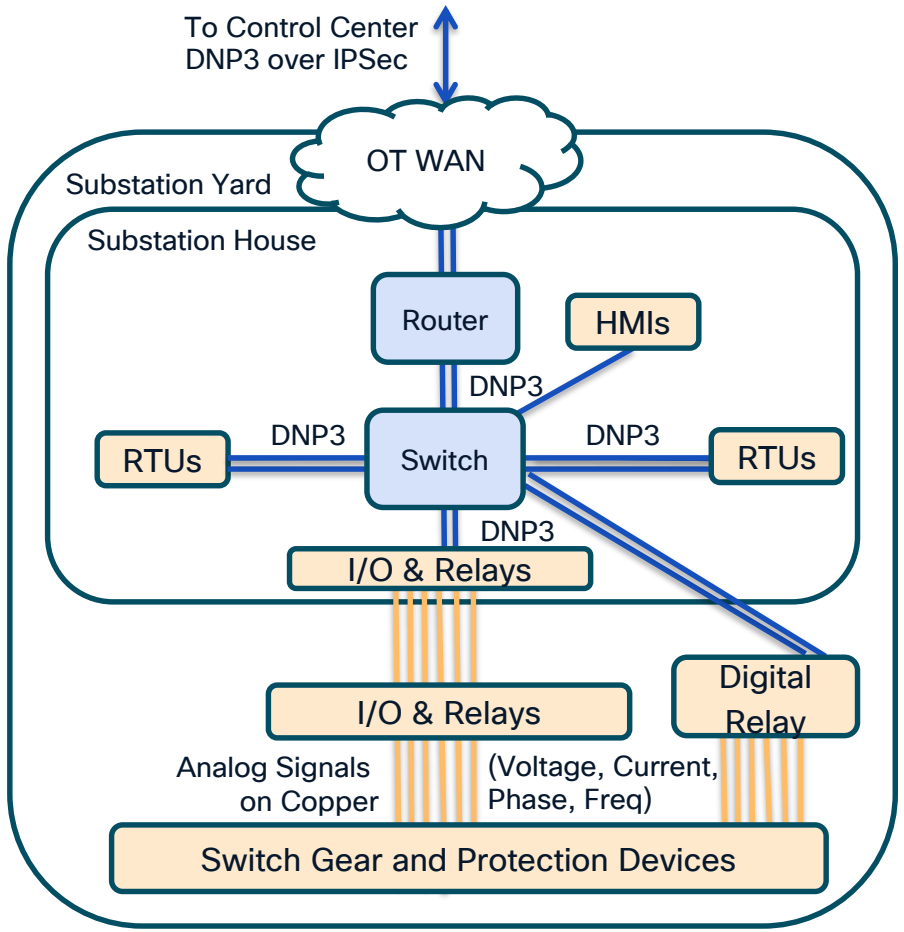
- Update to CVD to include ‘Terrestrial Timing’ solution with Central PRC’s
- IR8340 at substation edge to convert PTP Telecom profile to Power profile
- In conjunction with Microchip Primary Ref clocks (Timemaster 4000, multi band/constellation)
  - Option to add Bluesky GPS firewall to protect against spoofing/jamming
- G8275.1 – PTP on path support across Segment Routing transport network
- CVD to be published July 2025 post Cisco Live

© 2025 Cisco and/or its affiliates. All rights reserved.

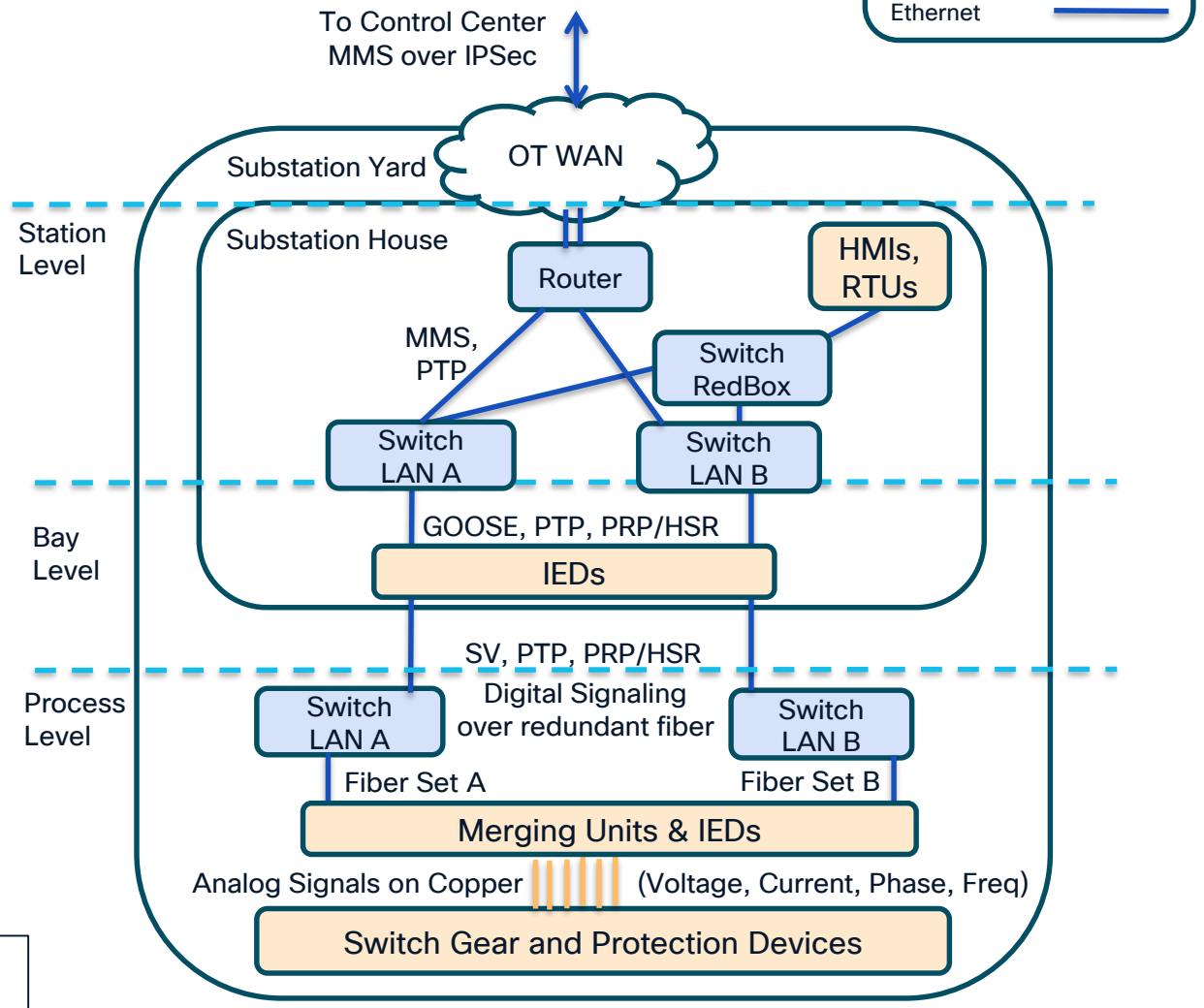
DNP3 Deployment Architectures

DNP3 vs IEC 61850 Topologies

DNP3 Substation



IEC 61850 Substation

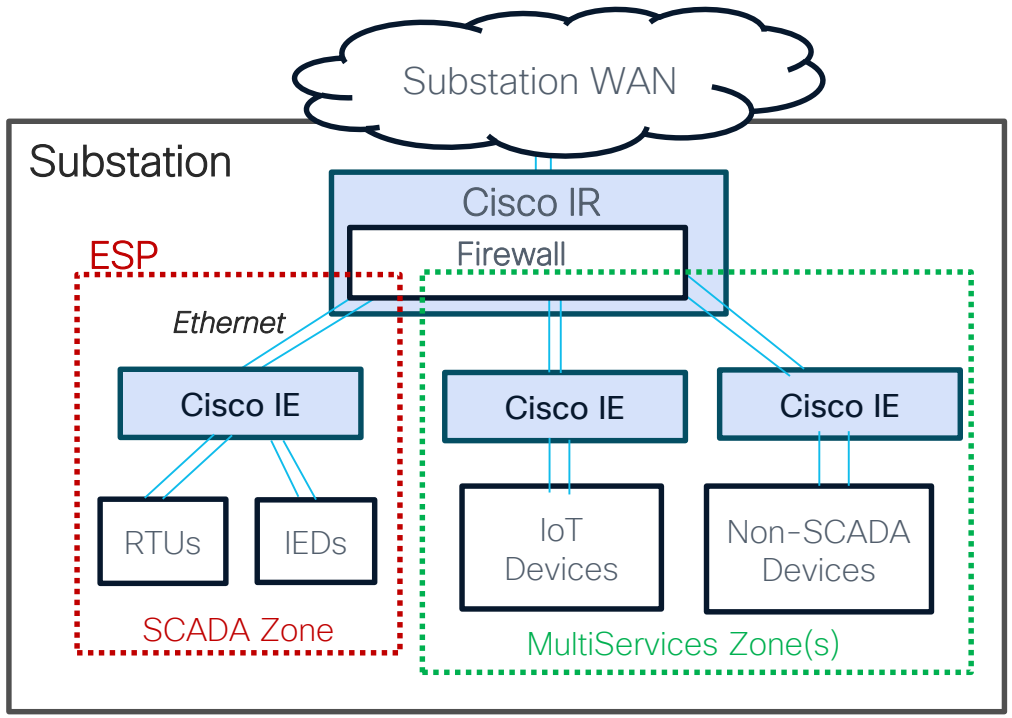


Summary: Major IEC 61850 Deltas vs DNP3

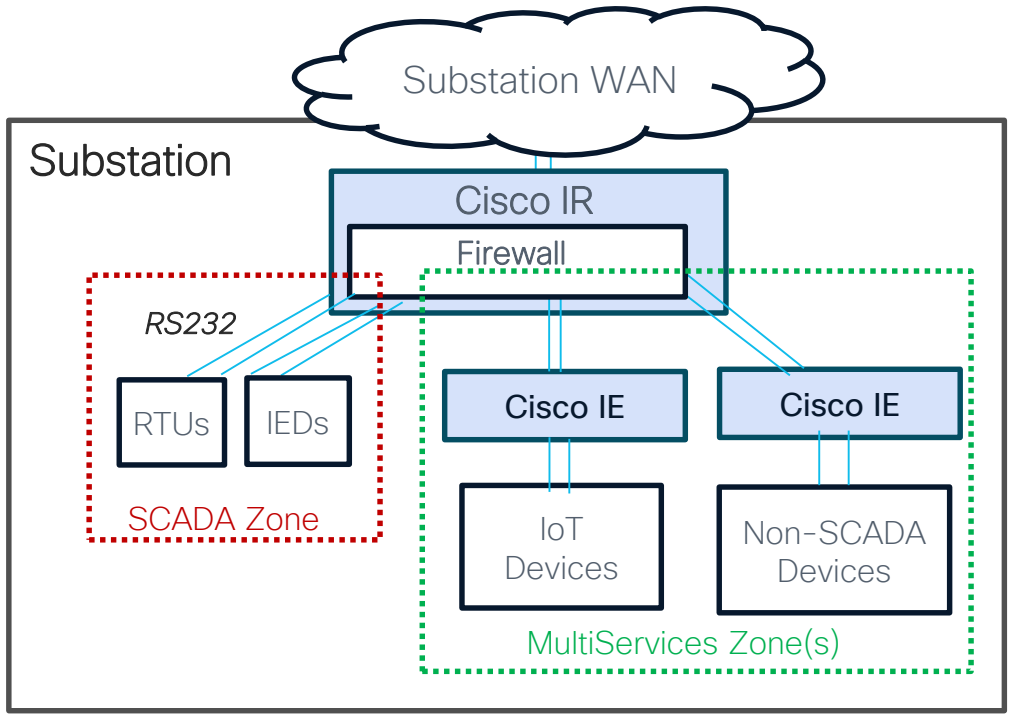
- Signal is always digitized in substation yard
- SV, GOOSE, PTP, PRP/HSR used for real time digital signaling and lossless ethernet redundancy

DNP3 Substation LAN Topologies

Ethernet DNP3 SCADA



Serial DNP3 SCADA



Cisco Industrial Routers (IR)

IR8340

IR1101

Cisco Industrial Ethernet Switches (IE)

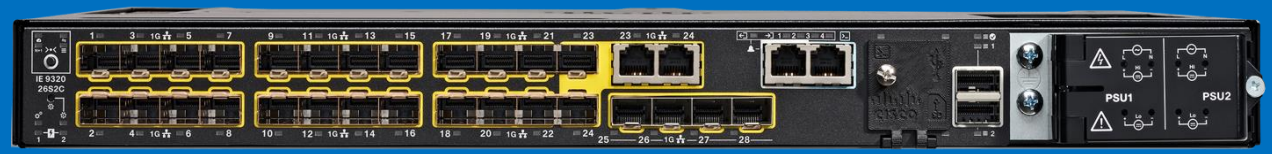
IE9300

IE3500

© 2025 Cisco and/or its affiliates. All rights reserved.

IR8340

IE9300



IR1101

IE3100
IE3200
IE3300
IE3400
IE3500

Substation Routers & Layer 3 Switches

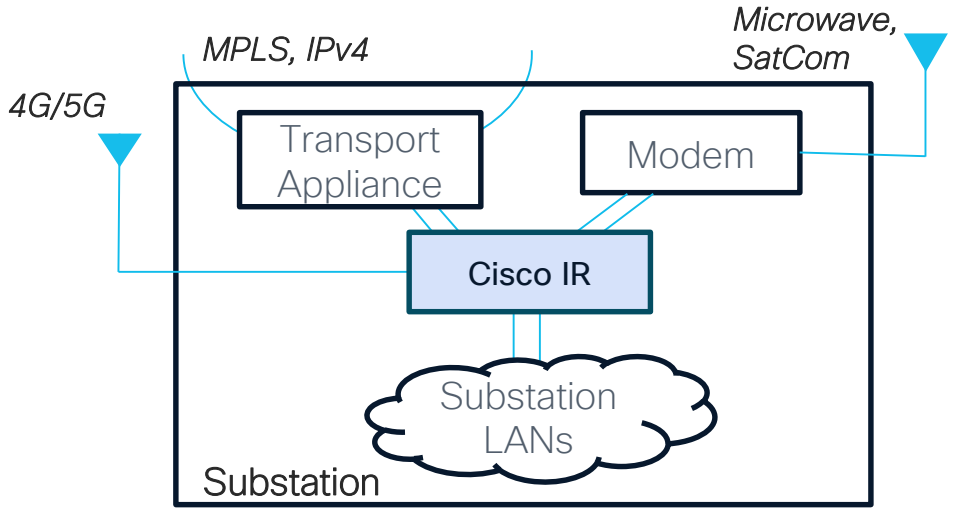
Leveraging operating system, chipsets, and security models as Cisco Enterprise Switches and Routers

- Substation Rated
- Advanced Security
- Network Automation
- End-To-End Architectures
- Modular & Extensible

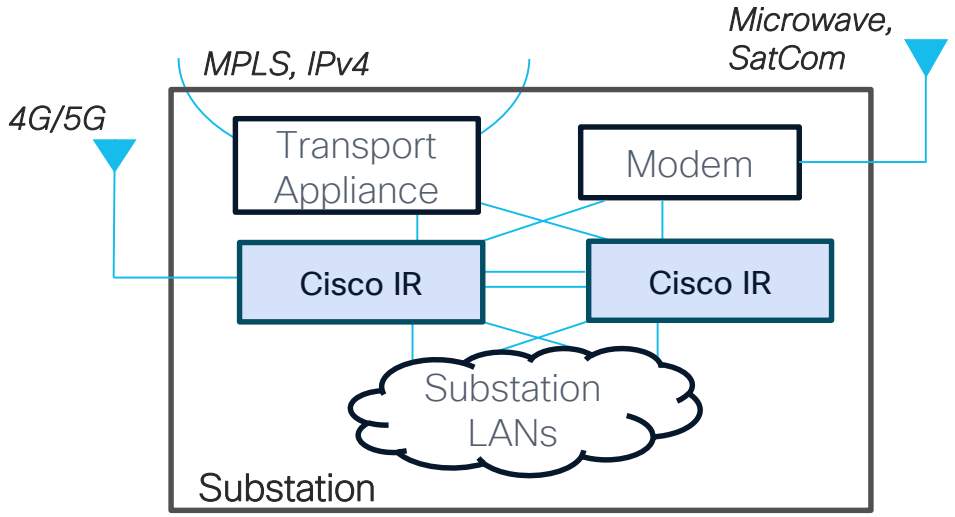
Substation WAN Topologies

Separate Transport and IP Services Layers

Single Router Topology



Dual Router Topology



Substation WAN Design Decisions:

Services	Options
Transport Types	MPLS, IPv4, Cellular, Microwave, SatCom
Transport Redundancy	Primary, Secondary, Tertiary
IP Services Redundancy	Single or Dual Routers
	Single/Dual WAN uplinks per router
Router Mode	SD-WAN vs Autonomous

Common Practice:

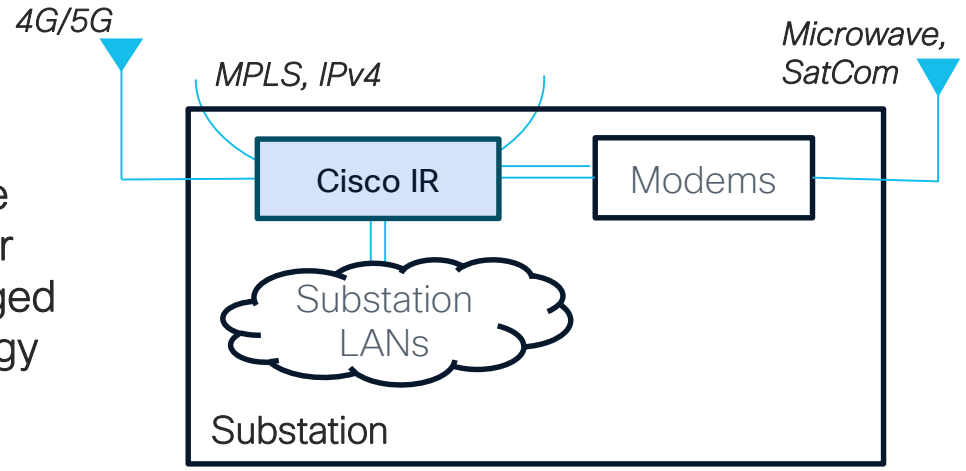
- Dual Routers at Transmission Substation or Large DER Site
- Single Router at Distribution Substation

© 2025 Cisco and/or its affiliates. All rights reserved.

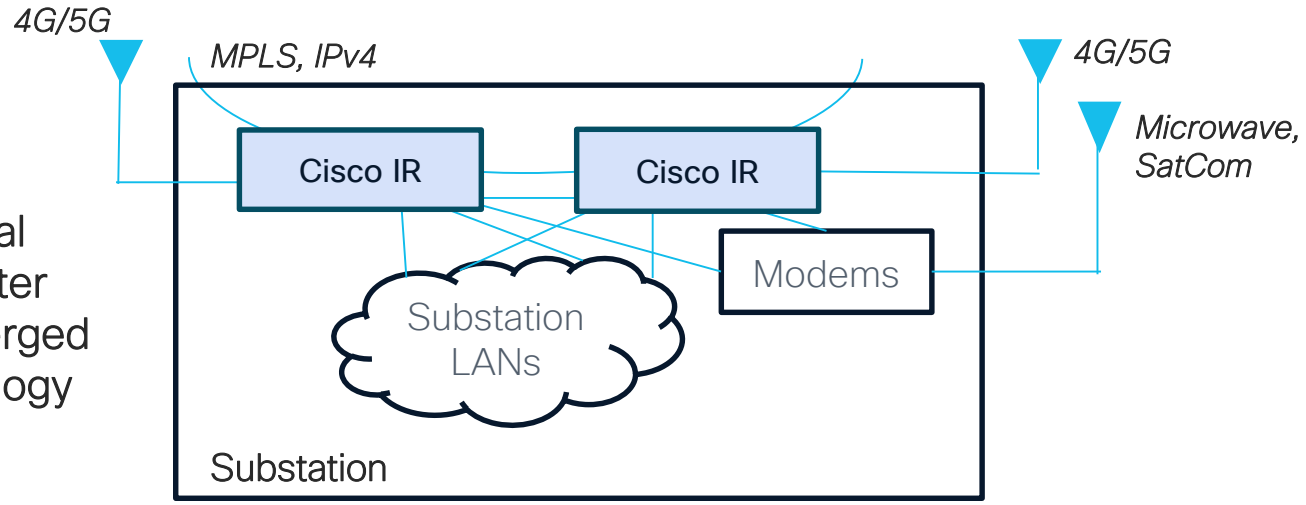
Substation WAN Topologies

Converged Transport and IP Services Layers

Single Router Converged Topology



Dual Router Converged Topology



Dedicated vs Converged Advantages:

Mode	Advantages
Separate Transport & IP Services Layers	Cleaner governance model, maintenance model, and regulatory compliance
	Greater Design Flexibility
Converged Transport & IP Services Layers	Less upfront cost, power, and rack space
	Potentially less management overhead

Common Practice:

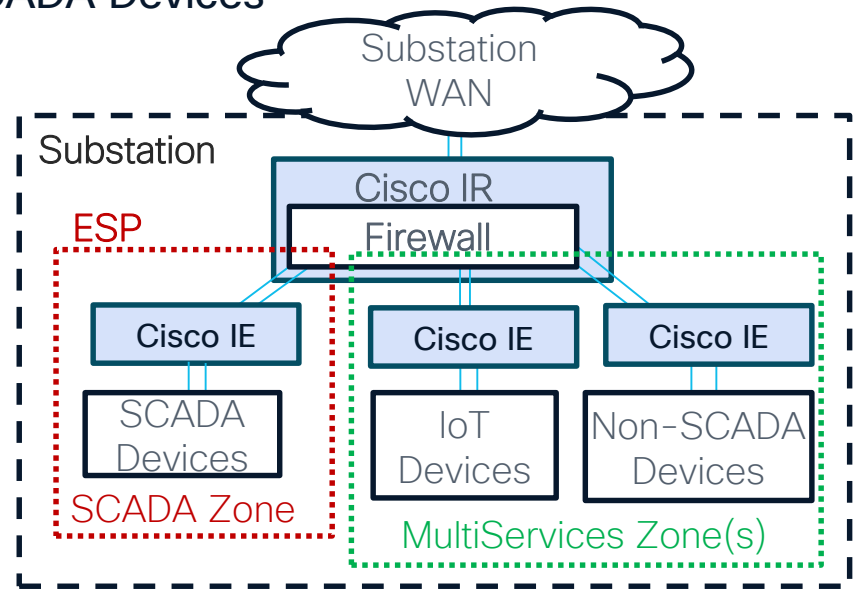
- Separate layers most common with private fiber substations (on-net)
- Converged layers most common wireless or leased services (off-net)

© 2025 Cisco and/or its affiliates. All rights reserved.

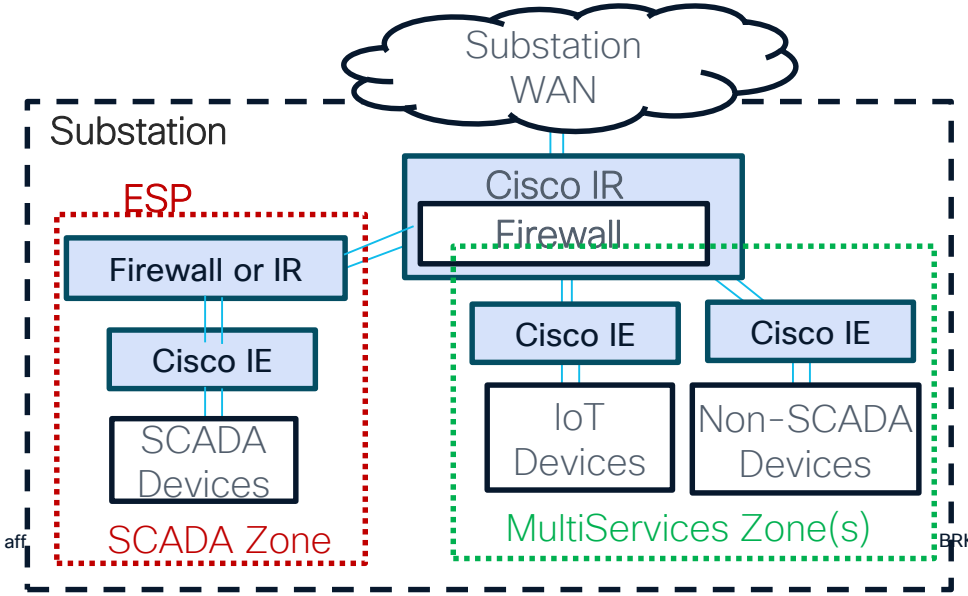
DNP3 Substation LAN Topologies

Ethernet SCADA Devices

Integrated Firewall Topology



Discrete Firewall Topology



Substation LAN Design Decisions:

Services	Options
Firewall Type	Integrated vs Discrete
Switching Redundancy	RSTP, Etherchannel
Segmentation Types	VPN, VRF, VLAN, Firewall
Firewall and Visibility Services	IPS/IDS, (INSM) Internal Network Security Monitoring (Cyber Vision)
Cisco IR Type	IR8340, IR1101
Cisco IE Type	IE9300, IE3x00
Extensibility Options	Zero Trust Architectures, IEC-61850 Protocols

Common Practice:

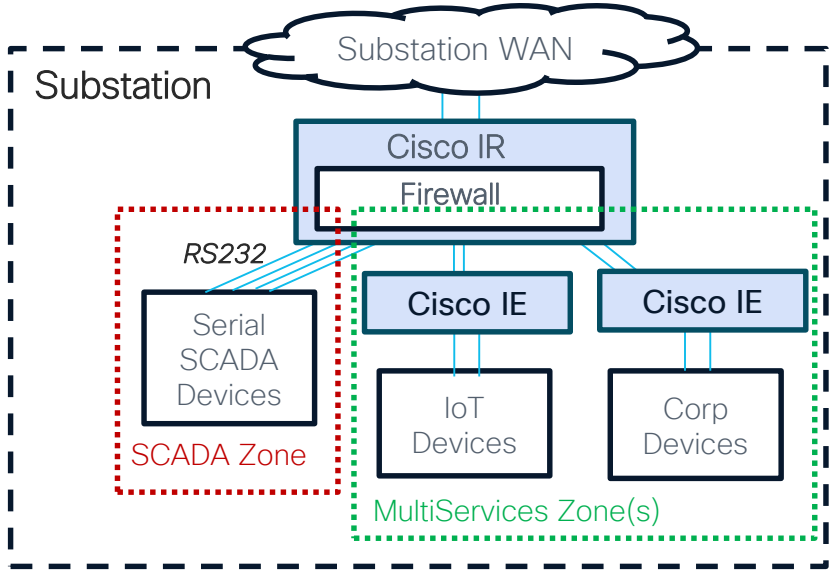
- Integrated firewall most common for non-NERC and NERC-Low substations
- Discrete firewall most common for NERC-Medium

© 2025 Cisco and/or its aff

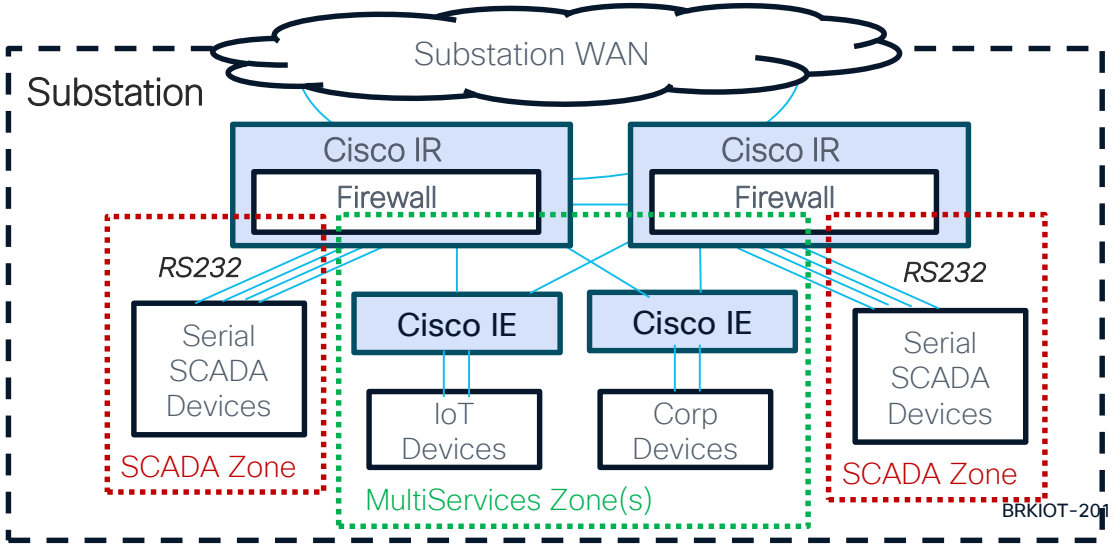
DNP3 Substation LAN Topologies

Serial SCADA Devices

Single Router Topology



Dual Router Topology



Serial SCADA Design Decisions:

Services	Options
Serial Redundancy	Single vs Dual RS-232 Connections
L2 Encapsulation	Pseudowire (Ethernet-Based) MPLS labeling options
L3 Encapsulation	Raw Sockets (IP-based) VRF-Aware options

Common Practice

- L3 encapsulation most common for non-NERC and NERC-Low substations
- L2 encapsulation (considered non-routable) most common for legacy substations

Serial SCADA Support

IR8340

Up to 16 RS-232 Ports

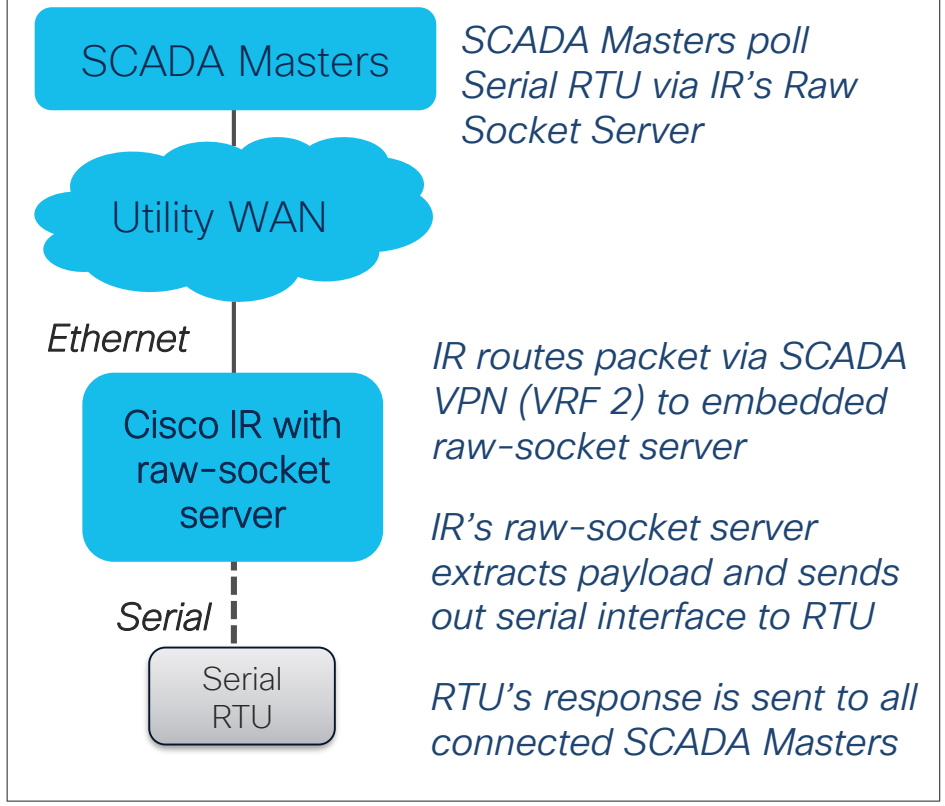
IR1101

1 RS-232 Port

1 RS-232 Port
4 RS-232/485 Ports

1 RS-232 Port
8 RS-232/485 Ports

Serial SCADA Transport using Cisco IRs is very mature technology & used commonly across Utility OT networks



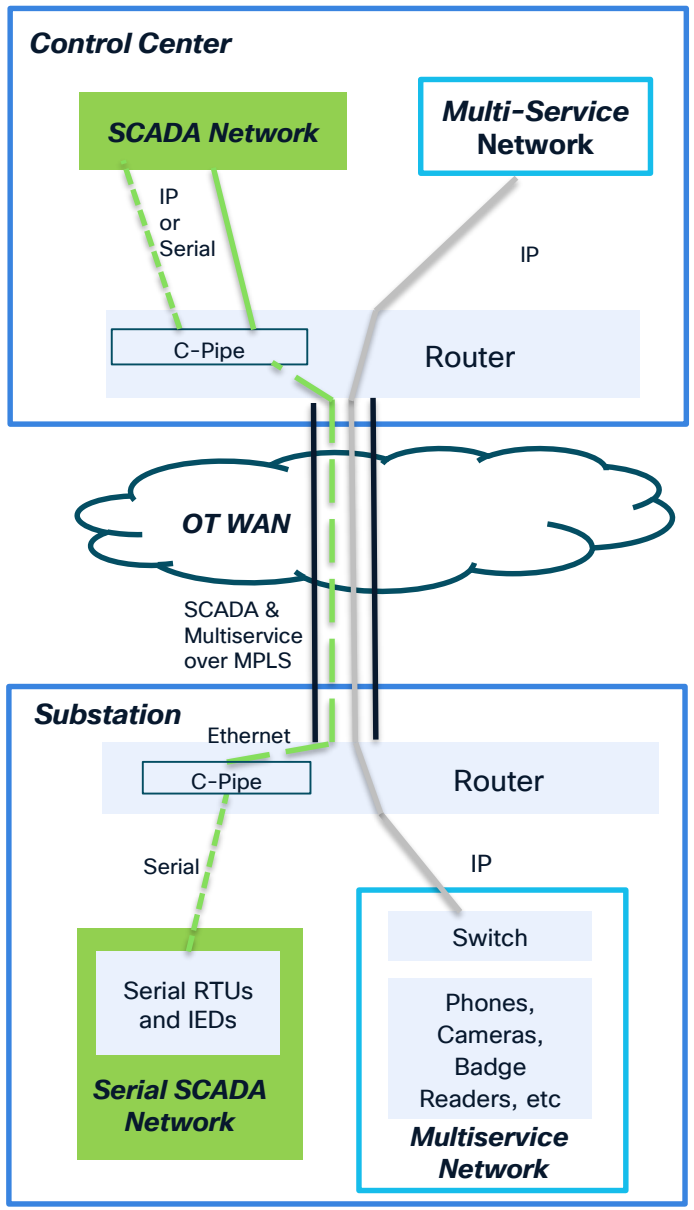
IR8340 Raw-Socket Config Example

```
69  interface Serial0/2/0
70   physical-layer async
71   vrf forwarding 2
72   no ip address
73   ip nbar protocol-discovery
74   encapsulation raw-tcp
75  !
76  line 0/2/0
77   raw-socket tcp server 20000 10.0.11.50
78   raw-socket packet-timer 500
79   raw-socket packet-length 1400
80   stopbits 1
81   speed 38400
```

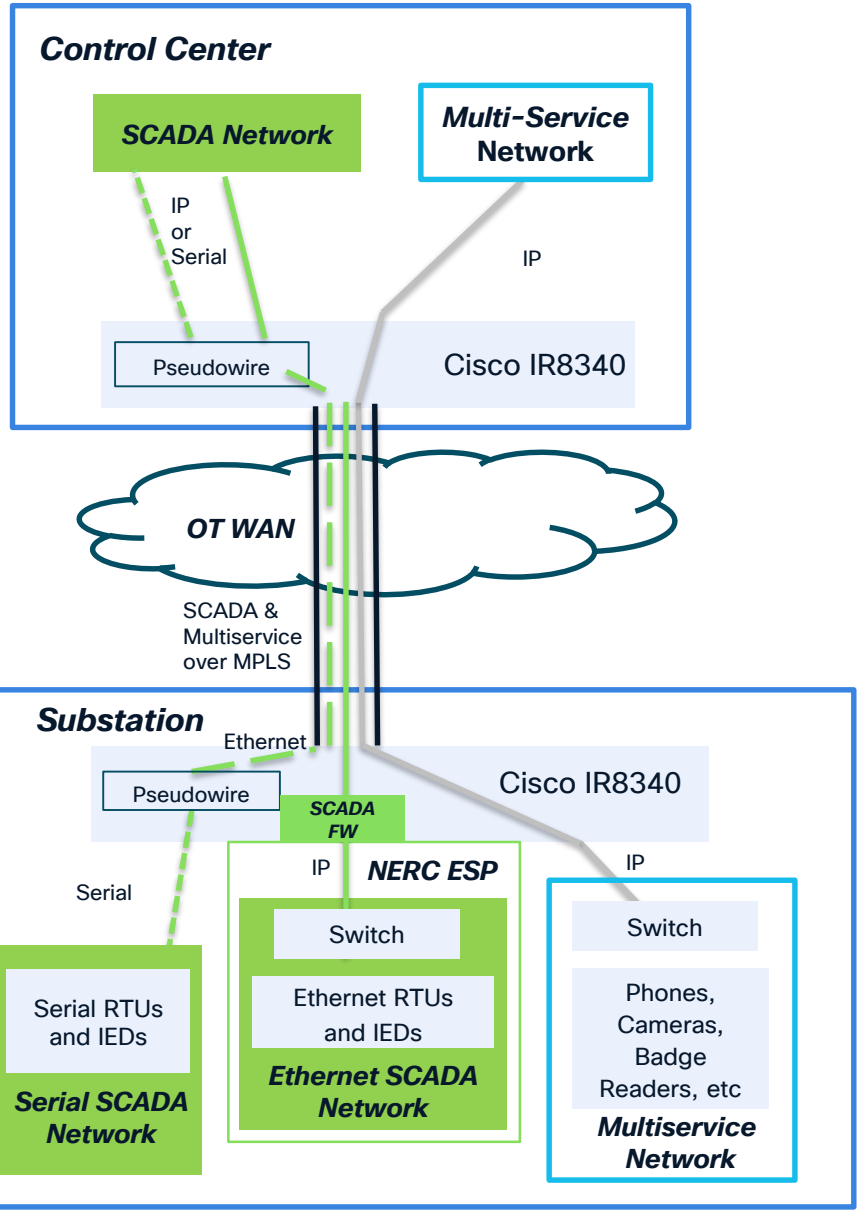
© 2025 Cisco and/or its affiliates. All rights reserved.

Example Phased Transition from Serial to IP SCADA

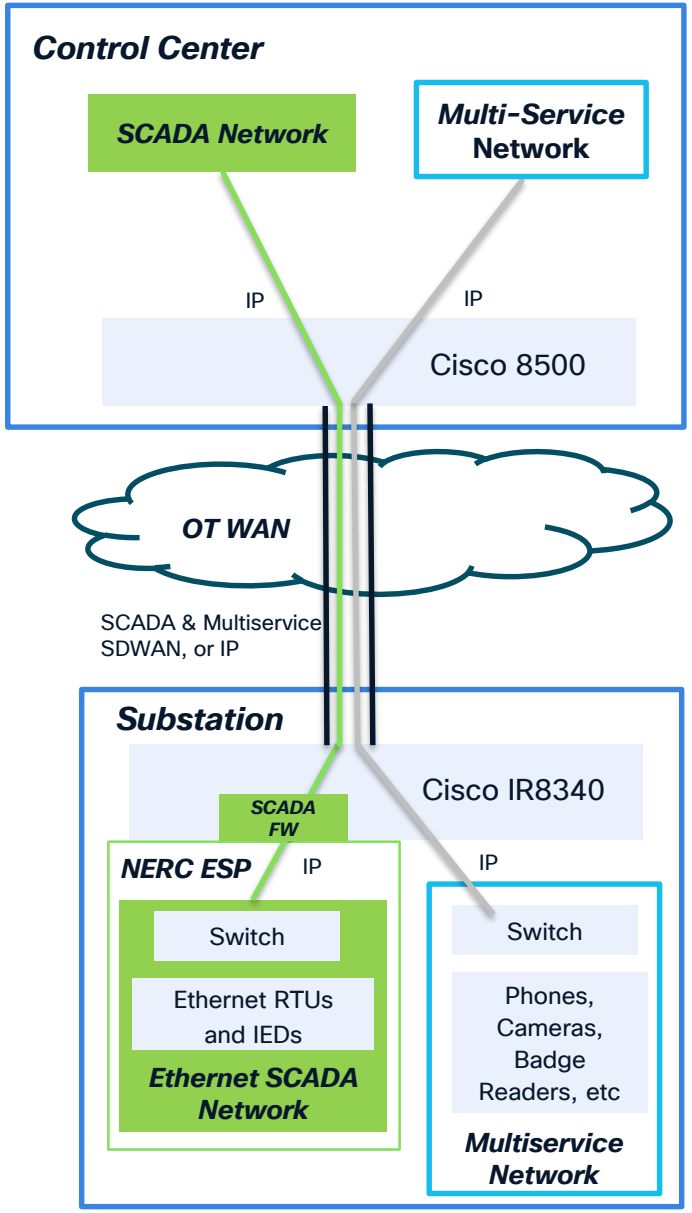
Phase 1: Serial SCADA in Substation
"Non-routable" SCADA transport via MPLS



Phase 2: Transition to Ethernet Based SCADA



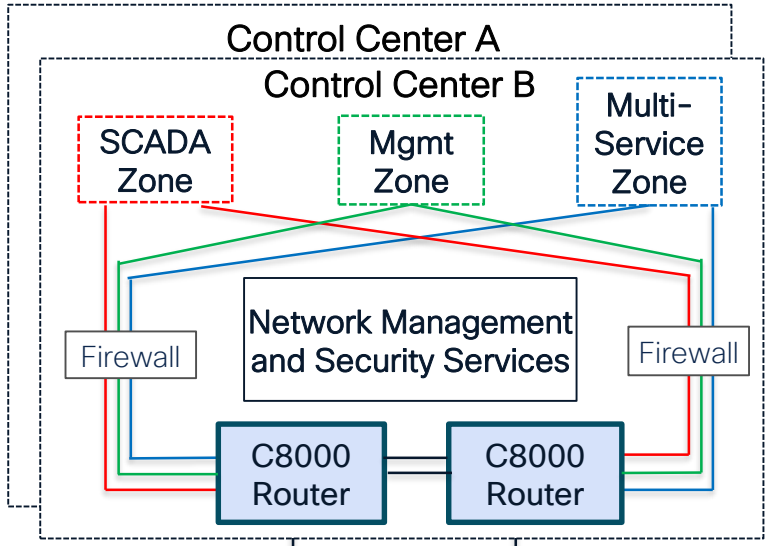
Phase 3: Ethernet Based SCADA



End-to-End Topology Example

Control Center Design Considerations

Services	Options
High Availability	Geographical Redundancy of Data Centers
	Multiple Head End Routers per Data Center
	Network Management Applications Redundancy
Management Options	SD-WAN, Catalyst Center, 3rd Party
Security Extensibility	Cyber Vision, ISE, Splunk



Control Center Management & Security Options

Head End Router Options

IR8340

IE9320

IR1101

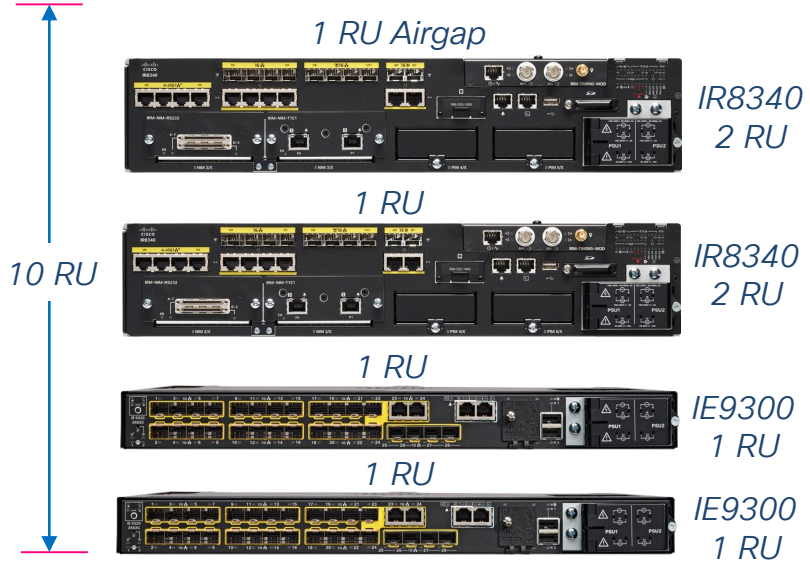
IE3x00

© 2025 Cisco and/or its affiliates. All rights reserved.

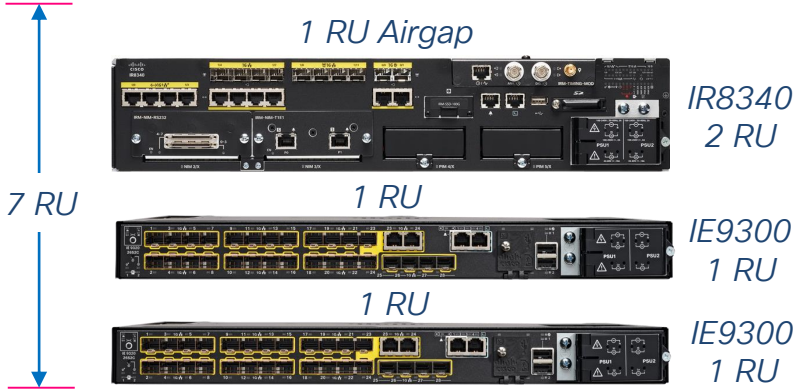
Substation Topology Examples

Features and Rack Space

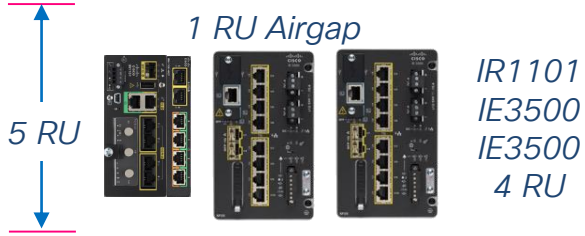
Dual IR8340 + IE9300s



Single IR8340 + IE9300s



Single IR1101 + IE3500s



	Dual IR8340 Topology	Single IR8340 Topology	Single IR1101 Topology
Management Options	Best	Best	Best
Redundancy Options	Best	Better	Good
Network Services	Best	Best	Good
Security Services	Best	Best	Good
Utility Services	Best	Best	Good

© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Topology Examples

Router Feature Comparison

	Dual IR8340	Single IR8340	Single IR1101
Management Options			
SD-WAN	■	■	■
Autonomous	■	■	■
Redundancy Options			
Redundant Routers	■		
Redundant Power Supplies	■	■	
Redundant L3 Uplinks	■	■	■
Network Services			
VPN, VRF, VLAN, VXLAN	■	■	■
STP	■	■	■
Etherchannel, REP	■	■	

	Dual IR8340	Single IR8340	Single IR1101
Security Services			
Firewall	■	■	■
Cyber Vision IDS	■	■	
SD-WAN IPS/IDS	■	■	
TrustSec and Zero Trust	■	■	
MACsec	■	■	
Utility Services			
Raw Socket Serial SCADA	■	■	■
Pseudowire Serial SCADA	■	■	
Precision Time Protocol	■	■	
IEC-61850 PRP, HSR	■	■	

© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Visibility

NERC CIP-015 Internal Network Security Monitoring (INSM)

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

M1. Evidence must include each of the documented process(es) that collectively include each of the requirement Parts in Requirement R1 and evidence to demonstrate implementation of the process(es). Examples of evidence of implementation of the requirement Parts may include, but is not limited to:

Part 1.1.

- Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.

Part 1.2.

- Documentation of anomalous network detection events;
- Documentation of configuration settings of internal network security monitoring systems;
- Documentation of network communication baseline used to detect anomalous network activity; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response to detected anomalies; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

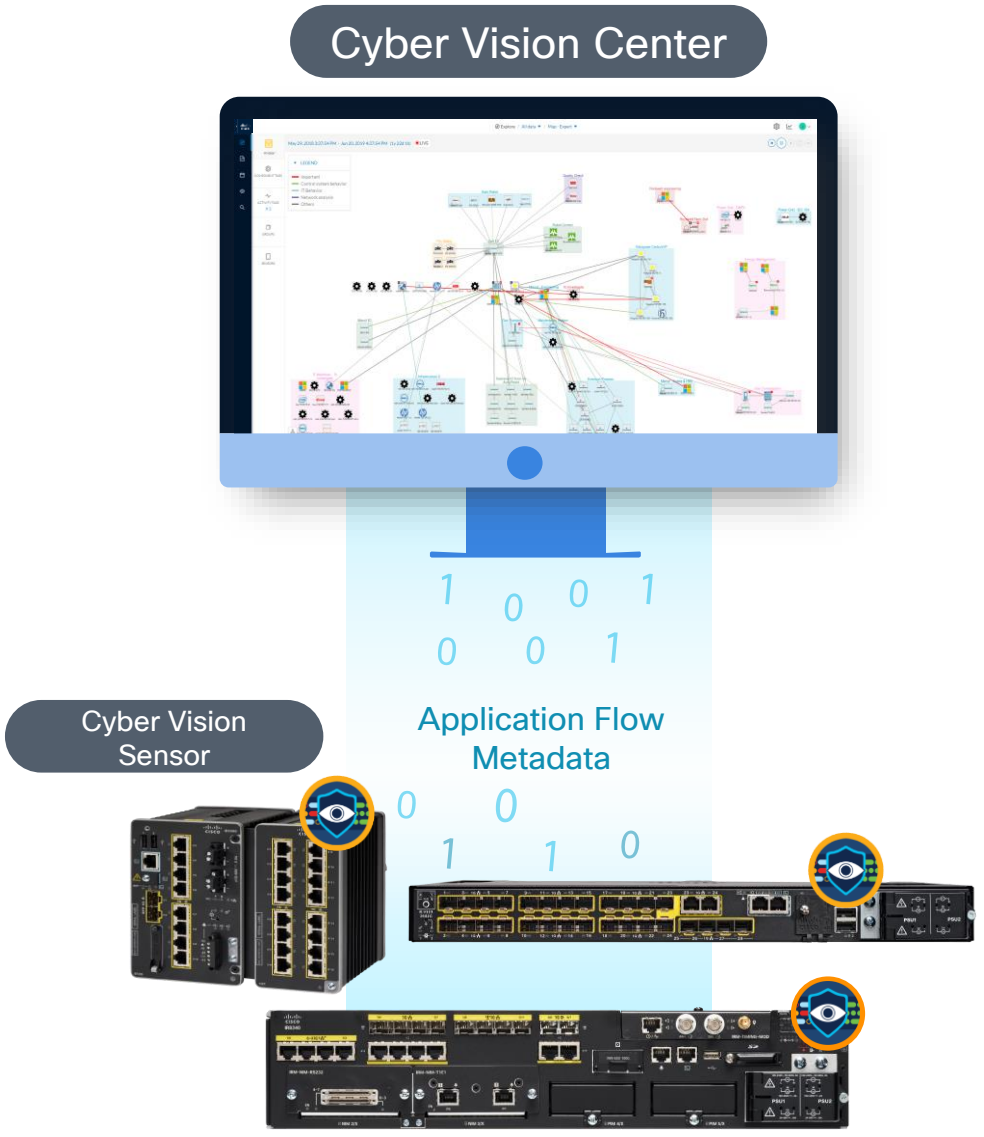
© 2025 Cisco and/or its affiliates. All rights reserved.

Visibility
Asset inventory
Communication patterns

Security Posture
Device vulnerabilities
Risk scoring

Operational Insights
Track process/device modifications
Record control system events

Cisco substation LAN switches and WAN routers ***see everything*** that attaches to them so you can gain ***visibility at scale***



Deep Packet Inspection & Active Discovery built into your network infrastructure

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Cyber Vision

Cyber Vision Center
(Centralized analytics)

Application Flow

IR 1101 Router

IR 8340 Router

IR8140 Router

Catalyst 9000 Series Switch

IE 9300 Switch

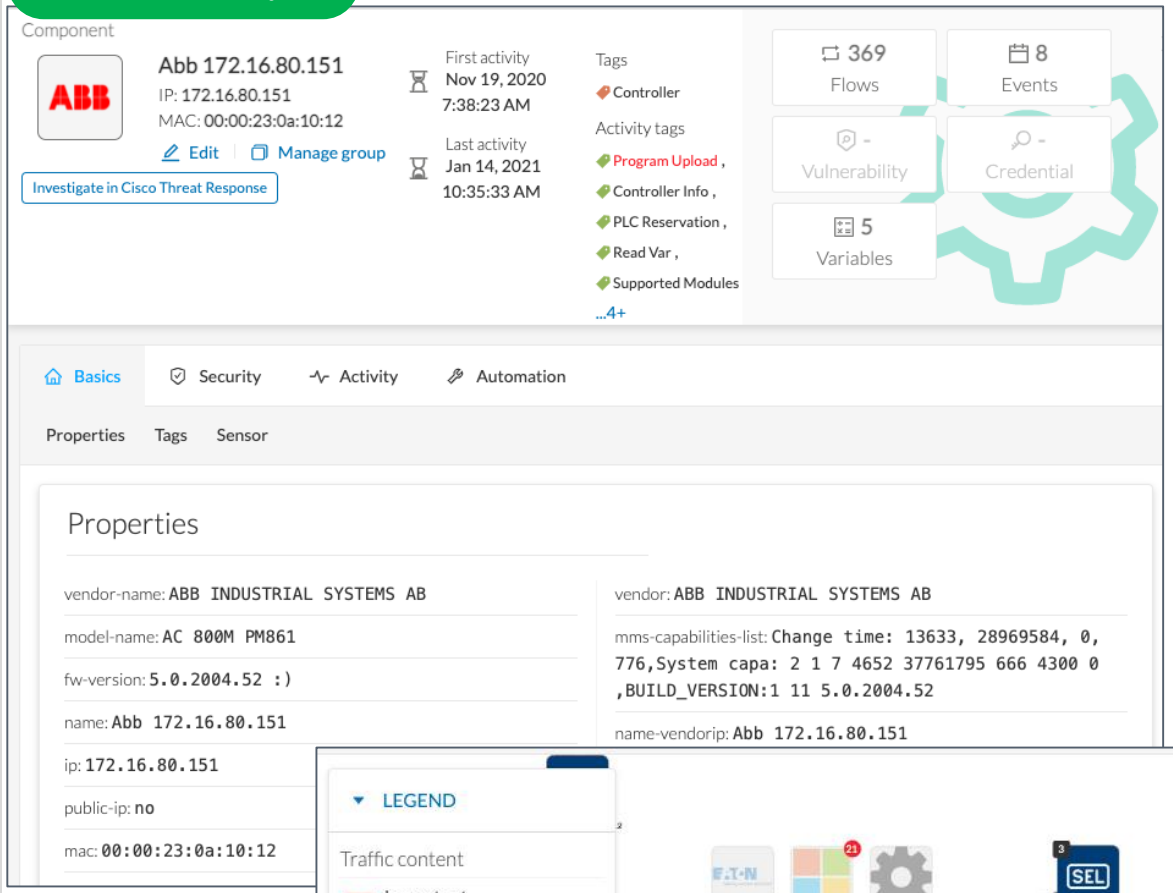
IE 3400
IE 3500H
Heavy Duty

IE 3100
2x10G Switch

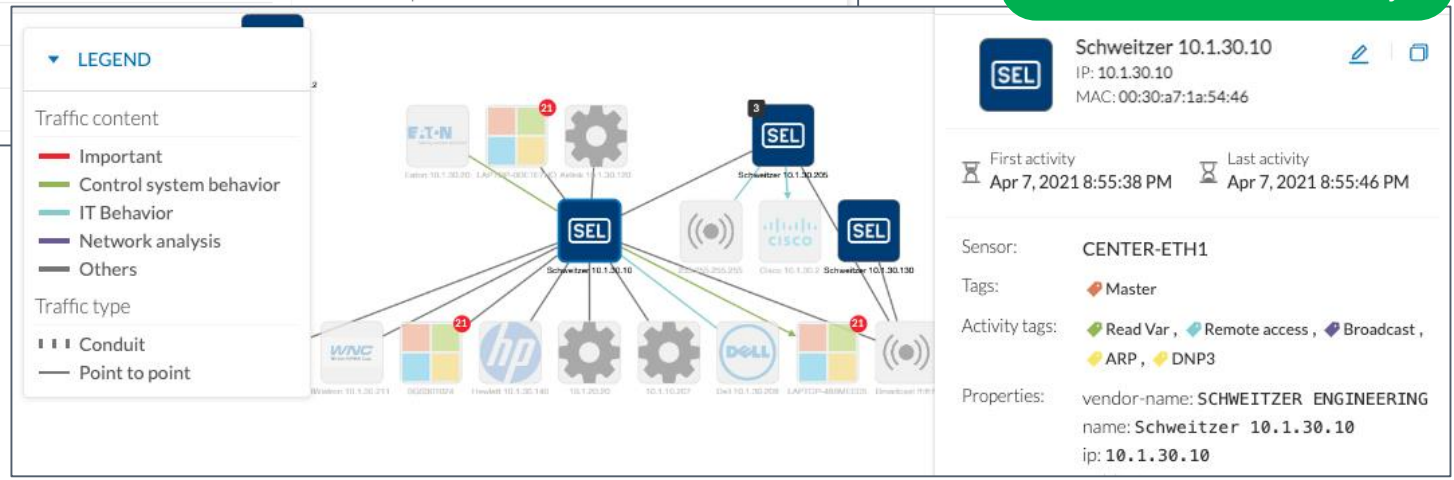
IE-3300
IE-3400
IE-3500
Switch

Network-Sensors
(Built in Deep Packet Inspection)

Asset Visibility



Communications Visibility



Cisco Cyber Vision

Cyber Vision Center
(Centralized analytics)

Application Flow

IR 1101 Router

IR 8340 Router

IR8140 Router

Catalyst 9000 Series Switch

IE 9300 Switch

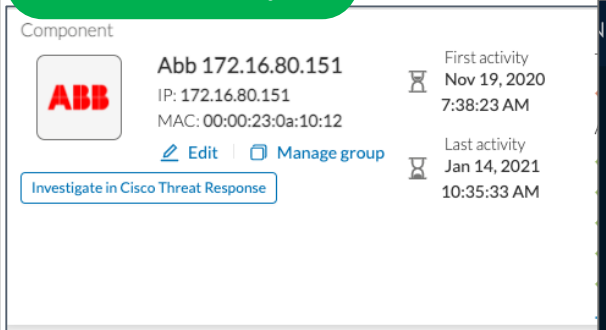
IE 3400
IE 3500H
Heavy Duty

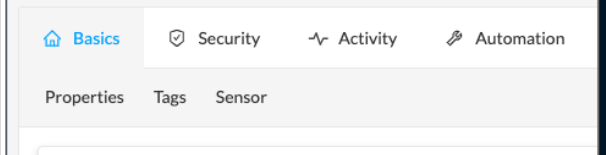
IE 3100
2x10G Switch

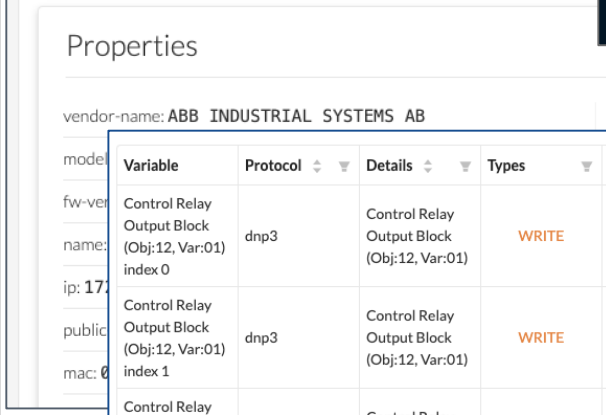
IE-3300
IE-3400
IE-3500
Switch

Network-Sensors
(Built in Deep Packet Inspection)

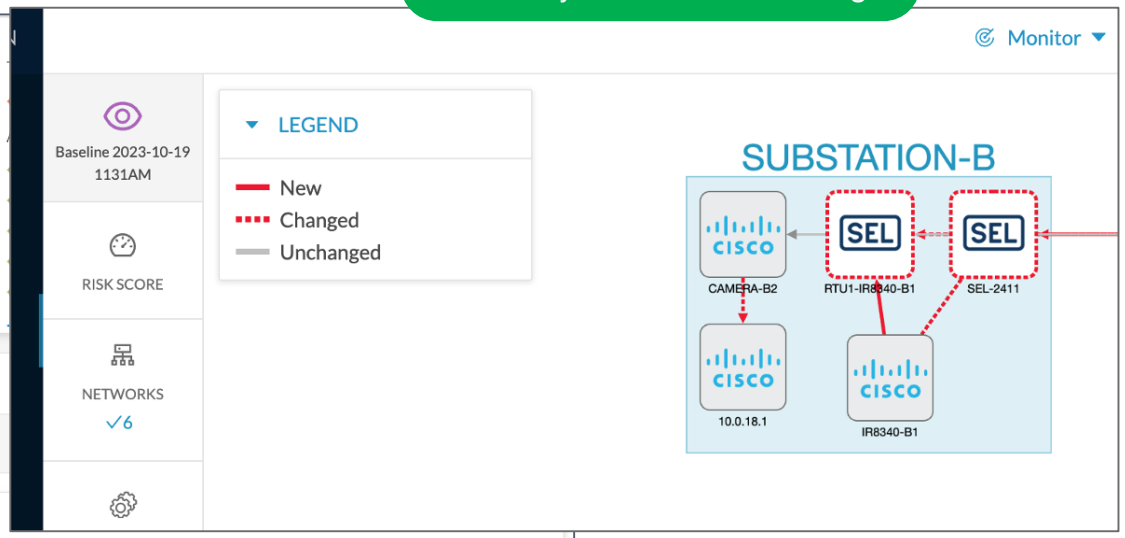
Asset Visibility





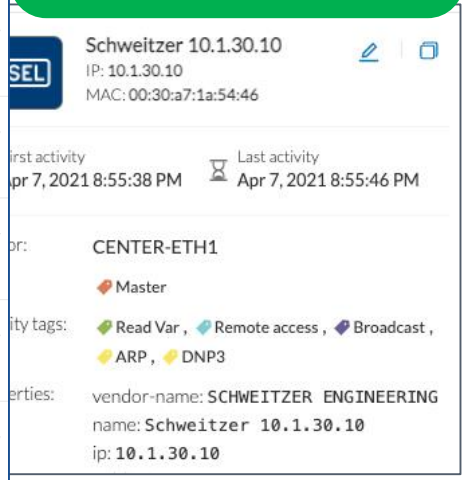


Anomaly Detection & Tracking



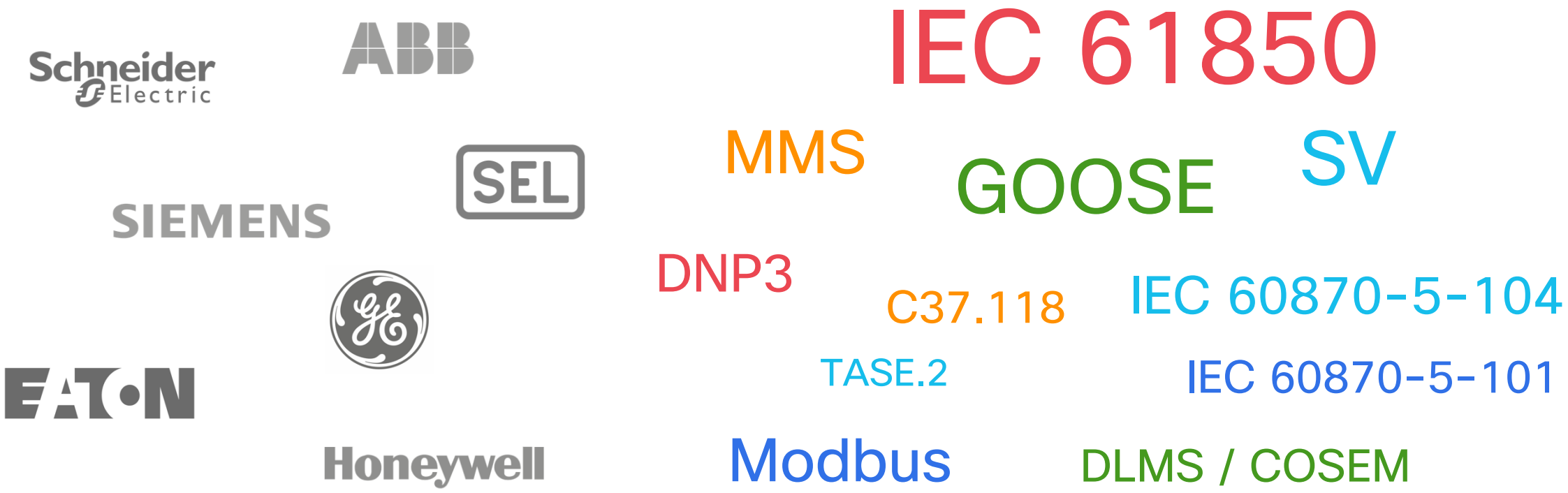
Variable	Protocol	Details	Types	Accessed by	First access	Last access
Control Relay Output Block (Obj:12, Var:01) index 0	dnp3	Control Relay Output Block (Obj:12, Var:01)	WRITE	Intel 192.168.0.1	Jan 15, 2021 11:35:27 AM	Jan 15, 2021 11:35:27 AM
Control Relay Output Block (Obj:12, Var:01) index 1	dnp3	Control Relay Output Block (Obj:12, Var:01)	WRITE	Intel 192.168.0.1	Jan 15, 2021 11:35:27 AM	Jan 15, 2021 11:35:27 AM
Control Relay Output Block (Obj:12, Var:01) index 127	dnp3	Control Relay Output Block (Obj:12, Var:01)	WRITE	Intel 192.168.0.1	Jan 15, 2021 11:35:27 AM	Jan 15, 2021 11:35:27 AM
Control Relay Output Block (Obj:12, Var:01) index 128	dnp3	Control Relay Output Block (Obj:12, Var:01)	WRITE	Intel 192.168.0.1	Jan 15, 2021 11:35:27 AM	Jan 15, 2021 11:35:27 AM
Control Relay Output Block (Obj:12, Var:01) index 255	dnp3	Control Relay Output Block (Obj:12, Var:01)	WRITE	Intel 192.168.0.1	Jan 15, 2021 11:35:27 AM	Jan 15, 2021 11:35:27 AM
Control Relay Output Block	dnp3	Control Relay Output Block	WRITE	Intel 192.168.0.1	Jan 15, 2021 11:35:27 AM	Jan 15, 2021 11:35:27 AM

Communications Visibility



Deep Operational Insights

Cyber Vision understands GRID protocols you use

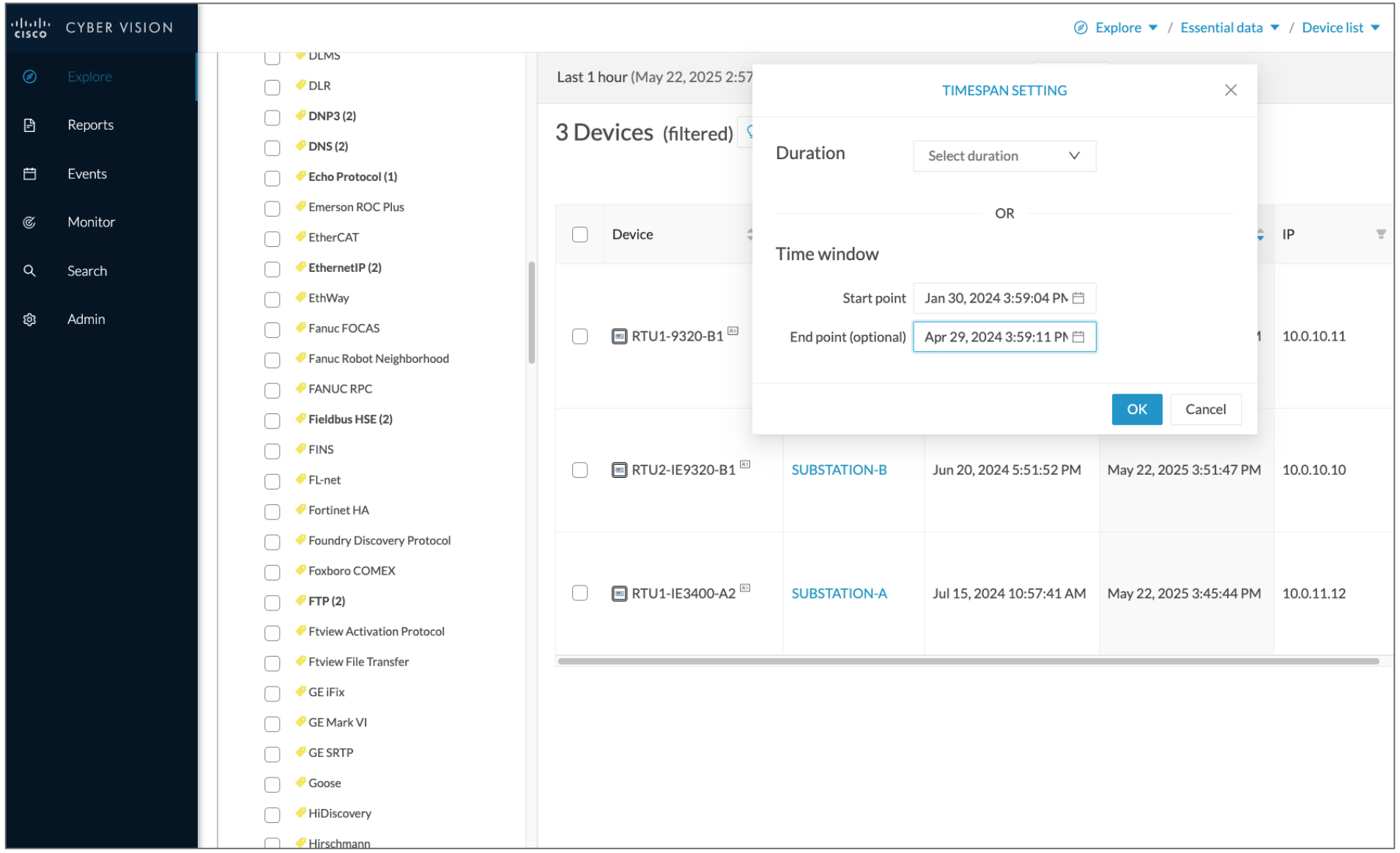


Cisco's Deep Packet Inspection understands process information even when using proprietary protocols

© 2025 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Asset Visibility

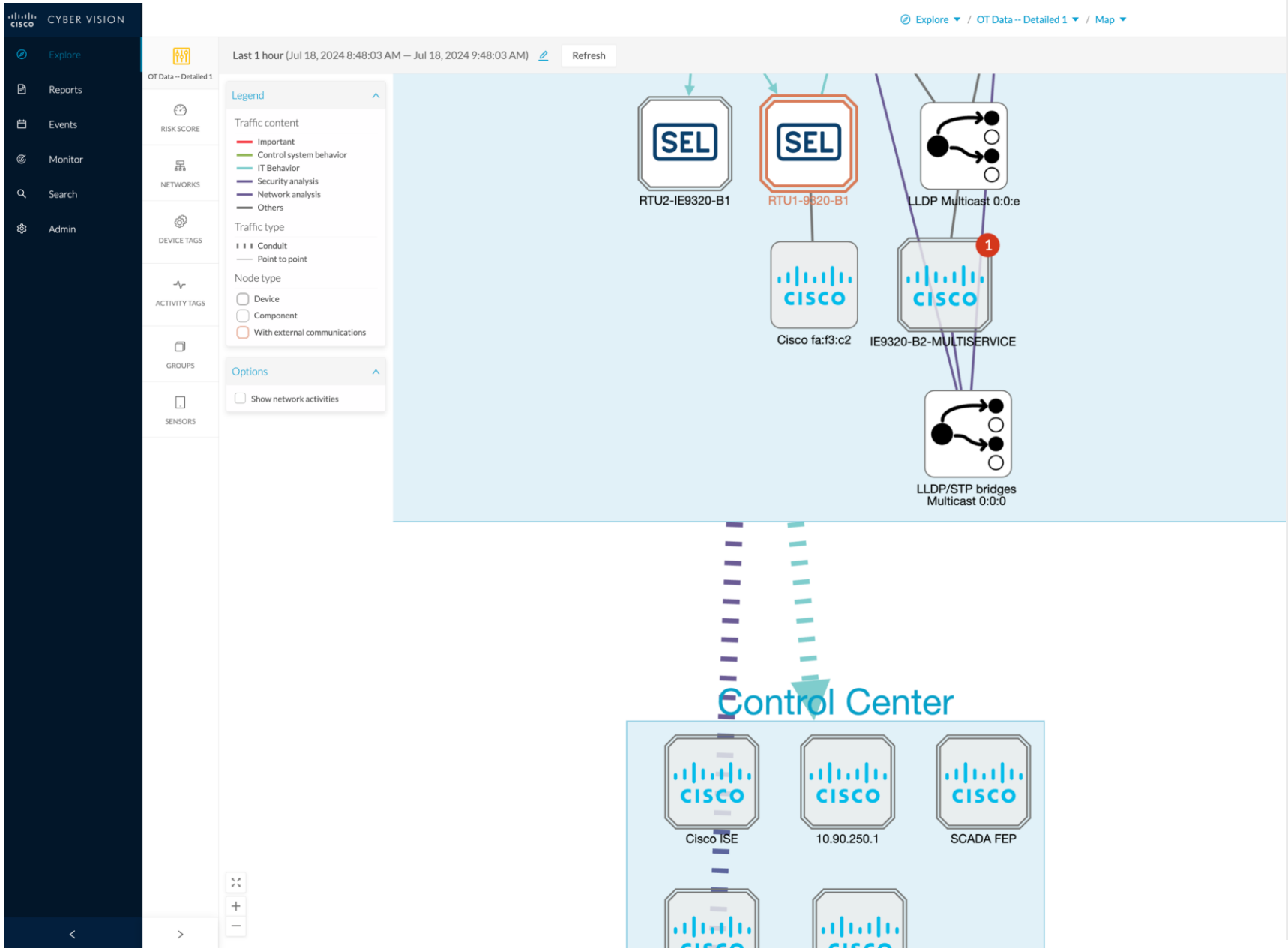
Real Time & Historical Monitoring of Substation Devices



© 2025 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Communication Flow Visibility

Real Time & Historical Monitoring of Substation Network Traffic



RTU1-9320-B1
SUBSTATION-B None
IP: 10.0.10.11
MAC: 00:30:a7:0f:fc:d0

First activity
Jun 20, 2024 5:51:52 PM

Last activity
Jul 18, 2024 9:50:57 AM

Device with external communications

Sensors: IE9320-B1, IE9320-B2, IR8340-B1

Tags: Controller, Slave, Admin Server, Database Server, Email Server, File Transfer Server, Log Server, Printer Server, Remote Admin Server, Routing Capability, ...1+

Activity tags: PLC Clock, Unestablished, Insecure, Port Scan Activity, Read Var, Write Var, Authentication, Database, Email, IT File Sync, ...27+

Risk score: 55 See details

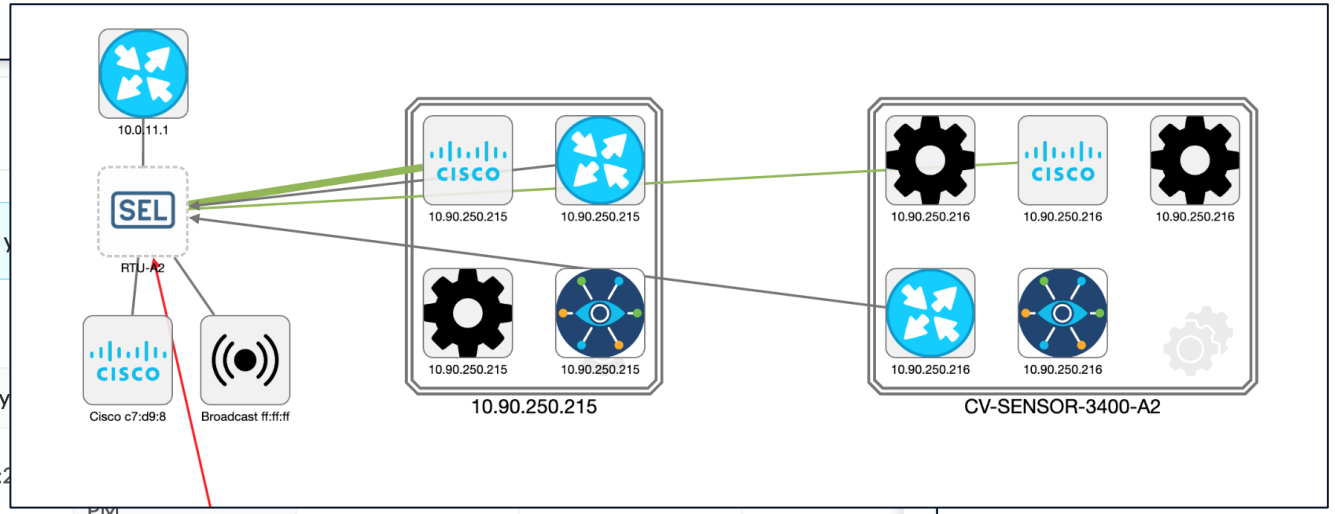
Components: SEL-2411

Properties:

```
fw-version: SEL-2411-R315-V2-Z007007-D20160507
hw-version: 241101A1A5X0X0X0130
ip: 10.0.10.11
mac: 00:30:a7:0f:fc:d0
model-name: SEL2411
name: SEL-2411
public-ip: no
serial-number: 3160950154
vendor-name: SCHWEITZER ENGINEERING
vlan-id: 202
```

(hide)

Deep Visibility into Substation Traffic



Flows

The flow storage policy can affect this feature. Please ensure you've enabled the flow storage for networks y

Export to CSV

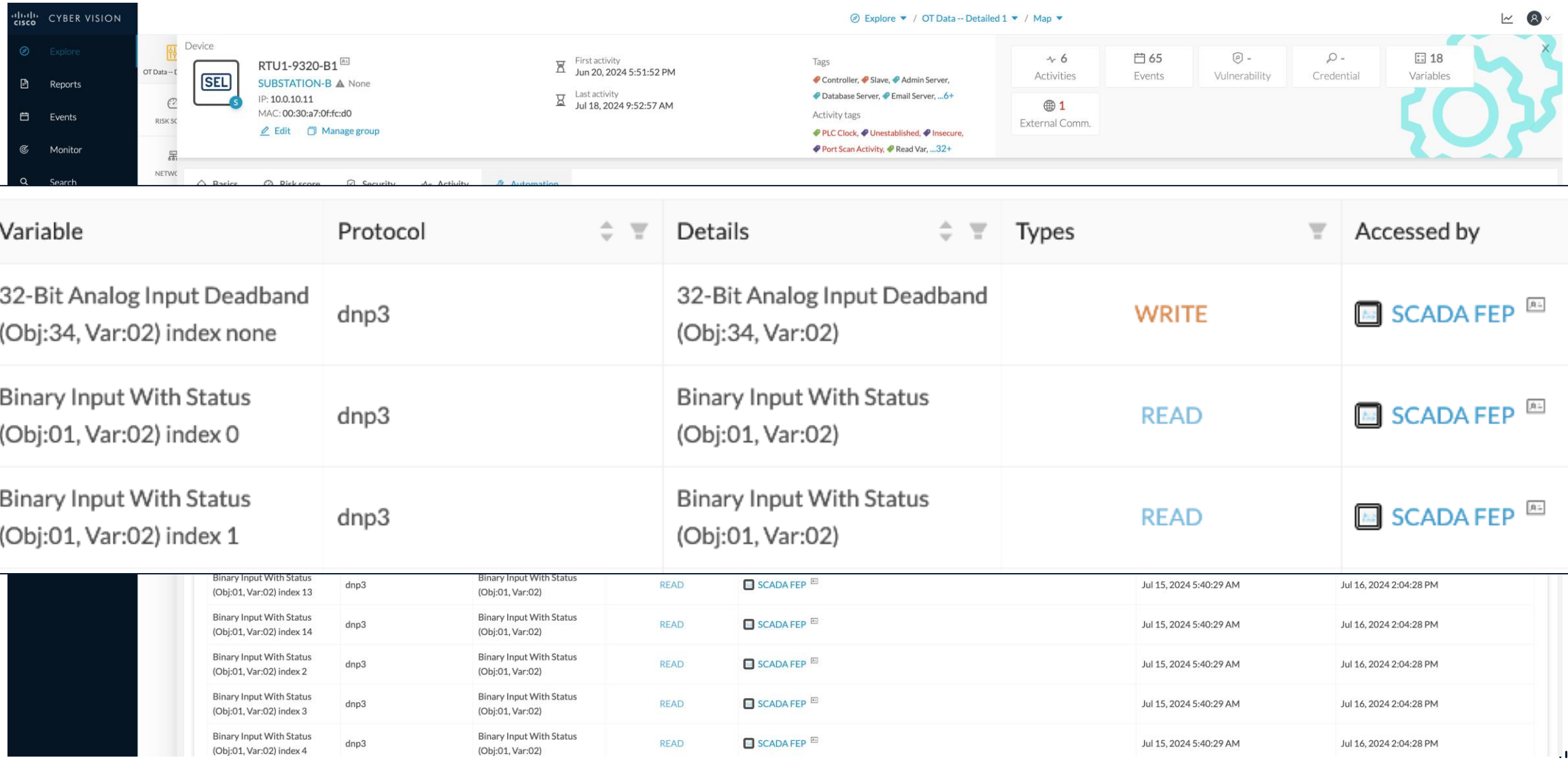
Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Tags		
RTU-A2	20000	-	10.90.250.215	57682	TCP	Mar 7, 2024 1:2 PM	PM	DNP3		
10.90.250.215	57682	→	RTU-A2	20000	TCP	Mar 7, 2024 1:23:41 PM	Mar 7, 2024 1:23:41 PM	Low Volume, Multicast, DNP3	8	1
RTU-A2	20000	-	10.90.250.216	49922	TCP	Mar 7, 2024 1:23:36 PM	Mar 7, 2024 1:23:36 PM	Read Var, Low Volume, DNP3	9	8

Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Tags
RTU-A2	20000	-	10.90.250.215	57682	TCP	Mar 7, 2024 1:23:41 PM	Mar 7, 2024 1:23:41 PM	Read Var, Low Volume, DNP3
10.90.250.215	57682	→	RTU-A2	20000	TCP	Mar 7, 2024 1:23:41 PM	Mar 7, 2024 1:23:41 PM	Low Volume, Multicast, DNP3

© 2025 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Packet Payload Visibility

Decoding of DNP3 Read/Write Commands



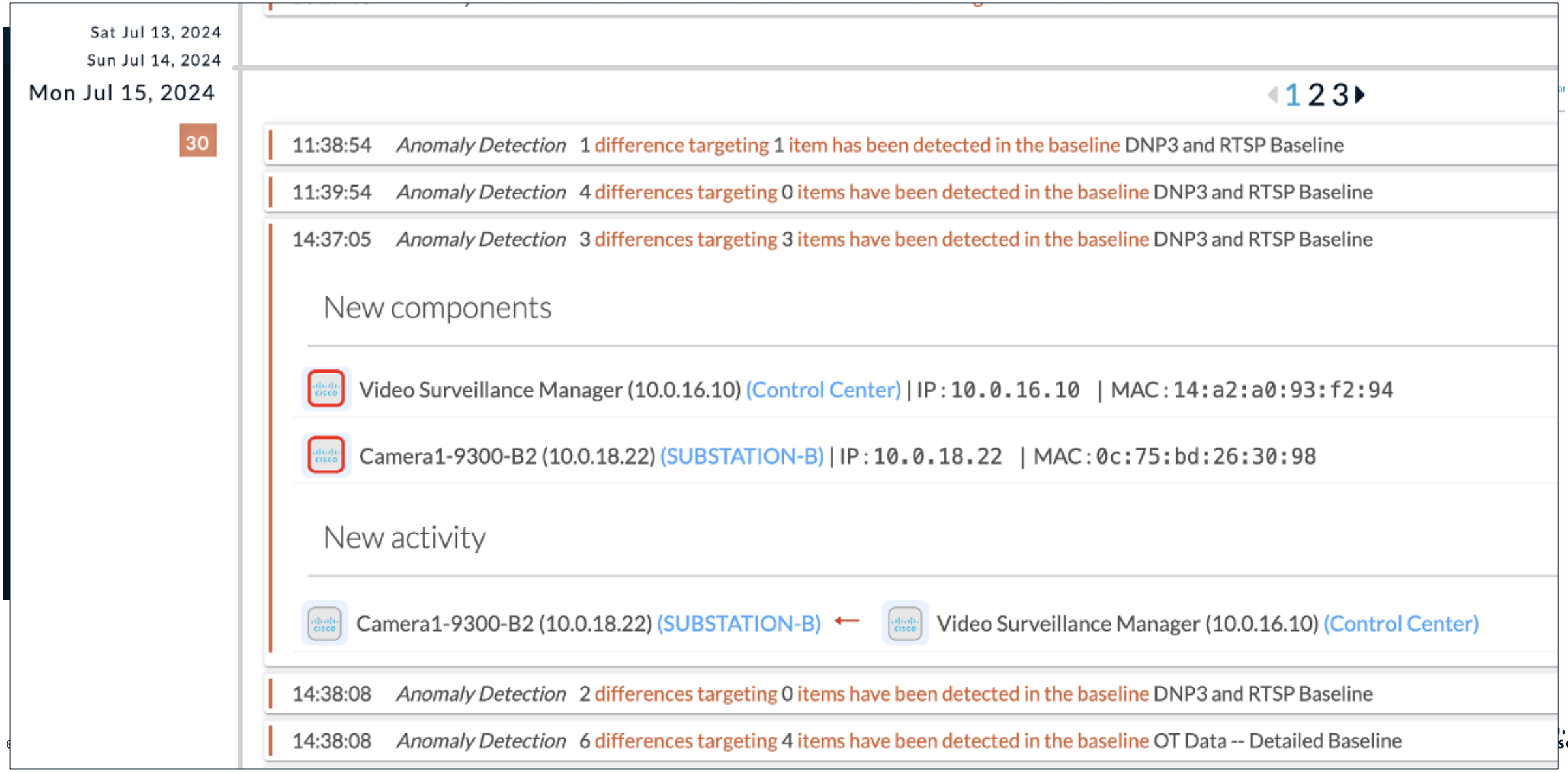
Variable	Protocol	Details	Types	Accessed by
32-Bit Analog Input Deadband (Obj:34, Var:02) index none	dnp3	32-Bit Analog Input Deadband (Obj:34, Var:02)	WRITE	SCADA FEP
Binary Input With Status (Obj:01, Var:02) index 0	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP
Binary Input With Status (Obj:01, Var:02) index 1	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP

Binary Input With Status (Obj:01, Var:02) index 13	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP	Jul 15, 2024 5:40:29 AM	Jul 16, 2024 2:04:28 PM
Binary Input With Status (Obj:01, Var:02) index 14	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP	Jul 15, 2024 5:40:29 AM	Jul 16, 2024 2:04:28 PM
Binary Input With Status (Obj:01, Var:02) index 2	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP	Jul 15, 2024 5:40:29 AM	Jul 16, 2024 2:04:28 PM
Binary Input With Status (Obj:01, Var:02) index 3	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP	Jul 15, 2024 5:40:29 AM	Jul 16, 2024 2:04:28 PM
Binary Input With Status (Obj:01, Var:02) index 4	dnp3	Binary Input With Status (Obj:01, Var:02)	READ	SCADA FEP	Jul 15, 2024 5:40:29 AM	Jul 16, 2024 2:04:28 PM

© 2025 Cisco and/or its affiliates. All rights reserved.

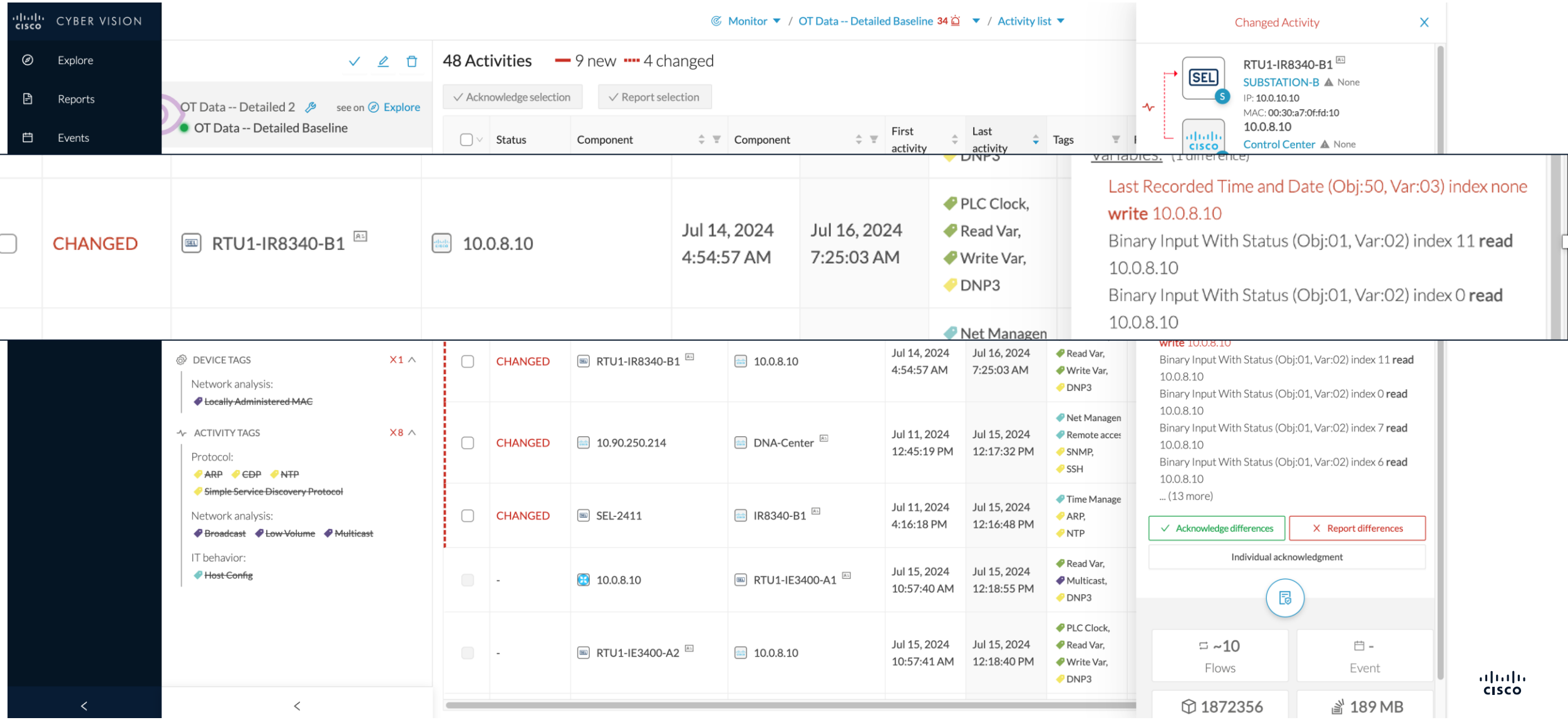
Cyber Vision Anomaly Detection

Reporting on Changes to Assets and Communication Flows



Cyber Vision Anomaly Detection

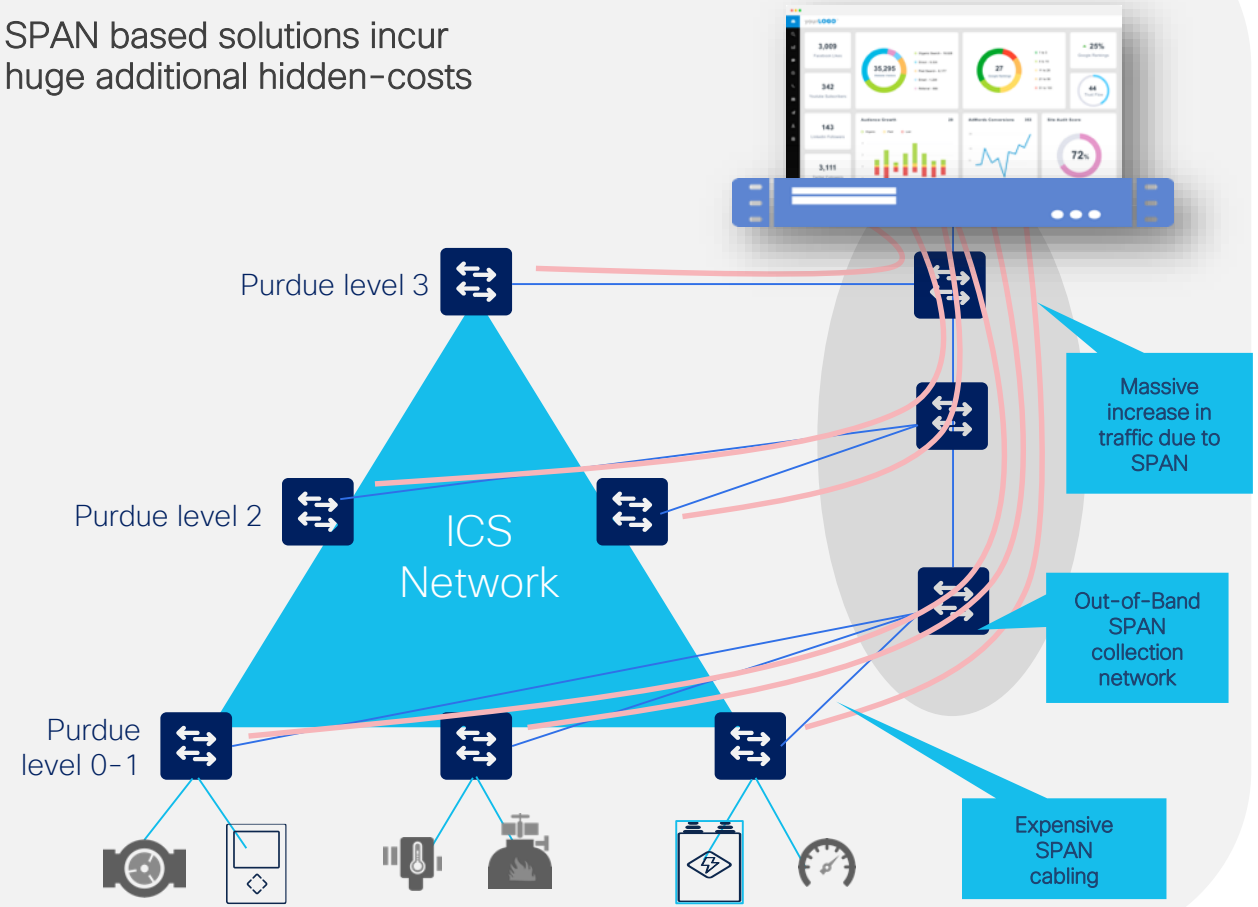
Reporting on Changes to SCADA Variables (e.g. DNP3 Write vs Read)



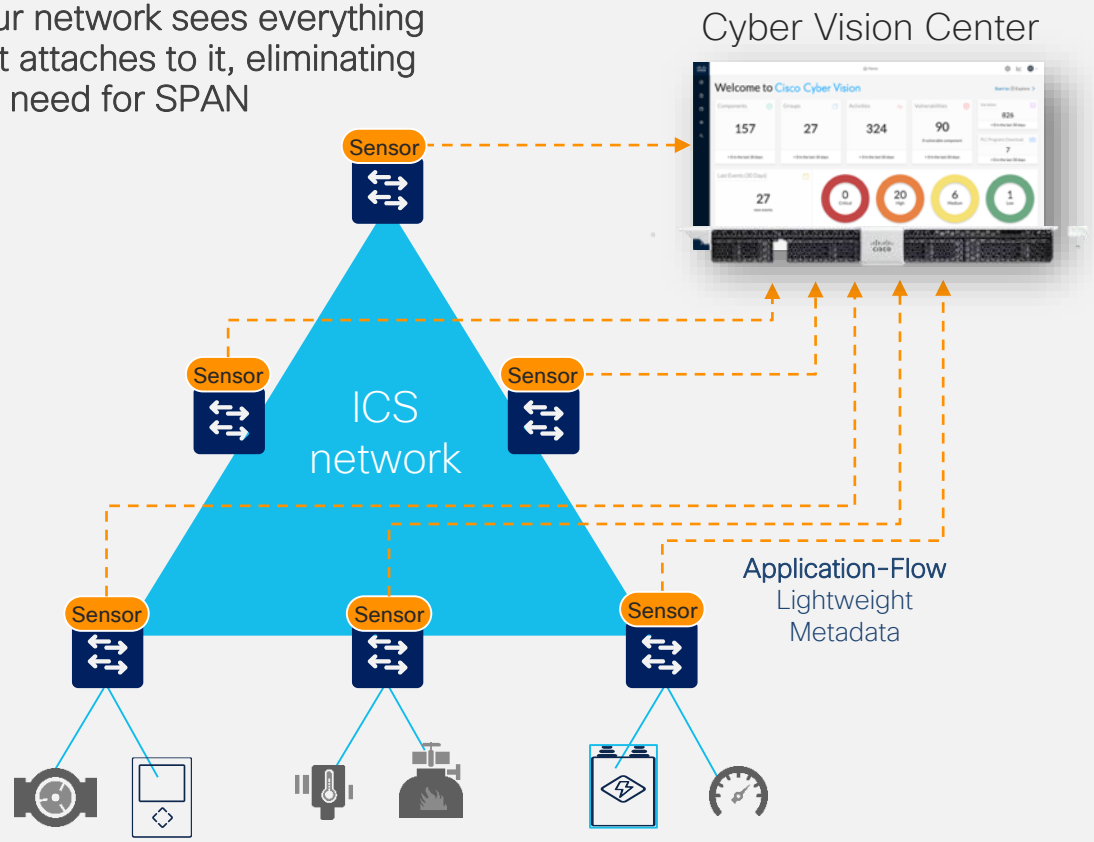
Cyber Vision Topology Advantages

Other solutions

SPAN based solutions incur huge additional hidden-costs



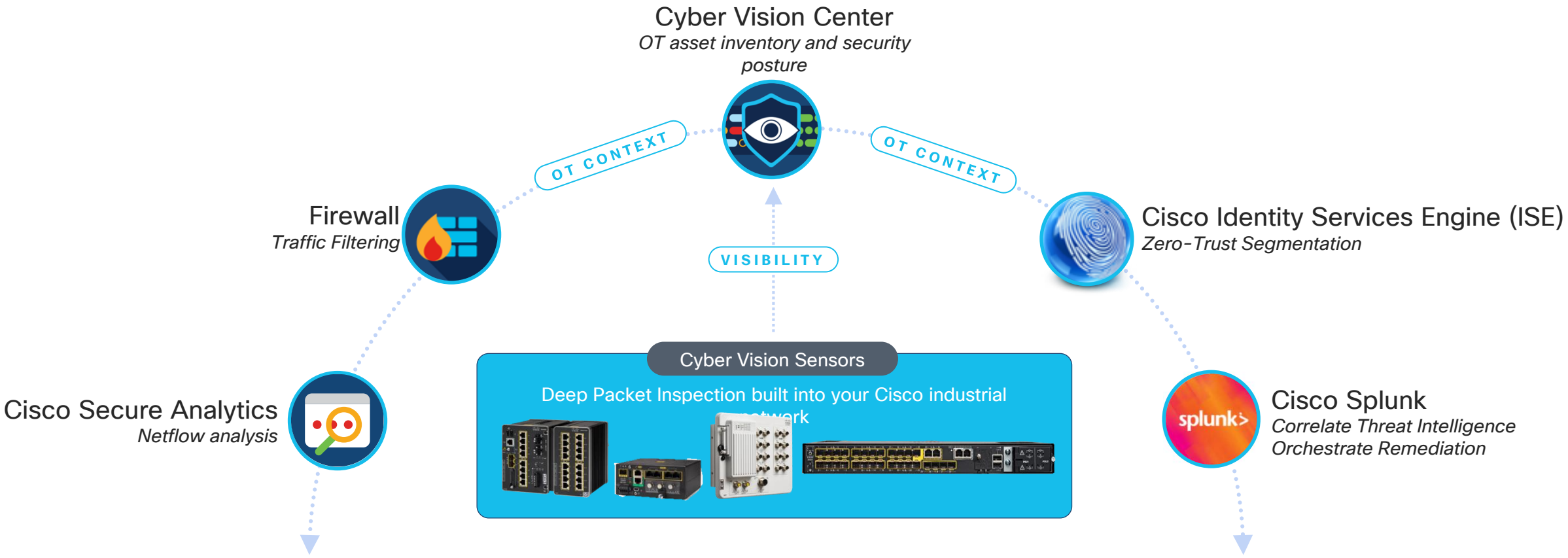
Your network sees everything that attaches to it, eliminating the need for SPAN



© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Visibility & Zero Trust

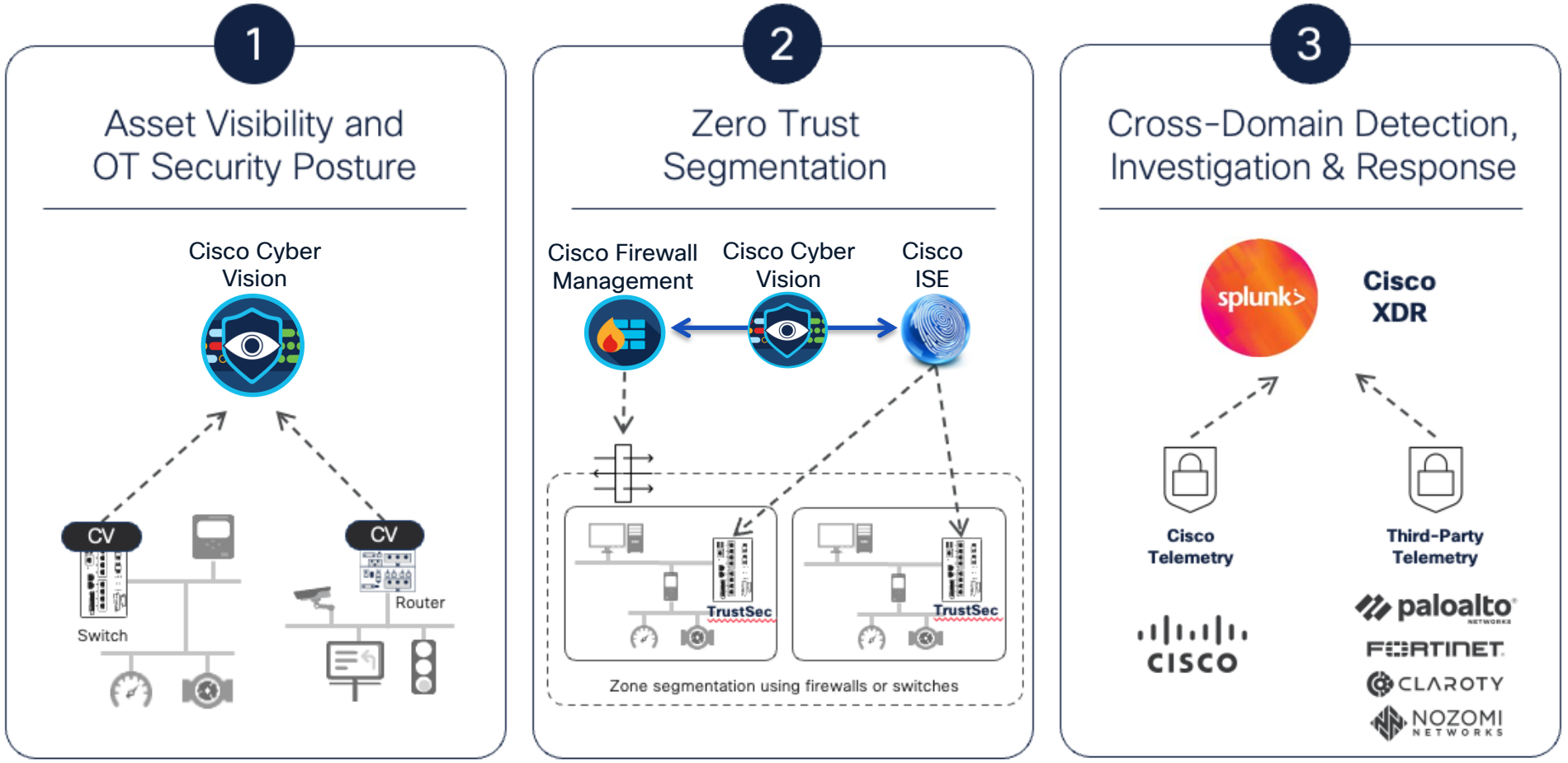
Cyber Vision Extensibility Options



Cisco's fully integrated IT-OT security solution, Powered by Talos Threat Intelligence

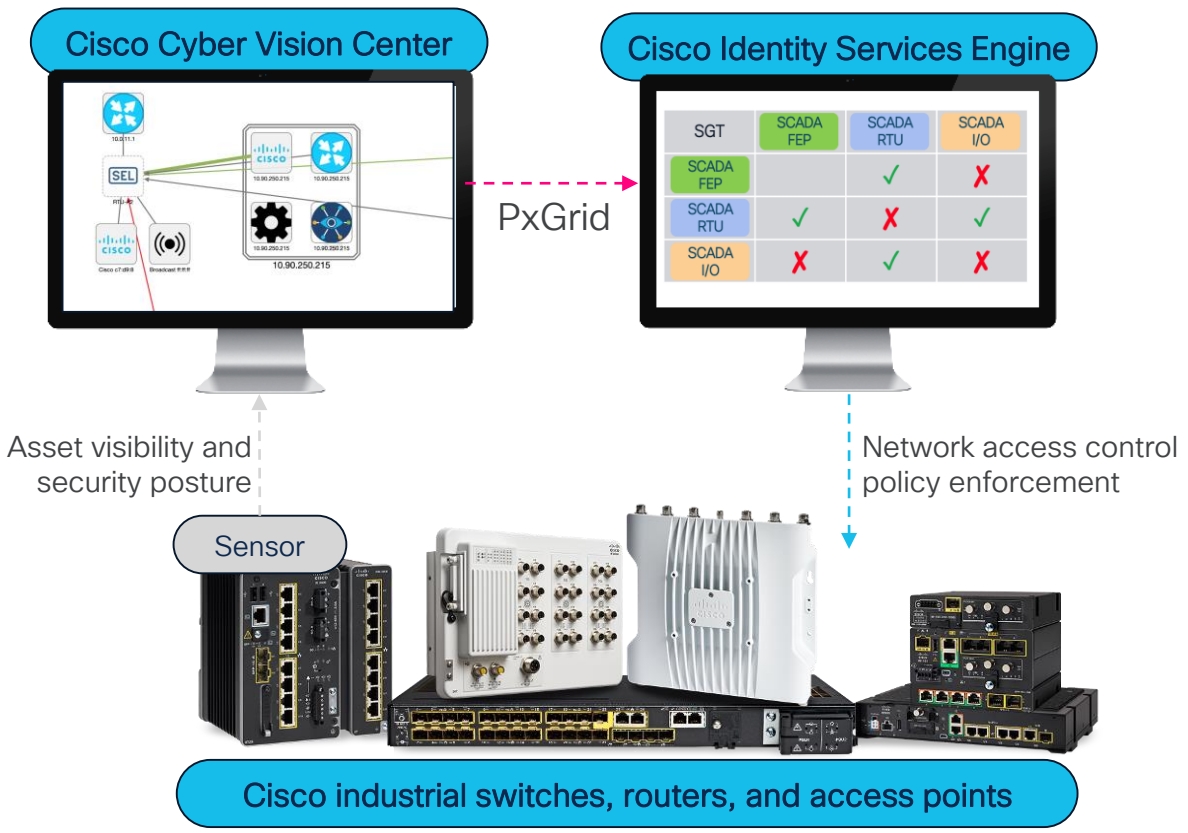
© 2025 Cisco and/or its affiliates. All rights reserved.

Zero Trust Concept



© 2025 Cisco and/or its affiliates. All rights reserved.

Zero Trust with IOS-XE, Cyber Vision, and ISE



Cisco Cyber Vision
Gain full visibility into assets, and group them according to their role in the industrial process

Cisco Identity Services Engine (ISE)
Automatically update access control policies for the network to enforce zero-trust segmentation based on Cyber Vision groups

Enforcing network access policies for each device connected to the industrial networks

© 2025 Cisco and/or its affiliates. All rights reserved.

Microsegmentation with Cyber Vision and ISE

SEL-2411 Example

Cyber Vision Device Profiling

PxGrid

Identity Services Engine (ISE) Device Attributes

assetDeviceType	Controller, Slave
assetName	10.0.10.11,SEL-2411,SEL:0f:fc:d0
assetProductID	SEL2411
assetProtocol	DNP3
assetSerialNumber	31660950154
assetSWRevision	SEL-2411-R315-V2-Z007007-020160507
assetVendor	SEL
assetGroup	Substation-B
assetCustomName	RTU1-9320-B1

ISE Scalable Group Tag (SGT) Policy

If ***SEL-2411*** AND ***Substation-B*** THEN apply SGT ***SCADA I/O***

ISE Scalable Group ACL (SGACL) Matrix

SGT	SCADA FEP	SCADA RTU	SCADA I/O
SCADA FEP		✓	✓
SCADA RTU	✓	✗	✓
SCADA I/O	✓	✓	✗

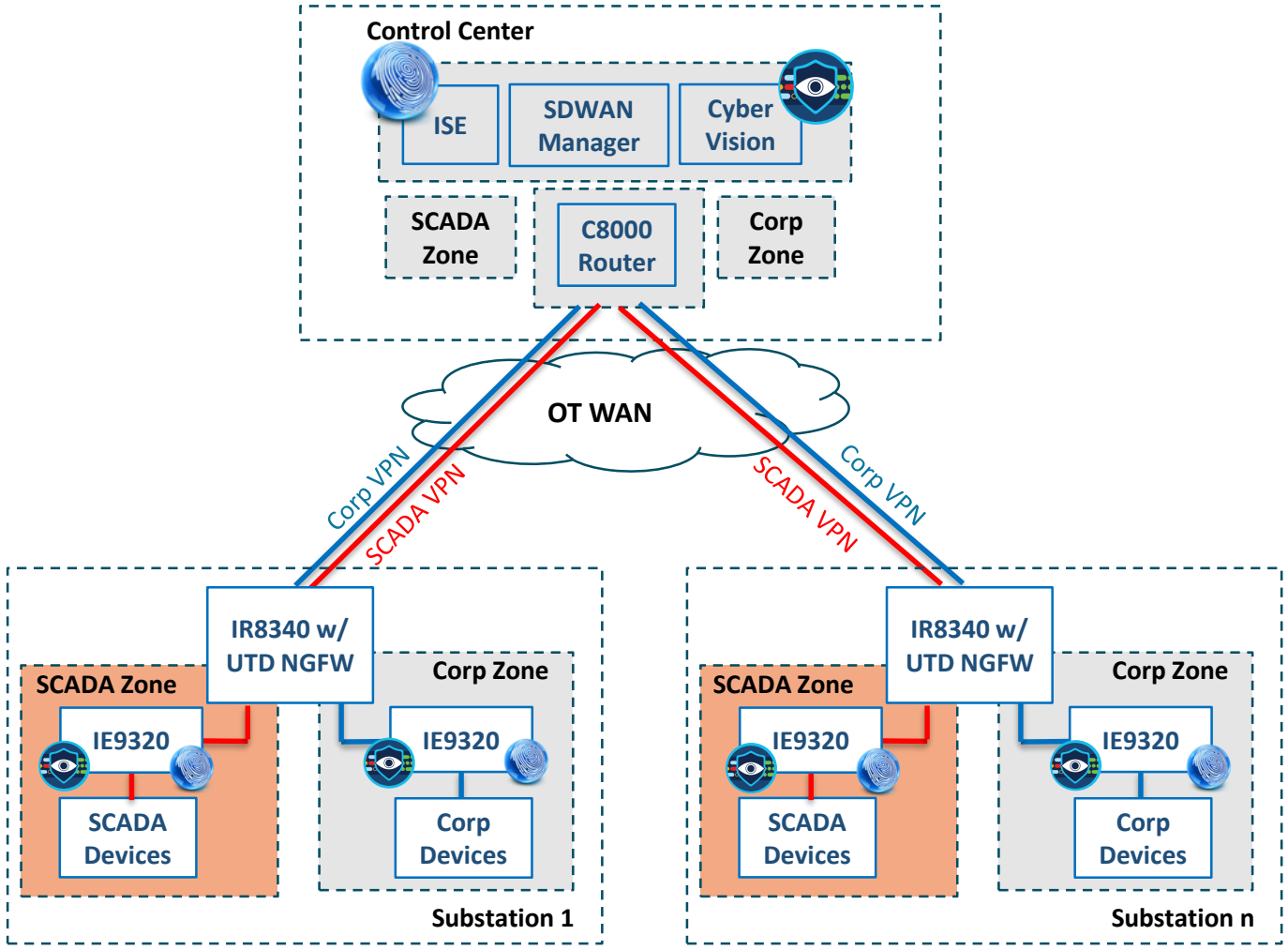
SGT (TrustSec)

SGACL Enforcement

dACL

IE Switch

Cisco Substation Zero-Trust Example



Grey = Macro-Segmentation Zone
Orange = Micro-Segmentation Zone

Segmentation Services Summary

Service	SubSystem	Enforcement Mechanism	
VPN	SDWAN Manager	Router IPSec VPN services	MACRO
VRF	SDWAN Manager	Router and Switch Layer 3 VRF and VRF-Lite	
VLAN	SDWAN Manager	Router and Switch Layer 2 VLAN services	
IP & Port Based Authorization	SDWAN Manager	Router UTD FW Services	
IDS/IPS	SDWAN Manager	Router UTD IDS/IPS engine	
Context-Based Authorization	ISE + Cyber Vision	Switch TrustSec SGT Services	MICRO

Segmentation Policy Summary

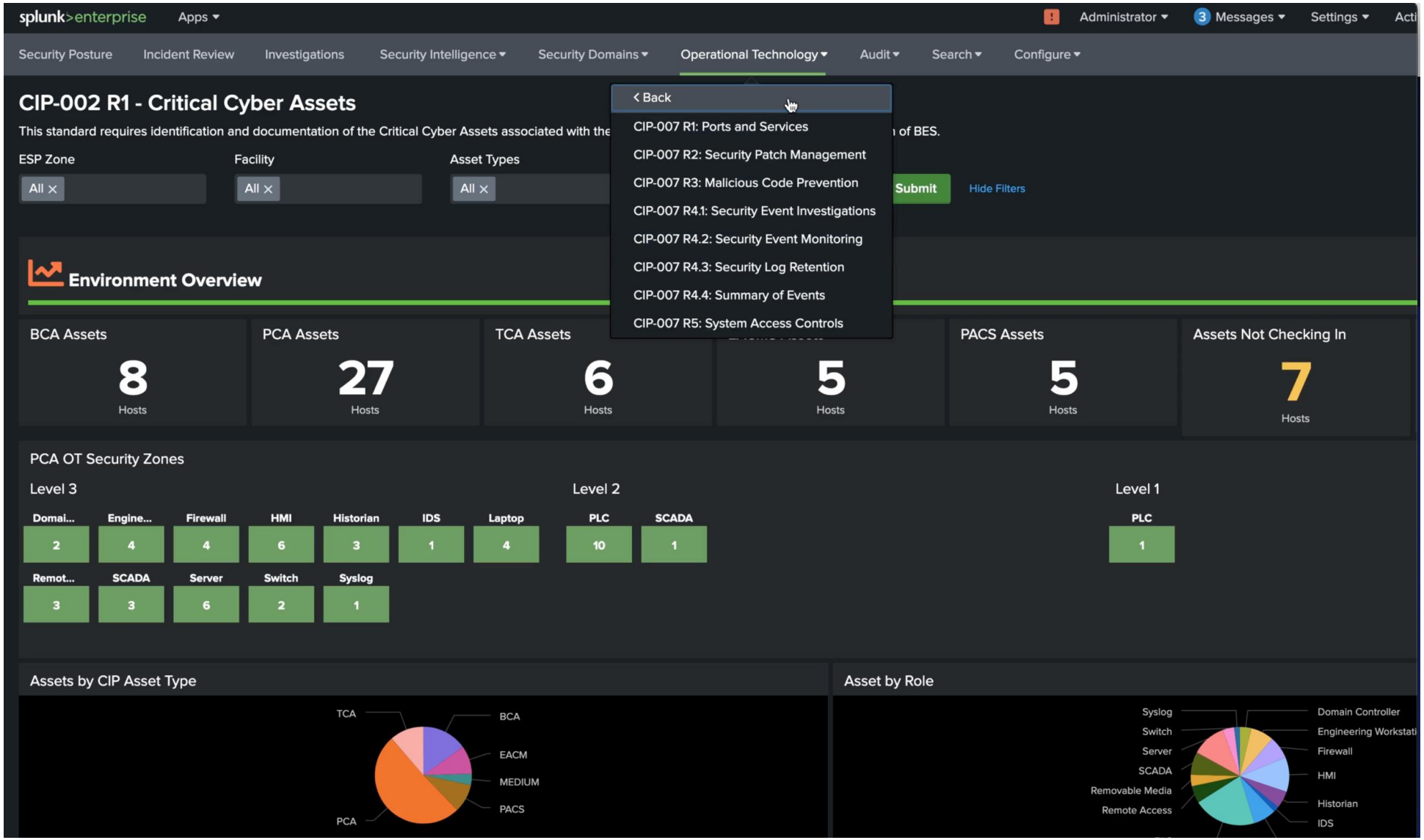
Segmentation Zones	Control Center SCADA	Substation SCADA	Control Center Corp	Substation Corp
Control Center SCADA	✓	✓	✗	✗
Substation SCADA	✓	MICRO	✗	✗
Control Center Corp	✗	✗	✓	✓
Substation Corp	✗	✗	✓	✓

SGT	SCADA FEP	SCADA RTU	SCADA I/O
SCADA FEP		✓	✓
SCADA RTU	✓	✗	✓
SCADA I/O	✓	✓	✗

Microsegmentation Policy (SGACL)

© 2025 Cisco and/or its affiliates. All rights reserved.

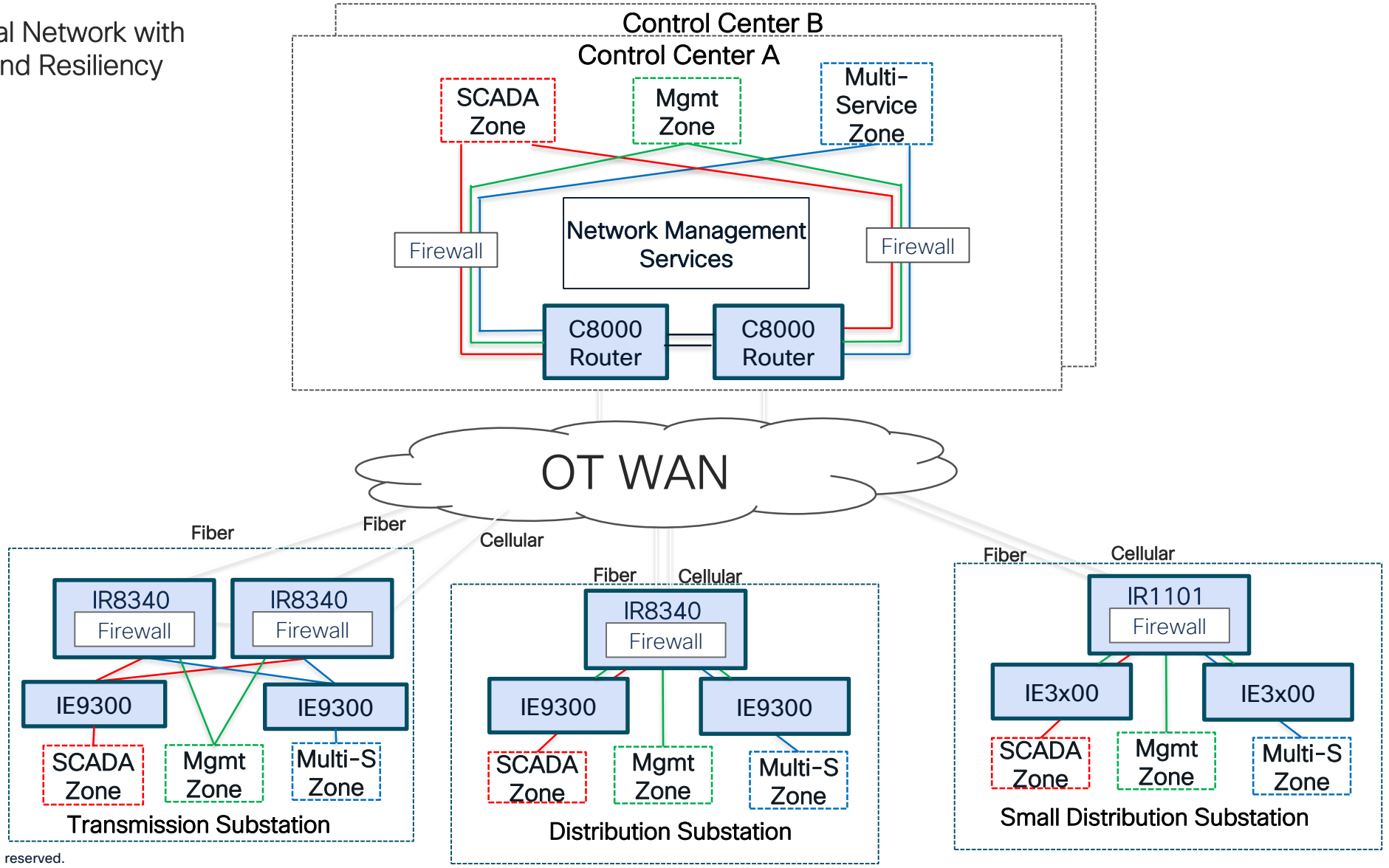
Splunk NERC CIP dashboard



© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Network – Phased Approach

Phase 1: Cisco Industrial Network with Fundamental Security and Resiliency Services

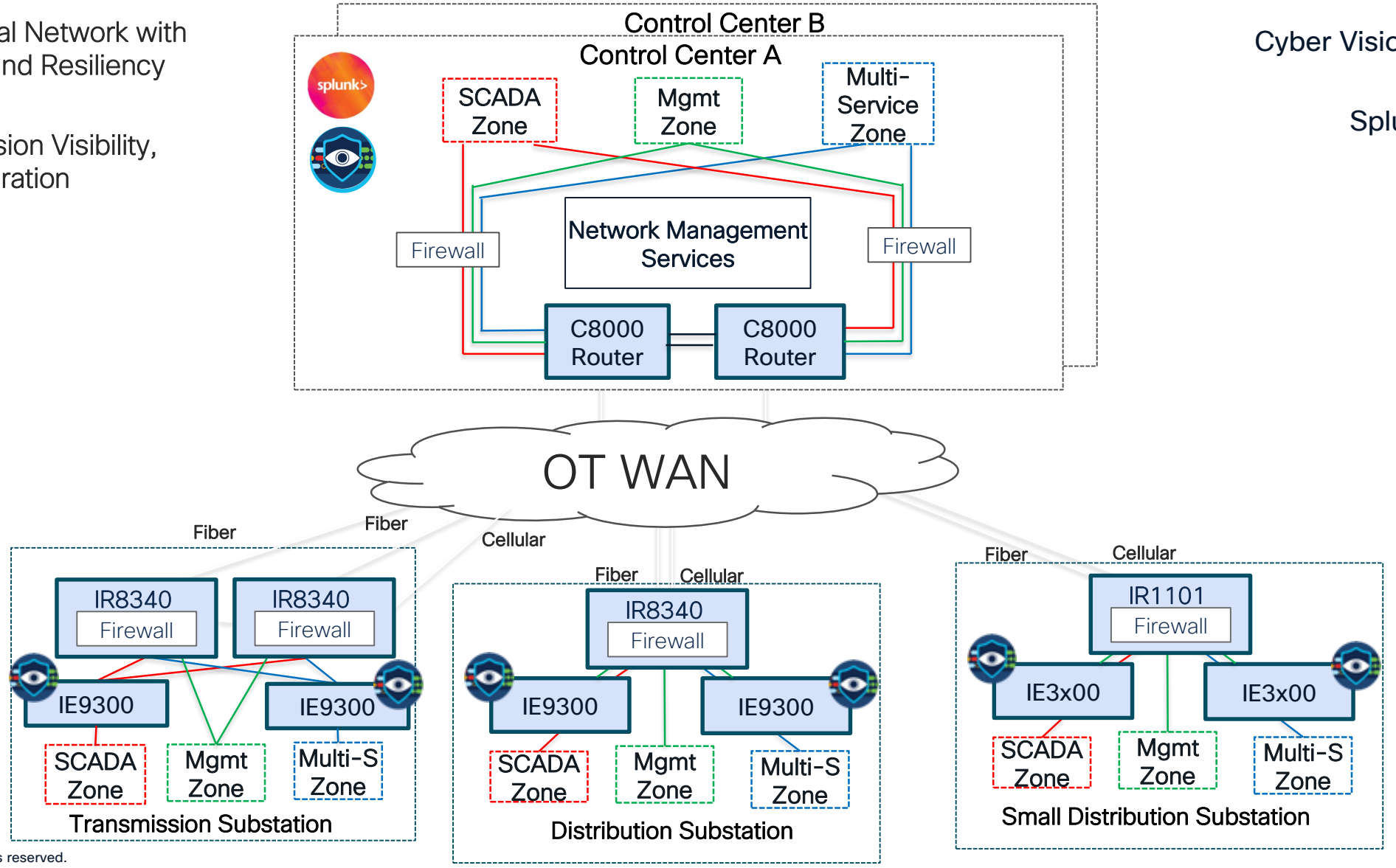


© 2025 Cisco and/or its affiliates. All rights reserved.

Substation Network – Phased Approach

Phase 1: Cisco Industrial Network with Fundamental Security and Resiliency Services

Phase 2: Add Cyber Vision Visibility, INSM, and Splunk Integration



Cyber Vision

Splunk

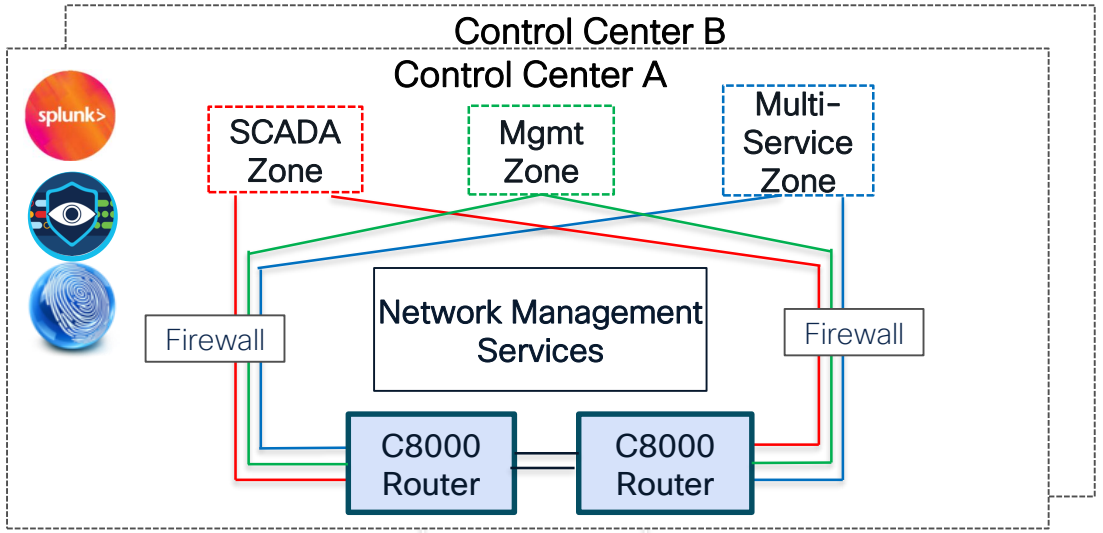
© 2025 Cisco and/or its affiliates. All rights reserved.

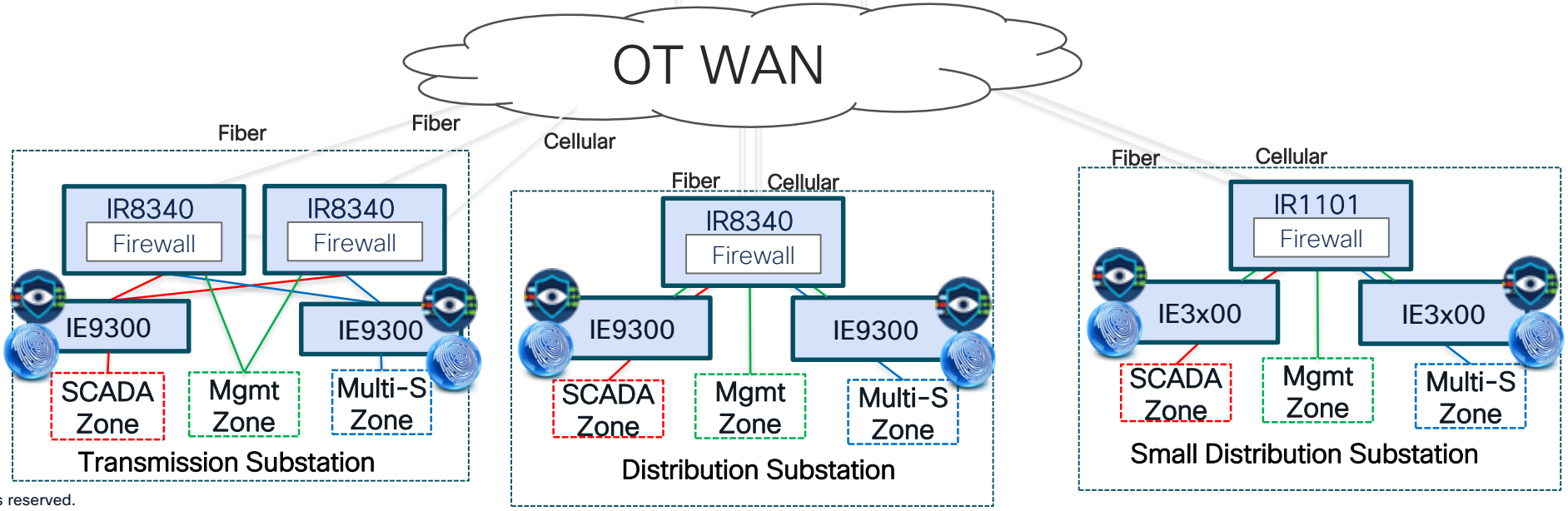
Substation Network – Phased Approach

Phase 1: Cisco Industrial Network with Fundamental Security and Resiliency Services

Phase 2: Add Cyber Vision Visibility, INSM, and Splunk Integration

Phase 3: Add ISE / Cyber Vision Integration for Zero Trust Microsegmentation





Cyber Vision

Splunk

Identity Services Engine

IEC 61850 Support

© 2025 Cisco and/or its affiliates. All rights reserved.

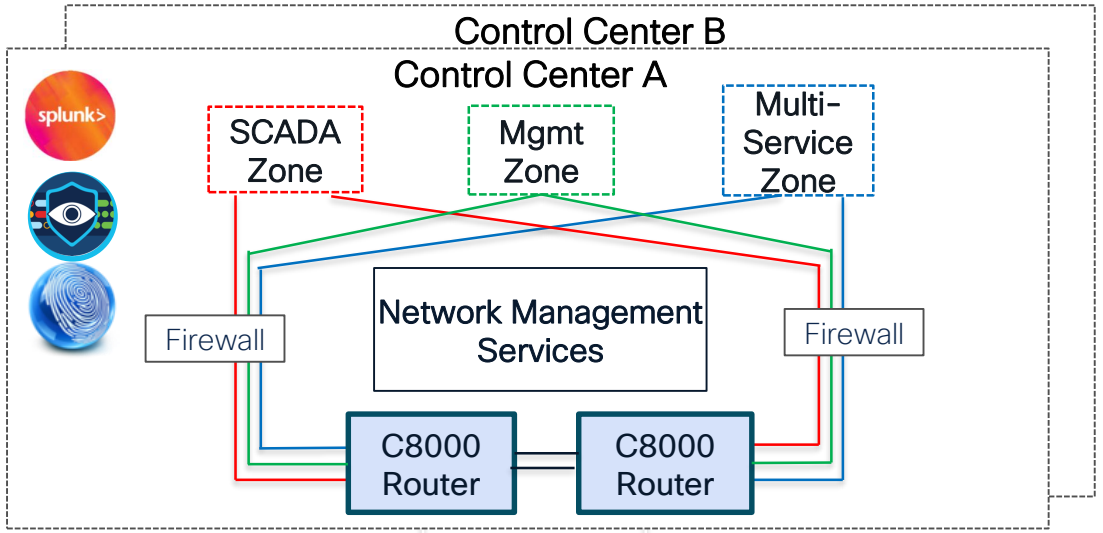
Substation Network – Phased Approach

Phase 1: Cisco Industrial Network with Fundamental Security and Resiliency Services

Phase 2: Add Cyber Vision Visibility, INSM, and Splunk Integration

Phase 3: Add ISE / Cyber Vision Integration for Zero Trust Microsegmentation

Phase 4: SW Config changes to support 61850 substation architectures

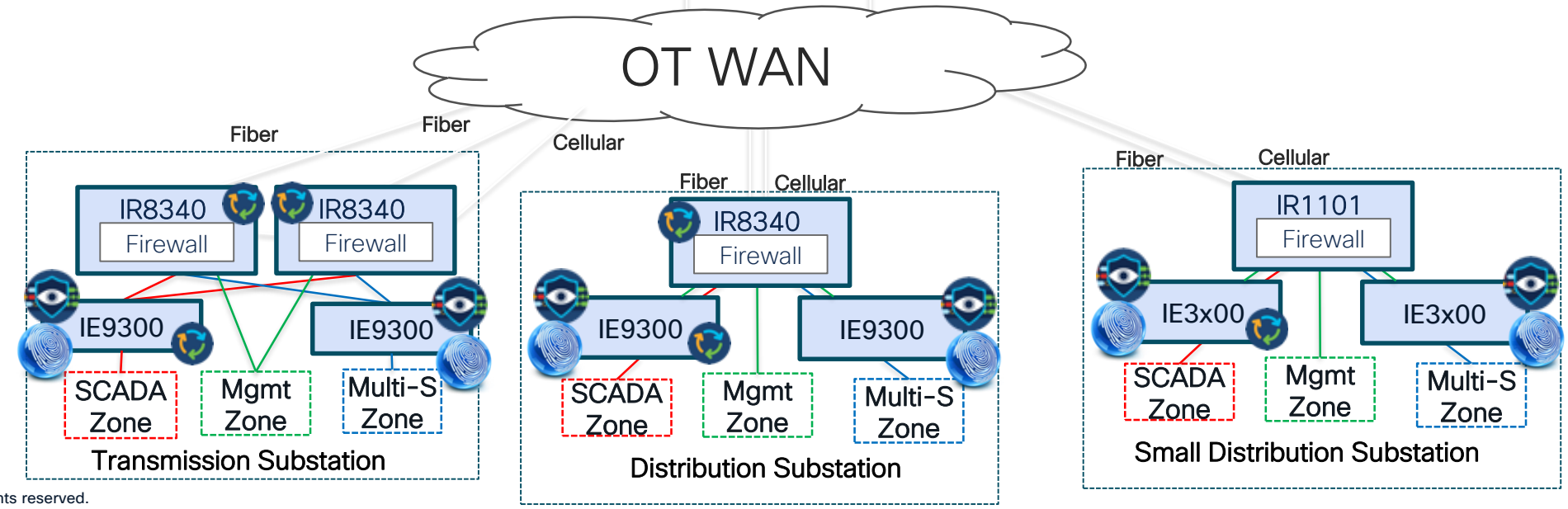


Cyber Vision

Splunk

Identity Services Engine

IEC 61850 Support



© 2025 Cisco and/or its affiliates. All rights reserved.

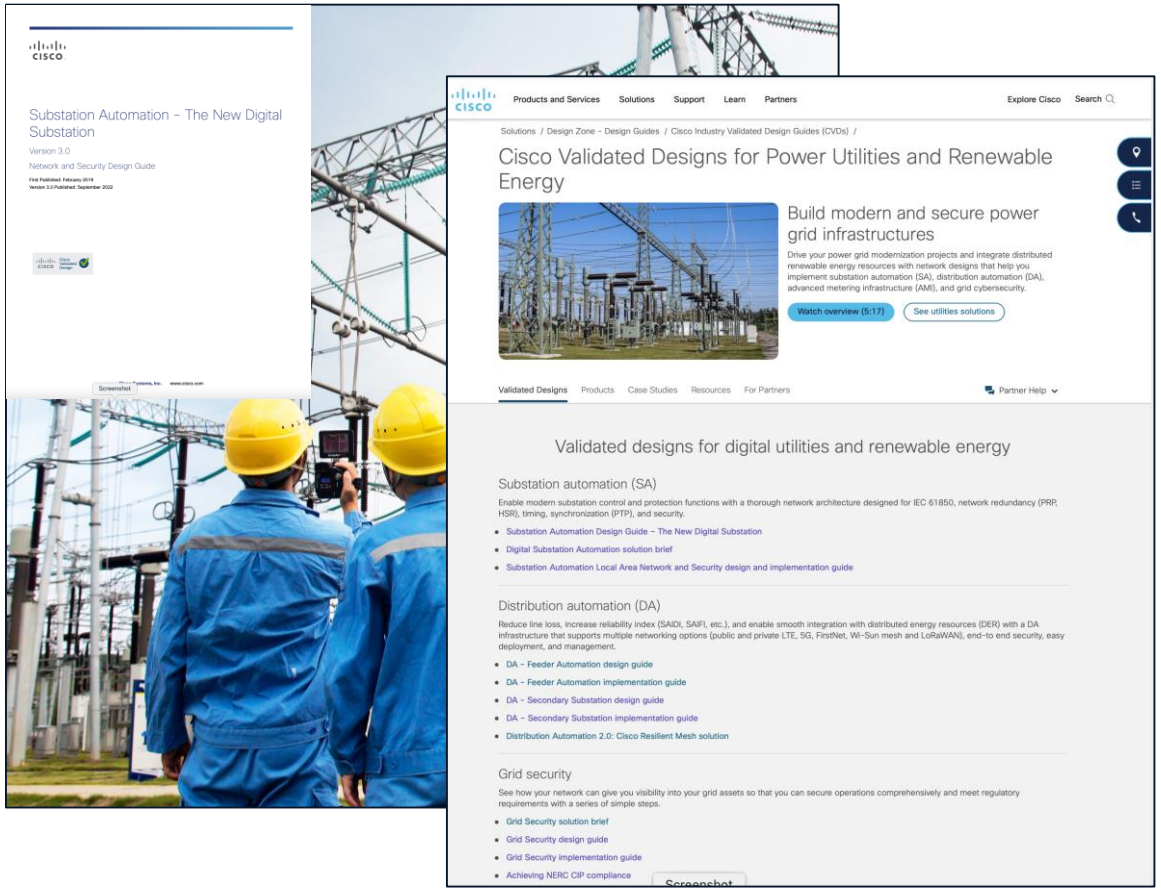
Conclusion

Key Take Aways

- Cisco Validated Designs provide best practice design and implementation guidance
- The New Digital Substation products offer enhanced capabilities to help utilities migrate to IP/Ethernet based architectures
- The New Digital Substation also extends to the WAN
- Gaining asset visibility is a key first step to securing your grid applications
- Future innovation is only possible through digitising your grid infrastructure (e.g Centralised or Virtualised protection)

© 2025 Cisco and/or its affiliates. All rights reserved.

Also Investing in Utilities CVD Solutions



- Distribution Automation
  Feeder & Secondary Substations
- Renewable Energy Offshore Wind Farms
- SDWAN for Industrial Routers
  SDWAN for DA Use Cases
- Substation Automation (inc WAN)
- Grid Security

www.cisco.com/go/iotcvd

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

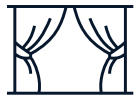
Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related IIoT demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact us at: marcusmi@cisco.com, dmadey@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !


CISCO