

Cisco Provider Connectivity Assurance

White Paper

September 2025

Contents

Abstract 3

Introduction..... 3

Assuring Three Common Substation Use Cases..... 6

Cisco Provider Connectivity Assurance for Utility Networks..... 13

Benefits of PCA for Utility Networks 15

Conclusion..... 15

Appendix A. Design Guide and Implementation for PCA..... 16

 Provider Connectivity Assurance Solution 16

 Design 17

 Provider Connectivity Assurance Configurations 21

 Provider Connectivity Assurance Analytics 31

Abstract

This whitepaper details Cisco Provider Connectivity Assurance (PCA), a purpose-built solution for ensuring the reliability and performance of network services. As the utilities sector increasingly relies on IP connectivity for mission-critical Operational Technology (OT) services like SCADA, and Teleprotection, proactive service assurance becomes essential.

PCA uniquely addresses these demands through smart-pluggable sensor SFP modules that provide hardware-timestamped, microsecond-precision measurements and continuous, high-frequency synthetic packet generation. An advanced analytics platform enriches data with contextual metadata, to deliver unparalleled service-centric visibility. This enables proactive detection and rapid remediation of even transient network degradations, ensuring stringent Layer 2 and 3 service level agreement (SLA) compliance, continuous operational continuity, and enhanced resilience for vital substation interconnects.

Introduction

While using routed IP networks to interconnect remote enterprise sites is well established, critical Industrial IoT (IIoT) use cases such as electrical substation connectivity for the industry has historically relied on connectivity PSTN, SONET/SDH, or direct connections to ensure consistent latency and fail-safe connectivity.

However, the ongoing digital transformation within the utilities sector now necessitates a shift towards highly reliable, secure, and high-performance IP connectivity between these vital infrastructure points.

Traditional network monitoring tools often lack the capabilities required to meet the stringent network demands of mission-critical operational technology (OT) systems like SCADA, Teleprotection, and inter-substation communications.

The consequences of network issues in these environments range from operational inefficiencies to grid instability and safety hazards. This whitepaper introduces Cisco Provider Connectivity Assurance (PCA), a comprehensive solution engineered to address these performance challenges by transforming network management from reactive troubleshooting to proactive optimization.

This whitepaper explores the critical need for advanced service assurance in utilities, explores unique technical capabilities of the Provider Connectivity Assurance platform, and examines its detailed application in substation use cases (specifically SCADA, IEC61850 GOOSE, and Traditional TDM-based Teleprotection). Ultimately, the paper aims to demonstrate how assurance enables utilities to achieve and maintain strict Layer 2 and /Layer 3 SLA compliance for their critical OT services, enhancing operational efficiency.

Why Service Assurance is Important for Utilities

The Utility Wide Area Network (WAN) is often a dedicated WAN infrastructure that connects the Transmission System Operator (TSO) Control Center with various Substations and other field networks and assets. This WAN transports critical services that require deterministic and predictable network performance to ensure operational continuity and reliability.

Service Assurance provides continuous verification that the network consistently meets the stringent performance and reliability criteria required by Operational Technology (OT) services, such as SCADA, IEC61850 GOOSE, and Teleprotection. This is essential for maintaining high availability and low latency, both critical in utility environments where downtime or increased latency can have significant consequences.

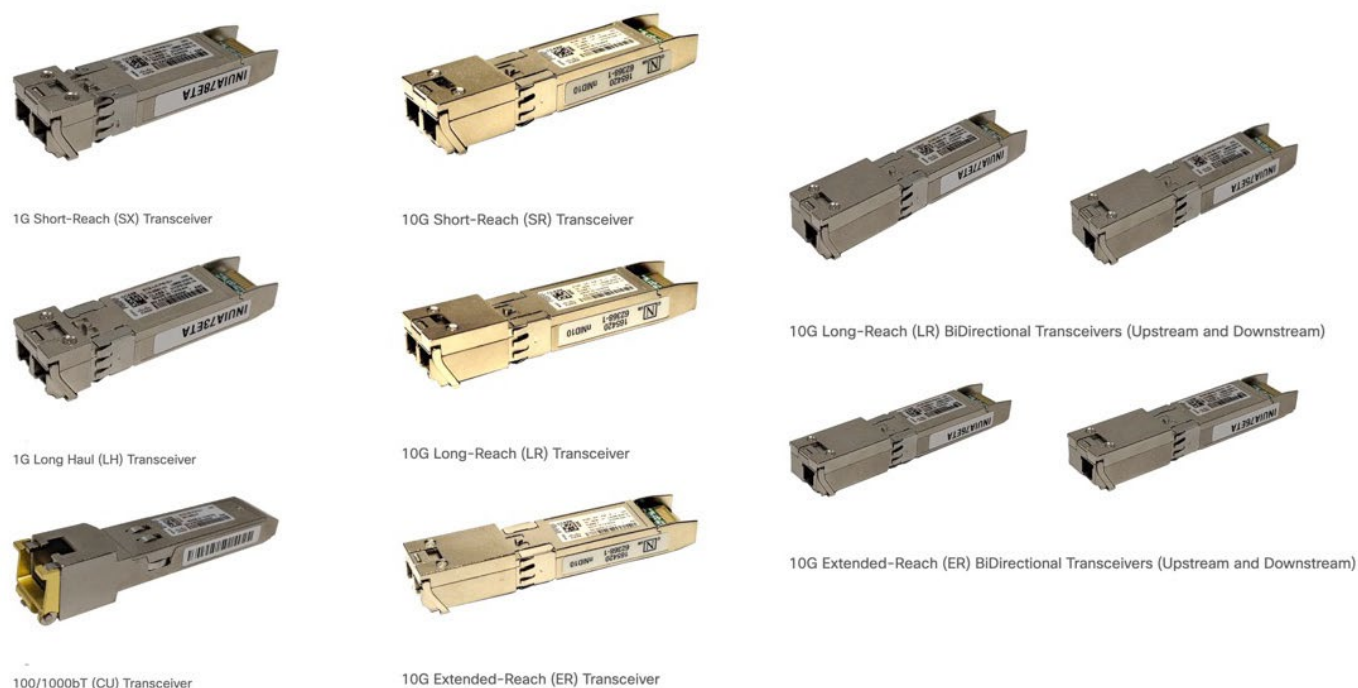
By continuously monitoring the transport services, service assurance plays a key role in meeting SLAs for the various OT services. It allows for proactive detection of potential issues before they affect operations, reducing downtime and improving overall network health.

Many network monitoring tools lack the granularity and accuracy required for utility WANs, especially where high reliability and low latency are required. These limitations make it difficult to detect transient issues or microevents that may impact critical services.

Cisco Provider Connectivity Assurance (PCA) addresses these challenges by providing high detailed, service-centric visibility with microsecond accuracy and millisecond sampling intervals. This fine granularity enables detection of short-lived issues that other assurance solutions may miss.

Smart-pluggable Sensor SFP modules combine the precision of hardware-based monitoring with simple, flexible installation—requiring no additional computing resources, space, or power.

Figure 1. Cisco PCA Sensor SFPs



Key Assurance Sensor SFP features include:

- **Hardware timestamping:** Delivers microsecond-level accuracy for precise low-latency measurements
- **Continuous, high-frequency synthetic packet generation:** Enables millisecond-level sampling without overloading the CPU or impacting the measurements
- **One-way metric support** Accurately detects directional performance issues, unlike round-trip measurements that may mask such problems
- **Measurement of the real service path.** Synthetic measurement packets travel alongside actual user traffic using same Class of Service (CoS) or DSCP or VLAN tags to accurately reflect real network behaviour
- **Granular throughput measurements.** Ultra granular real time throughput measurement, based on L2/L3 user defined parameters such as VLANs, IPs, DSCP, ports, and so on)

PCA uses well-known and widely used standard protocols for network assurance such as TWAMP (RFC 5357) for Layer-3 and Y.1731 is used for Layer-2 measurement. However, it goes beyond standard implementations by providing a broader set of KPIs and deeper insights, enabling utilities to benefit from granular assurance while leveraging existing capabilities in their own infrastructure and facilitating the deployment of the solution. For example, it is possible to use TWAMP reflector capabilities that already exist in most routers (IR or NCS family for example support TWAMP based reflectors via IP SLAs).

Without a robust and reliable assurance, solution disruptions or degradations in network performance can lead to delays or outages. By proactively assuring network services, utilities can gain the ability to act on long-term trends, prevent unforeseen issues, ensure business continuity, protect critical infrastructures, and deliver uninterrupted service to their customers

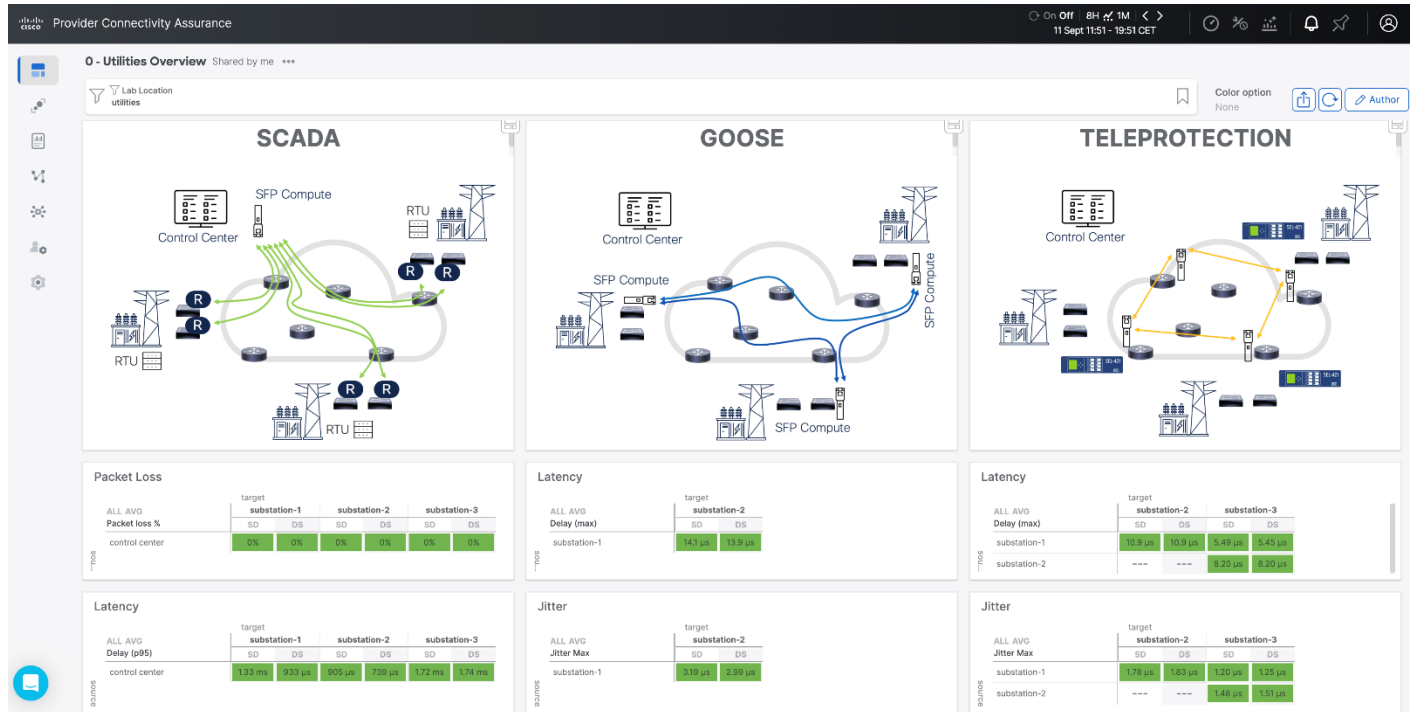
Assuring Three Common Substation Use Cases

Provider Connectivity Assurance is used to monitor the transport paths connecting the Transmission System Operator (TSO) Control Center and the Transmission Substations regardless of whether the service connectivity is on-net (via utility owned MPLS/IP or Segment Routing network) or off-net (public backhaul, leased line or cellular backhaul), and irrespective of the service protocol (L2 or L3 VPN)

In this paper, we will focus on the assurance of three types of services that are transported across the transport network and are either critical or require low latency:

- **SCADA:** Assurance of the Hub and Spoke connectivity over Layer-3 from Control Center to all substation locations across the MPLS backbone
- **IEC61850 Goose:** Assurance of the Layer-2 low -latency traffic between substations for protection applications.
- **Teleprotection:** Hop-by-hop monitoring of interconnecting Layer-2 ring topology requiring strict low-latency and high availability

Figure 2. Cisco Provider Connectivity Assurance dashboard with SCADA, GOOSE, and Teleprotection assurance



Additionally, assurance can be extended to any new services that will require network support, including services under the responsibility of the transport team:

- Corporate traffic: data, video, IP voice
- AMI: Smart metering data from aggregation point to a datacenter
- IP CCTV
- Other OT traffic such as Phasor Measurement Units (PMU) or metering data

Extending assurance to those services, will help the transport team to improve quality and increase their operational efficiency.

SCADA

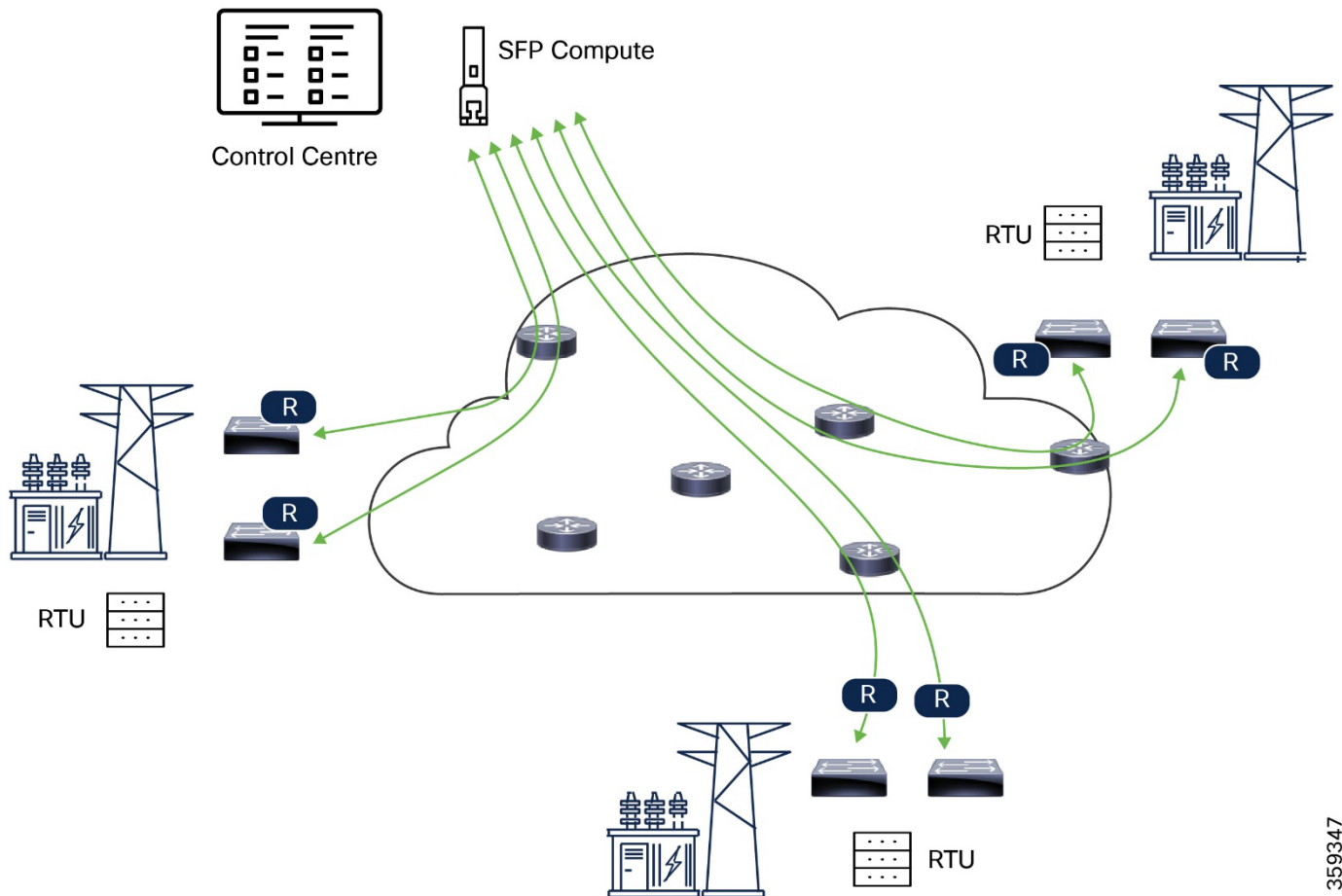
A modern electrical utility network operates as a distributed environment, where remote substations are managed from a centralized Control Center via a wide area network (WAN) infrastructure.

Utility operators use Supervisory Control and Data Acquisition (SCADA) applications to gather supervision information of site status and health, typically using Remote Terminal Units (RTU).

The SCADA traffic is transported via VRF aware L3 VPN, from each substation to the Control Center across the MPLS or Segment Routing backbone in a hub-and-spoke topology.

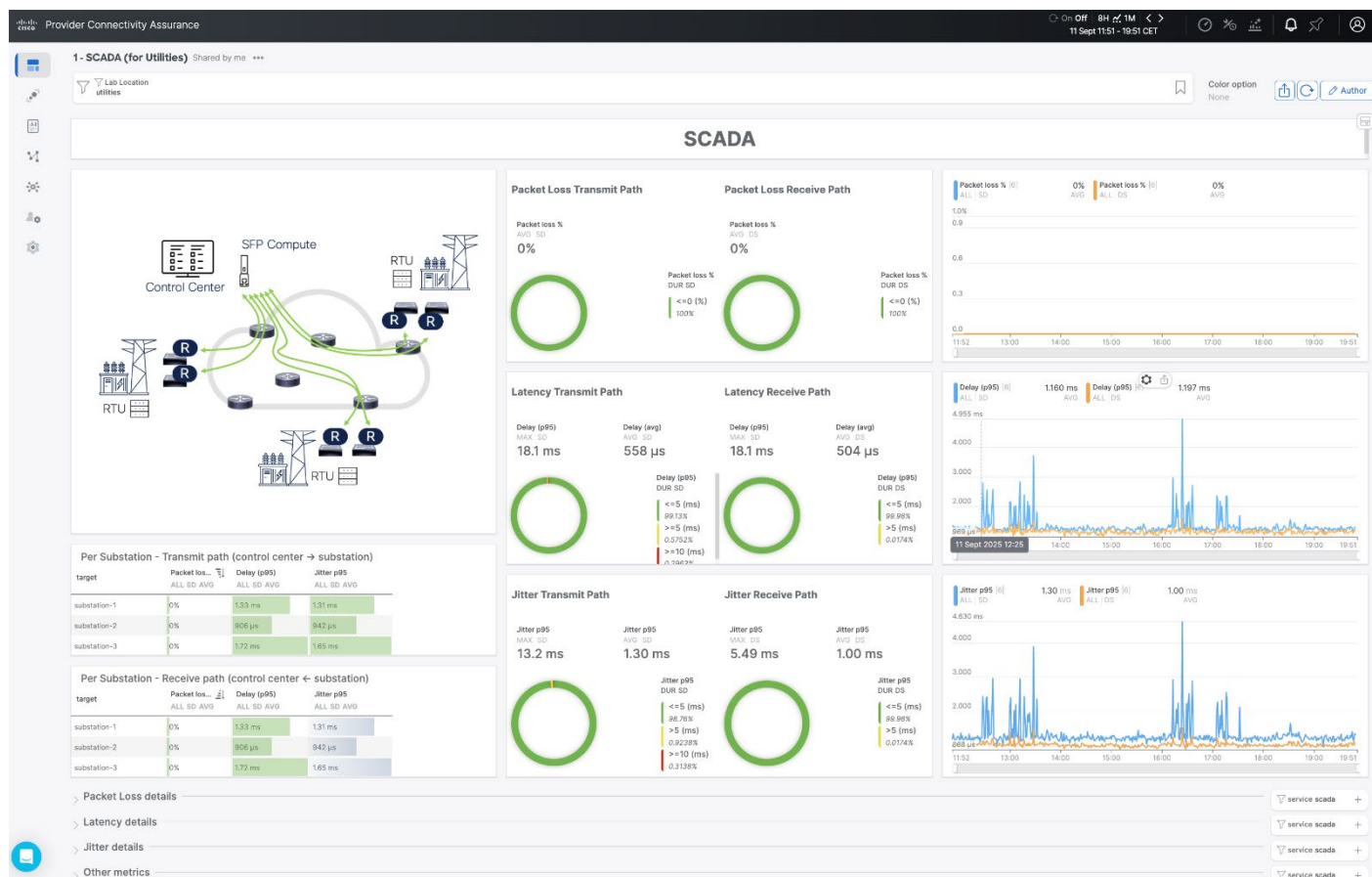
Service assurance uses a single PCA Sensor SFP installed centrally at the Headend router in an unused port (out-of-line). From that SFP Sensor, TWAMP sessions are created towards the built-in responders in IR/IE/NCS devices located in the sub-stations carrying the SCADA traffic to continuously monitor latency and packet loss, among others.

Figure 3. Provider Connectivity Assurance for SCADA



Enabling the TWAMP responder in the substation routers means there is no need to deploy separate assurance hardware. It is possible to monitor multiple substations using a single SFP as the TWAMP sender. It is in the Control Center Headend Router and benefits from the advantages of proactive service assurance.

Figure 4. Provider Connectivity Assurance Dashboard for SCADA



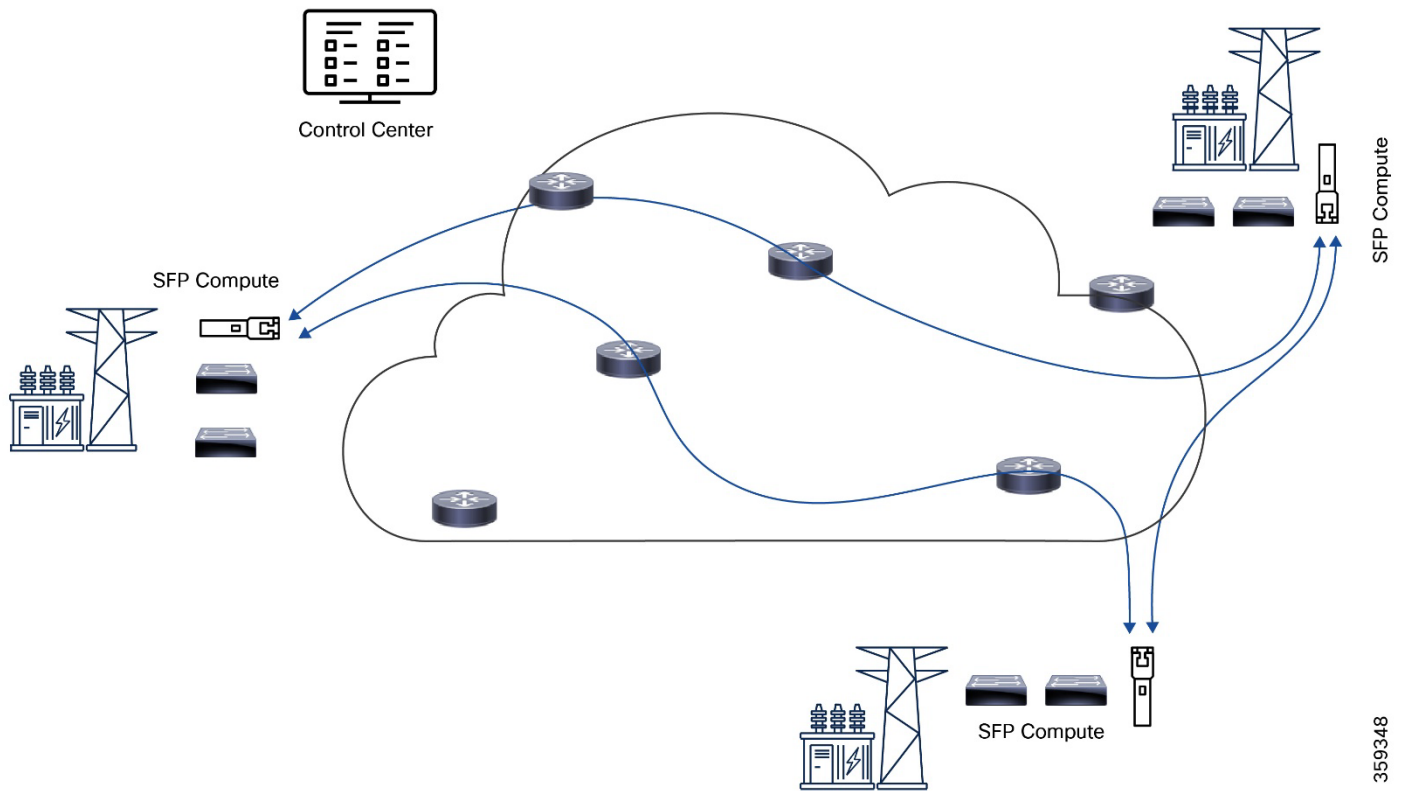
IEC61850 GOOSE

Generic Object-Oriented Substation Events (GOOSE) was originally introduced with IEC61850 as a substation Layer-2 LAN protocol for notification of protection events. Today's distributed grid architectures require this communication to span several substations in a region through low-latency connections.

The Cisco validated substation automation CVD provides an assured Layer-2-VPN mesh topology between substations in a region. According to IEC61850, GOOSE messages should be transmitted across communication networks within 5 milliseconds (for the most stringent current differential protection schemes).

The Assurance Sensor SFP is installed in all the substations or in selected locations, in the L2 switches connecting to the WAN router. The Sensor SFP uses L2 ETH-OAM to continuously monitor loss and one-way latency and jitter related metrics between Substations on the VLAN(s) used by GOOSE.

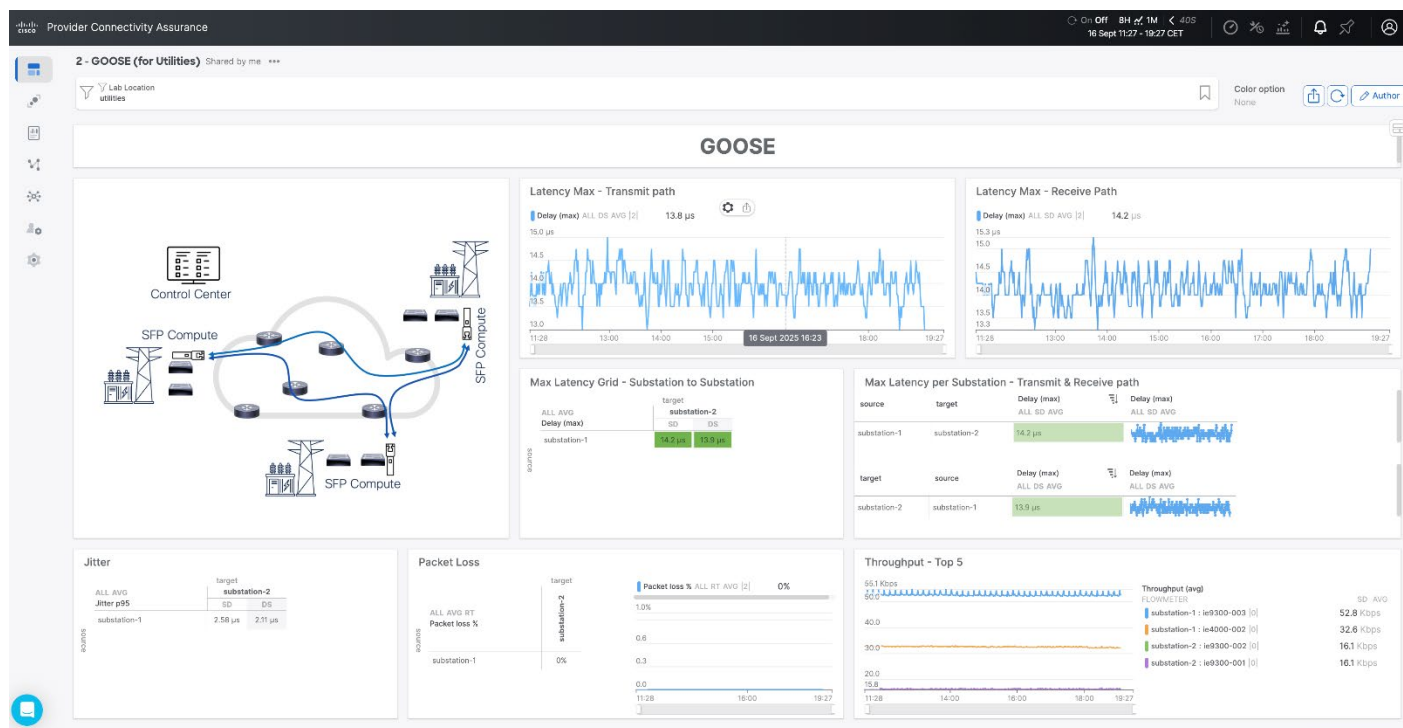
Figure 5: Provider Connectivity Assurance for GOOSE



With assurance it is possible to validate site-to-site latency and detect and act on any degradations before it affects the GOOSE traffic.

Additionally, the Sensor SFP continuously measures throughput on a per VLAN basis with high granularity to detect microburst, peaks of traffic or any anomaly affecting the substations. The Sensor SFP can also be leveraged for on-demand throughput testing capabilities up to line-rate for troubleshooting or site bring-up validation.

Figure 6. Provider Connectivity Assurance Dashboard for IEC61850 GOOSE



TELEPROTECTION (non-GOOSE based)

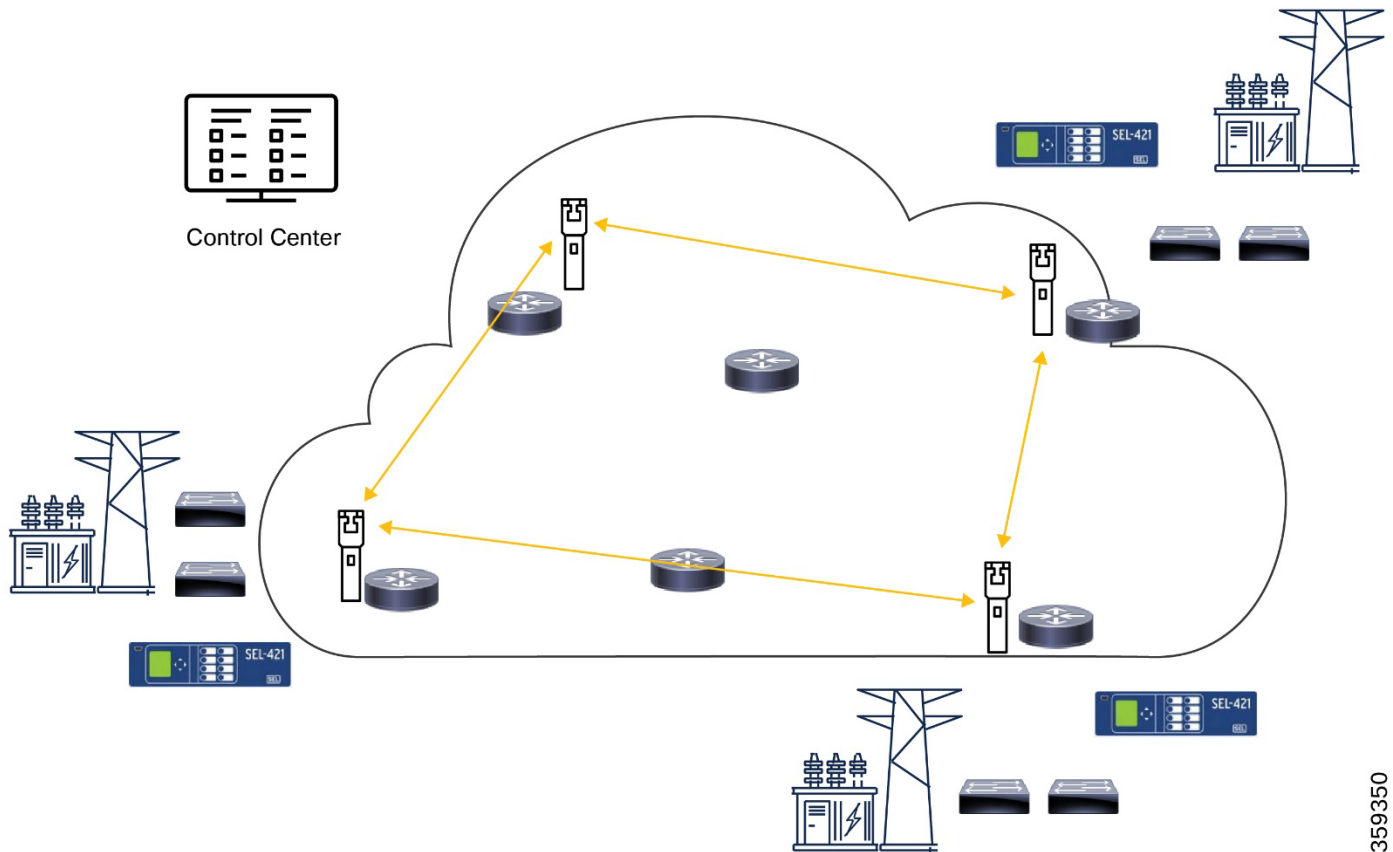
The purpose of Teleprotection in power grids is to ensure the rapid, selective, and coordinated isolation of faults, to maintain grid stability and prevent widespread outages. Teleprotection information is transmitted between substations through dedicated communication channels that traditionally used POTS, radio links or SDH/PDH, but those protocols have transitioned to using Ethernet services.

For the purposes of this paper, Teleprotection relates to the use of SEL ICON platforms for interfacing to traditional Protection relays using interfaces such as E1, C37.94, 4W E&M, G703, Serial. These then provide dual ethernet connections onto the transport network (MPLS or Segment Routing) forming a ring between ICON platforms at different substations.

To interconnect the Teleprotection equipment (SEL-421 relay in the example) in the Cisco CVD substations are connected using a hop-by-hop Layer-2 ring topology between the endpoints using EVPN VPWS.

Assurance sensor SFPs are connected to the PE-routers (Cisco NCS540) monitoring these Layer-2 EVPN using ETH-OAM. The millisecond sample resolution can detect a small amount of packet loss that might go unnoticed by systems supporting less granularity. The microsecond accuracy provided by the hardware timestamping capabilities of the Sensor SFPs can measure the small amount of latency (in the order of a few milliseconds) and jitter (hundreds of microseconds) required for the Teleprotection services to function correctly.

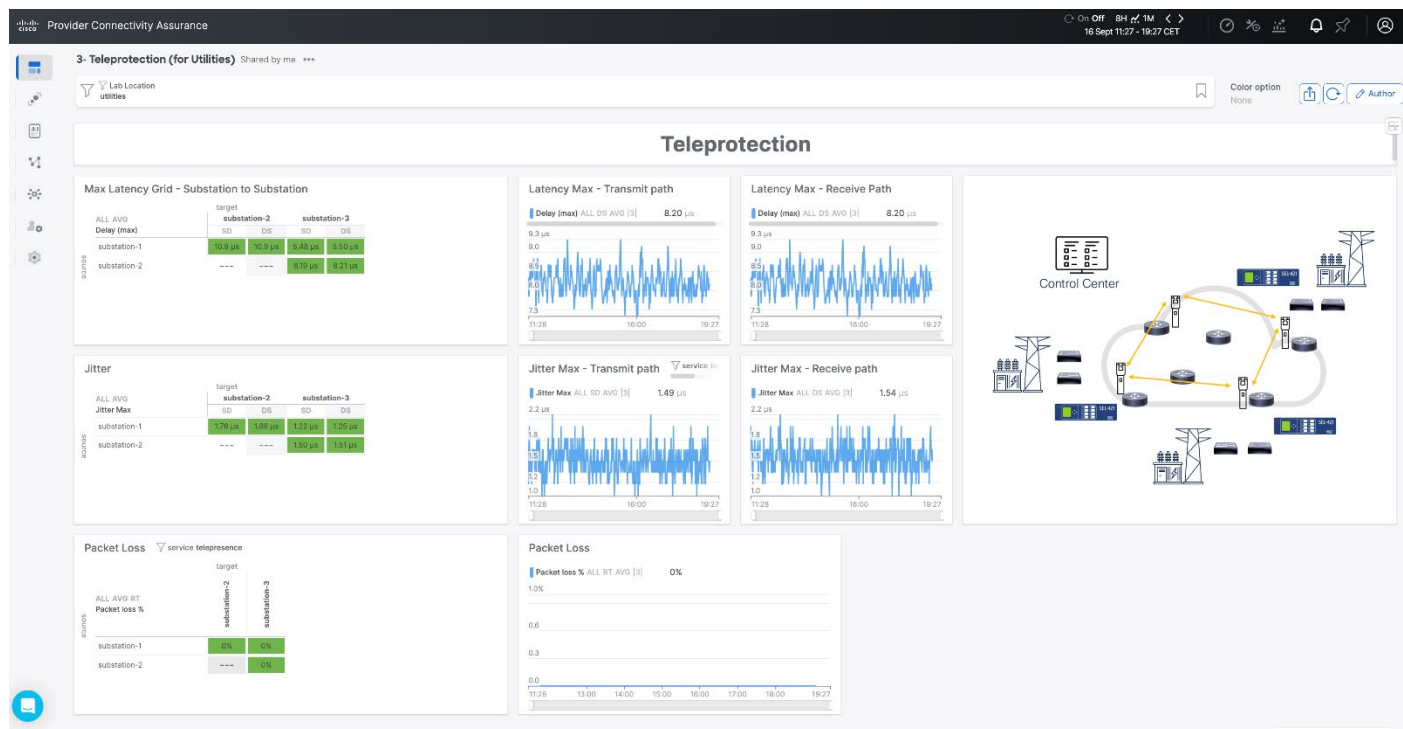
Figure 7. Provider Connectivity Assurance for Teleprotection



By continuously monitoring latency, jitter and loss, PCA can detect any degradations, for example network congestion due to buffering that increases latency and jitter. This allows network operators to act and take corrective actions before SLAs are affected.

359350

Figure 8. Provider Connectivity Assurance Dashboard for Teleprotection



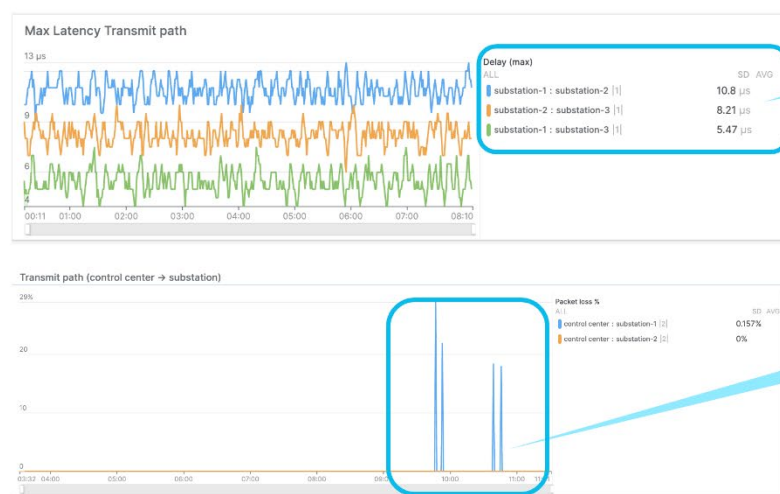
Cisco Provider Connectivity Assurance for Utility Networks

Cisco Provider Connectivity Assurance (PCA) architecture includes Assurance Sensors and Analytics, designed to provide not just raw data, but actionable and precise intelligence.

Assurance Sensors are designed to generate and collect high-quality service measurements over the transport network with synthetic traffic for continuous service assurance. The Assurance Sensors can also be used to collect telemetry or any time-series data from devices in the network, using the Sensor Collector.

Sensor SFPs are used in the use cases outlined in the paper. They are available in 1G or 10G form factor that act as any other SFP but have an internal FPGA that adds a measurement layer to its capabilities. They can be installed in-line with the traffic, as in the GOOSE use case, replacing another SFP, or in an unused port in any device (out of line mode) with any measurements sent via the host side.

Figure 9. PCA Granular Assurance capabilities



Accuracy: Ability to measure micro-second latency

Detection of short-lived spikes that could have an impact!

Sensor SFPs are managed by a platform that can be installed in any centralized location with computing resources. That centralized platform is used to configure the Assurance Sensors, the measurements, and to collect the data to be streamed to the Analytics platform.

While Assurance Sensors generate the right ‘high-quality’ metrics, the power lies in the Provider Connectivity Assurance analytics platform ability to transform this data into meaningful performance insights to efficiently run your day-to-day business. PCA Analytics, provides near real-time visibility by correlating performance data from the Assurance Sensors with contextual metadata to provide the insights needed for reporting, analysis and troubleshooting.

The ingested data is enriched with contextual information or metadata related to your own use case needs. For the utilities use cases outlined in this document, metadata fields can include, for example:

- Service: SCADA, goose, telepresence, and so on
- Substation related information: geo-coordinates, region, city, site, and so on
- Equipment related information: model, type, vendor, and so on
- Connectivity related information: fiber, leased line, and so on
- Other business or operational related information: site maintenance company, business criticality, and so on

This metadata is widely used in the system, for filtering, grouping or aggregation, correlation to find commonalities used for root cause analysis and troubleshooting. It also adds flexibility to suit

multiple reporting scenarios and personalized dashboards that can be used by different teams, for example, engineering, operations, and others.

The Provider Connectivity Assurance platform is available as a SaaS hosted in cloud or on-premises.

Benefits of PCA for Utility Networks

Cisco Provider Connectivity Assurance (PCA) delivers substantial value to utilities by transforming operations from reactive troubleshooting to proactive optimization. Key benefits include:

- **Maximize Reliability, Performance, and Operational Continuity:** Assures continuous reliability, optimal performance, and operational continuity for critical utilities networks. Through proactive network quality assurance, it minimizes service disruptions, protects vital infrastructure, and supports regulatory compliance, guaranteeing uninterrupted service delivery.
- **Real-time assurance platform for Critical OT services:** For critical Operational Technology (OT) services like SCADA, GOOSE, and Teleprotection, PCA provides the precise, real-time assurance needed to meet stringent high availability and ultra-low latency requirements, ensuring crucial SLAs are maintained
- **Exceptional Granular Visibility to detect microsecond issues:** PCA provides deep, near real-time visibility into network services with microsecond precision and millisecond sampling. This exceptional granularity, enabled by dedicated hardware within the Sensor SFP modules, ensures the detection of even transient issues or microevents that might otherwise go unnoticed, providing a complete and accurate picture of service health.
- **Minimize downtime with actionable Insights:** Advanced analytics enrich performance data with contextual metadata relevant to utility operations to facilitate correlation, reporting, analysis and troubleshooting. This enables proactive detection of potential issues and degradations, empowering operational teams to take timely corrective actions. This significantly reduces downtime, preventing service interruptions, and improving overall infrastructure efficiency and resilience.

Conclusion

Cisco Provider Connectivity Assurance (PCA) is a powerful solution for modern utilities networks, addressing the growing need for reliable, high-performance, and assured connectivity in an increasingly digitalized operational landscape.

The whitepaper highlights the unique capability of assurance to provide granular, real-time visibility into critical network parameters like latency, jitter and packet loss, with the precision needed for

critical networks. This level of detail is crucial for proactive fault detection and ensuring the strict performance requirements of essential OT services such as SCADA, GOOSE, and Teleprotection, ultimately safeguarding operational continuity and enabling compliance with rigorous industry standards.

By moving beyond the limitations of traditional monitoring tools, PCA offers a comprehensive assurance framework that transforms network management from reactive troubleshooting to proactive optimization.

Given the critical nature of utilities infrastructure and the significant repercussions of network disruptions, utilities benefit from real-time performance visibility and proactive assurance by integrating Cisco PCA as a foundational element of their network architecture.

Leveraging smart-pluggable sensor SFPs and advanced analytics platform, utilities can continuously verify they meet the required SLAs and ensure early detection of performance degradations across L2 or L3 networks.

By adopting PCA, utilities can significantly enhance their network resilience, improve operational efficiency, and ensure uninterrupted service delivery, ultimately protecting their critical assets and maintaining public trust.

Appendix A. Design Guide and Implementation for PCA

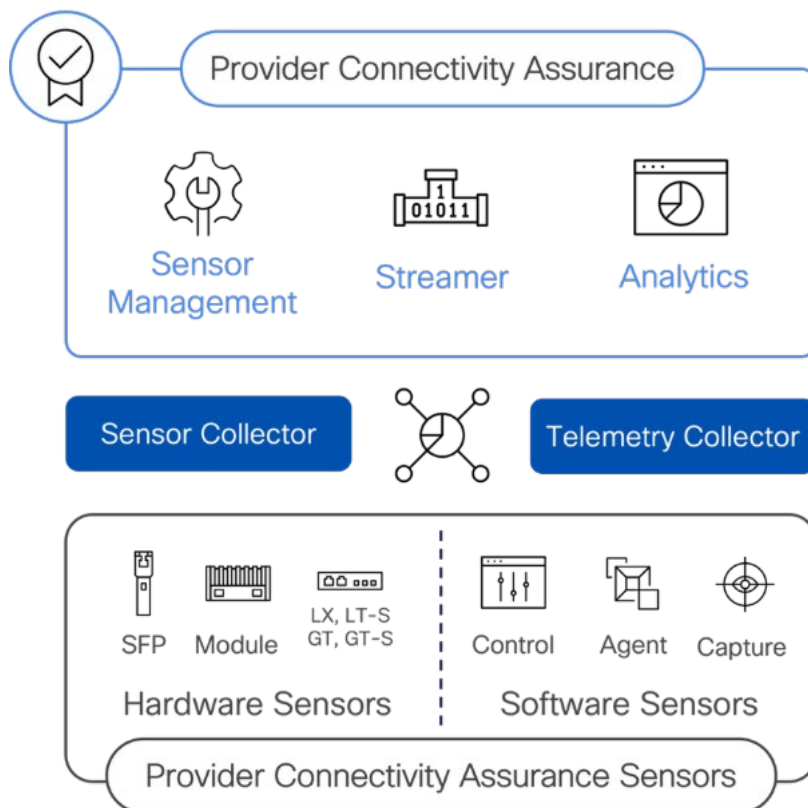
Provider Connectivity Assurance Solution

Components of the solution include:

- Sensor SFPs: they are 1G/10G hardware Sensors for ultra-accurate synthetic performance assurance supporting various testing capabilities: L3 TWAMP, L2 Y.1731, Service Activation Testing (RFC2544 and Y.1564), and granular per flow bandwidth metering
- PCA platform: typically installed in a centralized location and composed of various elements:
 - Sensor Control: configures, manages and collects data from Sensor SFP/Modules
 - PCA sensor management UI: part of the platform, configures sensors, creates and manages performance sessions and collects and processes KPIs
 - Sensor Collector: Acts as a proxy between sensors and analytics to facilitate split domains when sensors are on-prem and analytics is deployed in the Cloud, or in a full on-prem solution as a gateway function.

- Other software (docker container) Sensor Agents not included in this design, but available in the platform: Actuate TWAMP/ICMP Echo, Telemetry Collector, Transfer (DNS, http, port), Trace (traceroute), TCP Throughput (RFC 6349)
- Analytics: contextual performance assurance for advanced visualization, reporting and analysis. It processes the data received from the Collector that is enriched with metadata.

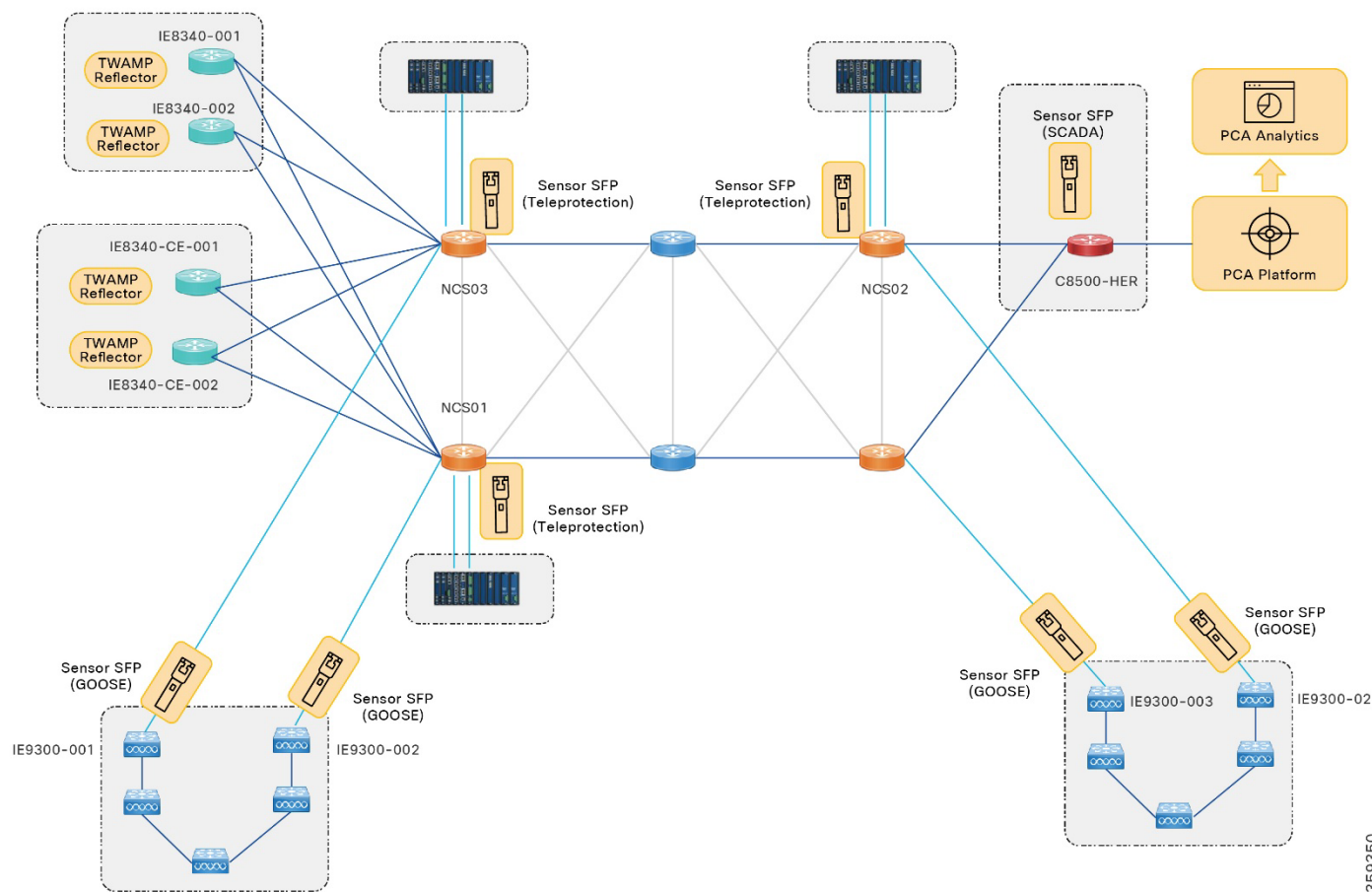
Figure 10. Provider Connectivity Assurance solution



Design

The figure that follows represents how the different components of the PCA solution are deployed in a utilities network so they can cover the three use cases described in this document.

Figure 12. Deployment of Provider Connectivity Assurance in a utility network



The Sensor SFPs are installed in different parts of the network, either in a trunk port in-line with the traffic, or in an unused port of the routers (mode out-of-line):

- For the SCADA use case, the Sensor SFP is in mode out-of-line in a Headend router
- For the GOOSE use case, the Sensor SFPs are in-line in a trunk port connecting the substation switch with the router of the WAN network (NCS)
- For the Telepresence use case, the Sensor SFPs are in mode out-of-line in a port of the NCS routers that connect the SEL ICON with the WAN

The platform is typically installed in a centralized location where computing is available, in this case in the Control Center. Analytics can be installed on-premises or in the cloud depending on your preference.

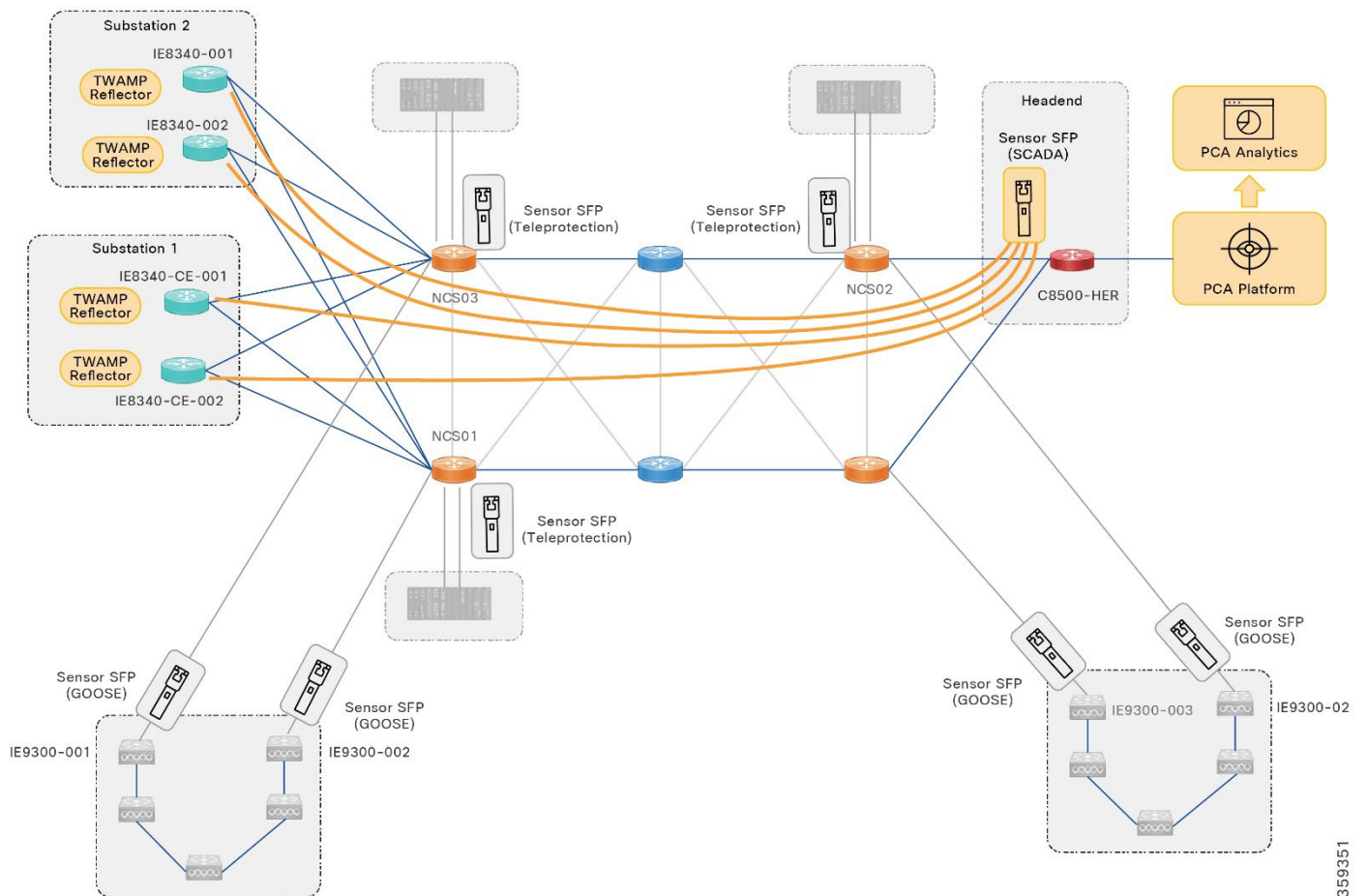
As part of the solution, we are activating and making use of the TWAMP reflection capabilities of the Routers when appropriate.

SCADA use case:

Layer-3 TWAMP performance sessions are deployed in a hub-and-spoke topology from the Sensor SFPs installed in the Headend router towards the TWAMP reflectors in the SCADA routers of each of the substations.

The TWAMP sessions can be configured to travel with the SCADA traffic using the same VLAN and DSCP or TOS marking.

Figure 13. TWAMP sessions for SCADA use case



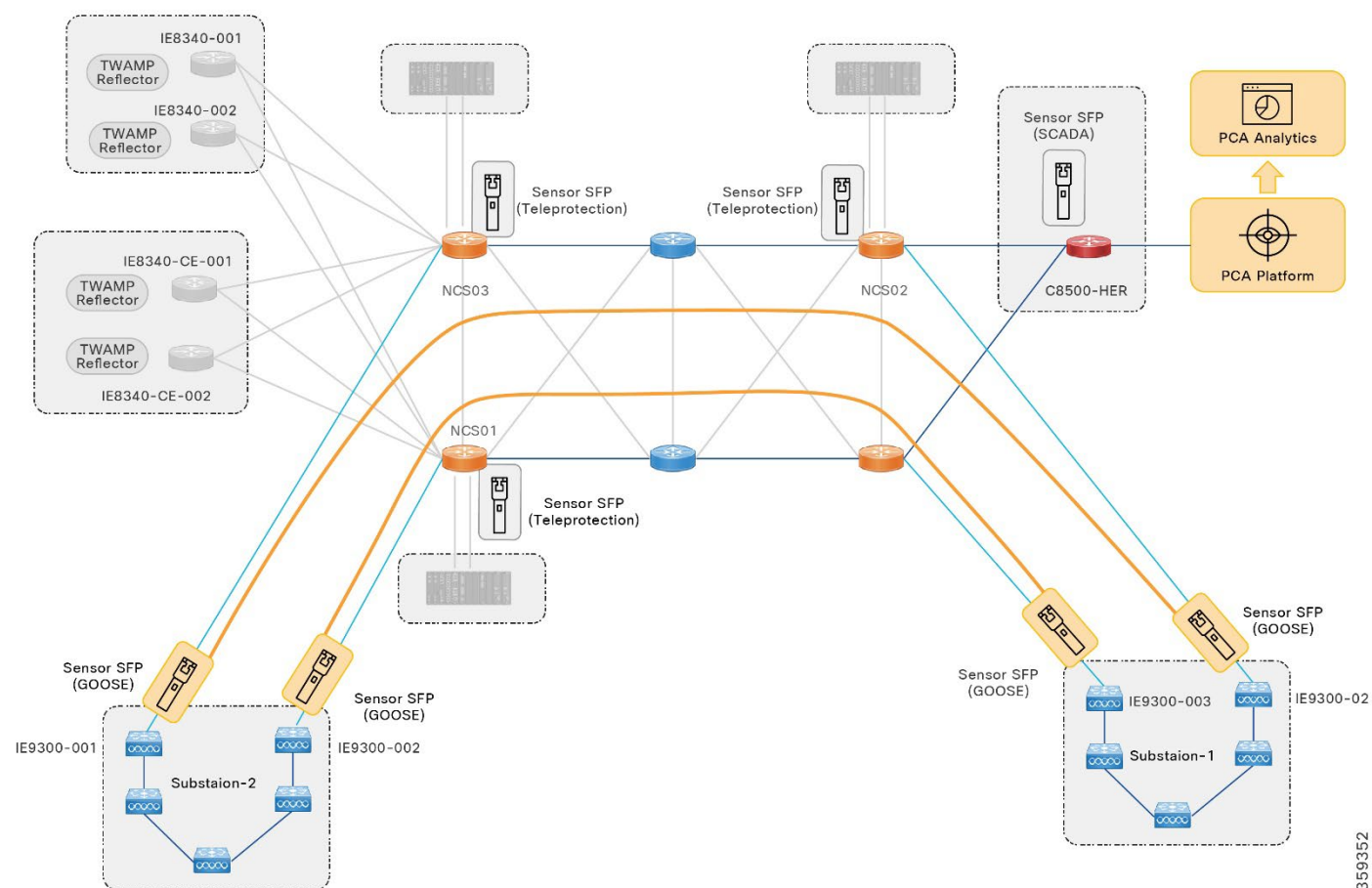
359351

GOOSE use case:

Layer-2 ETH-DM Y.1731 sessions are configured to monitor the connectivity of L2VPNs between substations providing latency, jitter and packet loss KPIs among others.

The Sensor SFPs are placed in a trunk port in-line with the traffic, so not only we can get synthetic measurement packets, but we can also use the throughput per-flow measurement feature available in the Sensor SFPs to provide high-granular throughput information of those links.

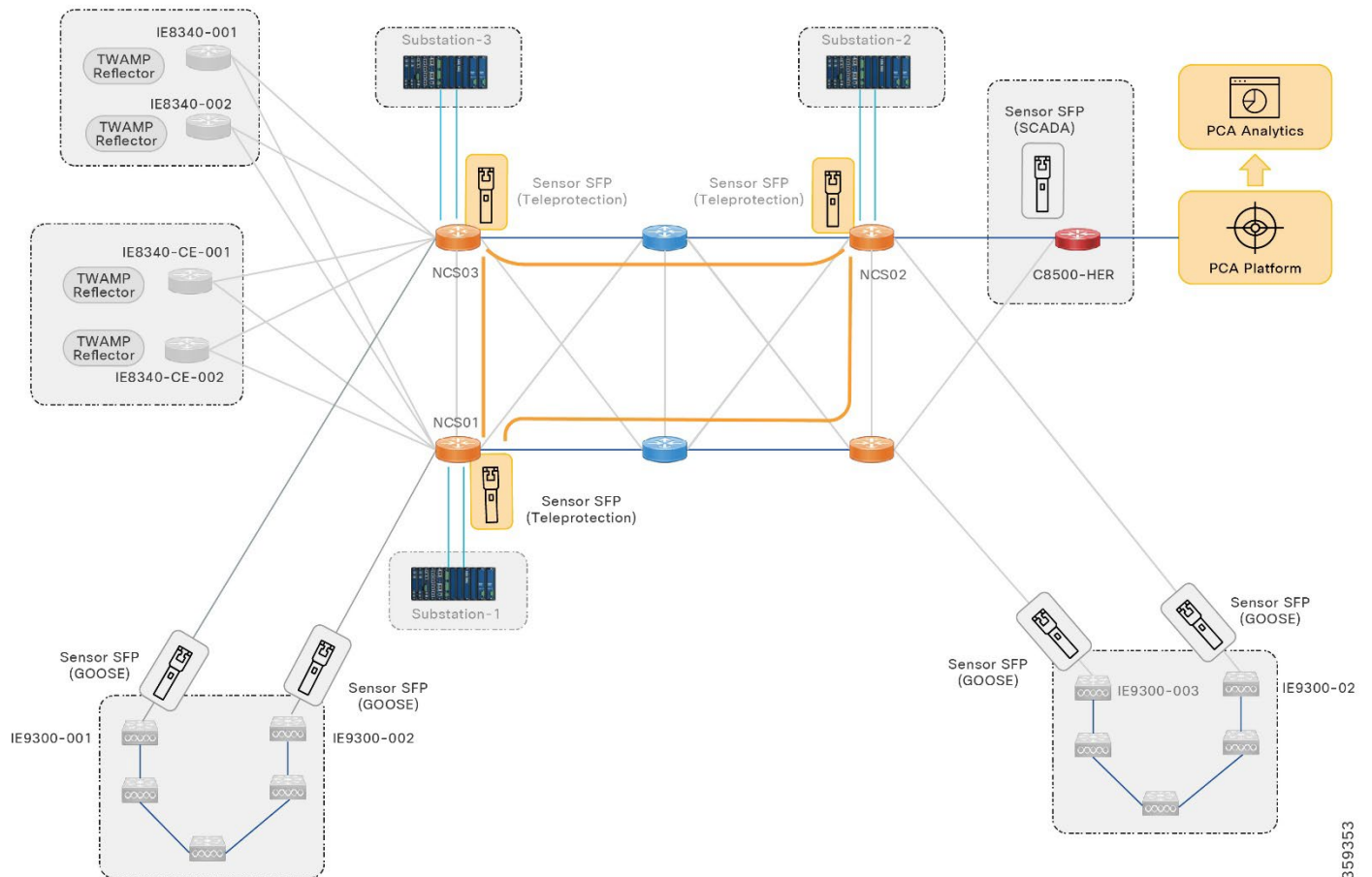
Figure 14. ETH-OAM sessions for GOOSE use case



Teleprotection use case:

We are also using Layer-2 ETH-DM sessions to monitor hop-by-hop, the Layer-2 Ring used by the Teleprotection traffic.

Figure 15. ETH-OAM sessions for Teleprotection use case



359353

Provider Connectivity Assurance Configurations

Sensor SFPs typically uses a management IP address to connect with Sensor Control as shown in Figure 16.

Figure 16: Sensor SFP Management interface configuration

The screenshot displays the Cisco Provider Connectivity Assurance Sensor Control web interface. The top navigation bar includes the Cisco logo, the title "Provider Connectivity Assurance Sensor Control", a "Remote Device" dropdown set to "None", a timestamp "2025-08-07 16:50:11+00:00", user status "MIN MAJ CRIT", and the role "pcaadmin : Sensor_Control". A "Help Center" link is also present. The main navigation menu includes Home, Remote Devices, Discovery, Virtual Connection, Port, Traffic, System (selected), Loopback, SOAM, SAT, Show, and Debug. The sub-navigation menu includes Configuration (selected), Alarm, Agent, Maintenance, Session, ACL, and OS Service. The "Interface" tab is active, showing the "IE9300-003-intf0 interface settings". The configuration form includes: "State" (checked "Enable"), "Interface name" (IE9300-003-intf0), "Interface type" (VLAN), "On port" (IE9300-003-NNI), "VLAN settings" (VLAN ID: 302, Ethertype: C-VLAN, VLAN priority: 0), "IPv4" settings (Automatic IP (DHCP) selected, Use DHCP Unicast Mode unchecked), "Manual configuration" (selected), "IP address" (17.0.0.4), "Network mask" (255.255.255.0), "Default gateway" (17.0.0.2), "IPv6 settings" (IPv6 enable unchecked), and "Apply" and "Delete" buttons.

From Sensor Control, one or more discovery instances are configured to discover the Sensor SFPs deployed in the network. Discovery can be done per specific IP address, subnet, or even at layer 2.

Figure 17. Example of unicast discovery instance in Sensor Control

The screenshot displays the Cisco Provider Connectivity Assurance Sensor Control web interface. The top navigation bar includes the Cisco logo, the title "Provider Connectivity Assurance Sensor Control", a "Remote Device" dropdown set to "None", a timestamp "2025-08-07 16:48:42+00:00", user status "MIN MAJ CRIT", and the role "pcaadmin : Sensor_Control". A "Help Center" link is also present. The main navigation menu includes Home, Remote Devices, Discovery (selected), Virtual Connection, Port, Traffic, System, Loopback, SOAM, SAT, Show, and Debug. The sub-navigation menu includes Configuration (selected) and Inventory. The "Discovery" tab is active, showing the "Remote Device discovery 14-0-0-2 configuration". The configuration form includes: "Name" (Discovery-14-0-0-2), "Enable" (checked), "Method" (IPAD), "Rate" (3 secs), "Hop limit" (255), "Timeout (sec)" (3), "Destination IP address" (14.0.0.2), "Type" (UNICAST), and "Apply", "Reset", and "Delete" buttons.

Figure 18: Inventory of discovered Sensor SFPs by Sensor Control

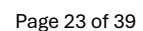



Figure 19: List of managed devices by Sensor Control


Provider Connectivity Assurance Sensor Control

Remote Device :

None

2025-08-07 16:42:47+00:00
MIN MAJ CRIT
pcaadmin : Sensor_Control
Help Center

[Home](#)
[Remote Devices](#)
[Discovery](#)
[Virtual Connection](#)
[Port](#)
[Traffic](#)
[System](#)
[Loopback](#)
[SOAM](#)
[SAT](#)
[Show](#)
[Debug](#)

[Configuration](#)
[Security Key Management Feature Suites Management](#)
[Export/Import](#)
[Import Status](#)

Filter:

Device

Search

Remote Devices configuration

Inst.	Device	Serial Number	MAC Address	Linked	State	Admin State	Active Feature	Current Feature Suite	Update Status
1	C8500-HER	P810-0753	00:15:AD:7F:98:3C	Yes	Managed	IS	PMON 20.11	24.11_15982	Idle
3	IE9300-003	P809-6753	00:15:AD:7F:8B:5E	Yes	Managed	IS	PMON 20.11	24.11_15982	Idle
4	IE9300-001	P809-6382	00:15:AD:7F:88:78	Yes	Managed	IS	PMON 20.11	24.11_15982	Idle
7	IE9300-002	P801-1885	00:15:AD:57:85:DE	Yes	Managed	IS	PMON 20.11	24.11_15982	Completed
9	IE4000-002	P801-2045	00:15:AD:57:87:1E	Yes	Managed	IS	PMON 20.11	24.11_15982	Completed
10	IE5K-002-PRP	P801-1852	00:15:AD:57:85:9C	Yes	Managed	IS	PMON 20.11	24.11_15982	Completed
11	IE5K-005-PRP	P801-1792	00:15:AD:57:85:24	Yes	Managed	IS	PMON 20.11	24.11_15982	Completed
12	NCS01-TEL	P810-3015	00:15:AD:7F:A9:20	Yes	Managed	IS	PMON 23.12	24.11_15982	Completed
13	NCS02-TEL	P810-2998	00:15:AD:7F:A8:FE	Yes	Managed	IS	PMON 23.12	24.11_15982	Completed
14	NCS03-TEL	AAO2831006U	00:15:AD:81:0D:4E	Yes	Managed	IS	PMON 23.12	24.11_15982	Completed

From Sensor Control, it is possible then to create or change the configuration on the Sensor SFPs for any testing we want to perform.

Configuration of TWAMP Session

For the SCADA use case, we use the Sensor SFP as TWAMP sender. These are the configuration steps. Those steps can be replicated for any other TWAMP session. The process can be automated using scripting, APIs or using automation orchestration platforms like Cisco Network Service Orchestrator (NSO), or Cisco Network Controller (CNC).

To configure, complete the steps below.

1. Create a layer-3 sub-interface in the Sensor SFP to be used as Sender Virtual Connection Endpoint ((VCE).

Figure 20. Layer-3 VCE TWAMP Sender sub-interface

The screenshot shows the 'VCE configuration' page in a network management interface. The page has a top navigation bar with tabs: Home, Remote Devices, Discovery, Virtual Connection (selected), Port, Traffic, System, Loopback, SOAM, SAT, Show, and Debug. Below the navigation bar are three main sections: VCA VLAN, VCE (selected), and VCA. Under the VCE section, there are two sub-sections: Configuration and Statistics. The Configuration section contains a form with the following fields and values:

- VCE Name: VCE-C8500-HER
- Remote Device Name: C8500-HER
- Type: Customer
- Component ID: 0
- TPID: 0x8100
- Frame Type: untagged
- TP A: External
- TP A Port: UNI
- TP A VID: 0
- CoS Mapping: TP A PCP Mapping: 8POD-8POD
- Relay Action: none
- TP Z: External
- TP Z Port: NNI
- TP Z VID: ---
- TP Z PCP Mapping: 8POD-8POD
- L3 Domain State: ☒ Enable
- TP A L3 State: ☒ Enable
- TP Z L3 State: ☒ Enable
- IPv4: ☒ Manual configuration (selected), ☐ Automatic IP (DHCP), ☐ Use DHCP route information
- IP address: 13.0.0.3
- Network mask: 24
- Default gateway: 13.0.0.1
- IPv6: ☐ IPv6 enable
- IPv6 address: ::
- Prefix Length: 0
- Default gateway: ::

At the bottom of the form are two buttons: 'Apply' and 'Delete'.

One Sensor SFP can have multiple Layer-2 or Layer-3 VCEs. The VCEs can be VLAN tagged, so the measurements generated using the VCEs are encapsulated using that VLAN.

Figure 21. List of all VCEs in Sensor Control (layer-2 and layer-3)

The screenshot shows the Cisco Provider Connectivity Assurance Sensor Control web interface. The top navigation bar includes the Cisco logo, the title "Provider Connectivity Assurance Sensor Control", and a "Remote Device" dropdown set to "None". Below the navigation bar, there are tabs for "Home", "Remote Devices", "Discovery", "Virtual Connection" (selected), "Port", "Traffic", "System", "Loopback", "SOAM", "SAT", "Show", and "Debug". Under the "Virtual Connection" tab, there are sub-tabs for "VCA VLAN", "VCE" (selected), and "VCA". The "VCE" sub-tab has further options for "Configuration" and "Statistics". The main content area displays a table of VCE configurations with a search filter and a search button.

VCE Name	Remote Device Name	TPID	TP A	TP A VID	TP Z	TP Z VID	DHCP	IP Address	Gateway	ComponentId
VCE-C8500-HER	C8500-HER	0x8100	UNI	---	NNI	---	Disabled	13.0.0.3 / 24	13.0.0.1	1
VCE-L2-IE9300-003	IE9300-003	0x8100	UNI	11	NNI	11	Disabled	---	---	2
VCE-L2-IE4000-002	IE4000-002	0x8100	UNI	11	NNI	11	Disabled	---	---	3
VCE-L2-IESK-005-PRP	IESK-005-PRP	0x8100	UNI	11	NNI	11	Disabled	---	---	4
VCE-L2-NCS01-100-TEL	NCS01-TEL	0x8100	UNI	100	NNI	100	Disabled	---	---	5
VCE-L2-NCS01-300-TEL	NCS01-TEL	0x8100	UNI	300	NNI	300	Disabled	---	---	5
VCE-L2-NCS02-200-TEL	NCS02-TEL	0x8100	UNI	200	NNI	200	Disabled	---	---	6

At the bottom of the table, it shows "[1-7] of 7" and pagination controls: "<< < 1 2 3 4 > >>".

2. Enable the TWAMP reflector in the substation SCADA IR router using this configuration:

```
ip sla responder twamp
```

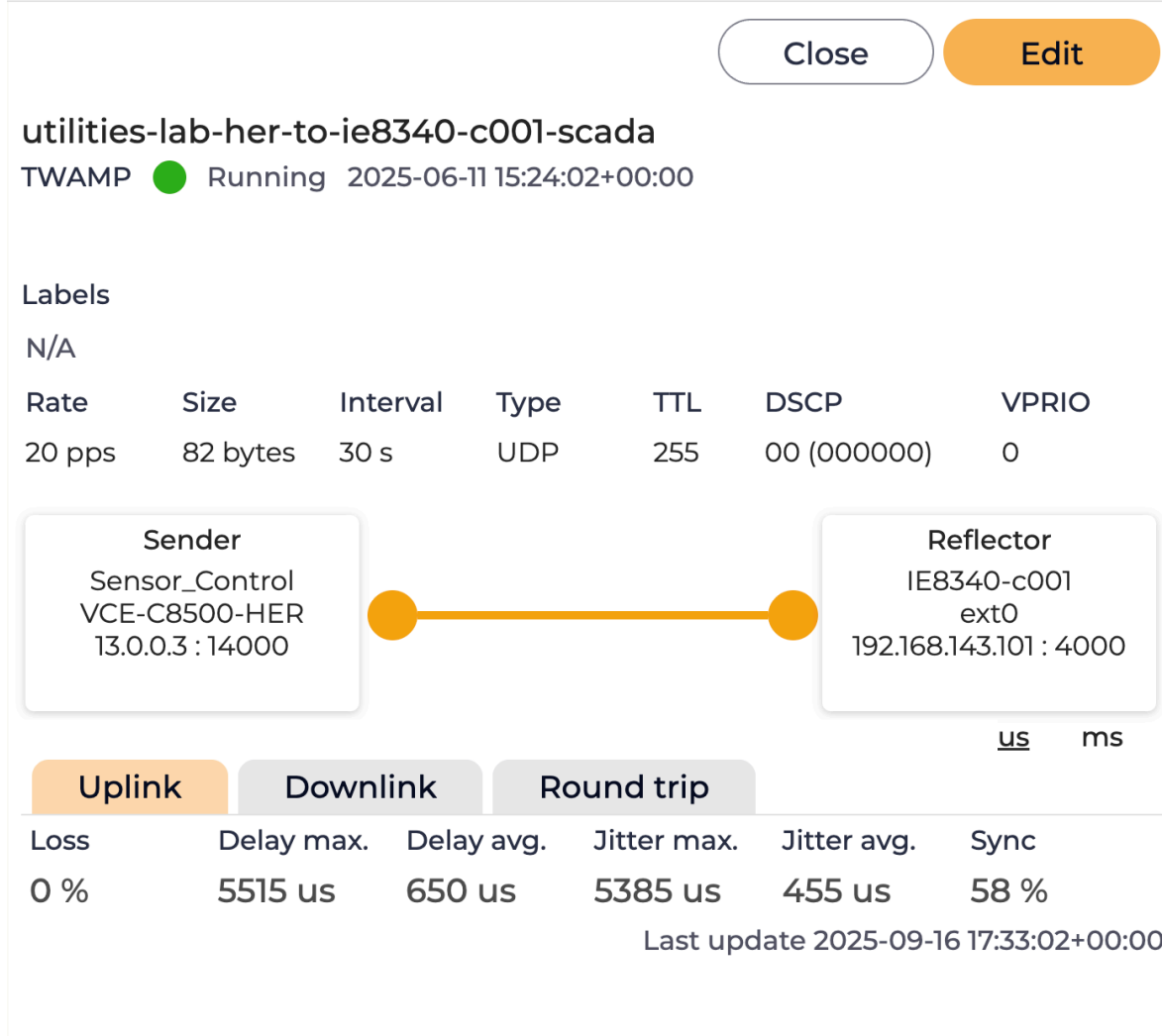
```
ip sla responder twamp-light test-session 1 local-ip 192.168.143.101
```

```
local-port 4000 remote-ip 13.0.0.3 remote-port any timeout 604800
```

3. In the sensor management UI create a TWAMP Session using the VCE as TWAMP Sender and the Scada router as TWAMP Reflector. The same sender interface can be used to reach multiple reflectors.

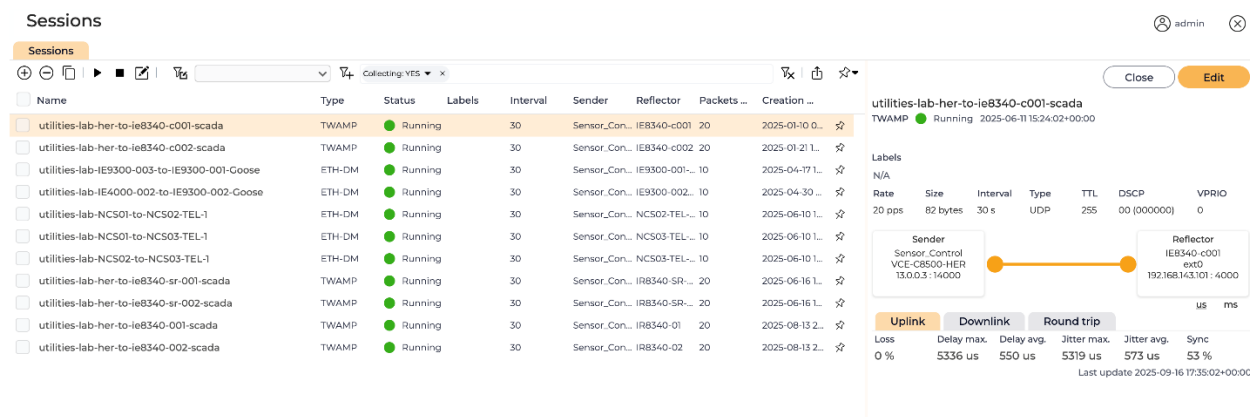
For each TWAMP session, you can define the number of measurement packets per second, size of the packets, collection interval (down to 1 second), DSCP marking, or VLAN priority.

Figure 22: TWAMP Session parameters



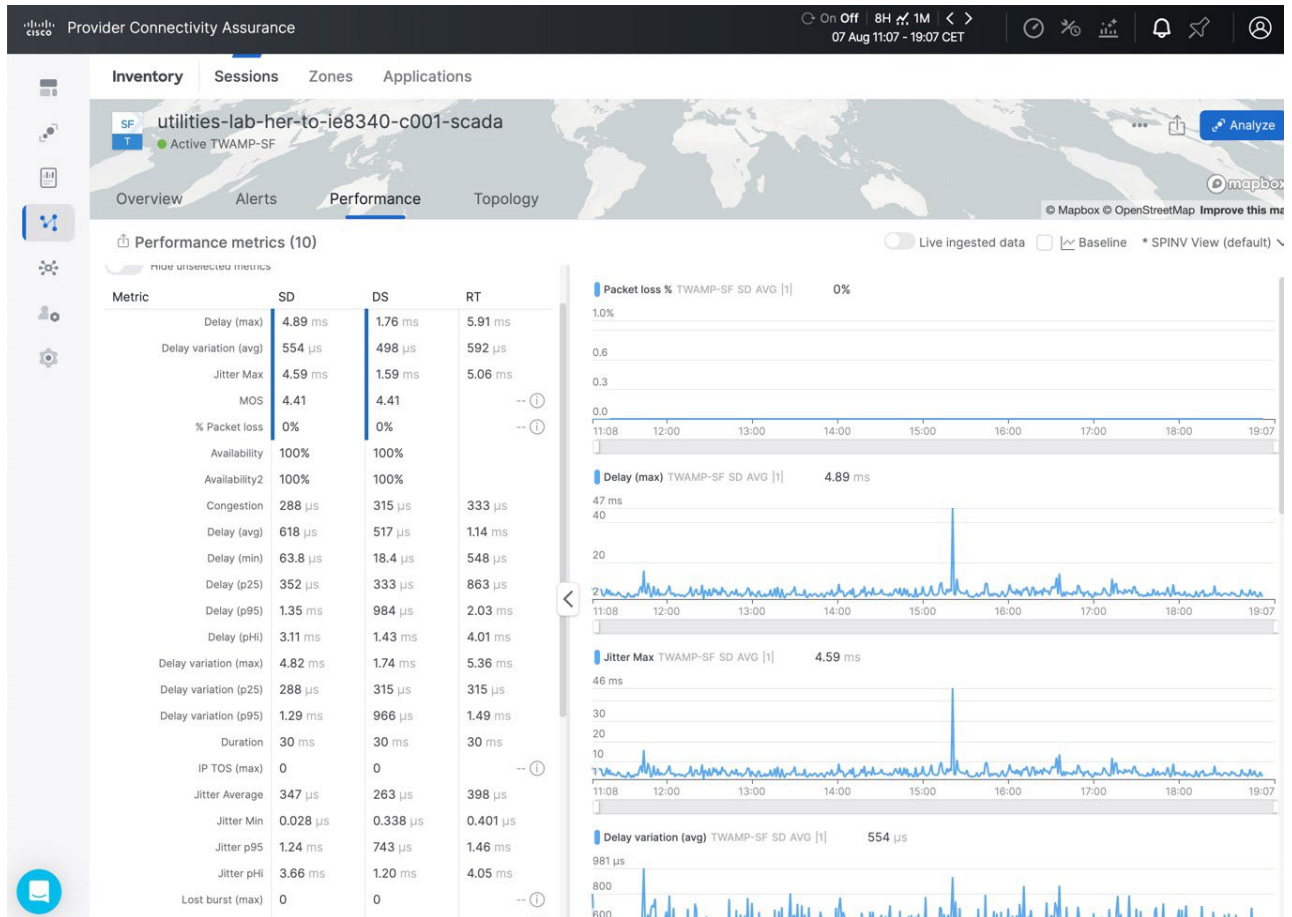
4. Start the TWAMP Session and verify that is up and Running.

Figure 23: SCADA TWAMP session running



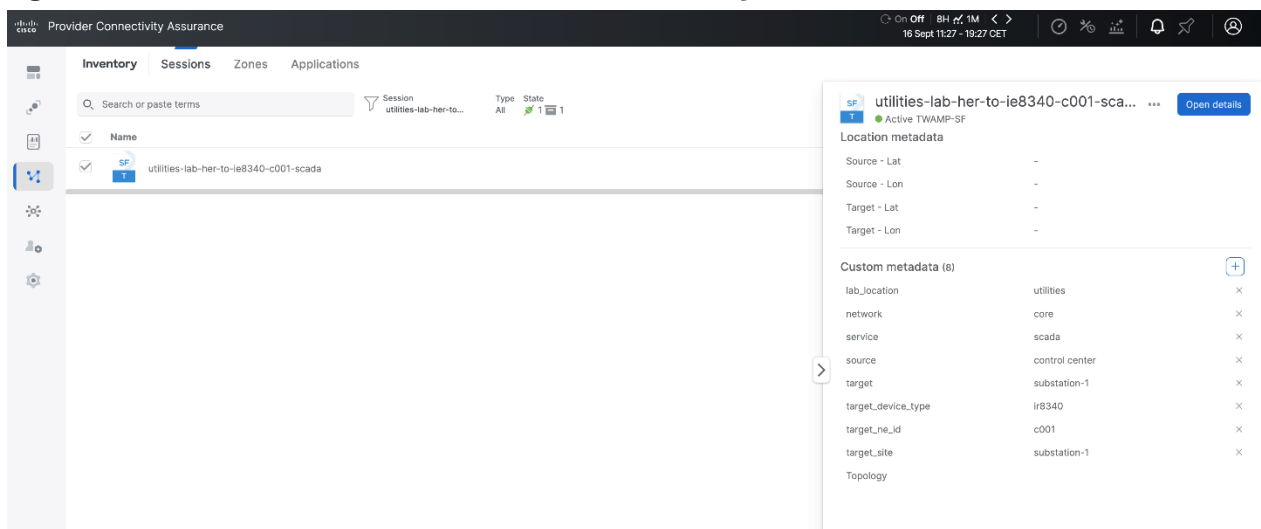
- Once the session is running, the KPIs that is generating will be automatically streamed to PCA Analytics using the Sensor Collector. The session will appear in the Analytics inventory.

Figure 24: SCADA TWAMP session KPIs in Analytics



- Add the appropriate metadata to the TWAMP session, so the session automatically will be added to any relevant dashboards, and can be filtered, correlated, and so on.

Figure 25: SCADA TWAMP session metadata in Analytics



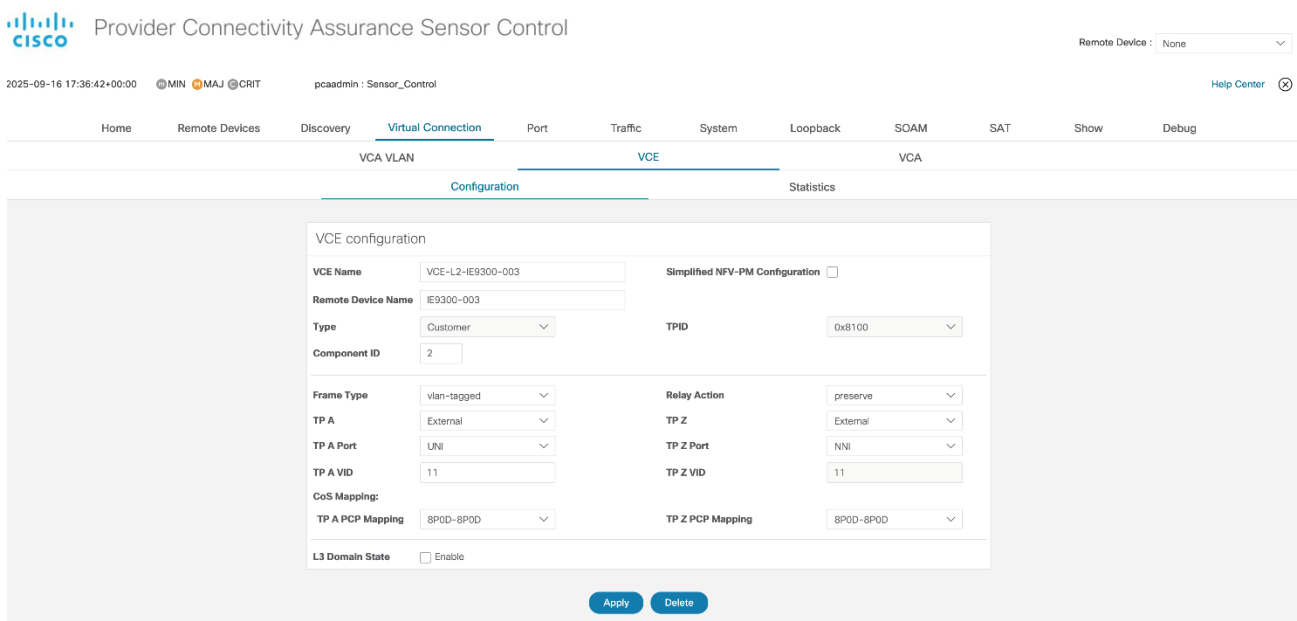
Configuration of Y.1731 Session

Layer-2 service assurance is being used for the GOOSE and Teleprotection use cases where the Sender and Reflectors are Sensor SFPs.

The configuration steps are similar as the ones used for TWAMP:

- 1. Create a layer-2 sub-interface in the Sensor SFP to be used as Sender (VCE or Virtual Connection Endpoint), with the correct VLAN id.

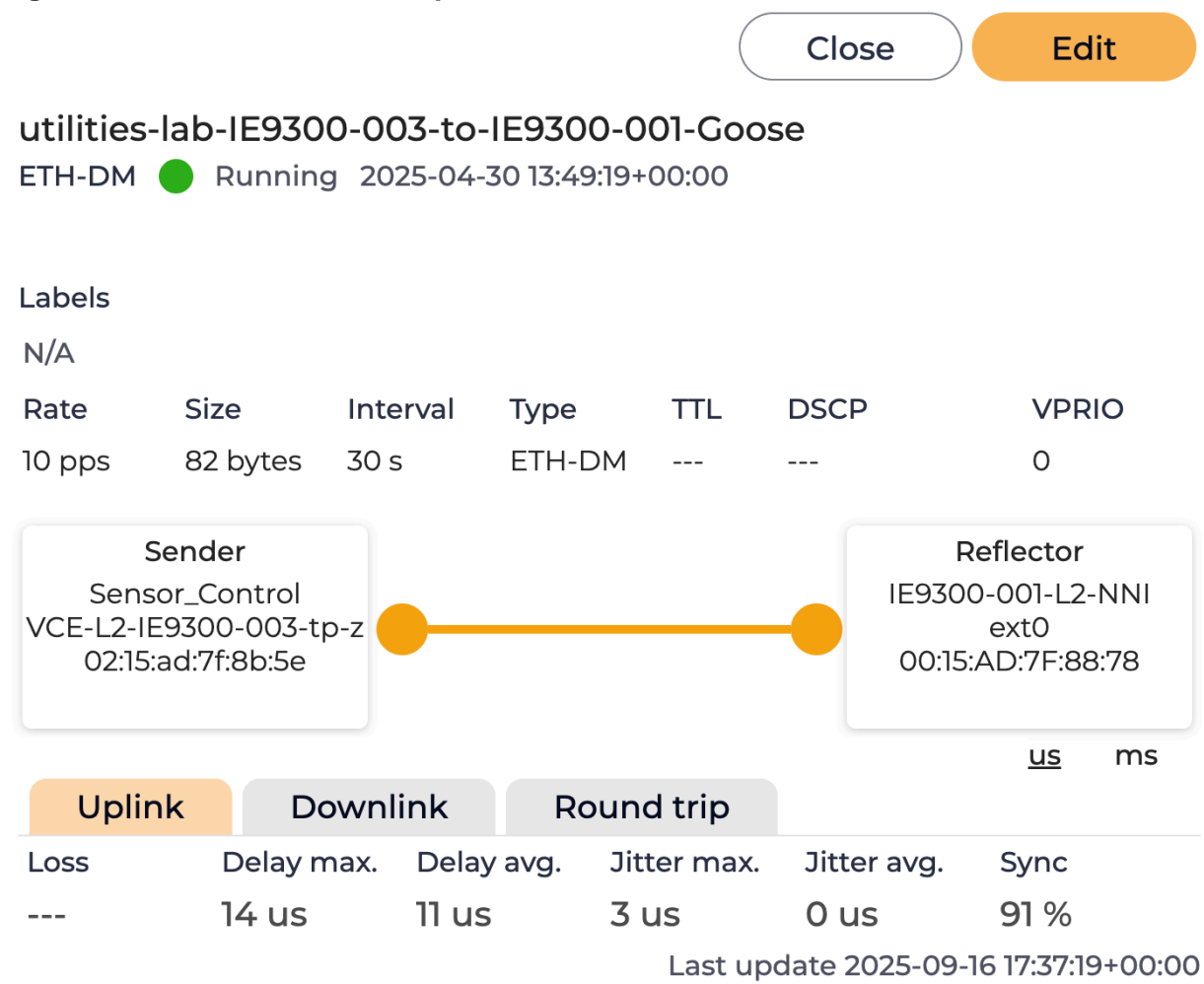
Figure 26. Layer-2 VCE Sender sub-interface



2. In PCA sensor management, create an ETH-DM type of session using the VCE as a Sender and the other Sensor SFP as a Reflector. Make sure you use the 'VCE-tp-z' port for the sender and the NNI port for the reflector.

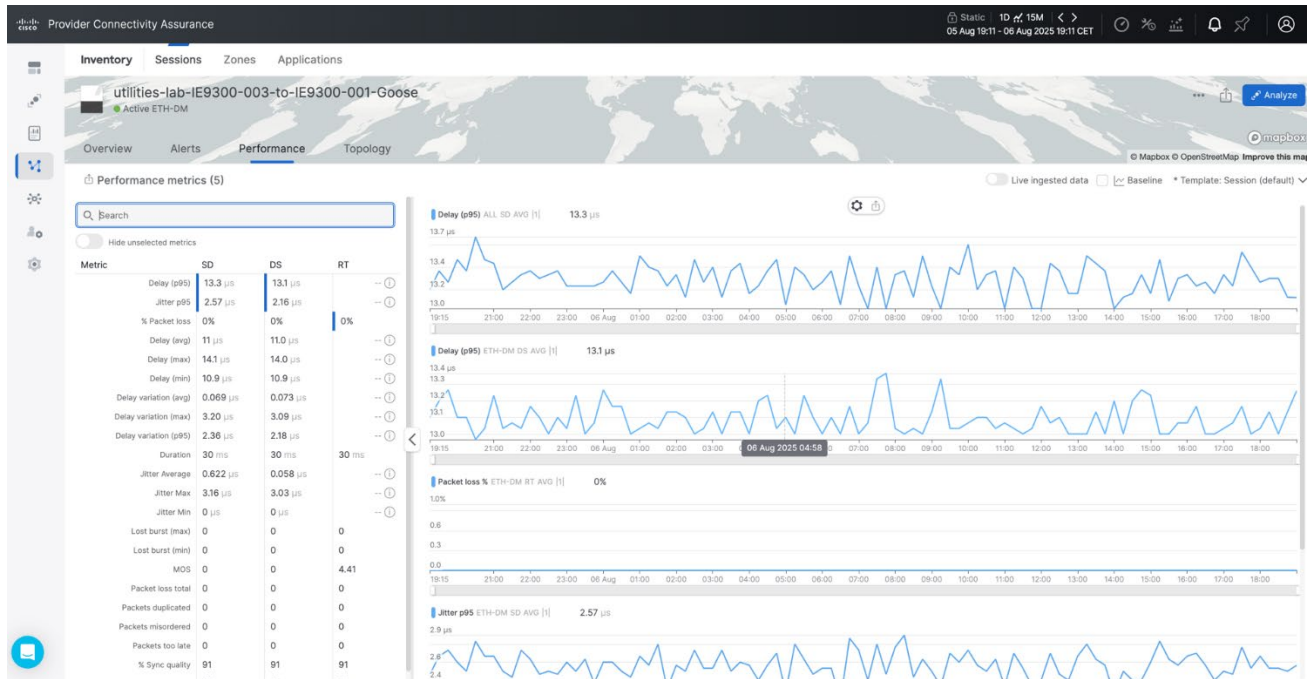
For each ETH-DM session, you can define the number of packets per second, size of the packets, collection interval (down to 1 second), and VLAN priority.

Figure 27. L2 ETH-DM Session parameters



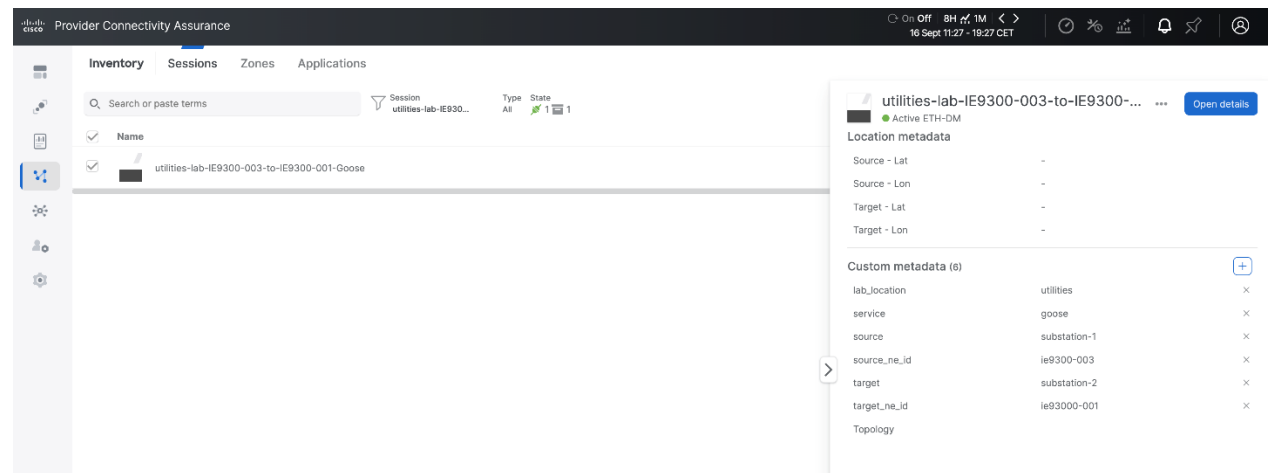
3. Start the ETH-DM Session and verify that is up and Running.
4. Once the session is running, the KPIs that is generating will be automatically sent to PCA Analytics by the Sensor Collector. The session will be automatically streamed to PCA using the Sensor Collector. The session will appear in the Analytics inventory. Note the richness of the KPIs generated for that layer-2 assurance session.

Figure 28. GOOSE L2 ETH-DM session KPIs in Analytics



Add the appropriate metadata to the TWAMP session, so the session automatically will be added to any relevant dashboards, and can be filtered, correlated, and so on.

Figure 29. GOOSE L2 ETH-DM session Metadata in Analytics



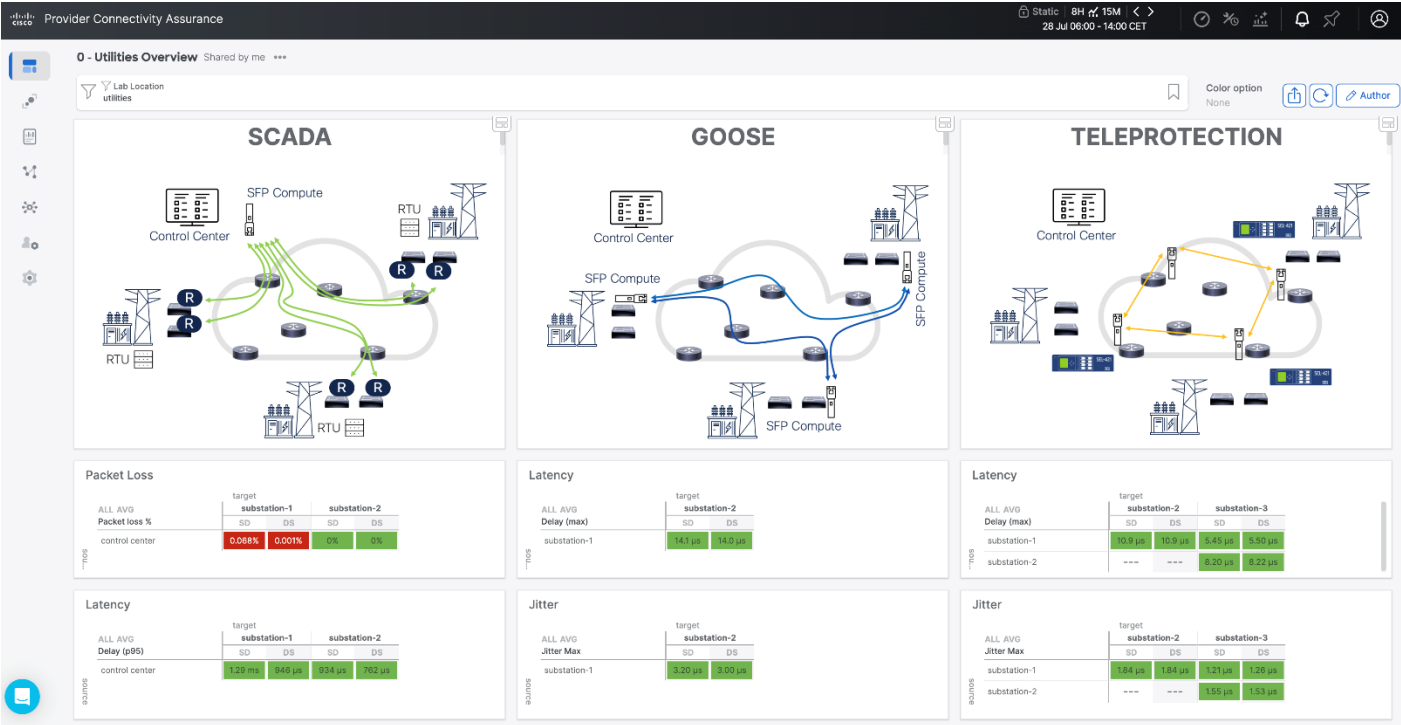
Provider Connectivity Assurance Analytics

Analytics offers great flexibility in the creation and customization of dashboards where users can visualize KPIs and performance data. Users can tailor visualization and reporting to their specific operational needs. In the context of the use cases described in this document, we suggest starting with generic dashboards for each of the use cases and create drill-down dashboards or sections for

more details. Any user or group of users can create their own dashboards to accommodate any specific needs that they might have.

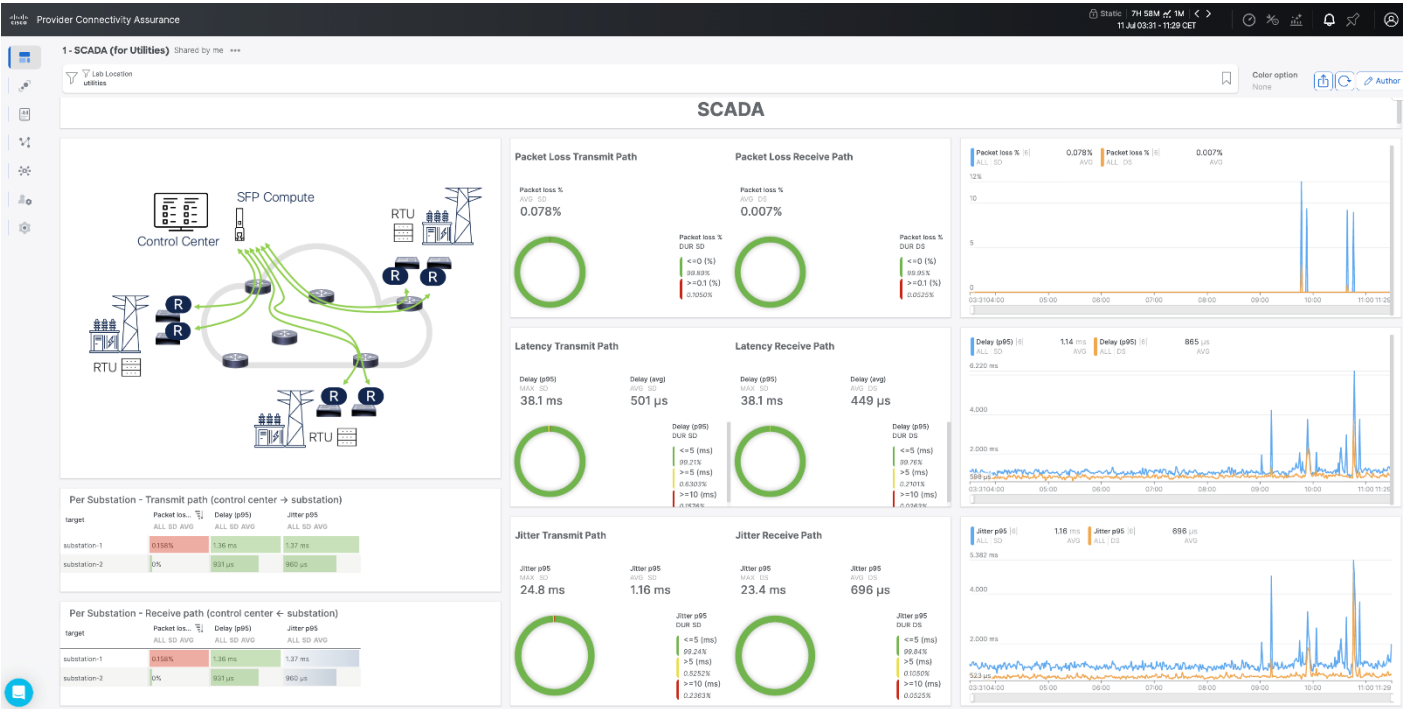
This is our suggested initial global dashboard. It offers an overall view of the performance of the three use cases – SCADA, GOOSE, Teleprotection – based on latency, jitter and packet loss. From that main page, it is possible to navigate to each of the individual use cases for more details.

Figure 30. PCA Analytics for utilities: main dashboard example



SCADA main dashboard

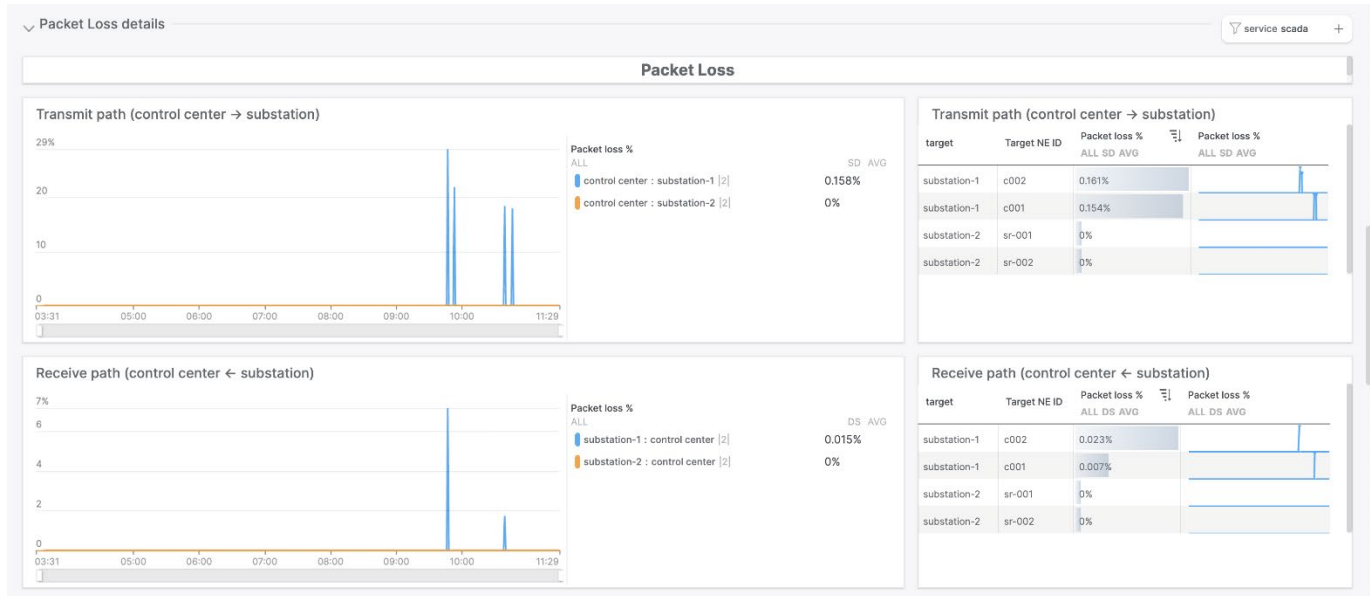
Figure 31. PCA Analytics for utilities: SCADA dashboard example



Drill-down into the sections for the different metrics.

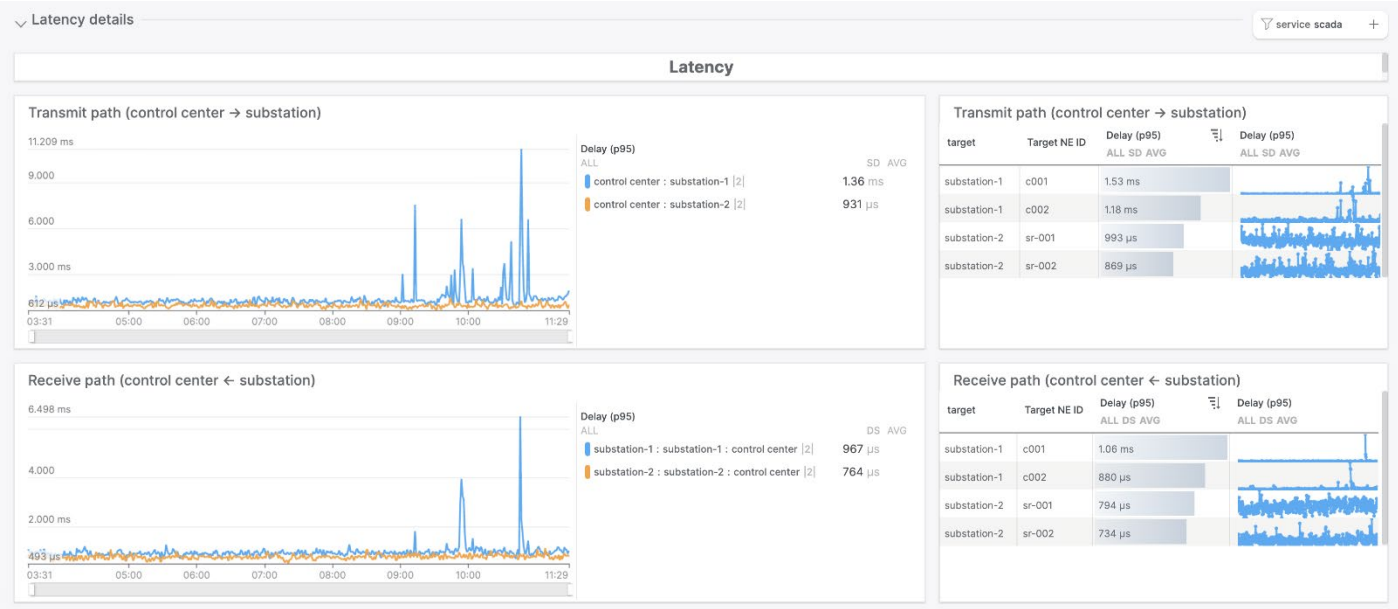
For Packet Loss:

Figure 32. PCA Analytics for utilities: SCADA Packet Loss drill down example



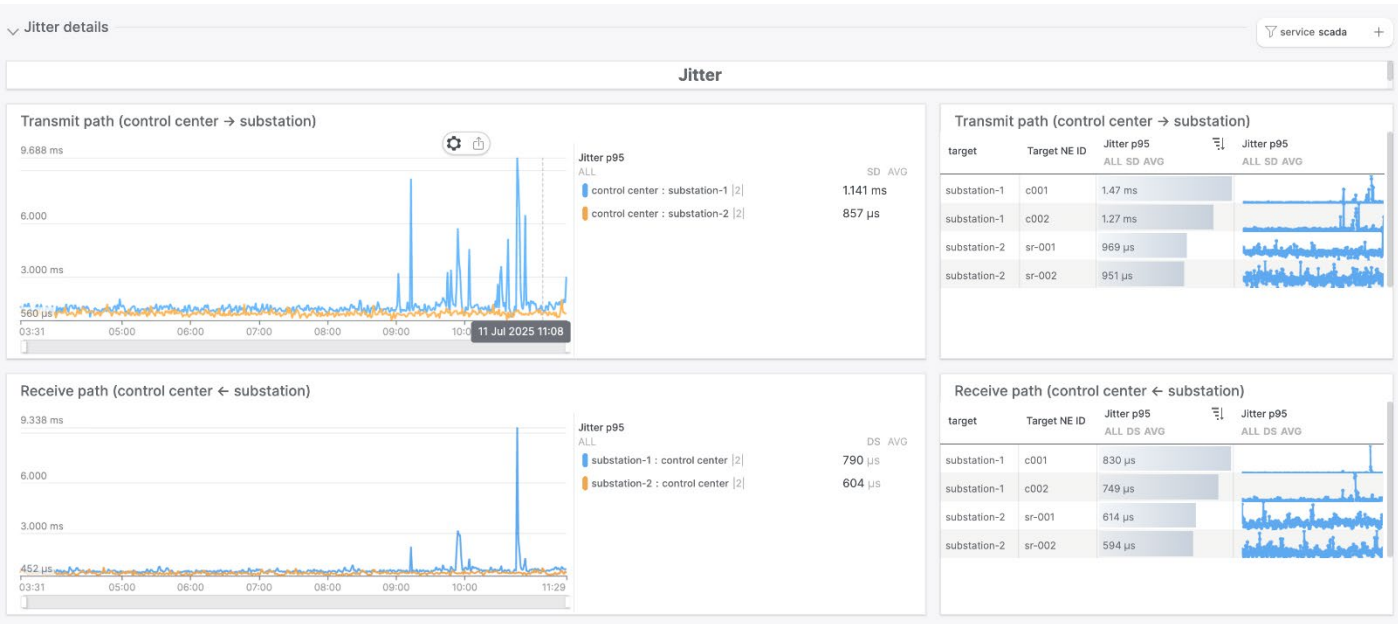
For Latency:

Figure 33. PCA Analytics for utilities: SCADA Latency drill down example



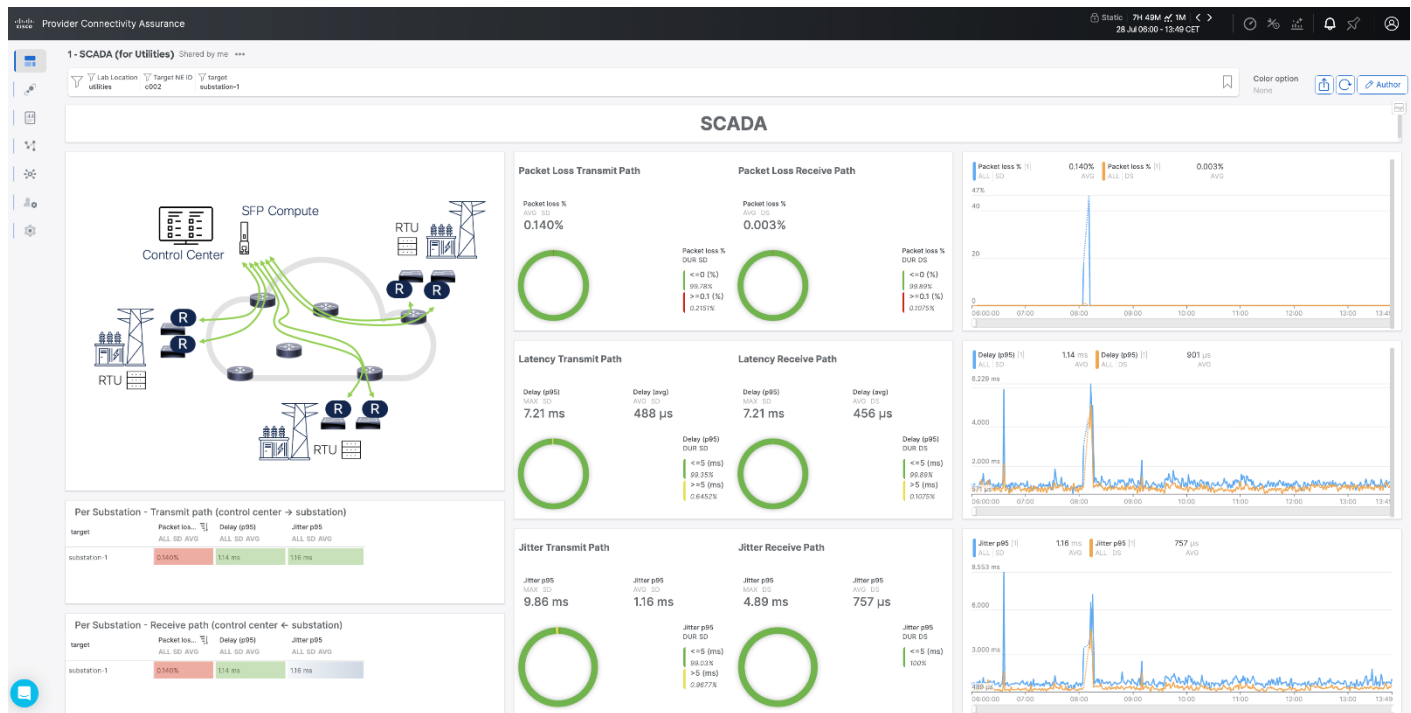
For Jitter:

Figure 34: PCA Analytics for utilities: SCADA Jitter drill down example



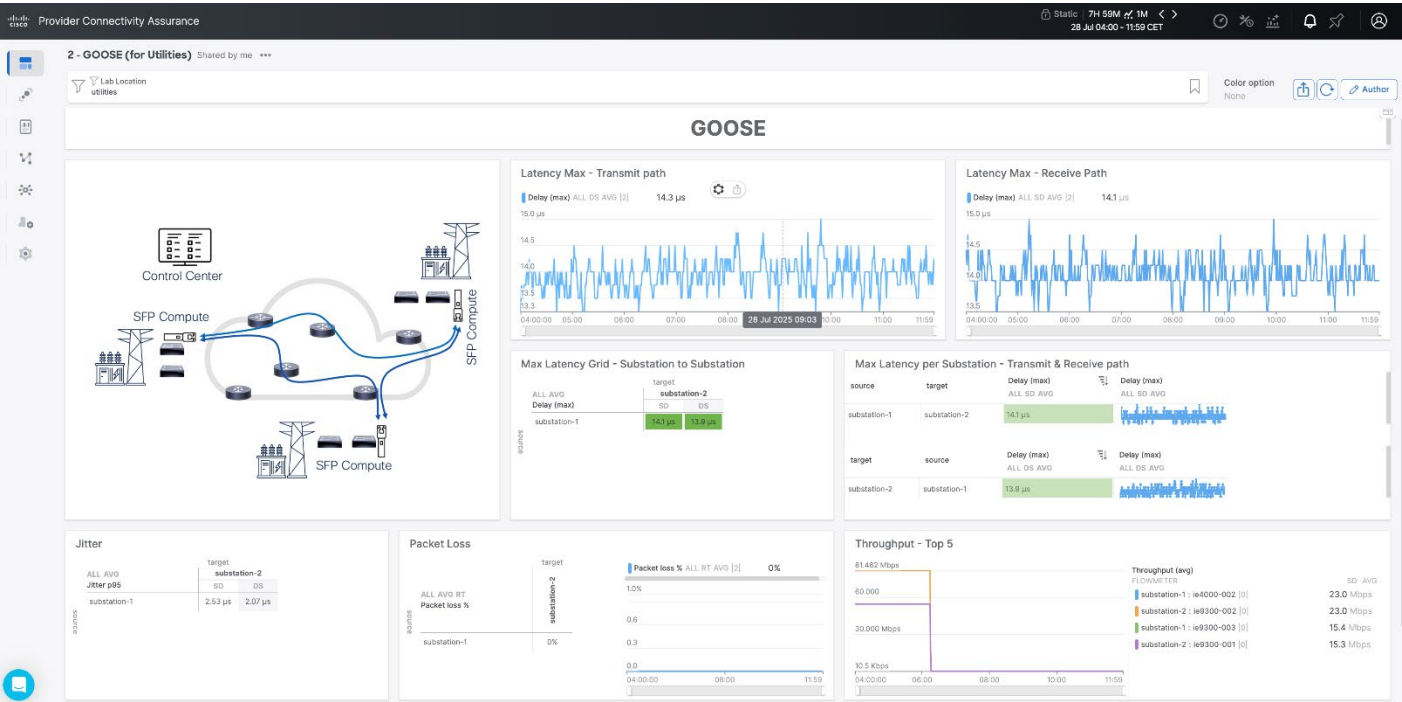
It is possible to directly select specific metadata from the tables for dynamically update the dashboards. As an example, in the figure below, we are selecting metadata target=substation-1, NE-ID=C002 that shows packet loss and latency issues.

Figure 35. Provider Connectivity Assurance for utilities: SCADA metadata filtering for drill down example



GOOSE main dashboard:

Figure 36. Provider Connectivity Assurance for utilities: GOOSE dashboard

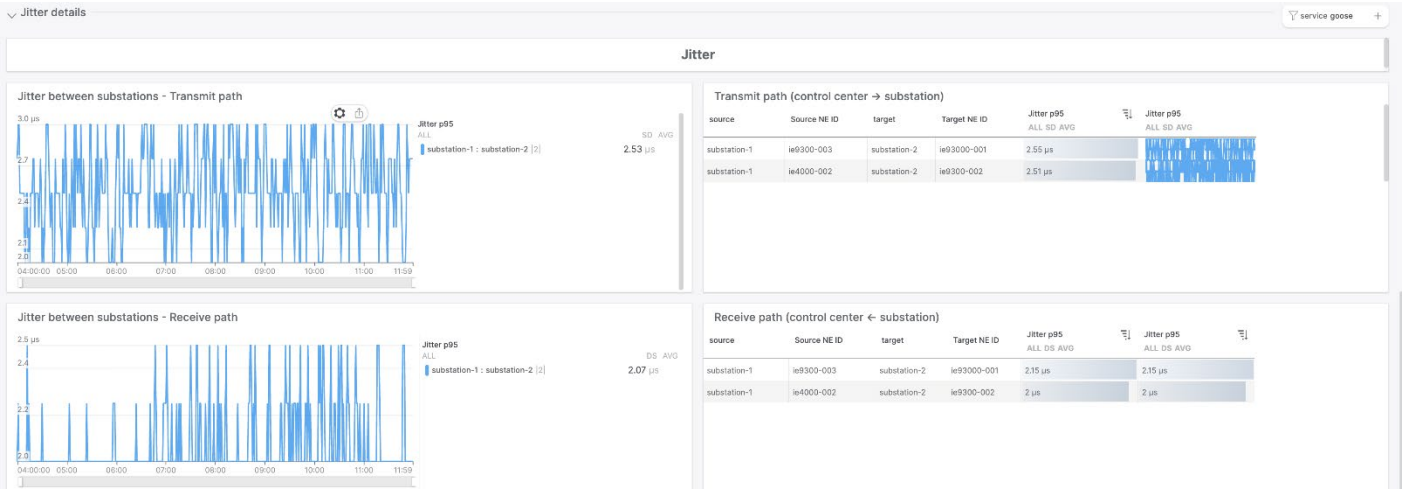


Drill-down into the sections for the different metrics.

Figure 37. Provider Connectivity Assurance for utilities: GOOSE Latency drill down example

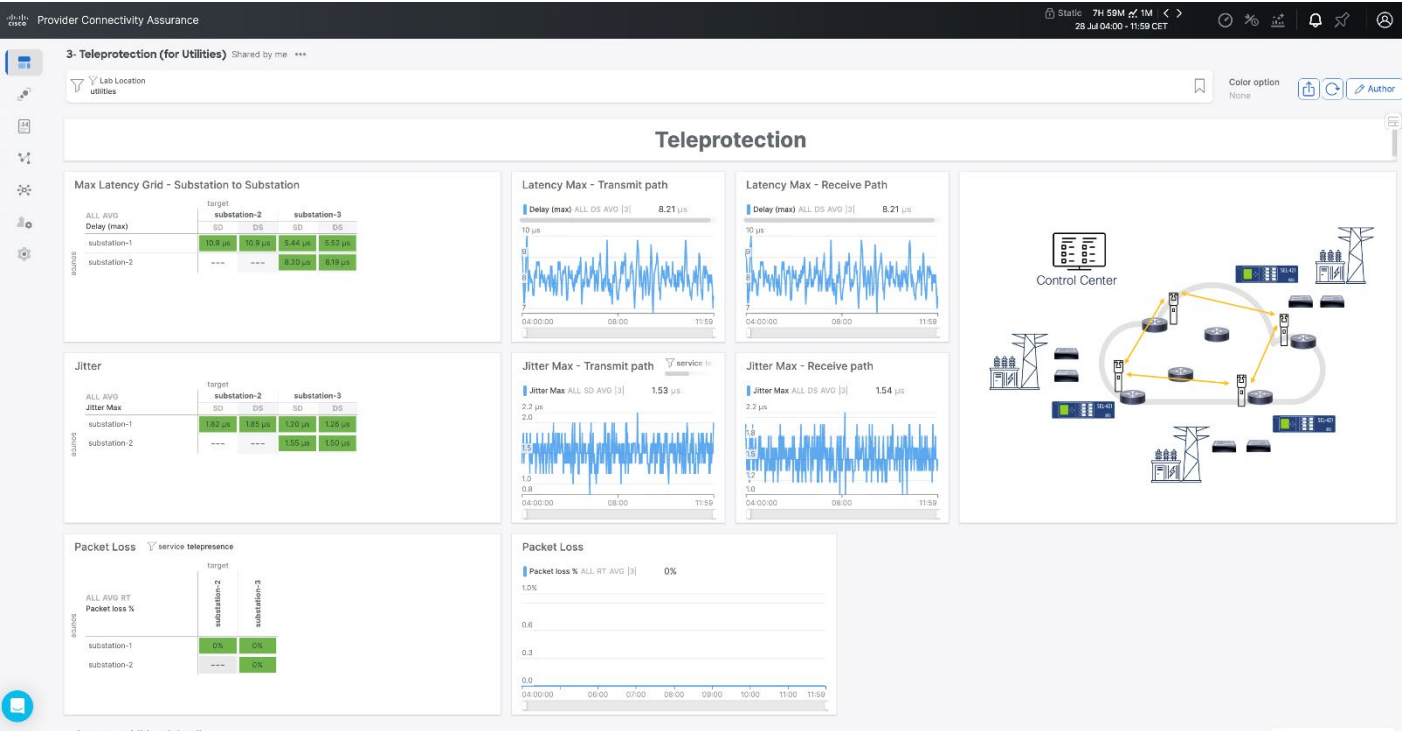


Figure 38. PCA Analytics for utilities: GOOSE Jitter drill down example



Teleprotection main dashboard:

Figure 39. PCA Analytics for utilities: Teleprotection dashboard example



And drill down:

Figure 40: PCA Analytics for utilities: Teleprotection Packet Loss drill down example

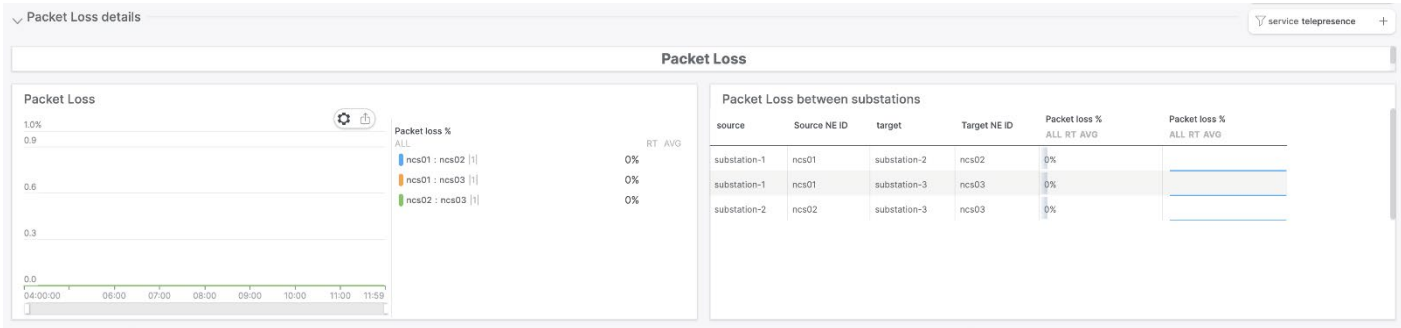


Figure 41: Provider Connectivity Assurance for utilities: Teleprotection Latency drill down example

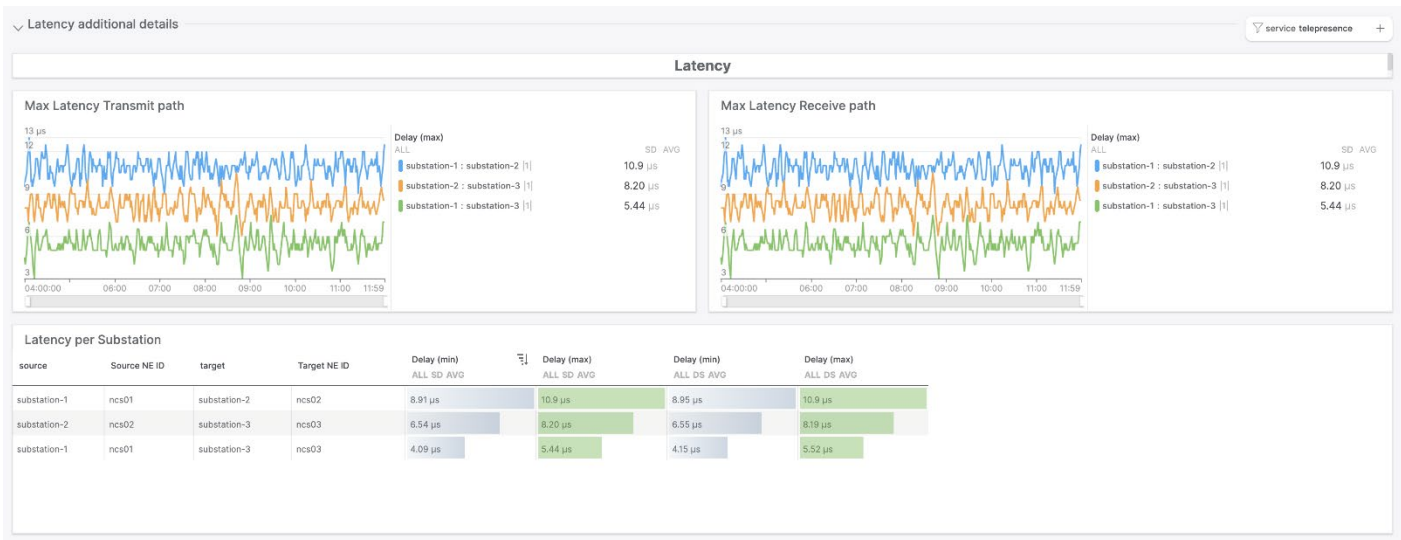


Figure 42: PCA Analytics for utilities: Teleprotection Jitter drill down example

