Substation Automation - The New Digital Substation

Version 3.2

Implementation Guide

November 2024

Cisco Systems, Inc. www.cisco.com

Table of Contents

Substation Automation – The New Digital Substation Implementation Guide

Introduction

Smart Grid is an electricity delivery system that is integrated with communications and information technology to enhance grid operations, improve customer service, lower costs, and enable new environmental benefits. This document describes the overall use of the network to monitor and manage the electrical system from power generation, through transmission and distribution, to end users in smart buildings, smart homes, and other sites connected to the utilities network. As the OT world collides with the traditional IT world, security is becoming increasingly important for utilities customers. Today's news includes many stories about hackers and terrorists that seek to gain access to critical networks to steal money, information, or even to disrupt service.

This solution seeks to address many of these concerns by providing a holistic approach to restricting access, protecting data, logging events and changes, and monitoring activity in the substation.

Audience

The audience of this guide comprises system architects, network/computer/systems engineers, field consultants, Cisco customer experience specialists, and customers. Readers may be familiar with networking protocols, security concepts of firewall, encryption, deep packet inspection, public key infrastructure and Cisco substation automation solution architecture.

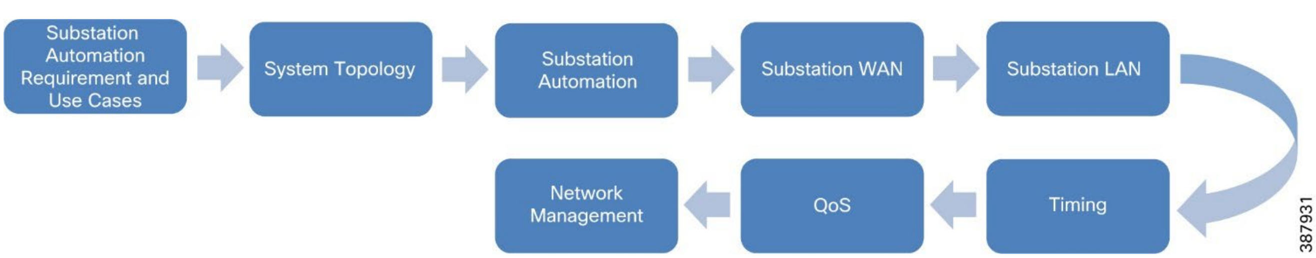
Document Objective and Scope

This guide helps provide details of Substation Automation – The new digital substation design implementation. The scope addressed in this document is Cisco Information and Communication Technology (ICT) solution architecture and implementation for modern transmission substations, including the Cisco solution for process and station buses in substation LAN environment per IEC 61850 protocol standard. It describes how the fault-tolerant multi service network design is implemented.

Implementation Workflow

The following figure shows the flow of information in this implementation guide. The guide may also have cross references to other sections in this document or related guides to help the reader understand the bigger picture.

Figure 1 Implementation Workflow



Substation Automation Requirements and Use Cases

The capabilities offered by the Cisco SA LAN, WAN and Security solution have evolved since the previous validation effort. This version of the Substation Automation – The New Digital Substation emphasizes some of the more significant developments since the last validation cycle listed below.

- Validate Segment Routing enabled core using NCS540 series routers in PE or P roles for different services as listed below:
  - Layer 3 Scada substation to datacenter – Catalyst IR8340 – including security and timing (ZBFW, IDS/IPS, CyberVision sensor and IEEE1588 PTP, NTP timing)
  - Layer 2 Ethernet based protection substation to substation – Catalyst IE9300 – Extending PRP between substations., HSR, PTP
  - Teleprotection interfaces within the substation – SEL ICON
  - Transport Network (WAN) substation edge – NCS540

- Cisco Crosswork Network Controller is the WAN circuit management tool for Segment Routing over Cisco NCS platforms.
- Validate Industrial Substation Router Cisco IR8340 for use in a Substation Automation network.
- Validate Industrial Ethernet switch, Cisco IE 9300, for use in a Substation Automation network.
- Support of network resiliency protocols on the new substation router IR8340 with the availability of PRP, HSR.
- High-Availability Seamless Redundancy (HSR) singly attached node (SAN).
- Parallel Redundancy Protocol (PRP) Redbox.
- Support of network-based timing on IR8340 with the introduction of:
  - Global Navigation Satellite System (GNSS) and Global Positioning System (GPS) support
  - Precision Time Protocol (PTP) 1588 v2 timing protocol.
- Support of network-based timing on IE9300 with the introduction of:
  - Precision Time Protocol (PTP) 1588 v2 timing protocol.
  - Precision Time Protocol (PTP) 1588 v2 timing protocol over both PRP LANs (A and B)
- SDWAN WAN Manager to manage Cisco Substation Router IR8340
- Cisco Catalyst Center to manage Cisco Substation Router IR8340 and IE9300

System Overview

Solution Validation Topologies

The following are the different topologies that were used to validate various designs discussed in the design guide. The substation routers as seen in the following topologies are configured as PE routers and are MPLS enabled. These routers have various network resiliency protocols configured as per the design recommendations and act as Layer 3 Gateway for Substation LAN devices connected to the various LAN networks to reach the Operations Control Center. The Operations Control Center and the MPLS WAN connections are not shown in the following topologies. Refer to the earlier versions of Grid Security Implementation Guide for those details.

Figure 2 PRP on Substation Router

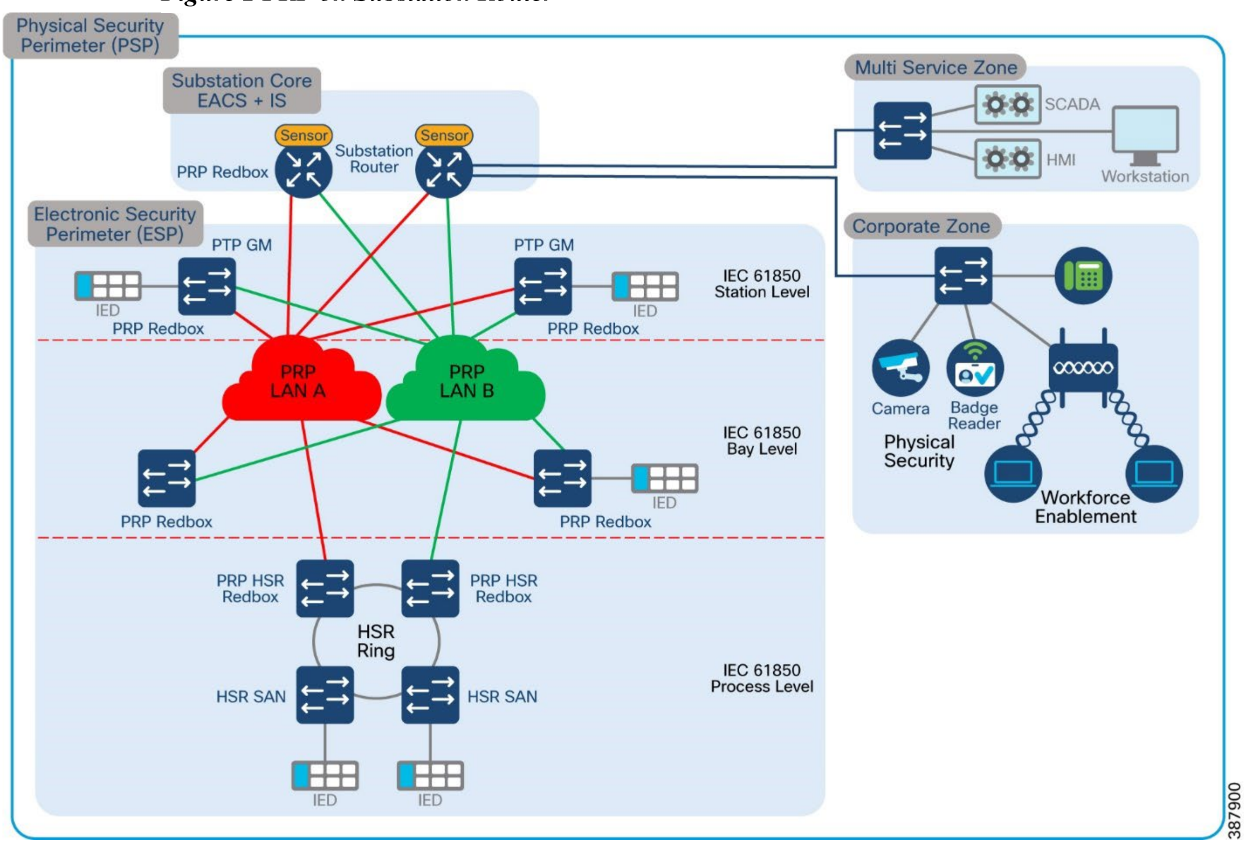


Figure 3 HSR on Substation Router

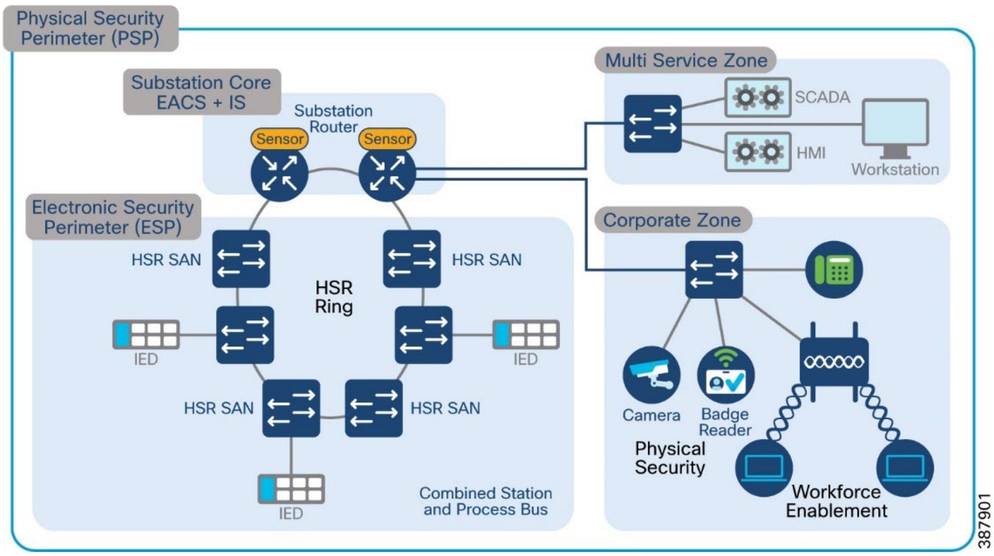


Figure 4 REP on Substation Router

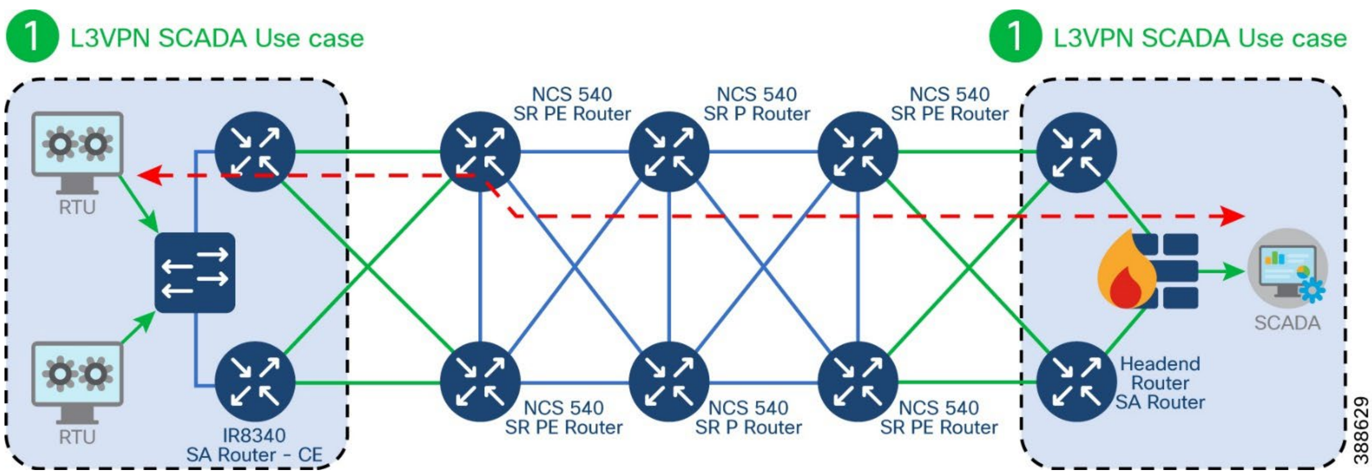


Figure 5 IR8340 Substation Router as PE over SR

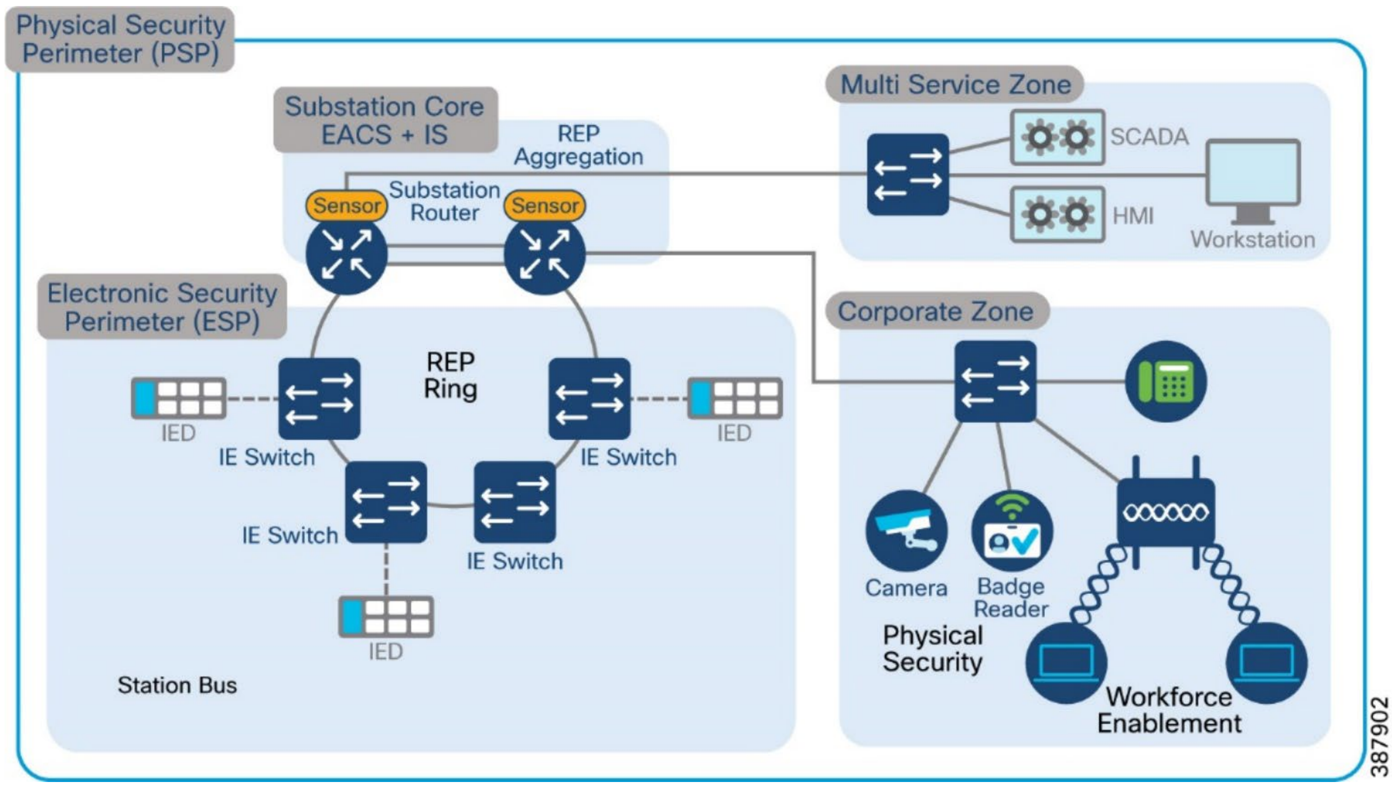


Figure 6 IR8340 Substation Router as PE over SR

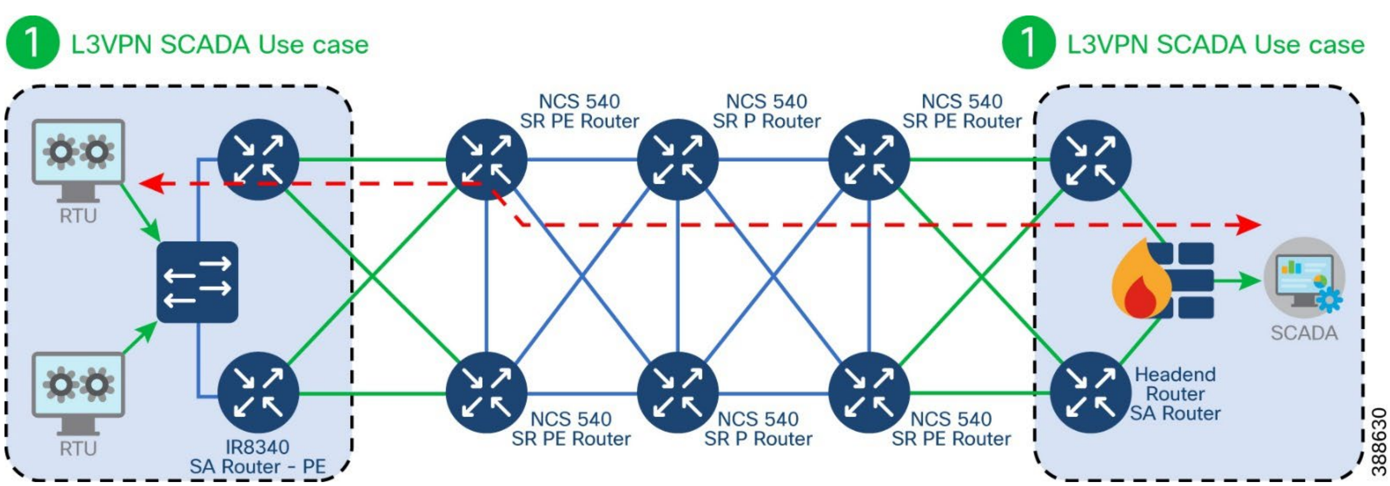


Figure 7 Dual IE9300 as L2 Gateway for L2 Teleprotection services with CS – SR

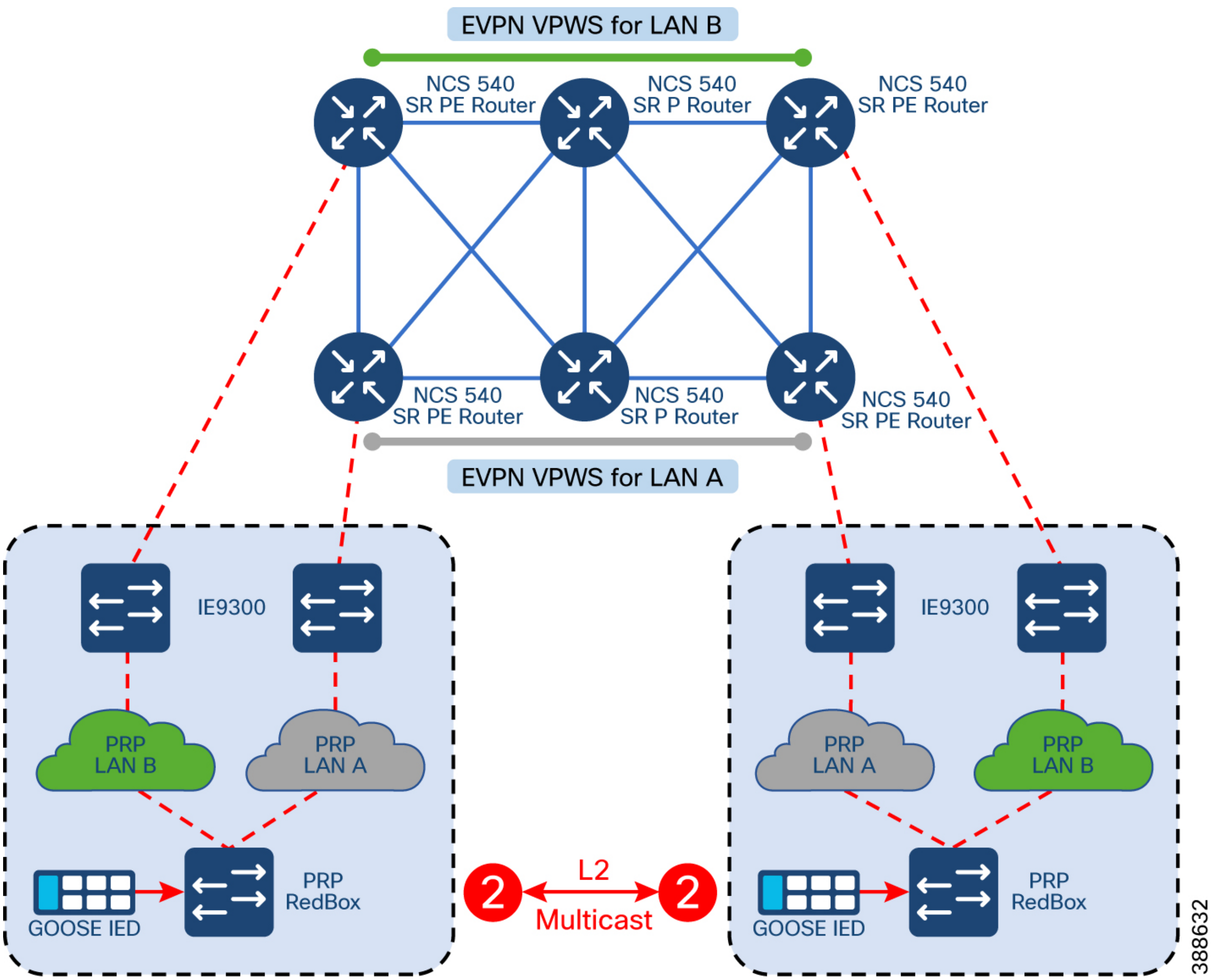


Figure 8 NCS540 as L3 Gateway for Substation LAN

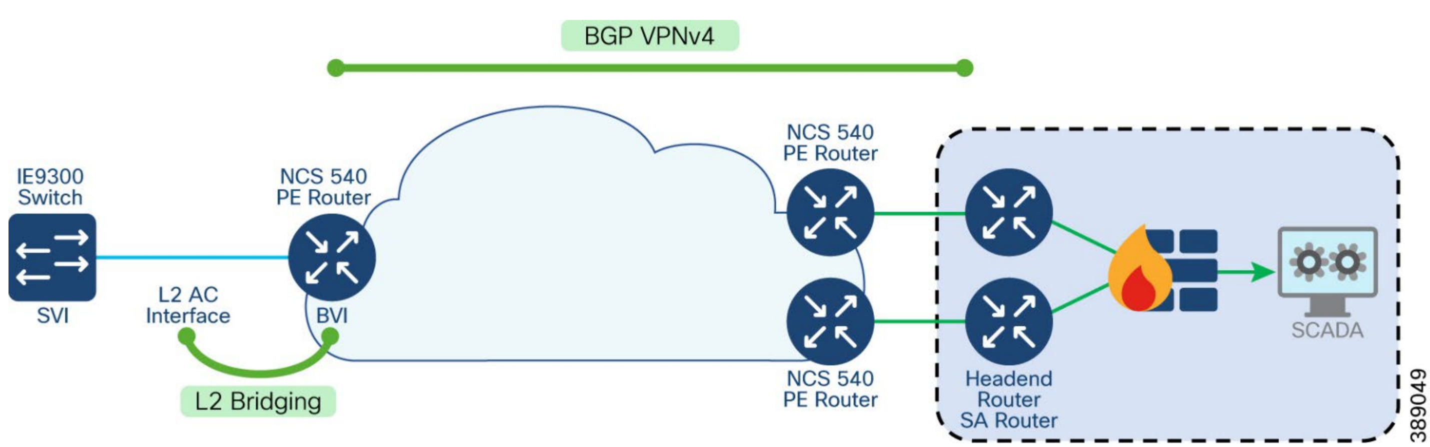
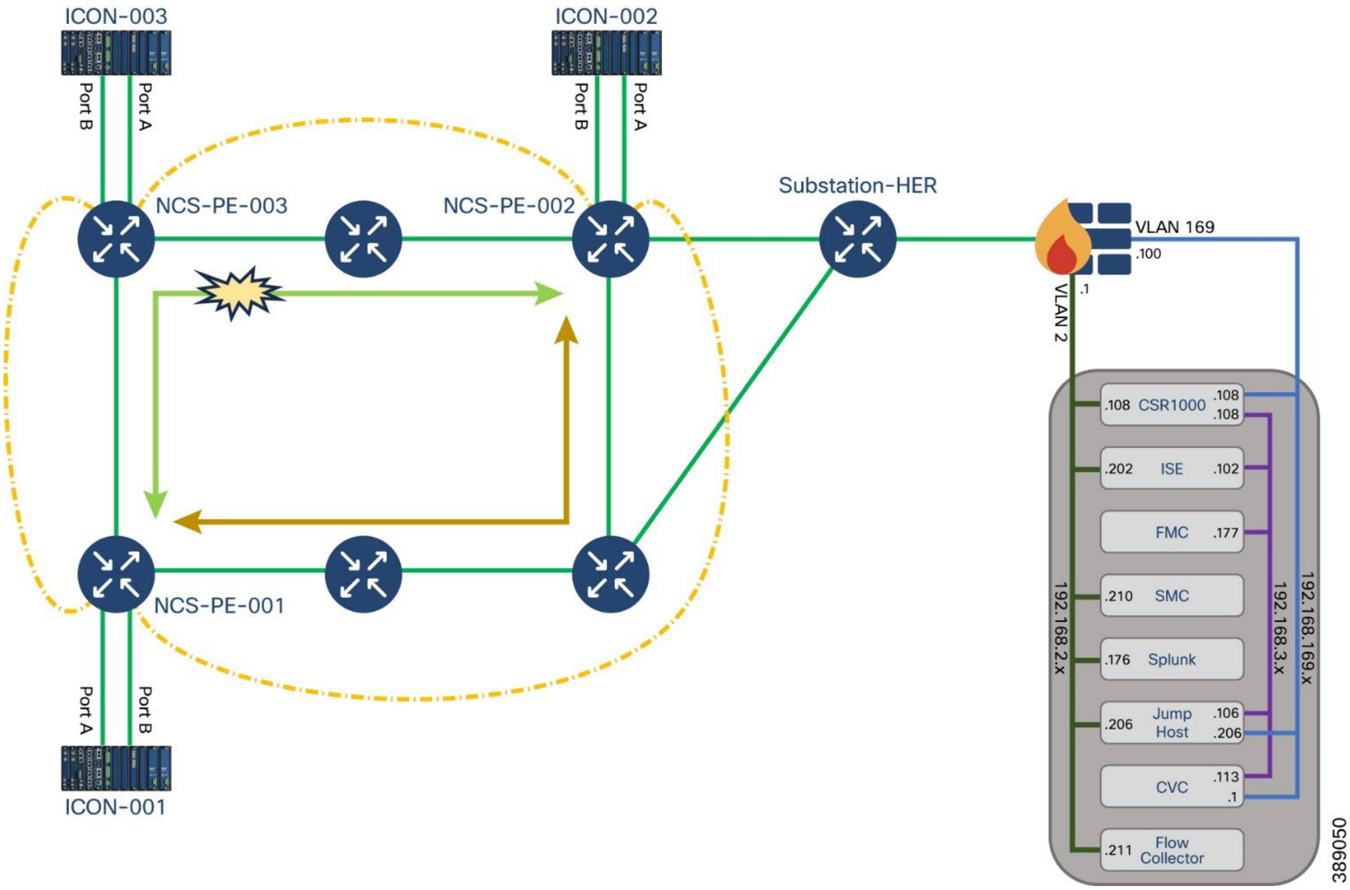


Figure 9 Teleprotection over Segment Routed Core using SEL ICON



Key components of a Substation design include:

Network resiliency

High availability for Information and Communication Topology network layer provides network resiliency and better convergence at times of network faults. Various protocols can be used. Some legacy resiliency protocols within ring topology deployments are:

- Rapid Spanning Tree (RSTP) is a variant of spanning tree protocol (STP) that is known, used, and trusted by IT professionals who have used Cisco switches.

- Resilient Ethernet Protocol (REP) -- a Cisco proprietary protocol described below.

IEC 61850 implementation standards in the station bus and process bus, high performance applications in the utility substation mandate several key requirements to be addressed. The substation architecture must meet design requirements for GOOSE and Sample Values, both of which are multicast traffic types. This includes high availability (HA) and topology choices to meet scale, segmentation, and communications requirements. IEC 61850-5 provides guidance for HA and communication requirements based on several use cases in the standards.

With these failover and recovery times at ZERO milli-seconds for some use cases, a truly “hitless” architecture is required. There are two choices to meet this hitless requirement:

- Parallel Redundancy protocol (PRP) supports either tree or ring topologies with no limits on node counts, and it can deliver a ZERO millisecond failover/recovery requirement. However, PRP has one drawback. PRP requires duplicate LANs (named LAN-A & LAN-B) and double the networking equipment hardware.

- Highly Available Seamless Ring (HSR) also delivers a ZERO millisecond fail-over/recovery requirement but is only available in ring topology and scales to a limited number of devices. HSR does NOT require duplicate LANs (double the switching infrastructure) in the ESP.

Corporate Substation (CORPSS) zone

The Corporate Substation zone is a natural extension to the corporate/enterprise “General Purpose” network. Traffic from this zone can only access other corporate assets directly by passing through the Outside zone. Access to the other zones (CIP and ESP) requires additional credentials and access restrictions.

All employees can leverage this zone for basic connectivity to business resources including email, file shares, and general access to the Internet via the Outside zone

Critical infrastructure Perimeter (CIP) zone

The CIP zone also known as Multiservice zone is a “DMZ” for the Substation. This zone is “semi-trusted” and has a Firewall security level between the Corporate Substation zone and the ESP zone.

As such, this zone is designed to allow proxied user-level access between both the Corporate Substation and ESP zones — leveraging an information security (InfoSec) hardened Bastion host. Other support infrastructure may also exist in this zone such as a Secure Policy Server such as Cisco ISE or ACS, Network Services, and/or a user management server such as Lightweight Directory Access Protocol (LDAP) or Active Directory (AD).

Electronic Security Perimeter (ESP) zone

The ESP zone contains components that play an active role in the proper functionality of the Critical Infrastructure/Smart Grid. These components should be regarded as being the most valued and trusted resources on the Substation network and highly protected.
With very few exceptions, outbound communications from this portion of the network must be significantly restricted. Any communication from this zone to any lower-security zone should leverage a "Pull" model – initiating the connection from the ESP zone. Inbound connections into the ESP zone should be discouraged except for any business-critical applications.

This zone is intended to provide limited network connectivity for industrial components such as IEDs and Protection Relays with direct user-level access restricted to appropriately vetted employees that require direct Substation access for machine maintenance. Depending on the security model employed, access to the IEDs and Protection Relays can also be restricted to specific, well vetted, and highly audited hosts, denying access from personal/corporate laptops. Outbound connections are highly restricted from this zone.

Substation Core Zone

This zone connects the Substation topology to the rest of the infrastructure, whether the infrastructure is owned by the Utility Corporation or provided by a third-party Service Provider. This zone is untrusted. The security postures of assets within this outside zone are, in most cases, outside of the control of the Utility Corporation.
The traffic allowed to traverse this interface should be encrypted, authenticated, and/or originally initiated from the inside zones (ESP, CIP, and CORPSS) of the firewall. Because this zone is considered outside the Substation architecture, the protection of this zone is varied and relies solely on the protections provided by the WAN infrastructure.

Hardware and Software Matrix

The table that follows describes the hardware, software, and role of the main components of the solution. These software versions were used in the Cisco solution validation lab, and all were publicly available when this document was published.

Table 1 Hardware and Software Matrix

Device Role	Description	Hardware Platform	Software Release
Substation Router	Ruggedized Router, Layer 3 Gateway, Layer 2 Aggregator	IR8340	IOS-XE 17.15.1
Substation WAN Router	Layer 3 Gateway, Layer 2 Aggregator	NCS540	IOS XR 24.1.2
Substation Firewall	Ruggedized firewall, Virtual Private Network (VPN) head-end (Site-to-site, RA), FirePOWER Intrusion Prevention System (IPS)	ISA3000	FTD: 7.0.1
Ruggedized Switch	Access switch-DANH,SANH,RedBox,etc., switch port security	IE4000	15.2(8)E1
Ruggedized Switch	Access switch, switch port security	IE5000	15.2(8)E1
Ruggedized Switch	Access switch, switch port security	IE4010	15.2(8)E1
Ruggedized Switch	Access switch, PRP Redbox, switch port security	IE9300	IOS-XE 17.15.1
Ruggedized Switch with Cyber Vision Sensor	Edge compute platform hosting Cisco Cyber Vision Sensor application (release 4.1.2) and acts as Network Sensor	IE3400	IOS-XE 17.15.1
Control/Data Center Firewall	Firewall	FPR4150	FTD: 7.0.1
AAA	Authentication, Authorization server for policy definition	Identity Services Engine (running as a virtual machine on Cisco Unified Computing System)	2.4.0.357 Patch 10
IPS	Centralized management and monitoring server for FirePOWER IPS devices	Firepower Management Center for VMWare	FMC: 7.0.1
Cisco Cyber Vision Center	Cisco Cyber Vision Center used to manage Cisco Cyber Vision sensor applications hosted on IR8340 and or IE3400 platforms.	CVC	4.2.6
SDWAN	WAN Management	SDWAN	20.13

Catalyst Center	LAN Management	Catalyst Center	2.3.4
Cisco Crosswork	SR WAN Management	Cisco Crosswork	6.0.2

IP Addressing

This implementation assumes a simple topology for lab validation efforts. The following table lists the various IP Addresses and VLANs used for various components of the topology installed on a Cisco UCS server. ASR1K-Virtual acts as both NTP server and gateway to other components. Networks are defined for the virtual instances of different components for the reachability required. The following list includes networks defined in the UCS.

- VM_Network - Uses IP addresses in the lab subnet for access to the Internet. Traffic is untagged.
- VM_Internal_Communication - Uses IP addresses in subnet 192.168.3.x for internal communication between various VMs. Traffic is untagged.
- ISE_VLAN - Uses IP addresses in subnet 192.168.2.x for communication to Next Generation Firewall (NGFW). Traffic is tagged with VLAN 2.
- Collection_Network - Uses IP addresses in subnet 192.168.169.x for communication between Cyber Vision Center and Cyber Vision Sensors. Traffic is encrypted on IPSec tunnel when flowing over WAN or Internet. Traffic is tagged with VLAN 169.

Table 2 IP Addressing Scheme

Component	IP Addresses
Jump Host – Windows	192.168.3.106 192.168.2.206 192.168.169.206
Active Directory- Microsoft	192.168.2.204 192.168.3.104
Identity Services Engine	192.168.3.102 192.168.2.202
Cyber Vision Center	192.168.3.113
Firepower Management Console	192.168.3.177
Stealth Watch Management Console	192.168.2.210
Flow Collector	192.168.2.211

ASR 1K – Virtual – NTP Server	192.168.3.108 192.168.2.108 192.168.169.108
Substation LAN Management	192.168.21.0/24 192.168.201.0/24 50.1.0.0/24
Substation LAN Services	VRF_SCADA VRF_TSCADA VRF_PLANTLINK VRF_MGMT VRF_GRIDMON VRF_BUSINESS

Licensing

The following table describes the hardware, software, and the corresponding licenses required to enable features and functions relevant to the solution. These licenses were certified in the Cisco solution validation lab, and all were publicly available at the time this document was published.

Table 3 Licenses and components

Device Role	Hardware Platform	License	Reference
Substation Router	IR8340	network-advantage IPSEC-HSEC (for >250Mbps traffic)	https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17-8/m_installing_software.html https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17_7/m-sle-license.html#Cisco_Concept.dita_83d701d7-5072-4685-aadd-4080bb61a1f4
Substation WAN Router	NCS540		https://www.cisco.com/c/en/us/products/collateral/routers/network-convergence-system-500-series-routers/datasheet-c78-740296.html
Substation Firewall	ISA3000	Base Subscription required for the following licenses. Malware Threat	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
Ruggedized Switch	IE9300	network-advantage	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie9300-rugged-series/catalyst-ie9300-rugged-series-ds.html#Productspecifications
Ruggedized Switch	IE4000	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html

Ruggedized Switch	IE5000	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-5000-series-switches/datasheet-c78-734967.html
Ruggedized Switch	IE4010	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4010-series-switches/datasheet-c78-737279.html?cachemode=refresh
Secondary Substation Router	IR1101	network-advantage	https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html#Softwarelicensing
Ruggedized Switch	IE3400	network-advantage	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie3400-rugge d-series/datasheet-c78-741760.html
Control/Data Center Firewall	FPR4150	Base Subscription required for the following licenses. Malware Threat	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
AAA - ISE	Identity Services Engine running as a virtual machine on Cisco Unified Computing System.	Traditional License with the following features: • Base • Plus • Apex • Device Admin	https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_0110.html

Substation Automation Solution Implementation

References

Refer to the previous releases of the SA LAN and Security solution CVDs at the following links on Cisco SalesConnect:

- https://www.cisco.com/c/en/us/solutions/design-zone/industries/power-utilities.html

Notes

- The content of this implementation guide applies mainly to platforms like IR8340, IE9300, and NCS540. It uses IR8340 as a router for substation in roles specified in this document, IE9300 as an Industrial Ethernet switch, and NCS540 as WAN routers. Although substation zones are mentioned, this release of the Substation Automation - The New Digital Substation version 3.1 focuses on enhancements to the WAN design with the introduction of new products NCS540 as either PE or P router and Segment Routing over MPLS using these products.

- Please refer to older releases of the solution document listed above if you are looking for designs relevant to endpoints communicating via serial-based protocols like Modbus or DNP3, different flavors of HSR and PRP other than the designs covered in the following section.

- If you do not have direct access to the links, please ask your Cisco account team to help provide the documentation to you. Your company must be covered under a non-disclosure agreement (NDA) with Cisco.

WAN and Core Implementation

The Utility WAN is often a dedicated WAN infrastructure that connects the Transmission Service Operator (TSO) Control Center with various Substations and other field networks and assets. Utility WAN connections can include a host of technologies like Cellular LTE/5G options for public backhaul, Fiber ports to connect utility owned private network, leased lines, MPLS PE or Segment Routing over MPLS connectivity options and legacy Multilink PPP backhaul aggregating multiple T1/E1 Circuits based on the core. The following table lists different modules supported on IR8340 enabling the option to use different connections.

Table 4 IR8340 Supported Modules

Product	Description
IRM-NIM-2T1E1	2 port T1/E1 Network Interface Module
IRM-NIM-RS232	RS232 8 Port Serial Network Interface Module
P-LTEAP18-GL	4G/CAT18 LTE Advanced Pro Pluggable – Global
P-LTE-MNA	4G/CAT6 LTE Advanced Pluggable for North American and Europe
P-LTE-EA	CAT6 Advanced Pluggable for Europe and North America
P-LTE-LA	CAT6 Advanced Pluggable for APAC, LATAM and ANZ

The IR8340 is designed to support the communications needs of the energy delivery infrastructure that includes substation applications supporting electrical transmission and distribution. In a Substation Automation Network environment, the IR8340 is positioned at the edge of the ESP Zone. With support for many security features including zone-based firewall and encryption, IR8340 provides a secure boundary to protect the most critical assets in the substation.
IR8340 supports Ethernet, T1/E1, Cellular interfaces that can be used as WAN backhaul. This solution positions IR8340 as an On Net Substation Router or as an Off Net Substation Router.

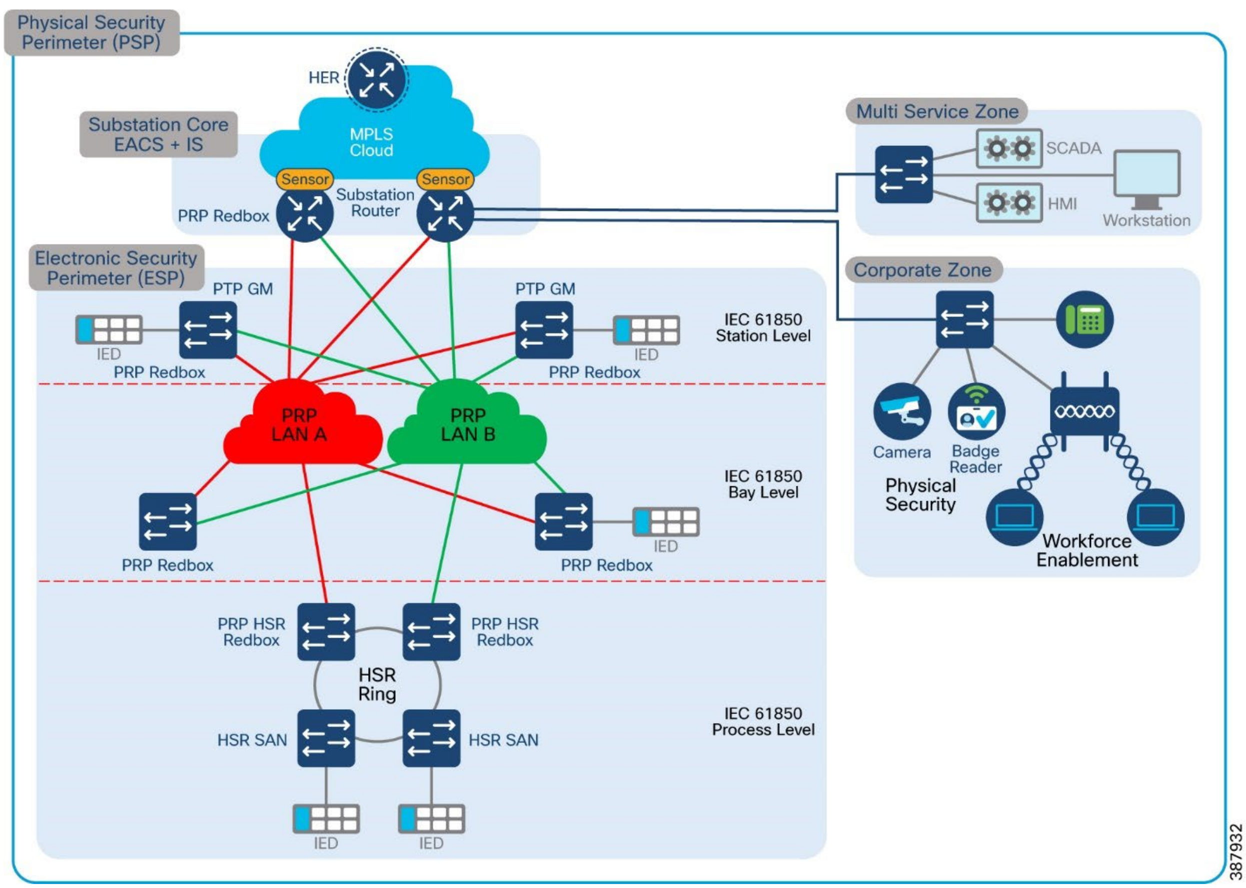
- On Net Substation
  - Utility Owned MPLS/IP Backhaul
  - Substation router IR8340 acting as MPLS PE or CE
- Off Net Substation
  - Public Backhaul (Leased Line/ Cellular Backhaul)
  - Substation Router IR8340 acting as IPSEC (FlexVPN/DMVPN) Spoke

Note: IR8340 in the role of a PE for Segment Routing is limited. Refer to the appropriate section for details.

Substation Router MPLS Backhaul

The following topology depicts Cisco IR8340 being used as a substation router in this solution. The router is configured as Provider Edge. The implementation here uses OSPF and BGP for the MPLS connectivity. Different services like SCADA, Network Management, etc are provisioned with different SVI's. The SVI's are part of the Layer 2 Resiliency network that the Substation LAN network. Refer relevant sections for configuration steps of different resiliency protocols that can be used as per requirements. Cisco IR8340 acts as the Layer 3 gateway to these different services. These different services and the related subnets are exchanged over the MPLS network using BGP as the node is being configured as a Provider Edge Router. IR8340 can also be used as a Customer Edge Router and connected to a Provider Edge Router with relevant routing protocols like OSPF, EIGRP to exchange subnets relevant to the different services.

Figure 10 Substation Router with MPLS Backhaul



Detailed end-to-end configuration of all aggregation devices in the core is not covered in this section as it is out of scope. This section shows the limited configuration on the two PE devices necessary to understand the MPLS VPN/L3VPN setup discussed. This section lists the configurations required on Ethernet and Serial interfaces to act as MPLS WAN Backhaul interfaces

IR8340

WAN Interface Ethernet:

```
!
interface GigabitEthernet0/0/0
description connected to asr903-003
ip flow monitor StealthWatch_Monitor output
ip address 192.168.100.1 255.255.255.0
no ip redirects
ip ospf network point-to-point
load-interval 30
negotiation auto
mpls ip
bfd interval 200 min_rx 200 multiplier 3
lacp max-bundle 2
!
```

Substation Router MLPP Backhaul:

```
!
controller T1 0/2/0
 framing esf
 clock source internal
 linecode b8zs
 cablelength long 0db
 channel-group 2 timeslots 1-24
 controller T1 0/2/1
 framing esf
 clock source internal
 linecode b8zs
 cablelength long 0db
 channel-group 1 timeslots 1-24
 description connected to T10/2/3 on asr903
!

!
interface Serial0/2/0:2
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/2/1:1
no ip address
encapsulation ppp
ppp multilink
 ppp multilink group 1
```

```
!

!
interface Multilink1
 ip address 3.3.3.2 255.255.255.0
 zone-member security OUTSIDE
 load-interval 30
 mpls ip
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string mlp1
!
```

OSPF

```
!
router ospf 1
router-id 192.168.199.1
network 3.3.3.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
network 192.168.199.1 0.0.0.0 area 0
bfd all-interfaces
!
```

MPLS Global Configuration:

```
!
mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp router-id Loopback0
!
```

BGP Configuration:

```
!
interface Loopback0
ip flow monitor StealthWatch_Monitor input
ip address 192.168.199.1 255.255.255.255
!

!
router bgp 200
bgp router-id interface Loopback0
```

```
bgp log-neighbor-changes
neighbor 192.168.201.6 remote-as 200
neighbor 192.168.201.6 update-source Loopback0
!
address-family ipv4
  network 11.9.0.0 mask 255.255.255.0
  network 19.90.0.0 mask 255.255.255.0
  network 20.1.0.0 mask 255.255.255.0
  network 20.2.0.0 mask 255.255.255.0
  network 50.1.0.0 mask 255.255.255.0
  network 177.177.177.0 mask 255.255.255.0
  network 192.168.0.0
  network 192.168.53.0
  network 192.168.54.0
  network 192.168.55.0
  network 192.168.56.0
  network 192.168.57.0
  network 192.168.58.0
  network 192.168.59.0
  network 192.168.60.0
  network 192.168.101.0
  network 192.168.110.0
  network 192.168.155.0
  network 192.168.199.2 mask 255.255.255.255
  network 192.168.210.0
  network 192.168.211.0
  neighbor 192.168.201.6 activate
  neighbor 192.168.201.6 send-community extended
  neighbor 192.168.201.6 next-hop-self
  neighbor 192.168.201.6 send-label
exit-address-family
!
address-family vpnv4
  neighbor 192.168.201.6 activate
  neighbor 192.168.201.6 send-community extended
  neighbor 192.168.201.6 next-hop-self
exit-address-family
!
address-family ipv4 vrf VRF_BUSINESS
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
```

```
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_PLANTLINK
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_TSCADA
  redistribute connected
exit-address-family
!
```

HER

WAN Interface Ethernet:

```
!
interface GigabitEthernet0/0/1
description connected to asr920-001
ip address 192.168.69.1 255.255.255.0
ip ospf network point-to-point
ip ospf 1 area 0
load-interval  30
negotiation auto
cdp enable
mpls ip
bfd interval 200 min_rx 200 multiplier 3
!
```

OSPF:

```
!
router ospf 1
router-id 192.168.201.6
network 192.168.201.6 0.0.0.0 area 0
bfd all-interfaces
mpls ldp sync
!
```

MPLS Global Configuration:

```
!
mpls label protocol ldp
```

```
mpls ldp graceful-restart
mpls ldp router-id Loopback0
!
```

BGP Configuration:

```
!
interface Loopback0
ip address 192.168.201.6 255.255.255.255
!

!
router bgp 200
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor 192.168.60.2 remote-as 2001
 neighbor 192.168.60.2 shutdown
 neighbor 192.168.60.2 ebgp-multihop 255
 neighbor 192.168.70.1 remote-as 1001
 neighbor 192.168.70.1 ebgp-multihop 255
 neighbor 192.168.70.1 update-source Loopback0
 neighbor 192.168.111.1 remote-as 200
 neighbor 192.168.111.1 ebgp-multihop 255
 neighbor 192.168.111.1 update-source Loopback0
 neighbor 192.168.113.1 remote-as 200
 neighbor 192.168.113.1 ebgp-multihop 255
 neighbor 192.168.113.1 update-source Loopback0
 neighbor 192.168.198.1 remote-as 200
 neighbor 192.168.198.1 update-source Loopback0
 neighbor 192.168.198.1 fall-over
 neighbor 192.168.198.1 fall-over bfd
 neighbor 192.168.199.1 remote-as 200
 neighbor 192.168.199.1 update-source Loopback0
 neighbor 192.168.199.1 fall-over
 neighbor 192.168.199.1 fall-over bfd multi-hop
 neighbor 192.168.201.4 remote-as 200
 neighbor 192.168.201.4 shutdown
 neighbor 192.168.201.4 update-source Loopback0
 neighbor 192.168.201.10 remote-as 200
 neighbor 192.168.201.10 update-source Loopback0
 neighbor 192.168.202.1 remote-as 101
 neighbor 192.168.202.1 ebgp-multihop 255
 neighbor 192.168.202.1 update-source Loopback0
 neighbor 192.168.203.1 remote-as 200
 neighbor 192.168.203.1 update-source Loopback0
 neighbor 192.168.220.2 remote-as 102
 neighbor 192.168.220.2 ebgp-multihop 255
```

```
neighbor 192.168.220.2 update-source Loopback0
!
address-family ipv4
 bgp additional-paths install
 bgp nexthop trigger delay 1
 network 30.1.0.0 mask 255.255.255.0
 network 30.2.0.0 mask 255.255.255.0
 network 140.140.140.0 mask 255.255.255.0
 network 141.141.141.0 mask 255.255.255.0
 network 192.168.189.0
 network 192.168.200.1 mask 255.255.255.255
 network 192.168.205.2 mask 255.255.255.255
 network 192.168.205.4 mask 255.255.255.255
 network 192.168.220.2 mask 255.255.255.255
 network 192.168.223.1 mask 255.255.255.255
 redistribute connected
 redistribute eigrp 99
 neighbor 192.168.60.2 activate
 neighbor 192.168.60.2 next-hop-self
 neighbor 192.168.60.2 send-label
 neighbor 192.168.70.1 activate
 neighbor 192.168.70.1 next-hop-self
 neighbor 192.168.70.1 send-label
 neighbor 192.168.111.1 activate
 neighbor 192.168.111.1 send-community extended
 neighbor 192.168.111.1 next-hop-self
 neighbor 192.168.113.1 activate
 neighbor 192.168.113.1 send-community extended
 neighbor 192.168.113.1 next-hop-self
 neighbor 192.168.198.1 activate
 neighbor 192.168.198.1 next-hop-self
 neighbor 192.168.198.1 soft-reconfiguration inbound
 neighbor 192.168.198.1 send-label
 neighbor 192.168.199.1 activate
 neighbor 192.168.199.1 weight 40000
 neighbor 192.168.199.1 next-hop-self
 neighbor 192.168.199.1 soft-reconfiguration inbound
 neighbor 192.168.199.1 send-label
 neighbor 192.168.201.4 activate
 neighbor 192.168.201.4 next-hop-self
 neighbor 192.168.201.4 soft-reconfiguration inbound
 neighbor 192.168.201.4 send-label
 neighbor 192.168.201.10 activate
 neighbor 192.168.201.10 next-hop-self
 neighbor 192.168.201.10 soft-reconfiguration inbound
 neighbor 192.168.201.10 send-label
 neighbor 192.168.202.1 activate
```

```
 neighbor 192.168.202.1 next-hop-self
 neighbor 192.168.202.1 soft-reconfiguration inbound
 neighbor 192.168.202.1 send-label
 neighbor 192.168.203.1 activate
 neighbor 192.168.203.1 next-hop-self
 neighbor 192.168.203.1 soft-reconfiguration inbound
 neighbor 192.168.203.1 send-label
 neighbor 192.168.220.2 activate
 neighbor 192.168.220.2 next-hop-self
 neighbor 192.168.220.2 send-label
exit-address-family
!
address-family vpnv4
 neighbor 192.168.70.1 activate
 neighbor 192.168.70.1 send-community extended
 neighbor 192.168.70.1 next-hop-self
 neighbor 192.168.198.1 activate
 neighbor 192.168.198.1 send-community extended
 neighbor 192.168.198.1 next-hop-self
 neighbor 192.168.199.1 activate
 neighbor 192.168.199.1 send-community extended
 neighbor 192.168.199.1 next-hop-self
 neighbor 192.168.201.4 activate
 neighbor 192.168.201.4 send-community extended
 neighbor 192.168.201.4 next-hop-self
 neighbor 192.168.201.10 activate
 neighbor 192.168.201.10 send-community extended
 neighbor 192.168.201.10 next-hop-self
exit-address-family
!
address-family ipv4 vrf VRF_BUSINESS
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_PLANTLINK
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
```

```
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_TSCADA
 redistribute connected
exit-address-family
!
```

IR8340 – Cellular Backhaul

The IR8340 supports both integrated pluggable modules and external cellular gateway modules with LTE/5G capability for improved throughputs that address these use cases. Based on a specific branch direct line of sight and cellular coverage, either an integrated or external gateway can be chosen.

Here we can discuss the Cellular WAN backhaul implementation on the IR8340. Secure FlexVPN tunnels are established to the Headend in the Demilitarized Zone (DMZ).

IR8340 OFF Net Substation Implementation

This section discusses the implementation of Cellular backhaul scenarios on Cisco IR8340 Substation Router. Here FlexVPN tunnel is established over the primary Cellular interface using Tunnel interface, the Tunnel connects to the public IP address configured on the HER. The configurations that follows are required to establish FlexVPN tunnel.

The following configuration, which uses the interface names that are applicable to IR8340, is applicable to other platforms using the appropriate interface naming convention applicable to the platform on which the configuration is applied.

Installation of 4G/5G module on IR8340

Refer the following guide for the detailed explanation on how to install the SIM on pluggable module and bringing up the Cellular interface.

https://www.cisco.com/c/en/us/td/docs/routers/iot-antennas/cellular-pluggable-modules/b-cellular-pluggable-interface-module-configuration-guide.html

IR8340 SIM installation (requires a pluggable LTE module installed on the gateway)

IR8340 Cellular Interface Example Configuration:

```
!
!
interface Cellular0/1/0
description Cellular Connection to HER Public IP
mtu 1430
ip address negotiated
```

```
ip nat outside
ip tcp adjust-mss1460
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
dialer-group 1
ipv6 enable
pulse-time 1
ip virtual-reassembly
end

!
!
ip route 0.0.0.0 0.0.0.0 Cellular0/4/0
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
!
```

Encrypted Traffic by Cisco FlexVPN over Cellular backhaul

The Substation traffic between the IR8340 and HER can be encrypted end to end by using FlexVPN tunnels. There are various ways to bring up tunnel and the recommended configuration for Flex tunnels is by configuring the Certificate based authentication. In this solution, the Flex Tunnels are established based on PSK (Pre-Share-Key).

The sample configuration used for this Substation solution is shown below.

```
!
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
aaa session-id common
!
!
crypto ikev2 authorization policy default_no_cert
 route set interface
 route set access-list FLEX_ACL
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
crypto ikev2 keyring FLEX_KEYS
 peer Substation-HER
```

```
 address x.x.x.x
 pre-shared-key xxxxx
 !
crypto ikev2 profile FLEX_CLIENT_PROF
 match identity remote address x.x.x.x 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEX_KEYS
 dpd 30 3 periodic
 aaa authorization group psk list FlexVPN_Author default_no_cert
crypto ikev2 fragmentation mtu 1200
crypto ikev2 client flexvpn IKEv2_CLIENT_PROFILE
  peer 1 x.x.x.x
  client connect Tunnel100
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-
hmac
 mode transport
no crypto ipsec profile default
crypto ipsec profile default_No_cert
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FLEX_CLIENT_PROF
```

The Tunnel interface Configuration is listed below.

```
interface Tunnel100
  ip unnumbered Loopback100
 ip mtu 1200
 ip nat outside
 ip tcp adjust-mss 1160
 bfd interval 50 min_rx 50 multiplier 3
 tunnel source Cellular 0/4/0
 tunnel destination dynamic
tunnel protection ipsec profile default_No_cert
!
```

With the above configuration, FlexVPN tunnels can be established with the HER. See HER configurations in the Appendix section.

After the FlexVPN tunnel is established, the routes between the control center and Substation router can be exchanged using the IKEV2 prefix injection or any of the Dynamic routing protocols such as BGP/OSPF/EIGRP.

Establish the routes using the IKEv2 prefix injection using the access-list below. Set the same in crypto IKEv2 authorization policy to allow the shared routes between the secure tunnels.

```
ip access-list standard FLEX_ACL
 10 permit x.x.x.x
```

11 permit x.x.x.x
12 permit x.x.x.x

Substation Router Multilink Backhaul

A multilink interface is a virtual interface that represents a multilink PPP bundle. The multilink interface coordinates the configuration of the bundled link and presents a single object for the aggregate links. However, the individual PPP links that are aggregated must also be configured. Therefore, to enable multilink PPP on multiple serial interfaces, you first need to set up the multilink interface, and then configure each of the serial interfaces and add them to the same multilink interface.

The IR8340 router has two Network Interface Module (NIM) slots, 0/2 and 0/3. The T1/E1 Network Interface Module IRM-NIM-2T1E1 can be installed in these two slots. It is a 2-port channelized data module and supports 24/31 channel groups for T1/E1 per port. Each T1/E1 module has two ports, P0 and P1. Each port is linked to a controller in the following configuration:

- If the module is in slot 0/2, it has two controllers 0/2/0 and 0/2/1.
- If the Module is in slot 0/3, it has two controllers 0/3/0 and 0/3/1.

IR8340 Configuration
In this solution, OSPF/EIGRP is used to exchange routes between the Routers after the Multilink interface is configured, and is up and running.

1. Configuring the Card Type

The T1/E1 network interface module will not be operational until a card type is configured.

card type t1 0 2   (if E1 is required, use no card type t1 and use E1)

2. Configure T1/E1 controller
controller T1 0/2/0
framing esf
framing clock source internal
framing linecode b8zs
framing cablelength long 0db
framing channel-group 2 timeslots 1-24

Similarly configure controller T1 0/2/1.

3. Configure Multilink interface
Interface multilink1
ip address x.x.x.x y.y.y.y
ppp multilink
ppp multilink group 1
ppp multilink endpoint string < m1p1>

4. Configure Serial interface 0/2/0 and 0/2/1 and bundle the interfaces to Multilink interface.

```
interface Serial 0/2/0:1
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

Similarly configure serial interface 0/2/1:1 and apply the ppp configuration.

Verifying the Multilink configuration

```
Router#sh ppp multilink interface Multilink 1

Multilink1
  Bundle name: mlp1
  Remote Endpoint Discriminator: [1] mlp1
  Local Endpoint Discriminator: [1] Router
  Bundle up for 19:10:19, total bandwidth 3072, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
  Bundle is Distributed
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 2 reordered
    0/0 discarded fragments/bytes, 0 lost received
  0x95D3 received sequence, 0x5B8E sent sequence
  Platform Specific Multilink PPP info
    NOTE: internal keyword not applicable on this platform
  Interleaving: Disabled, Fragmentation: Disabled
  Member links: 2 active, 0 inactive (max 16, min not set)
  Se0/2/0:2, since 19:10:18
    Se0/2/1:1, since 19:10:17
```

Exchange routes between routers using any Dynamic Routing Protocol, in this case EIGRP is used.

```
!
!
router eigrp 1
 router-id <loopback/Multilink address>
 network < x.x.x.x y.y.y.y>
!
!
```

WAN Redundancy

WAN Backhaul Redundancy over Cellular/Ethernet

In the Substation Router, secure tunnels are established with the HERs. A tunnel could be established over Cellular/Ethernet interface, with the tunnel terminating in the HER. The primary tunnel is established over a cellular interface. The secondary (or backup) tunnel is established over an Ethernet interface. The primary/backup tunnels would operate in active/standby mode, which means:

- Failover – if the primary tunnel fails, the secondary tunnel would be activated.
- Recovery – if the primary tunnel is up, the secondary tunnel would be de-activated
- The automatic failover/recovery is handled with the help of EEM

Backhaul Redundancy Configuration

The redundant configuration of the Substation router is described below.

- Tunnel 0 is the primary tunnel; it is established over the cellular interface
- Tunnel 1 is the secondary tunnel; it is established over the ethernet interface

Both tunnels use the same IPSec tunnel protection mode. Both the tunnels connect to the same public IP address configured on the HER. The configurations below are required to establish the FlexVPN tunnels, the tunnel configurations, and the interface configurations.

The following configuration, which uses the interface names that are applicable to IR8340, is applicable to other platforms using the appropriate interface naming convention applicable to the platform on which the configuration is applied.

```
!
interface Tunnel0
description Primary IPSec tunnel to HER1.ipg.cisco.com
ip unnumbered Loopback0
tunnel source Cellular0/4/0
tunnel destination <HER_Public_IP_address>
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
interface Tunnel1
description IPSec tunnel to HER1.ipg.cisco.com
ip unnumbered Loopback0
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet0/0/0
tunnel destination <HER_Public_IP_address>
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
interface Cellular0/4/0
mtu 1430
ip address negotiated
dialer in-band
dialer idle-timeout 0
dialer-group 1
ipv6 enable
pulse-time 1
!
interface GigabitEthernet0/0/0
ip address dhcp
```

!

EEM Script—Automatic Failover/Recovery

In a normal operational mode, the Substation Router connects to the HER securely via Tunnel 0 over Cellular interface. Tunnel 0 becomes the primary mode of communication between the Substation Router and the HER. If connectivity over the cellular interface fails, the communication between the router and the HER must be restored and secured. This restoration of connectivity between the router and the HER over a different medium (Ethernet) must be operational. This failover operation of the network helps minimize packet loss and enables secure connectivity over Tunnel 1. The activation of Tunnel 1 to carry the load in the event of Tunnel 0 failure is referred to as Failover.

When connectivity over cellular is restored, the router and the HER can communicate securely using Tunnel 0. This switchover from tunnel 1 to tunnel 0 is known as Recovery.

For the switchover to be automatic, EEM script is configured on the Substation Router. The EEM script tracks the line-protocol of the cellular interface. The following configuration is applied on the Router.

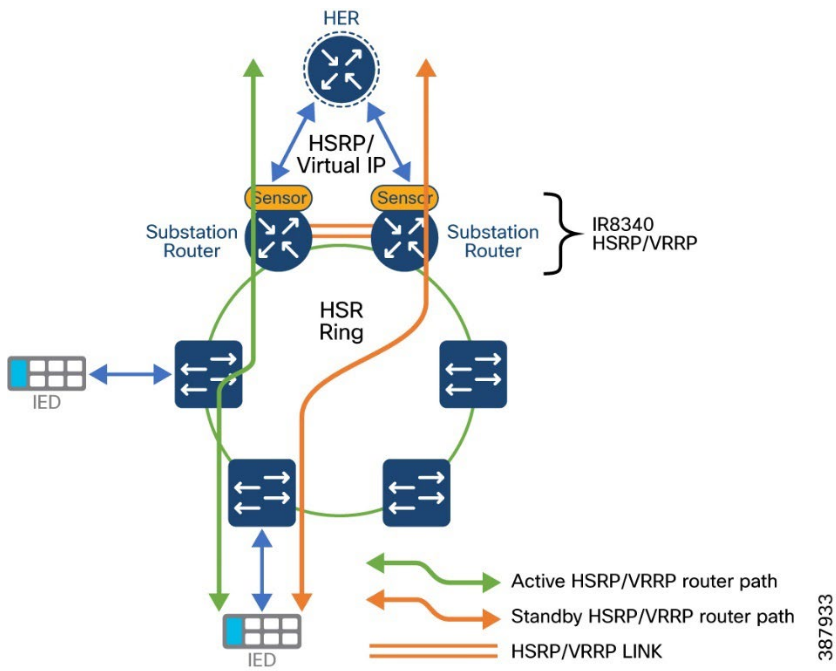
Note: The listed configuration is for reference purposes only.

```
!
!
track 20 interface Cellular0/4/0 line-protocol
delay down 5
!
event manager applet ACTIVATE_SECONDARY
event track 20 state down
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 200"
action 4 cli command "interface GigabitEthernet0/0/0 "
action 5 cli command "no shutdown"
action 6 cli command "end"
action 99 syslog msg "NOTE: Cellular down, switching to Ethernet "
!
event manager applet DEACTIVATE-SECONDARY
event track 20 state up
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface GigabitEthernet0/0/0 "
action 4 cli command "shutdown"
action 5 cli command "end"
action 99 syslog msg "NOTE: Connectivity Restored on Cellular"
!
!
```

Note: The above configuration is applicable to other substation router platforms and DA Gateways as well, with only difference being the change in the interface names across platforms.

Similarly, for the Cellular/Cellular, Cellular/MLPPP, MLPPP/MPLS the same EEM script can be used with appropriate changes.

Figure 11 HSRP/VRRP LAN Traffic Flow



HSRP

HSRP is the Cisco standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers.

HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

Note: Routers in an HSRP group can be any router interface that supports HSRP, including routed ports and switch virtual interfaces (SVIs).

HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over the routing duties when an active router fails or when preset conditions are met.

HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among router interfaces in a group of router interfaces running HSRP. The router selected by the protocol to be the active router receives and routes packets destined for the group MAC address. For *n* routers running HSRP, there are *n +1* IP and +MAC addresses assigned.

HSRP detects when the designated active router fails, and a selected standby router assumes control of the Hot Standby group MAC and IP addresses. A new standby router is also selected at that time. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are disabled by default for the interface.

You can configure multiple Hot Standby groups among switches that are operating in Layer 3 to make more use of the redundant routers. To do so, specify a group number for each Hot Standby command group you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

The topology in Figure 11 above shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router, configure them with the IP address of the virtual router as their default router. When IED sends packets to north bound it sends them to the MAC address of the virtual router. If for any reason, Active Router stops transferring packets, standby router responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. IED continues to use the IP address of the virtual router to address packets destined for North bound, which Router now receives and sends to Host. Until the earlier router resumes operation, HSRP allows existing active Router to provide uninterrupted service to IED that needs to communicate with Data center on segment and continues to perform its normal function of handling packets between the hosts.

HSRP Configuration

For detailed configuration of HSRP, refer the following document,

https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

In this Substation solution, 3 hot standby HSRP group has been configured for various LAN traffic redundancy.

In this solution following VLANs are used for various Substation Traffic,

VLAN 753 – For MMS

VLAN 754 – SCADA DNP3 traffic

VLAN 755 – for IPV4 traffic

The example configuration follows.

```
interface Vlan753
 ip address  x.x.x.1 y.y.y.y
 standby 3 ip x.x.x.10
 standby 3 priority 10
 standby 3 preempt
 standby 3 track 100 decrement 10
 standby 4 priority 10
!
interface Vlan754
 ip address  x.x.x.1 y.y.y.y
 standby 4 ip x.x.x.10
 standby 4 priority 10
 standby 4 preempt
 standby 4 track 100 decrement 10
!
interface Vlan755
 ip address  x.x.x.1 y.y.y.y
 standby 5 ip x.x.x.10
 standby 5 priority 10
 standby 5 preempt
 standby 5 track 100 decrement 10
```

here the track command is used to check active routers reachability, if the reachability to the destination is fails, the priority will be decremented, and the standby becomes active router.

The reachability validation is made from WAN interface of the active router to the HER, if the reachability failed to HER from the active router's WAN interface, the standby router would become active, once the reachability is restored, it will do an automatic failover recovery.

WAN interface Configuration,

```
interface GigabitEthernet0/0/0
 description connected to HER on G0/2/6
 ip address x.x.x.x 255.255.255.0
sbfd interval 150 min_rx 450 multiplier 3
end
```

Track CLI configuration is as follows,

"track 100 ip route x.x.x.x 255.255.255.255 reachability"

Similarly on the other router, enable HSRP with less priority than '10' and make it as standby router. Once the Configurations are done on both the redundant routers, the one with highest priority becomes the active router.

To verify the HSRP after configuring 2 Groups:

```
Router# show standby
VLAN753 - Group 1
Local state is Standby, priority 9, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 192.168.x.x configured
Active router is 192.168.x.x expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01

VLAN754 - Group 2
Local state is standby, priority 9, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 192.168.x.x configured
Active router is 192.168.x.x expires in 00:00:05
Standby router is local
Standby virtual mac address is 0000.0c07.ac64
```

Best practices for configuring HSRP

One important factor to consider when tuning HSRP is its preemptive behavior. Preemption causes the primary HSRP peer to re-assume the primary role when it comes back online after a failure or maintenance event.

Preemption is the desired behavior because the STP/RSTP root should be the same device as the HSRP primary for a given subnet or VLAN. If HSRP and STP/RSTP are not synchronized, the interconnection between the distribution switches can become a transit link, and traffic takes a multi-hop L2 path to its default gateway.

HSRP preemption needs to be aware of switch boot time and connectivity to the rest of the network. It is possible for HSRP neighbor relationships to form and preemption to occur before the primary switch has L3 connectivity to the core. If this happens, traffic can be dropped until full connectivity is established.

The recommended best practice is to measure the system boot time and set the HSRP preempt delay statement to 50 percent greater than this value. This ensures that the HSRP primary distribution node has established full connectivity to all parts of the network before HSRP preemption is allowed to occur.

VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails.

VRRP Limitations

- The switch supports either HSRP or VRRP, but not both. The switch cannot join a stack that has both HSRP and VRRP configured.
- The VRRP implementation on the switch supports only text -based authentication.
- You cannot enable VRRP for IPv4 and IPv6 groups simultaneously.

Refer to details configuration and troubleshooting steps for VRRP below.

https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40crs1book_chapter10.html#:~:text=VRRP%20is%20an%20IP%20routing,router%20as%20their%20default%20gateway.

Example configurations follow.

```
!
interface Vlan751
 ip address x.x.x.1 255.255.255.0
 vrrp 1 ip x.x.x.x
 vrrp 1 timers advertise msec 150
 vrrp 1 track 1 decrement 20
```

```
end

interface Vlan752
 ip address x.x.x.1 255.255.255.0
 vrrp 1 ip x.x.x.x
 vrrp 1 timers advertise msec 150
 vrrp 1 track 1 decrement 20
end
!
```

To verify VRRP

```
Router#sh vrrp all
Vlan751 - Group 1
State is Master
  Virtual IP address is 192.168.x.100
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 0.150 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.x.1 (local), priority is 100
  Master Advertisement interval is 0.150 sec
  Master Down interval is 1.059 sec
  FLAGS: 1/1

Vlan752 - Group 2
  State is Master
  Virtual IP address is 192.168.x.100
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 0.150 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.x.1 (local), priority is 100
  Master Advertisement interval is 0.150 sec
  Master Down interval is 1.059 sec
  FLAGS: 1/1
```

Best Practices and Restrictions

- VRRP is designed for use over multi-access, multicast, or broadcast capable Ethernet LANs. VRRP is not intended as a replacement for existing dynamic protocols.
- VRRP is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.
- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must configure the VRRP advertise timer to a value equal to or greater

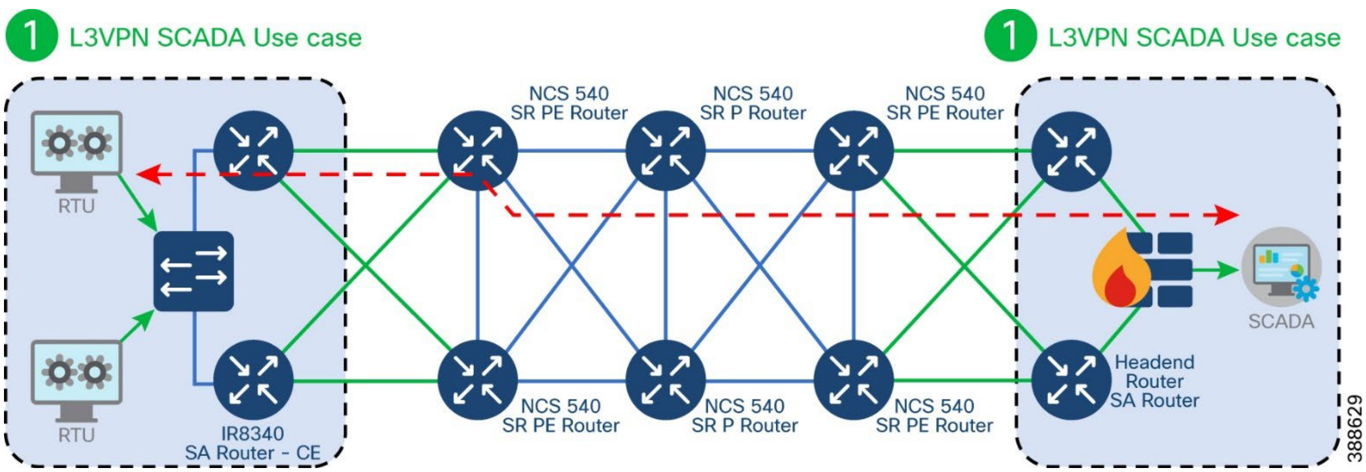
than the forwarding delay on the BVI interface. This setting prevents a VRRP router on a recently initialized BVI interface from unconditionally taking over the master role. Use the bridge forward-time command to set the forwarding delay on the BVI interface. Use the VRRP timers advertise command to set the VRRP advertisement time.

Segment Routing for Substation WAN

Earlier versions of Substation Automation Wide Area Network designs utilized MPLS for its core. The solution provided different roles for Substation router viz a customer edge router or a provider edge router in an ON-NET Substation model and as a Customer Edge router in an OFF-NET Substation model that utilized cellular backhaul. Various services were enabled from these routers in different roles. This guide proposes the use of Segment Routing over MPLS enabled network for various services as described previously in this guide.

IR8340 Substation Router as CE over SR

Figure 12 IR8340 Substation Router as CE over SR



In the above topology, the IR8340 router acts as a CE router with L3VPN services enabled for different services like SCADA, Physical Security, Network Management, and so on, using unique virtual routing and forwarding instances. OSPF or EIGRP or eBGP or static routing can be used to exchange VRF routes. NCS540 is configured as a Provider edge. NCS540 is also used as a P router in the core. Different services like SCADA, Network Management, and so on, are provisioned with different SVIs. The SVIs are part of the Layer 2 Resiliency network that are part of the Substation LAN network. Refer to the relevant sections for configuration steps of different resiliency protocols that can be used as per the requirements. Cisco IR8340 acts as the Layer 3 gateway to these different services.

Steps to configure:

1. Identify the services that need to be provided. Configure VRFs if required.

   VRF Instance:

```
!
ip vrf SCADA_RAW_SOCKET
 rd 803:1
 route-target export 803:1
```

```
 route-target import 803:1
!
ip vrf forwarding
!

!
interface Serial0/3/0
 physical-layer async
 ip vrf forwarding SCADA_RAW_SOCKET
 no ip address
 encapsulation scada
!
```

2. Identify the WAN facing interface on IR8340 and configure VRF. This interface is connected to NCS540 acting as PE.

   WAN Interface Ethernet:

```
!
interface GigabitEthernet0/0/0.103
 encapsulation dot1Q 103
 ip vrf forwarding SCADA_RAW_SOCKET
 ip address 15.15.15.2 255.255.255.0
!
```

3. Configure loopback interface required for BGP. Enable BGP on the IR8340 acting as CE . BGP peer is the NCS540 acting as PE node.

   IR8340 BGP Configuration:

```
!
interface Loopback803
 ip address 80.3.1.1 255.255.255.255
!

!
router bgp 803
 bgp router-id 80.3.1.1
 bgp log-neighbor-changes
 !
 address-family vpnv4
 exit-address-family
 !
 address-family ipv4 vrf SCADA_RAW_SOCKET
  redistribute connected
  neighbor 15.15.15.1 remote-as 600
  neighbor 15.15.15.1 ebgp-multihop 255
  neighbor 15.15.15.1 activate
 exit-address-family
!
```

4. Identify and configure the CE connecting interface on NCS540.

CE-PE Interface:

```
!
interface GigabitEthernet0/0/0/2.103
 vrf SCADA_RAW_SOCKET
 ipv4 address 15.15.15.1 255.255.255.0
 encapsulation dot1q 103
!
```

5. Identify and configure the core facing interface on NCS540.

Core Facing Interface:

```
!
interface TenGigE0/0/0/7
 ipv4 address 192.168.82.2 255.255.255.0
!
```

VRF Instance:

```
!
vrf SCADA_RAW_SOCKET
 address-family ipv4 unicast
  import route-target
   803:1
  !
  export route-target
   803:1
  !
 !
!
address-family ipv4 unicast
!
```

6. Enable Segment Routing at the global level before enabling Segment routing under IGP. The following configuration shows an example of segment routing and ospf as IGP.

Segment Routing Related Configuration:

```
!
segment-routing
 global-block 16000 24000
!
lldp
!

!
router ospf 1
 router-id 192.168.201.7
```

```
segment-routing mpls
area 0
 segment-routing mpls
 interface Loopback0
 network point-to-point
 prefix-sid index 7
 !
 interface TenGigE0/0/0/7
  network point-to-point
 !
!
!
```

7. [Optional] ISIS can also be used in place of OSPF as IGP protocol. If L3VPN services demand sub 50millisecond convergence FRR can be enabled.

```
!
router isis 1008
is-type level-2-only
net 49.0001.0000.0000.0001.00
distribute link-state
log adjacency changes
address-family ipv4 unicast
  metric-style wide
  router-id Loopback0
  segment-routing mpls
!
interface Loopback0
  address-family ipv4 unicast
  prefix-sid index 101
  !
!
interface TenGigE0/0/0/14
  point-to-point
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
   adjacency-sid index 11
  !
!
interface TenGigE0/0/0/15
  point-to-point
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
   adjacency-sid index 16
  !
!
interface TenGigE0/0/0/17
  point-to-point
  address-family ipv4 unicast
```

```
  fast-reroute per-prefix
  fast-reroute per-prefix ti-lfa
  adjacency-sid index 17
 !
!
!
```

8. Enable BGP route policy that should be applied for prefixes advertised using BGP. Enable BGP.

```
!
route-policy SID($SID)
set label-index $SID
end-policy
!
route-policy PASS_ALL
  pass
end-policy
!
```

BGP Configuration:

```
!
router bgp 600
 bgp router-id 192.168.201.7
 address-family ipv4 unicast
  network 2.2.2.2/32 route-policy SID(10)
  network 18.18.18.0/24 route-policy SID(11)
  allocate-label all
 !
 address-family vpnv4 unicast
 !
 address-family l2vpn evpn
!
!
 vrf SCADA_RAW_SOCKET
  rd 803:1
  address-family ipv4 unicast
   redistribute connected
  !
  neighbor 15.15.15.2
   remote-as 803
   ebgp-multihop 2
   update-source GigabitEthernet0/0/0/2.103
   address-family ipv4 unicast
    route-policy PASS_ALL in
    route-policy PASS_ALL out
    next-hop-self
   !
  !
 !
```

!

Best Practices

1. It is recommended to identify the type of interface required to achieve the scale, latency and jitter requirements for the intended traffic over SR core. IR8340 supports 1Gig WAN interface, whereas NCS540 supports 1G, 10G,25G and 40G interfaces. This test was carried out using 1G and 10G interfaces.

2. It is recommended to ensure that the number of hops in the network from end to end does not exceed 20 hops and a max distance of 500km.

3. It is recommended to enable appropriate features like SR PM hardware-offload for 3.3milliseconds, TI-LFA FRR under IGP to help achieve less than 50 milliseconds convergence in case of network failure in the core.

4. It is recommended to enable appropriate QoS policies, both INGRESS and EGRESS for both access and core facing interfaces classifying various traffic flows as per the requirement and treating appropriately.

5. It is recommended to ensure that IR8340 is not part of the segment routed core network handling all the traffic. IR8340 should be positioned as a spur to the Segment routing enabled core as can be noted in the above figure.

Verification

```
RP/0/RP0/CPU0:NCS-PE-001#show mpls forwarding prefix 192.168.201.8
255.255.255.255
Mon Apr 17 08:18:07.835 UTC
Local  Outgoing    Prefix           Outgoing     Next Hop        Bytes
Label  Label       or ID            Interface                    Switched
------------- ------------- --------------- ------------------- ---------
16002  16002       SR Pfx (idx 2)   Te0/0/0/7    192.168.82.1    2647790
RP/0/RP0/CPU0:NCS-PE-001#show mpls forwarding prefix 192.168.201.8
255.255.255.255 detail
Mon Apr 17 08:18:11.616 UTC
Local  Outgoing    Prefix           Outgoing     Next Hop        Bytes
Label  Label       or ID            Interface                    Switched
------------- ------------- --------------- ------------------- ---------
16002  16002       SR Pfx (idx 2)   Te0/0/0/7    192.168.82.1    2647790
     Updated: Mar 31 04:22:41.059
     Version: 56, Priority: 1
     Label Stack (Top -> Bottom): { 16002 }
     NHID: 0x0, Encap-ID: 0x1185100000002, Path idx: 0, Backup path idx: 0,
Weight: 0
     MAC/Encaps: 14/18, MTU: 1500
     Outgoing Interface: TenGigE0/0/0/7 (ifhandle 0x3c0000a8)
     Packets Switched: 49437
```

```
  Traffic-Matrix Packets/Bytes Switched: 0/0
RP/0/RP0/CPU0:NCS-PE-001#


RP/0/RP0/CPU0:NCS-PE-001#ping 192.168.201.8
Mon Apr 17 08:13:48.945 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.8 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
RP/0/RP0/CPU0:NCS-PE-001#
RP/0/RP0/CPU0:NCS-PE-001#
RP/0/RP0/CPU0:NCS-PE-001#traceroute 192.168.201.8
Mon Apr 17 08:13:54.396 UTC
Type escape sequence to abort.
Tracing the route to 192.168.201.8
 1  192.168.82.1 [MPLS: Label 16002 Exp 0] 2 msec  2 msec  2 msec
2  192.168.73.1 [MPLS: Label 16002 Exp 0] 2 msec  2 msec  1 msec
3  192.168.72.1 [MPLS: Label 16002 Exp 0] 1 msec  2 msec  1 msec
4  192.168.71.1 [MPLS: Label 16002 Exp 0] 1 msec  1 msec  3 msec
5  192.168.83.2 2 msec  *  2 msec
RP/0/RP0/CPU0:NCS-PE-001#


RP/0/RP0/CPU0:NCS-PE-002#show mpls forwarding pre 192.168.201.7
255.255.255.255
Mon Apr 17 08:11:44.496 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------------------------------------------------------------------------------
16007  16007       SR Pfx (idx 7)     Te0/0/0/7    192.168.83.1    2645708
RP/0/RP0/CPU0:NCS-PE-002#

RP/0/RP0/CPU0:NCS-PE-002#show mpls forwarding pre 192.168.201.7
255.255.255.25$
Mon Apr 17 08:11:49.885 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------------------------------------------------------------------------------
16007  16007       SR Pfx (idx 7)     Te0/0/0/7    192.168.83.1    2645708
     Updated: Mar 31 04:10:33.119
     Version: 48, Priority: 1
     Label Stack (Top -> Bottom): { 16007 }
     NHID: 0x0, Encap-ID: 0x1184700000002, Path idx: 0, Backup path idx: 0,
Weight: 0
     MAC/Encaps: 14/18, MTU: 1500
     Outgoing Interface: TenGigE0/0/0/7 (ifhandle 0x3c0000a8)
     Packets Switched: 49387
  Traffic-Matrix Packets/Bytes Switched: 0/0
RP/0/RP0/CPU0:NCS-PE-002#
```

```
RP/0/RP0/CPU0:NCS-PE-002#ping 192.168.201.7
Mon Apr 17 08:06:01.865 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.201.7 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
RP/0/RP0/CPU0:NCS-PE-002#
RP/0/RP0/CPU0:NCS-PE-002#traceroute 192.168.201.7
Mon Apr 17 08:06:07.262 UTC
Type escape sequence to abort.
Tracing the route to 192.168.201.7
 1  192.168.83.1 [MPLS: Label 16007 Exp 0] 2 msec  2 msec  1 msec
2  192.168.71.2 [MPLS: Label 16007 Exp 0] 2 msec  2 msec  1 msec
3  192.168.72.2 [MPLS: Label 16007 Exp 0] 2 msec  1 msec  1 msec
4  192.168.73.2 [MPLS: Label 16007 Exp 0] 2 msec  3 msec  6 msec
5  192.168.82.2 2 msec  *  3 msec
RP/0/RP0/CPU0:NCS-PE-002#
```

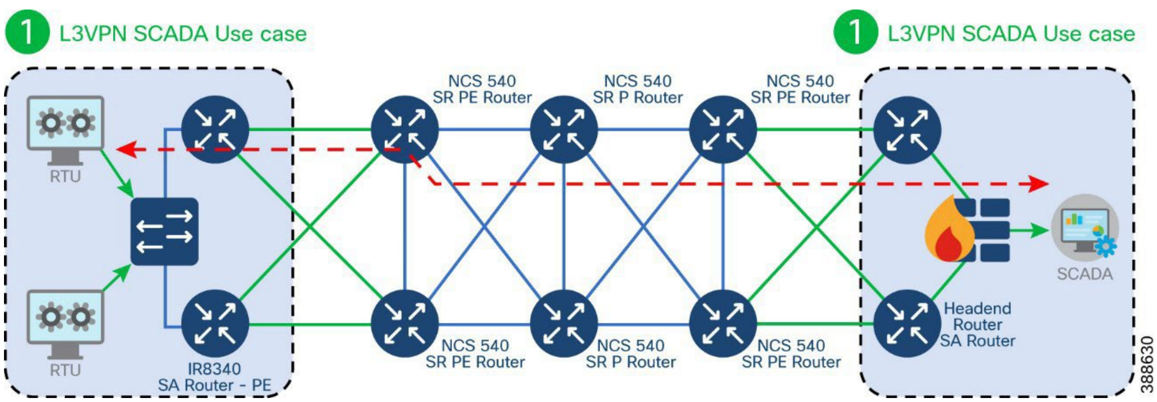
```
SA-WAN-CE-001#show ip route vrf SCADA
Routing Table: SCADA
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is not set
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.13.14.0/24 is directly connected, TenGigabitEthernet0/1/0.101
L        13.13.14.2/32 is directly connected, TenGigabitEthernet0/1/0.101
      14.0.0.0/24 is subnetted, 1 subnets
B        14.14.15.0 [20/0] via 13.13.14.1, 3d08h
SA-WAN-CE-001#
```

```
SA-WAN-CE-001#traceroute vrf SCADA 14.14.15.1
Type escape sequence to abort.
Tracing the route to 14.14.15.1
VRF info: (vrf in name/id, vrf out name/id)
  1 13.13.14.1 1 msec 1 msec 1 msec
  2 192.168.82.1 [MPLS: Labels 16002/24004 Exp 0] 2 msec 1 msec 1 msec
  3 192.168.73.1 [MPLS: Labels 16002/24004 Exp 0] 1 msec 1 msec 1 msec
  4 192.168.72.1 [MPLS: Labels 16002/24004 Exp 0] 1 msec 2 msec 0 msec
  5 192.168.71.1 [MPLS: Labels 16002/24004 Exp 0] 1 msec 1 msec 1 msec
  6 192.168.83.2 1 msec 1 msec 1 msec
```

```
 7 14.14.15.1 1 msec 1 msec *
SA-WAN-CE-001#


RP/0/RP0/CPU0:NCS-PE-002#show mpls forwarding vrf SCADA
Mon Apr 17 14:01:09.108 UTC
Local  Outgoing    Prefix          Outgoing      Next Hop       Bytes
Label  Label       or ID           Interface                    Switched
-----------------------------------------------------------------------
24004  Aggregate   SCADA: Per-VRF Aggr[V]   \
                           SCADA                    276
RP/0/RP0/CPU0:NCS-PE-002#
```

IR8340 Substation Router as PE over SR

Figure 13 IR8340 Substation Router as PE over SR



In the above topology, IR8340 router acts as a PE router with L3VPN services enabled for different services like SCADA, Physical Security, Network Management, etc., using unique virtual routing and forwarding instances. OSPF is used as IGP and BGP is used to exchange VRF routes. NCS540 is configured as a Provider edge. NCS540 is also used as a P router in the core. Different services like SCADA, Network Management, and so on, are provisioned with different SVIs. The SVIs are part of the Layer 2 Resiliency network that are part of the Substation LAN network. Refer to the relevant sections for configuration steps of different resiliency protocols that can be used as per requirements.

Cisco IR8340 acts as the Layer 3 gateway to these different services. It is not recommended to position IR8340 with Layer3 Segment Routing as part of the active SR data path that may transmit higher throughput of traffic from across the SR network. It is recommended to position IR8340 as a separate SR enabled PE node attached to the SR enabled core network.

IR8340 as PE:

Following are the configuration steps on IR8340 acting as PE with SR enabled.

1. Configure loopback and WAN facing interface.

```
!
```

```
interface Loopback0
ip address 192.168.201.15 255.255.255.255
!

!
interface GigabitEthernet0/0/1
description connected NCS-PE-002 GigabitEthernet0/0/0/18
ip address 192.168.97.1 255.255.255.0
ip ospf network point-to-point
load-interval 30
negotiation auto
mpls ip
mpls label protocol ldp
!
```

2. Identify the services and configure respective VRFs if required.

3. Globally enable segment routing on IR8340 acting as PE.

```
!
segment-routing mpls
!
set-attributes
  address-family ipv4
  sr-label-preferred
  exit-address-family
!
global-block 16000 24000
!
connected-prefix-sid-map
  address-family ipv4
   192.168.201.15/32 index 14 range 1
  exit-address-family
!
```

4. Configure IGP. This example shows OSPF as the IGP.

```
!
router ospf 1
router-id 192.168.201.15
nsr
nsf
segment-routing mpls
network 192.168.96.0 0.0.0.255 area 0
network 192.168.97.0 0.0.0.255 area 0
network 192.168.201.15 0.0.0.0 area 0
!
```

5. Enable iBGP session with other peer PE nodes. Ensure that the traffic from other parts of the segment routing is not routed via IR8340.

```
!
router bgp 600
```

```
bgp router-id 192.168.201.15
bgp log-neighbor-changes
neighbor 192.168.201.8 remote-as 600
neighbor 192.168.201.8 update-source Loopback0
neighbor 192.168.201.12 remote-as 600
neighbor 192.168.201.12 update-source Loopback0
neighbor 192.168.201.25 remote-as 600
neighbor 192.168.201.25 update-source Loopback0
!
address-family ipv4
 redistribute connected
 neighbor 192.168.201.8 activate
 neighbor 192.168.201.8 next-hop-self
 neighbor 192.168.201.12 activate
 neighbor 192.168.201.12 next-hop-self
 neighbor 192.168.201.25 activate
 neighbor 192.168.201.25 next-hop-self
exit-address-family
!
address-family vpnv4
 neighbor 192.168.201.8 activate
 neighbor 192.168.201.8 send-community extended
 neighbor 192.168.201.8 next-hop-self
 neighbor 192.168.201.12 activate
 neighbor 192.168.201.12 send-community extended
 neighbor 192.168.201.12 next-hop-self
 neighbor 192.168.201.25 activate
 neighbor 192.168.201.25 send-community extended
 neighbor 192.168.201.25 next-hop-self
exit-address-family
!
address-family ipv4 vrf TEST_1
 redistribute connected
exit-address-family
!
```

6. Refer to IR8340 as CE section for the configurations related to NCS540 as PE.

Best Practices

1) It is recommended to identify the type of interface required to achieve the scale, latency and jitter requirements for the intended traffic over SR core. IR8340 supports 1Gig WAN interface, whereas NCS540 supports 1G, 10G,25G and 40G interfaces. This test was carried out using 1G and 10G interfaces

2) It is recommended to ensure that the number of hops in the network from end to end does not exceed 20 hops and a max distance of 500km.

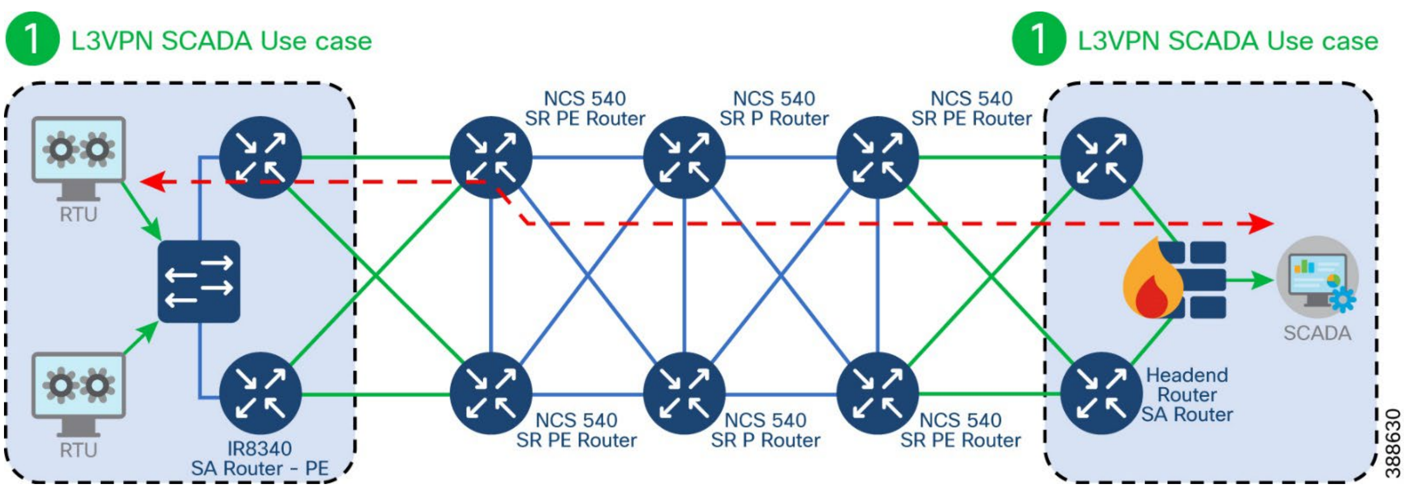
3) It is recommended to enable appropriate features like SR PM hardware-offload for 3.3milliseconds liveliness monitoring, BFD, TI-LFA FRR under IGP to help achieve less than 50 milliseconds convergence in case of network failure in the core.

4) It is recommended to enable appropriate QoS policies, both INGRESS and EGRESS for both access and core facing interfaces classifying various traffic flows as per the requirement and treating appropriately.

5) It is recommended to ensure that IR8340 is not part of the segment routed core network handling all the traffic. IR8340 should be positioned as a spur to the Segment routing enabled core as can be noted in the above figure.

IE9300 as L2 Customer Edge

Figure 14 Dual IE9300 as L2 Gateway for L2 Teleprotection services with CS - SR



The guide recommends positioning Cisco IE9300 as Layer 2 Substation LAN aggregation Edge device in BGP L2 EVPN deployment scenarios. As depicted in the above topology, to cater to the L2 Teleprotection use case with CE Resiliency, each CE is connected to one PRP LAN (LAN A or LAN B, not both). The CE IE9300s are not enabled with PRP redundancy and therefore each CE acts as a plain switch. One EVPN VPWS service extends PRP LAN A between the two substations, while the second EVPN VPWS service extends the PRP LAN B between the two. Single homed EVPN VPWS service with Preferred Path steering to a CS SR-TE policy is the building block for the CE Resiliency architecture design.

Following are the configuration steps.

Identify the VLANs that are required for different services. Identify the interface that needs to be connected to the NCS540 acting as PE and configure it as trunk port. Ensure the VLANs are enabled on the switch. Repeat the step on the resilient IE9300 connected to a resilient NCS540 acting as PE.

```
!
interface GigabitEthernet2/0/9
description connected to Fitzroy1 GigabitEthernet0/0/0/10
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
load-interval 30
carrier-delay msec 1
end
!
```

1. PRP LAN A and PRP LAN B switches are simple infrastructure switches with the respective VLANs enabled. Relevant interfaces are configured as trunk ports.
2. These PRP LAN A and PRP LAN B switches can help provide resiliency for PRP redboxes that need to be connected as depicted in the figure above.
3. Repeat the above steps on the other Substation LAN network if required.
4. Configure IE9300 facing interface on NCS540 acting as PE router. Repeat the step on the other NCS PE connecting to the resilient IE9300.

```
!
interface GigabitEthernet0/0/0/10
description "Connected to IE9300-1"
negotiation auto
l2transport
!
!
```

5. Globally enable segment routing on PE routers.As mentioned above, this scenario requires hw-offload and EVPN VPWS service with Preferred Path steering to a CS SR-TE policy for the CE Resiliency architecture design.

```
!
segment-routing
global-block 16000 23999
traffic-eng
 segment-list cs-protect-bck
  index 1 mpls label 15014
  index 2 mpls label 15017
 !
 segment-list cs-protect-fwd
  index 1 mpls label 15017
  index 2 mpls label 15014
 !
 segment-list cs-working-bck
  index 1 mpls label 15025
  index 2 mpls label 15016
```

```
   !
   segment-list cs-working-fwd
    index 1 mpls label 15016
    index 2 mpls label 15025
   !
   policy srte_1_ep_5.5.5.5
    color 1 end-point ipv4 5.5.5.5
    path-protection
    !
    candidate-paths
     preference 50
      explicit segment-list cs-protect-fwd
       reverse-path segment-list cs-protect-bck
      !
      lock
       duration 30
      !
     !
     preference 100
      explicit segment-list cs-working-fwd
       reverse-path segment-list cs-working-bck
      !
     !
    !
    performance-measurement
     liveness-detection
      liveness-profile backup name protect
      liveness-profile name working
     !
    !
   !
   pcc
    source-address ipv4 1.1.1.1
    pce address ipv4 4.4.4.4
    !
   !
!
!
lldp
!
performance-measurement
liveness-profile name protect
liveness-detection
   multiplier 3
  !
  probe
   tx-interval 100000
  !
!
liveness-profile name working
  liveness-detection
```

```
  multiplier 3
 !
 probe
  tx-interval 3300
 !
 npu-offload
  enable
 !
!
!

hw-module profile offload 4
```

6. Configure BGP with L2VPN service.

```
!
router bgp 110
bgp router-id 1.1.1.1
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
address-family l2vpn evpn
!
neighbor 3.3.3.3
  remote-as 110
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
   next-hop-self
  !
  address-family l2vpn evpn
  !
!
!
```

7. Identify the EVPN VPWS source and destination points. Use the relevant CS SR TE policy and create the service.

```
!
l2vpn
pw-class G-link-1
  encapsulation mpls
   preferred-path sr-te policy srte_c_1_ep_5.5.5.5 fallback disable
  !
!
xconnect group evpn-vpws-1
  p2p evpn-ixia-connect
   interface GigabitEthernet0/0/0/10
   neighbor evpn evi 115 target 22 source 20
```

```
    pw-class G-link-1
   !
  !
!
!
```

Best Practices

1. It is recommended to identify the type of interface required to achieve the scale, latency and jitter requirements for the intended traffic over SR core. IR8340 supports 1Gig WAN interface, whereas NCS540 supports 1G, 10G,25G and 40G interfaces. This test was carried out using 1G and 10G interfaces.
2. It is recommended to ensure that the number of hops in the network from end to end does not exceed 20 hops and a max distance of 500km.
3. It is recommended to enable appropriate features like SR PM hardware-offload for 3.3milliseconds liveliness monitoring, TI-LFA FRR under IGP to help achieve less than 50 milliseconds convergence in case of network failure in the core.
4. It is recommended to enable appropriate QoS policies, both INGRESS and EGRESS for both access and core facing interfaces classifying various traffic flows as per the requirement and treating appropriately.
5. It is recommended to ensure that IR8340 is not part of the segment routed core network handling all the traffic. IR8340 should be positioned as a spur to the Segment routing enabled core as can be noted in the above figure.

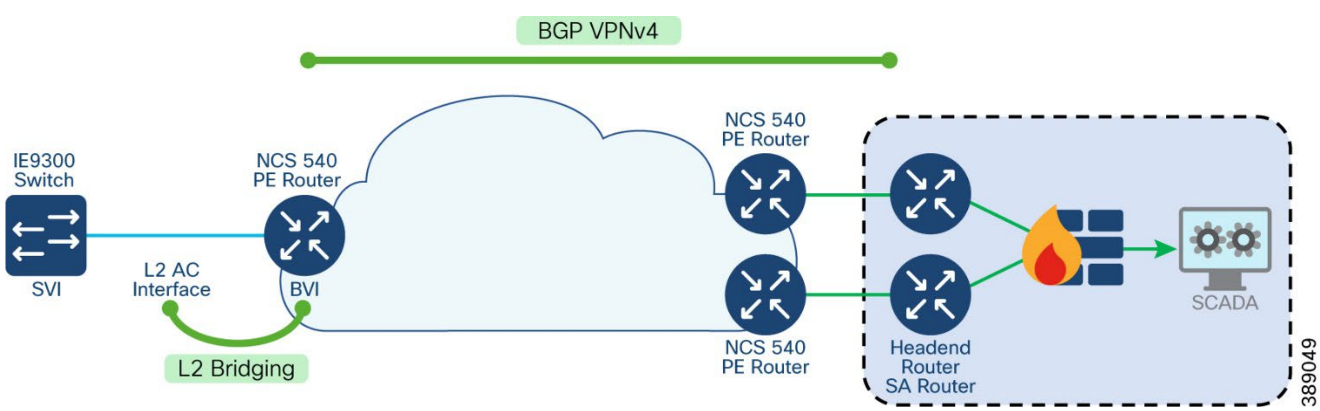
Verification

```
RP/0/RP0/CPU0:NCS-PE-001#show l2vpn xconnect group evpn-vpws-1

Thu Oct  3 09:06:21.660 IST

Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,

        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed,

        LU = Local Up, RU = Remote Up, CO = Connected, (SI) = Seamless Inactive


XConnect                Segment 1                 Segment 2

Group      Name       ST   Description          ST      Description          ST

------------------------   ----------------------------   ----------------------------
```

```
evpn-vpws-1

     evpn-ixia-connect

          UP   Gi0/0/0/10        UP      EVPN 115,22,5.5.5.5

                                              UP

-----------------------------------------------------------------------------------------



RP/0/RP0/CPU0:NCS-PE-001#show segment-routing traffic-eng policy tabular

Tue Oct  8 09:39:05.909 IST


 Color                      Endpoint  Admin   Oper           Binding

                                  State  State               SID

------ ------------------------------------ ------ ------ ----------------------

   1                        5.5.5.5     up     up              24115
```

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

Figure 15 Substation LAN to Control Centre Reachability(L3) via NCS540 WAN using IRB



IRB can be implemented by making use of BVI interface on NCS540. The BVI is a virtual interface within the router that acts like a normal routed interface. BVI provides a link between the bridging and the routing domains on the router. The BVI does not support bridging itself, but acts as a gateway for the corresponding bridge-domain to a routed interface within the router. Bridge-Domain is a layer 2 broadcast domain. It is associated to a bridge group using the *routed interface bvi* command.

The following are the steps to configure:

1. Identify the VLANs that are required for different services. Identify the interface that needs to be connected to the NCS540 acting as PE and configure it as Layer2 AC Interface. Ensure the VLANs are enabled on the switch. Repeat the step on the resilient IE9300 connected to a resilient NCS540 acting as PE.

```
interface GigabitEthernet0/0/0/4.4001 l2transport
encapsulation dot1q 4001
rewrite ingress tag pop 1 symmetric
!
```

2. Configure Bridge Group Virtual Interface on NCS540 for the corresponding VLAN. Configure it as part of VRF to isolate it from global route table.

```
interface BVI4001
 vrf SCADA
  ipv4 address 192.168.143.1 255.255.255.248
 load-interval 30
!
```

3. Be sure that the BVI network address is being advertised by running static or dynamic routing on the BVI interface. We are using BGP route redistribution to advertise the route.

```
router bgp 600
 address-family vpnv4 unicast
   next-hop-self
   route-policy PASS_ALL in
   route-policy PASS_ALL out
 neighbour <>
 address-family vpnv4 unicast
   next-hop-self
 vrf SCADA
  address-family ipv4 unicast
   redistribute connected
  !
 !
!
```

4. Configure SVI on IE9300 for corresponding VLAN in same subnet as IRB in NCS540.

```
 interface Vlan4001
 ip address 192.168.143.2 255.255.255.248
end
```

5. Add static routes on IE9300 for networks (Management Servers/ Control Centers) that need to be reached from the device.

```
ip route 192.168.169.0 255.255.255.0 192.168.143.1
```

6. Associate the BVI as the Routed Interface on a Bridge Domain on NCS540

```
l2vpn
bridge group CyberVision
  bridge-domain CV-1
   interface GigabitEthernet0/0/0/4.4001
   !
   routed interface BVI4001
   !
  !
!
!
```

Best Practices

1. It is recommended to identify the type of interface required to achieve the scale, latency, and jitter requirements for the intended traffic over SR core. IR8340 supports 1Gig WAN interface, whereas NCS540 supports 1G, 10G,25G and 40G interfaces. This test was carried out using 1G and 10G interfaces.

2. It is recommended to ensure that the number of hops in the network from end to end does not exceed 20 hops and a max distance of 500km.

3. It is recommended to enable appropriate features like SR PM hardware-offload for 3.3milliseconds liveliness monitoring, TI-LFA FRR under IGP to help achieve less than 50 milliseconds convergence in case of network failure in the core.

4. It is recommended to enable appropriate QoS policies, both INGRESS and EGRESS for both access and core facing interfaces classifying various traffic flows as per the requirement and treating appropriately. Refer to the document referenced below for more information on configuration and restrictions:

   https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/qos/24xx/b-qos-cg-24xx-ncs540/qos-on-bridge-group-virtual-interface.html

5. It is recommended to implement security measures such as ACLs to control incoming and outgoing traffic on the BVI. Proper security configurations help in mitigating potential threats.

   Refer to the tutorial below for more information:

   https://xrdocs.io/ncs5500/tutorials/acl-s-on-ncs5500-bvi-interfaces/

Verifications

```
RP/0/RP0/CPU0:NCS-PE-001#show l2vpn bridge-domain group CyberVision
Mon Oct  7 09:40:14.428 IST
Legend: pp = Partially Programmed.
Bridge group: CyberVision, bridge-domain: CV-1, id: 1, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 64000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of ACs:
    BV4001, state: up, BVI MAC addresses: 1
    Gi0/0/0/4.4001, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
  List of Access VFIs:

RP/0/RP0/CPU0:NCS-PE-001#show interfaces bvI 4001 detail
Wed Oct  9 09:20:13.548 IST
BVI4001 is up, line protocol is up
  Interface state transitions: 137
  Hardware is Bridge-Group Virtual Interface, address is a410.b6d7.6b82
  Description: CyberVision reachability to PRP-Network
  Internet address is 192.168.143.1/29
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,  loopback not set,
  Last link flapped 22:05:21
  ARP type ARPA, ARP timeout 04:00:00
  Last input Unknown, output Unknown
  Last clearing of "show interface" counters Unknown
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec


RP/0/RP0/CPU0:NCS-PE-001#show adjacency bvi 4001 detail
Wed Oct  9 09:20:20.315 IST
-------------------------------------------------------------------------------
0/RP0/CPU0
-------------------------------------------------------------------------------
Interface                   Address                  Version  Refcount Protocol
BV4001                      192.168.143.2            2619        3(    0) ipv4
                            84ebef6164dda410b6d76b820800
                            mtu: 1500, flags 1 0


BV4001                      (src mac only)           2617        2(    0) ipv4
                            000000000000a410b6d76b820800
```

```
                 mtu: 1500, flags 1 1
BV4001                (interface)              33       1(    0)
                 (interface entry)
                 mtu: 1500, flags 1 4

RP/0/RP0/CPU0:NCS-PE-001#show ip route vrf SCADA 192.168.143.2
Wed Oct  9 09:14:30.302 IST

Routing entry for 192.168.143.0/29
  Known via "connected", distance 0, metric 0 (connected)
  Installed Oct  8 11:14:52.321 for 21:59:38
  Routing Descriptor Blocks
    directly connected, via BVI4001
      Route metric is 0
  No advertising protos.
RP/0/RP0/CPU0:NCS-PE-001#

RP/0/RP0/CPU0:NCS-PE-001#show ip route vrf SCADA 192.168.169.1
Wed Oct  9 09:14:08.346 IST

Routing entry for 192.168.169.0/24
  Known via "bgp 600", distance 200, metric 0
  Tag 200, type internal
  Installed Sep 16 11:54:24.996 for 3w1d
  Routing Descriptor Blocks
    192.168.201.1, from 192.168.201.17
      Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
      Route metric is 0
  No advertising protos.

RP/0/RP0/CPU0:NCS-PE-001#ping vrf SCADA 192.168.143.2
Wed Oct  9 09:14:48.422 IST
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.143.2 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

IE9300-002#ping 192.168.143.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.143.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
IE9300-002#ping 192.168.169.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.169.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
IE9300-002#
```

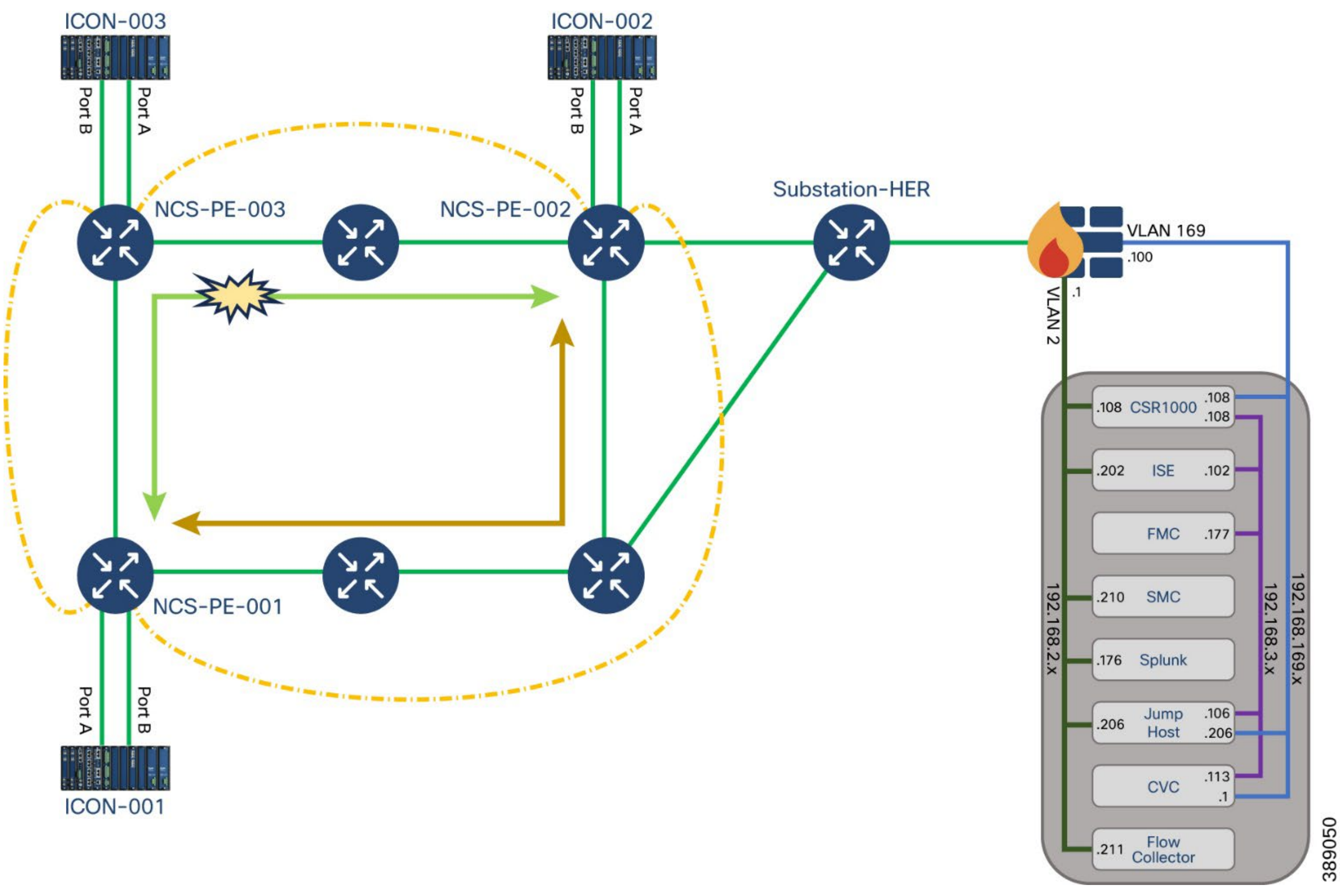
Teleprotection over Segment Routed Core using SEL ICON

The implementation guide revalidates the use case of the SEL ICON Virtual Synchronous Network (VSN) platform over the new Segment Routing enabled WAN.ICON packet transport delivers mission-critical traffic with low and deterministic latency over an Ethernet transport network. SEL are Cisco's chosen partner to support the low bit rate Teleprotection interfaces. In the converged mode of operation, the ICON operates as an edge multiplexer with support for all substation circuits (EIA-232, EIA-422, EIA-485, G.703, 2-wire FXO/FXS, 4-wire voice frequency, direct transfer trip [DTT], IEEE C37.94, and DS1).

ICON deterministic transport uses bidirectional point-to-point links provisioned through Segment Routing enabled core networks combined with an innovative, ultraefficient approach of packetizing TDM data to achieve <1 msec latency, <0.5 msec asymmetry, and <5 msec healing.
The ICON serves as an edge device that interfaces with the core transport routers or switches at 1 GigE. In this converged mode of operation, the ICON network is deployed in traditional ring topologies overlaid on top of the core network, as shown in the following figure.

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

Figure 16 Teleprotection over Segment Routed core using SEL ICON



The following are the steps to configure:

1. Identify the VLAN required for SEL ICON VSN session. Note that both the interfaces from the ICON are connected to the same PE node as SEL ICON has its own built in failover mechanism. This warrants the need to disable the failover mechanism for ELINE service provisioned between PE nodes to carry VSN traffic. The following example uses VLAN 100 and VLAN 300 for two connections from the same SEL ICON. These connections terminate on two different NCS PE routers thus enabling VSN connectivity between two different SEL ICONs for resiliency.

```
!
interface GigabitEthernet0/0/0/19.100 l2transport
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
!

!
interface GigabitEthernet0/0/0/17.300 l2transportncapsulation dot1q 300
rewrite ingress tag pop 1 symmetric
!
```

2. Configure relevant parameters for CS-SR static tunnel that would be attached to each ELINE service so as to have a deterministic path for VSN traffic to traverse between connected SEL ICON devices.

```
!
segment-routing
global-block 16000 24000
traffic-eng
  segment-list cs-working-bck
   index 1 mpls adjacency 192.168.83.2
   index 2 mpls adjacency 192.168.71.1
   index 3 mpls adjacency 192.168.72.1
   index 4 mpls adjacency 192.168.73.1
   index 5 mpls adjacency 192.168.91.1
  !
  segment-list cs-working-fwd
   index 1 mpls adjacency 192.168.91.2
   index 2 mpls adjacency 192.168.73.2
   index 3 mpls adjacency 192.168.72.2
   index 4 mpls adjacency 192.168.71.2
   index 5 mpls adjacency 192.168.83.1
  !
  segment-list cs-1-working-bck
   index 1 mpls adjacency 192.168.98.1
   index 2 mpls adjacency 192.168.93.2
   index 3 mpls adjacency 192.168.92.2
  !
  segment-list cs-1-working-fwd
   index 1 mpls adjacency 192.168.92.1
   index 2 mpls adjacency 192.168.93.1
   index 3 mpls adjacency 192.168.98.2
  !
  policy srte_1_ep_192.168.201.8
   color 1 end-point ipv4 192.168.201.8
   candidate-paths
    preference 100
     explicit segment-list cs-working-fwd
      reverse-path segment-list cs-working-bck
     !
    !
   !
  !
  policy srte_1_ep_192.168.201.25
   color 2 end-point ipv4 192.168.201.25
   candidate-paths
    preference 101
     explicit segment-list cs-1-working-fwd
     !
    !
   !
  !
!
!
```

3. Define the SR-TE template required to be attached to the ELINE service. Attach the template to the relevant ELINE services. Note that the fallback disable option has been enabled so as to avoid network recovergence in case of failure. This would ensure that the SEL ICON device takes care of its own switchover of VSN session in case of network failure adhering to the requirements discussed above.

```
!
l2vpn
pw-class EVPN1
  encapsulation mpls
   preferred-path sr-te policy srte_c_1_ep_192.168.201.8 fallback disable
  !
!
pw-class EVPN2
  encapsulation mpls
   preferred-path sr-te policy srte_c_2_ep_192.168.201.25 fallback disable
  !
!
xconnect group SEL-ICON-P2P-EVPN1
  p2p evpn1
   interface GigabitEthernet0/0/0/19.100
   neighbor evpn evi 101 target 12 source 10
   pw-class EVPN1
   !
  !
!
xconnect group SEL-ICON-P2P-EVPN2
  p2p evpn2
   interface GigabitEthernet0/0/0/17.300
   neighbor evpn evi 102 target 18 source 20
   pw-class EVPN2
   !
  !
!
```

4. Define appropriate QoS policy on various routers that are part of the SR network to ensure that the SEL ICON VSN traffic is treated appropriately. SEL ICON can be configured to set the COS value for VSN traffic. This example has COS value set to 7. The QOS policies on the interfaces connected between SEL ICON and NCS PE are configured based on this COS value.

```
!
class-map match-any COS-7
match cos 7
end-class-map
!

!
policy-map INGRESS-SEL-ICON
class COS-7
  set qos-group 7
```

```
  set traffic-class 7
!
class class-default

!
end-policy-map
!

!
interface GigabitEthernet0/0/0/19.100 l2transport
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
service-policy input INGRESS-SEL-ICON
!
interface GigabitEthernet0/0/0/17.300 l2transport
encapsulation dot1q 300
rewrite ingress tag pop 1 symmetric
service-policy input INGRESS-SEL-ICON
!
```

5. The egress interfaces that carry SEL ICON VSN traffic are configured with appropriate policies in both the INGRESS and EGRESS directions. SEL ICON VSN traffic is transmitted into the high priority queue in each hop to meet the requirements of end-to-end low latency and jitter.

```
class-map match-all EXP-7
match mpls experimental topmost 7
end-class-map
!
class-map match-any TC-CLASS-7
match traffic-class 7
end-class-map
!
class-map match-any QOS-GRP-7
match qos-group 7
match discard-class 0
end-class-map
!


!
policy-map TEST_SR_CORE_INGRESS
class EXP-7
  set traffic-class 7
  set qos-group 7
  police rate 630 mbps
  !
!
class class-default
  set qos-group 0
  set traffic-class 0
!
```

```
end-policy-map
!
policy-map TEST_SR_CORE_EGRESS_MARKING

class QOS-GRP-7
  set mpls experimental imposition 7
!
class class-default
  set mpls experimental imposition 0
!
end-policy-map
!
policy-map TEST_SR_CORE_EGRESS
class TC-CLASS-7
  priority level 1
!
class class-default
!
end-policy-map
!
```

Best Practices

1. It is recommended to identify the type of interface required to achieve the scale, latency, and jitter requirements for the intended traffic over SR core. IR8340 supports 1Gig WAN interface, whereas NCS540 supports 1G, 10G,25G and 40G interfaces. This test was carried out using 1G and 10G interfaces.

2. Note the number of SEL-ICON devices connected to each PE and the number of VSN services that are enabled through the core network. Each VSN service demands a bandwidth of about 205Mbps approximately. If the deployment warrants a greater number of SEL-ICON VSN services, choose appropriate core link to support the required bandwidth.

3. It is recommended to check the PDV settings on SEL-ICON for VSN service based on the numbers reported by it to achieve the required network peformance.

4. It is recommended to disable the fallback option for E-LINE services carrying VSN traffic as SEL-ICON uses its built-in resiliency mechanism to achieve required convergence.
5. It is recommended to enable appropriate QoS policies, both INGRESS and EGRESS for both access and core facing interfaces classifying various traffic flows as per the requirement and treating appropriately. The configuration of COS value for VSN traffic on SEL ICON should be considered for appropriate QOS policies.

6. It is recommended to ensure that IR8340 is not part of the segment routed core network handling all the traffic. IR8340 should be positioned as a spur to the Segment routing enabled core. This can be seen in the figure above.

7. Note that IR8340 does not support Segment Routing capabilities for L2 services as of the IOS-XE release that was validated for this implementation guide.

Verification

```
RP/0/RP0/CPU0:NCS-PE-001#show l2vpn xconnect summary
Wed Nov 15 10:33:04.257 IST
  Number of groups: 2
Number of xconnects: 2
  Up: 2  Down: 0  Unresolved: 0 Partially-programmed: 0
  AC-PW: 2  AC-AC: 0  PW-PW: 0 Monitor-Session-PW: 0
  AC-IP Tunnel: 0
Number of Admin Down segments: 0
Number of MP2MP xconnects: 0
  Up 0 Down 0
  Advertised: 0 Non-Advertised: 0
Number of CE Connections: 0
Advertised: 0 Non-Advertised: 0
Backup PW:
  Configured   : 0
  UP           0
  Down         0
  Admin Down     0
  Unresolved     0
  Standby        0
  Standby Ready: 0
Backup Interface:
  Configured     0
  UP           0
  Down         0
  Admin Down     0
  Unresolved     0
  Standby        0
RP/0/RP0/CPU0:NCS-PE-001#
RP/0/RP0/CPU0:NCS-PE-001#
RP/0/RP0/CPU0:NCS-PE-
001#RP/0/RP0/CPU0:NCS-PE-
001#show l2vpn xconnect detail
Wed Nov 15 10:33:19.599 IST

Group SEL-ICON-P2P-EVPN1, XC evpn1, state is up; Interworking none
  AC: GigabitEthernet0/0/0/19.100, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [100, 100]
    MTU 1500; XC ID 0x3; interworking none
    Statistics:
      packets: received 645479588629, sent 645445757295
```

```
    bytes: received 87785224053544, sent 86489731477530
    drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 192.168.201.8, PW ID: evi 101, ac-id 12, state is up (established)
   XC ID 0xc0000002
   Encapsulation MPLS
   Encap type Ethernet, control word enabled

   Sequencing not set
   Preferred path Active : SR TE srte_c_1_ep_192.168.201.8 (BSID:24010,
IFH:0x3c00800c), Statically configured, fallback disabled

   Ignore MTU mismatch: Enabled
   Transmit MTU zero: Enabled
   Tunnel : Up

    EVPN         Local                        Remote
    --------- ------------------------------ ---------------------------
    Label        24002                        24002
    MTU          1514                         unknown
    Control word enabled
    enabledAC ID                              10  12
    EVPN type    Ethernet                     Ethernet

    --------- ------------------------------ ---------------------------
   Create time: 12/09/2023 20:22:21 (9w0d ago)
   Last time status changed: 10/11/2023 10:59:35 (4d23h ago)
   Statistics:
    packets: received 645445757295, sent 645479588629
    bytes: received 86489731477530, sent 87785224053544

Group SEL-ICON-P2P-EVPN2, XC evpn2, state is up; Interworking none
  AC: GigabitEthernet0/0/0/17.300, state is up
   Type VLAN; Num Ranges: 1
   Rewrite Tags: []
   VLAN ranges: [300, 300]
   MTU 1500; XC ID 0x2; interworking none
   Statistics:
    packets: received 645479588629, sent 613789194458
    bytes: received 87785224053544, sent 82247752057372
    drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 192.168.201.25, PW ID: evi 102, ac-id 18, state is up ( established )
   XC ID 0xc0000001
   Encapsulation MPLS
   Encap type Ethernet, control word enabled
   Sequencing not set
   Preferred path Active : SR TE srte_c_2_ep_192.168.201.25 (BSID:24008,
IFH:0x3c00802c), Statically configured, fallback disabled
   Ignore MTU mismatch: Enabled
   Transmit MTU zero: Enabled
   Tunnel : Up
```

```
EVPN        Local                    Remote
--------- ------------------------- ---------------------
Label       24003                    24001
MTU         1514                     unknown
Control word enabled                 enabled
AC ID       20                       18
EVPN type   Ethernet                 Ethernet

--------- ------------------------- ---------------------
  Create time: 12/09/2023 20:22:21 (9w0d ago)
  Last time status changed: 10/11/2023 10:48:17 (4d23h ago)
  Statistics:
   packets: received 613789194458, sent 645479588629
   bytes: received 82247752057372, sent 87785224053544
RP/0/RP0/CPU0:NCS-PE-001#
RP/0/RP0/CPU0:NCS-PE-001#
```

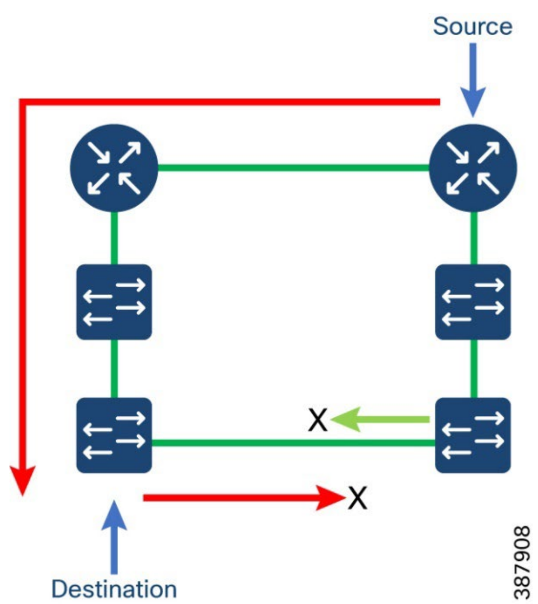
LAN Implementation

Legacy Protocols Implementation

RPVST

Rapid PVST+ is the IEEE 802.1w (RSTP) standard implemented per VLAN. A single instance of STP runs on each configured VLAN (if you do not manually disable STP). Each Rapid PVST+ instance on a VLAN has a single root switch. You can enable and disable STP on a per-VLAN basis when you are running Rapid PVST+. Rapid PVST+ is enabled by default on the default VLAN (VLAN1) and on all newly created VLANs in software. Rapid PVST+ interoperates with switches that run legacy IEEE 802.1D STP.

Figure 17 Rapid Per VLAN Spanning Tree



To enable Rapid PVST+ per VLAN, complete the steps below.

Steps to Configure

1. Identify the required VLANs and configure them on all the participating switches in the RPVST ring.

```
!
vlan 1,201,501,1501
no shut
end
!
```

2. Identify the interfaces for the RPVST ring and configure trunk port allowing the identified VLANs.

```
!
interface gigabitEthernet 0/1/5
switchport mode trunk
switchport trunk allowed vlan 1,201,501,1501
end
!
```

3. Configure the following to enable RPVST on the devices of interest.

```
!
spanning-tree mode rapid-pvst
spanning-tree vlan-range
!
```

4. Repeat the above steps across all the relevant devices participating in the spanning tree topology.

5. To display Rapid PVST+ configuration information, perform one of the following tasks:

Verification

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree portfast trunk
spanning-tree portfast trunk
!
```

switch# ***show spanning-tree [options]***

The following example displays the spanning tree details for VLAN 1.

```
Router#show spanning-tree vlan 1

G0:VLAN0001
 Spanning tree enabled protocol rstp
 Root ID    Priority    32769
            Address     0029.c23c.5bc0
            Cost        4
            Port        14 (GigabitEthernet0/1/4)
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
            Address     14a2.a093.fa71
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1/2             Desg FWD 4         128.12   P2p
Gi0/1/4             Root FWD 4         128.14   P2p
Gi0/1/8             Desg FWD 4         128.18   P2p Edge
Ap0/1/1             Desg FWD 2         128.22   P2p
```

Best Practices

- It is recommended to make the core switch as the root bridge. It is also recommended to select a backup root bridge. If there are dual redundant core switches, then one is the root bridge and the other becomes backup. Set the bridge priority on the primary root bridge to the best possible value—4096—and the backup root bridge to the next best value—8192.

- It is recommended to configure the command “spanning-tree portfast” on all the ports connecting to end devices.

REP

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment.

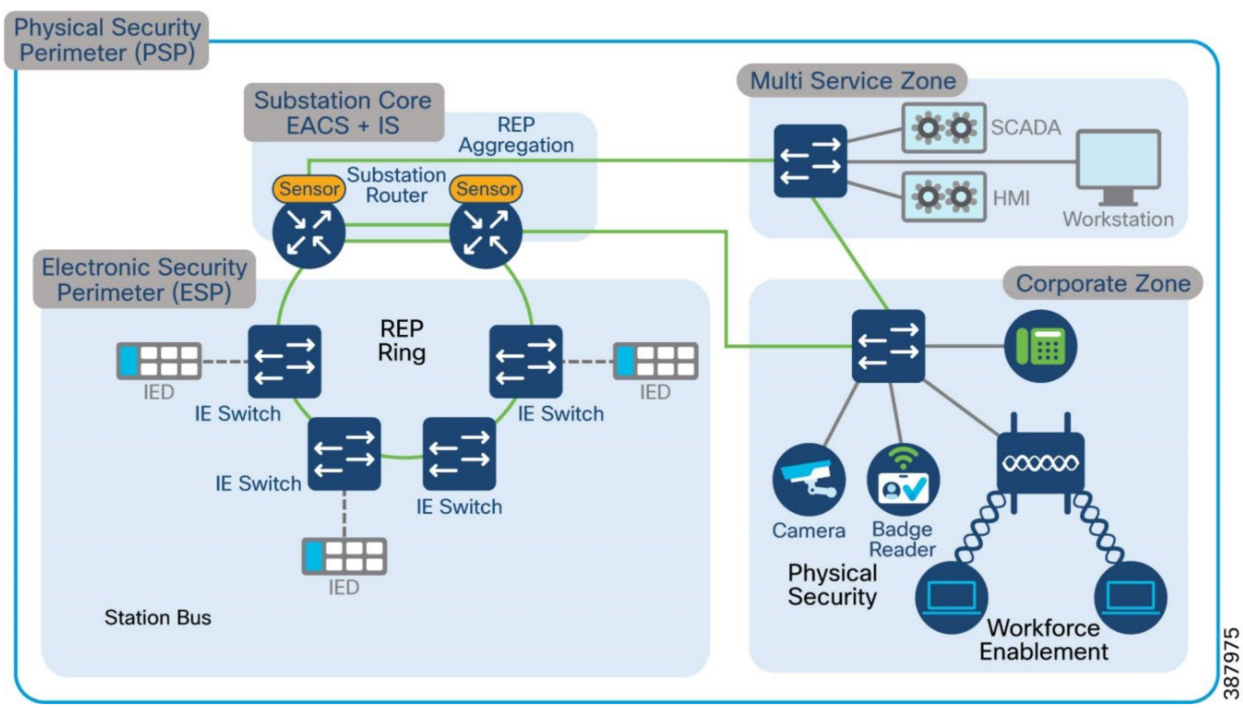
The following topology depicts a scenario where in the station bus is connected using REP as a resiliency protocol and both CORP & Multiservice zone also connected using REP. IR8340 Cisco Substation Router aggregates both the REP Rings and acts as Layer 3 gateway. NTP is used as the timing protocol over REP rings. The topology uses trunk ports as it helps to create multiple VLANs thus providing an option to create different services and or connect different devices and restrict the related traffic to the VLAN. Layer 3 Gateway Redundancy protocol like HSRP or VRRP can be enabled on IR8340. Refer respective sections in this implementation guide for HSRP or VRRP configuration steps.

The following REP features are **not** supported on IR8340:

- REP Fast
- REP Day Zero
- REP Segment Id Auto Discovery
- REP Negotiated

Note: PTP over REP is **not** supported on IR8340 and IE9300 in the tested IOS-XE version for this solution.

Figure 18 Substation Router with multiple REP rings for different zones



Steps to Configure

The following are the steps to configure REP interfaces.

1. Identify the required VLANs and configure them on all the participating switches in the REP ring.

```
!
vlan 1,201,501,1501
no shut
end
!
```

2. Identify the interfaces for the REP ring and configure trunk port allowing the identified VLANs.

```
!
interface gigabitEthernet 0/1/5
switchport mode trunk
```

```
switchport trunk allowed vlan 1,201,501,1501
!
```

3. Enable REP on the identified interfaces on all participating switches to form the REP Ring.

```
!
inte gigabitEthernet 0/1/5
rep seg 1 <edge> < preferred>   rep seg 1
end
!
```

Note You must configure two edge ports, including one primary edge port for each segment.

- (Optional) **edge** —configures the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports.
- (Optional) **primary**— configures the port as the primary edge port—the port on which you can configure VLAN load balancing.
- (Optional) **no-neighbor**— configures a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port.

Note Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** privileged EXEC command.

- (Optional) **preferred** —indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.

Note Configuring a port as preferred does not guarantee that it becomes the alternate port; it only gives it a slight advantage among equal contenders. The alternate port is usually a previously failed port.

Verification

After configuration of REP on all the participating switches in the ring and the respective interfaces on the switches the following command can be used for verification.

show rep topology segment <segment id>

```
Router#show rep to seg 1 REP Segment 1
BridgeName                PortName   Edge Role
-----------------------------------
Router                     Gi0/1/6    Pri  Alt
RIO-SA                      Gi1/1          Open
RIO-SA                      Gi1/2          Open
```

IE2KU-REP001 Gi0/1 Open
IE2KU-REP001 Gi0/2 Open
IE2KU-REP002 Gi0/2 Open
IE2KU-REP002 Gi0/1 Open
clarke-003-REP Gi1/0/25 Open
clarke-003-REP Gi1/0/26 Open
sumatra-PP-1 Gi0/1/5 Open
sumatra-PP-1 Gi0/1/7 Open
Router Gi0/1/5 Sec Open

Router#

Other similar commands that can be used to monitor REP are

> "rep detail"show interface<interface>

Displays REP configuration and status for an interface or for all interfaces.

- (Optional) detail—displays interface-specific REP information.

*Router#**show inte gigabitEthernet 0/1/5 rep detail***
GigabitEthernet0/1/5 REP enabled
Segment-id: 1 (Edge)
PortID: 000F14A2A093F9F0
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 001014A2A093F9F0E856
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Not supported
REP Segment Id Auto Discovery Status: Not supported
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 837, tx: 771
HFL PDU rx: 1, tx: 1
BPA TLV rx: 558, tx: 161
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 6
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 99, tx: 137

"**show rep topology detail**"

Displays REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.

- (Optional) archive— displays the last stable topology.

Note An archive topology is not retained when the switch reloads.

- (Optional) detail—displays detailed archived information.

Best Practices

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. You can control the flooding of these messages by configuring an administrative VLAN for the entire domain.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- There can be only one administrative VLAN on a switch and on a segment. However, this is not enforced by software.
- The administrative VLAN cannot be the RSPAN VLAN.

To configure the REP administrative VLAN, follow these steps,

```
Switch# configure terminal
Switch (config)# rep admin vlan <vlan id>
Switch (config-if)# end
```

Lossless Protocol Implementation

PRP

Parallel Redundancy Protocol (PRP) is defined in the International Standard IEC 62439-3. PRP is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks. Here the end nodes implement redundancy (instead of network elements) by connecting two network interfaces to two independent, disjointed, parallel networks (LAN-A and LAN-B). Each of these Dually Attached Nodes (DANs) then have redundant paths to all other DANs in the network.

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

PRP channel or channel group is a logical interface that aggregates two Gigabit Ethernet interfaces (access, trunk, or routed) into a single link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port and connects to LAN_A. The higher numbered port is the secondary port and connects to LAN_B. The PRP channel remains up if at least one of these member ports remains up and sends traffic. When both member ports are down, the channel is down.

The following table lists the different PRP modes and platform support.

Table 5 PRP Modes and Supported Platforms

PRP Modes	Platform
PRP Redbox	IR8340, IE9300, IE5000, IE4000, IE4010, IE3400
PRP HSR Redbox	IE4000
PTP over PRP	IE5000, IE3400, IE4010

The following section lists only the details with respect to PRP on IR8340. For details on other PRP modes refer to the earlier versions of Substation Automation Solution guides listed in the reference section earlier.

The total number of supported PRP channel groups on Cisco IR8340 is 2 per router, and the interfaces that can be utilized for each group are fixed.

- PRP channel group 1 always uses Gi0/1/4 for LAN_A and Gi0/1/5 for LAN_B
- PRP channel group 2 always uses Gi0/1/6 for LAN_A and Gi0/1/7 for LAN_B

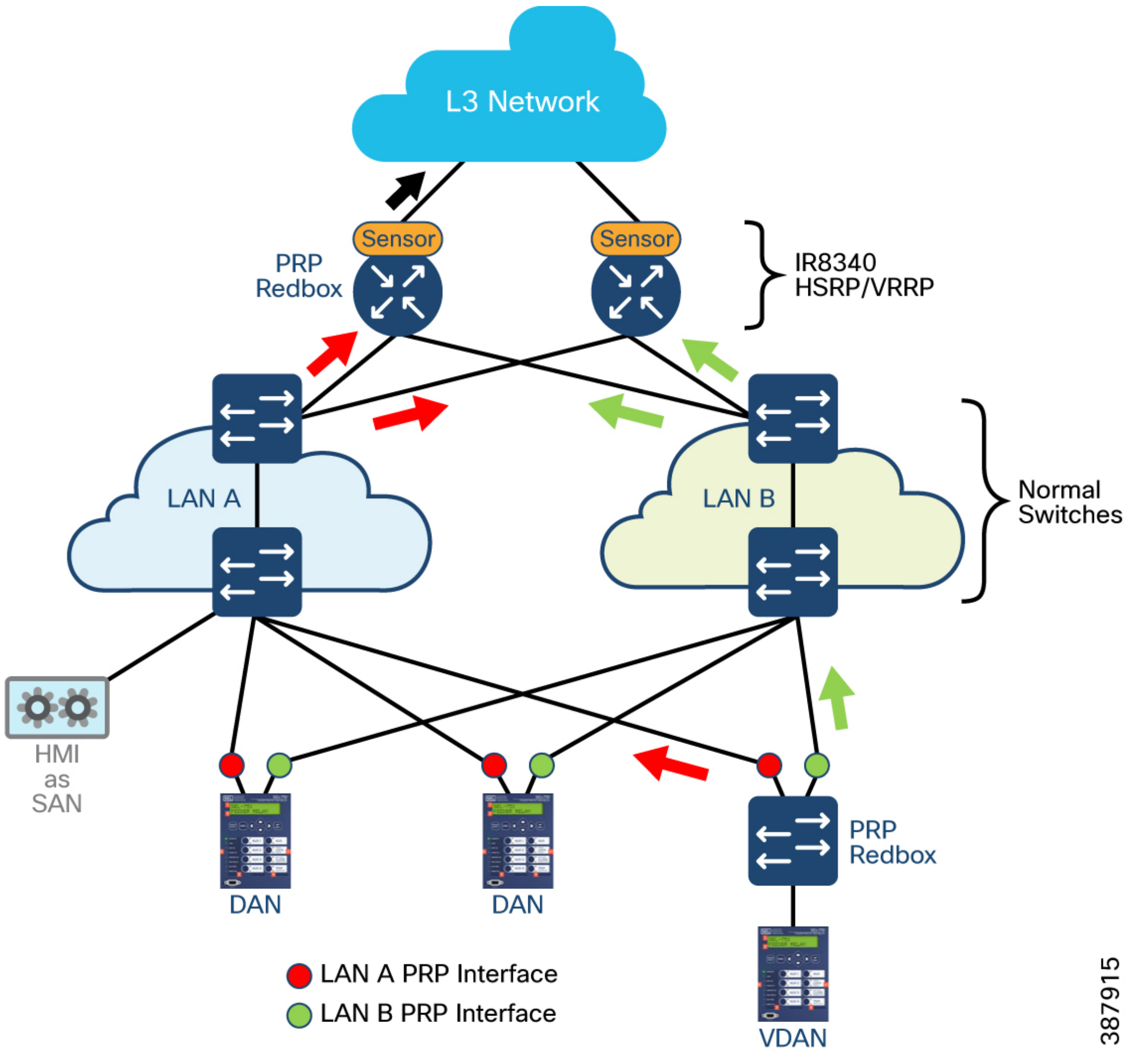
The total number of supported PRP channel groups on Cisco IE9300 i.e., IE-9320-26S2C-A and IE-9320-26S2C-E are 2 per switch, and the interfaces that can be utilized for each group are fixed.

- PRP channel group 1 always uses Gi1/0/21 for LAN_A and Gi1/0/22 for LAN_B
- PRP channel group 2 always uses Gi1/0/23 for LAN_A and Gi1/0/24 for LAN_B

The following topology shows two IR8340 Routers configured as PRP Redboxes. The IR8340 routers also act as L3 gateway for devices connected in the LAN segments of PRP, LAN A and LAN B. LAN A and LAN B of PRP are RSTP enabled. They can also be configured with other resiliency protocols like REP, STP, etc. Refer the respective sections in this guide for configuration of the resiliency protocols. NTP is used as the timing protocol over PRP LAN rings as IR8340 does not support PTP over PRP in the IOS-XE version that was used for validation of this implementation guide. The topology uses trunk ports as it helps to create multiple VLANs thus providing an option to create different services and or connect different devices and restrict the related traffic to the VLAN. Layer 3 Gateway Redundancy protocol like HSRP or VRRP can be enabled on IR8340. Refer respective sections in this implementation guide for HSRP or VRRP configuration steps.

The following section lists the steps to enable PRP Channel on Cisco IR8340 configured as PRP Redbox. The same steps can be followed to enable PRP Channel on Cisco IE9300 switch.

Figure 19 PRP Redbox with L3 Gateway Redundancy



Steps to Configure

1. Identify the required VLANs and configure them on all the participating switches in the PRP topology and unshut the VLANs configured

   vlan 1-2507,2509-4094

2. Identify the interfaces for the PRP channel and configure trunk port allowing the identified VLANs. Interfaces GigabitEthernet 0/1/4 and 0/1/5 are used in this sample topology and save the configurations.

   .

   interface gigabitEthernet 0/1/5
   switchport mode trunk
   switchport trunk allowed vlan 1-2507,2509-4094
   end

3. Configure PRP channel and respective vlans.

```
interface prp-channel 1
switchport
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
end
```

4. Attach PRP channel to the PRP member interfaces. Ensure that both the member interfaces are configured and save the configurations.

```
interface GigabitEthernet0/1/4
prp-channel-group 1
end
```

Verification

After configuration of PRP on the participating router or switch use the following commands for verification.

```
Router#show prp channel summary
Flags:  D - down        P - bundled in prp-channel
        R - Layer3      S - Layer2
        U - in use

Number of channel-groups in use: 1
Group  PRP-channel  Ports
-----+----------+-----------------------------
1      PR1(SU)      Gi0/1/4(P), Gi0/1/5(P)

Router#show prp channel 1 detail
PRP-channel: PR1
---------
 Layer type = L2
 Ports: 2    Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi0/1/4
   Logical slot/port = 0/4    Port state = Inuse
    Protocol = Enabled
  2) Port: Gi0/1/5
   Logical slot/port = 0/5    Port state = Inuse
    Protocol = Enabled

Router#
Router#show prp channel 1 status
PRP-channel: PR1
```

```
---------
 Port state = prp-channel is Inuse
 Protocol = Enabled
sumatra-pp-2#
```

Use the following commands to check various statistics related to PRP.

*Router#**show prp statistics ?***

```
  egressPacketStatistics   Egress packet statistics
  ingressPacketStatistics  Ingress packet statistics
  nodeTableStatistics      Node table statistics
  pauseFrameStatistics     Pause frame statistics
  ptpPacketStatistics      PTP packet statistics
```

*Router#**show prp statistics ingressPacketStatistics***

```
PRP channel-group 1 INGRESS STATS:
   ingress pkt lan a: 113060
   ingress pkt lan b: 145488
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 13168
   ingress danp pkt dscrd: 11625
   ingress supfrm rcv a: 78692
   ingress supfrm rcv b: 86607
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
   ingress oversize pkt a: 0
   ingress oversize pkt b: 0
   ingress byte lan a: 9408873
   ingress byte lan b: 11577700
   ingress wrong lan id a: 0
   ingress wrong lan id b: 88005
   ingress warning lan a: 0
   ingress warning lan b: 0
   ingress warning count lan a: 0
   ingress warning count lan b: 2
   ingress unique count a: 1456
   ingress unique count b: 0
   ingress duplicate count a: 7682
   ingress duplicate count b: 3943
   ingress multiple count a: 7682
   ingress multiple count b: 3943
PRP channel-group 2 INGRESS STATS:
   ingress pkt lan a: 0
   ingress pkt lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
```

```
  ingress danp pkt acpt: 0
  ingress danp pkt dscrd: 0
  ingress supfrm rcv a: 0
  ingress supfrm rcv b: 0
  ingress over pkt a: 0
  ingress over pkt b: 0
  ingress pri over pkt a: 0
  ingress pri over pkt b: 0
  ingress oversize pkt a: 0
  ingress oversize pkt b: 0
  ingress byte lan a: 0
  ingress byte lan b: 0
  ingress wrong lan id a: 0
  ingress wrong lan id b: 0
  ingress warning lan a: 0
  ingress warning lan b: 0
  ingress warning count lan a: 0
  ingress warning count lan b: 0
  ingress unique count a: 0
  ingress unique count b: 0
  ingress duplicate count a: 0
  ingress duplicate count b: 0
  ingress multiple count a: 0
  ingress multiple count b: 0

Router#
Router#show prp statistics egressPacketStatistics
PRP channel-group 1 EGRESS STATS:
  duplicate packet: 87990
  supervision frame sent: 13411
  packet sent on lan a: 111248
  packet sent on lan b: 111270
  byte sent on lan a: 7975915
  byte sent on lan b: 7977924
  egress packet receive from switch: 97949
  overrun pkt: 0
  overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
  duplicate packet: 0
  supervision frame sent: 0
  packet sent on lan a: 0
  packet sent on lan b: 0
  byte sent on lan a: 0
  byte sent on lan b: 0
  egress packet receive from switch: 0
  overrun pkt: 0
  overrun pkt drop: 0
```

Router#

Use the following commands to display PRP control information and supervision frame information.

```
Router#show prp control ?
  VdanTableInfo                      VDAN table information
  ptpLanOption                       PTP LAN option
  ptpProfile                         PTP profile
  supervisionFrameLifeCheckInterval  Supervision frame life check interval
  supervisionFrameOption             Supervision frame option
  supervisionFrameRedboxMacaddress   Supervision Redbox MacAddress
  supervisionFrameTime               Supervision frame time

Router#
```

Best Practices

- Configure *bpdufilter* on the prp-channel interface. The spanning-tree BPDU filter drops all ingress and egress BPDU traffic. This command is required to create independent spanning-tree domains (zones) in the network.

  spanning-tree bpdufilter enable

- Configure LAN-A/B ports to quickly get to FORWARD mode. This command is optional but highly recommended. It improves the spanning-tree convergence time on PRP RedBoxes and LAN-A and LAN-B switch edge ports. It is also highly recommended to configure this command on the LAN_A/LAN_B ports that are directly connected to a RedBox PRP interface.

  spanning-tree portfast edge trunk

```
!
interface prp-channel 1
spanning-tree bpdufilter enable
spanning-tree portfast trunk
!
```

HSR

International Standard IEC 62439-3-2016 clause 5 describes HSR, High-availability Seamless Redundancy. HSR achieves the same result as PRP but designed to work in a ring topology. Instead of two parallel independent networks of any topology (LAN-A and LAN-B), HSR defines two rings with traffic in opposite directions. PortA sends traffic counter clockwise in ringA, and portB sends traffic clockwise in ringB. The packet format is different than PRP, instead of RCT HSR introduces the HSR header with HSR Ethertype after the L2 MacSa address or VLAN tag fields.
The nodes connecting to the HSR ring are referred to as DANH. Similar to PRP, SANs are attached to the HSR ring via the service of a RedBox.

Each node in the HSR ring forwards frames received from one port to the other port of the HSR pair. There are three conditions that a node will not forward frames received on one port to the other port:

- The received frame came back around the ring to the node it originated from.
- Unicast frame with destination MAC address belonging to upstream of the receiving node.
- The node had already sent the same frame in the same direction. This rule is to prevent a frame from spinning in the ring in an infinite loop.

Platforms and feature support for HSR is shown in the table below. For detailed configuration refer to Substation Automation Local Area Network and Security Cisco Validated Design: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG/CU-2-3-2-DIG.html

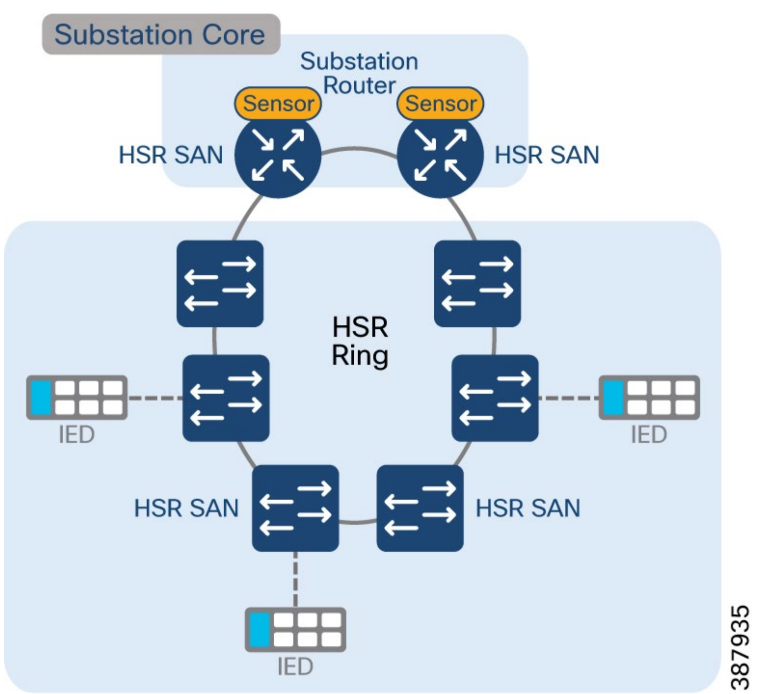
Table 6 HSR Modes and Supported Platforms

Feature	Platform	Cisco IOS software
HSR-SAN (Singly Attached Node)	IE4000/IE5000/IE4010 IR8340	15.2(8)E1 17.9.1
HSR-PRP Redbox	IE4000	15.2(8)E1
HSR-Quadbox	IE4000	15.2(8)E1

The total number of HSR rings supported on IR8340 is 1 ring per router, and the interfaces that can be used for each group are:

- HSR ring group 1 uses Gi0/1/4 or Gi0/1/6 for LAN_A and Gi0/1/5 or Gi0/1/7 for LAN_B

Figure 20 HSR Topology



Steps to Configure

1. Identify the required VLANs and configure them on all the participating switches in the HSR topology and unshut all the vlans in the global configuration mode

```
vlan 1-2507,2509-4094
```

2. Identify the interfaces for the HSR ring and configure trunk port allowing the identified VLANs. Interfaces GigabitEthernet 0/1/6 and 0/1/7 are used in this sample topology and save the configuration

```
interface gigabitEthernet 0/1/6
switchport mode trunk
switchport trunk allowed vlan 1-2507,2509-4094
end
```

3. Configure the HSR ring and respective vlans and unshut the interface hsr-ring

```
interface hsr-ring 1
switchport
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
```

4. Attach HSR Ring to the HSR member interfaces. Ensure that both the member interfaces are configured and save the configuration

```
interface GigabitEthernet0/1/6
hsr-ring 1
```

Verification

After configuration of HSR on the participating router or switch the following commands can be used for verification.

```
Router#sh hsr ring 1 detail
HSR-ring: HS1
---------
 Layer type = L2
 Operation Mode =
 mode-H Ports: 2
                    Maxports =
 2 Port state = hsr-ring
 is In use
 Protocol = Enabled  Redbox Mode = hsr-
san Ports in the ring:
  1) Port: Gi0/1/6
   Logical slot/port = 0/6      Port state =
        In use Protocol = Enabled
  2) Port: Gi0/1/7
   Logical slot/port = 0/7      Port state =
        In use Protocol = Enabled

Ring Parameters:
 Redbox MacAddr:
 38fd.f85b.c54e Node Forget
 Time: 60000 ms Node
 Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option:
 0 Supervision Frame CFI
 option: 0
 Supervision Frame VLAN Tag option:
 Disabled Supervision Frame MacDa: 0x00
 Supervision Frame VLAN
 id: 0 Supervision Frame
 Time: 3 ms Life Check
 Interval: 1600 ms Pause
 Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled

Router# sh hsr ring status
HSR-ring: HS1
---------
 Port state = hsr-ring is In use
 Protocol = Enabled  Redbox Mode = hsr-san
```

Router# ***sh hsr ring 1 summary***
Flags: D - down H - bundled in
HSR-ring R - Layer3 S - Layer2
U - in use s – suspended

Number of hsr-rings in
use: 1 Group HSR-ring
Po
rts
-----+----------+------------------------------
1 HS1(SU) Gi0/1/6(H), Gi0/1/7(H)

Use the following commands to check various statistics related to HSR Ring.

*Router#**sh hsr statistics egressPacketStatistics***
duplicate packets: 7477
supervision frames: 1140
packets sent on port A:
1239544 packets sent on
port B: 1152183 byte sent
on port a: 160600821 byte
sent on port b: 149151641

*Router#**sh hsr statistics ingressPacketStatistics***
HSR ring 1 INGRESS STATS:
ingress pkt port A:
1193537 ingress pkt
port B: 1281119
ingress crc port A: 0
ingress crc port B: 0
ingress danh pkt portAcpt:
1269191 ingress danh pkt
dscrd: 1181133 ingress supfrm
rcv port A: 4032 ingress
supfrm rcv port B: 4628
ingress overrun pkt port A: 0
ingress overrun pkt port B: 0
ingress byte port a:
154514635 ingress byte port
b: 165959497

The following commands can be used to check other HSR related

information, Router#sh hsr ?
node-table HSR Node Table
ring Ring information
statistics HSR Statistics information

Limitations and Restrictions

- Maximum one ring is supported per box
- Only HSR-SAN mode is supported
- Support for HSR alarms is not provided
- Maximum number of nodes in the ring is limited to 50
- HSR-PTP is not supported in this release

Multi-Bus implementations in LAN

Separating the Station bus and Process bus can enhance network resiliency. Large networks benefit from being segmented into multiple redundancy domains, each tolerant to one failure but isolated from others, thus reducing the impact of multiple failures.
Separation can be physical or logical:

- **Physical Separation:** Two separate networks with no connectivity. This isolates the process bus, making it a private domain for some IEDs, inaccessible directly by SCADA. A Proxy Logical Node can be used for control but increases complexity.
  - **Pros:** Simple process bus devices.
  - **Cons:** Requires a proxy IED, no interoperable firmware access, complex redundancy introduction, non-standardized multi-proxy procedures.
- **Logical Separation:** Both buses belong to one network with bridges filtering traffic. Bridges or layer 3 routers prevent unnecessary message transit and manage traffic exchange through protocol gateways.
  - **Pros:** Simpler IEDs, operational even if an IED is down.
  - **Cons:** Process bus devices need an IP stack and careful configuration of devices and routers.

Following sections explain various methods which can be used for separation station bus and process bus in substations.

RSTP for Station Bus and PRP for Process bus

The Rapid Spanning Tree Protocol (RSTP) and the Parallel Redundancy Protocol (PRP) are network protocols designed to ensure high availability and reliability in Ethernet-based networks.

RSTP provides rapid recovery from network topology changes, making it suitable for station bus applications in electrical substations.

PRP, on the other hand, offers seamless network redundancy with no switchover time, ideal for process bus applications where zero recovery time is essential.

For networks demanding very high availability, critical devices on the station bus should connect using RSTP to ensure rapid convergence and minimal downtime. The process bus, requiring zero recovery time, should utilize PRP, where each critical device connects to two independent LANs.

Following Table lists down some design recommendations while implementing station bus with RSTP and Process bus with PRP:

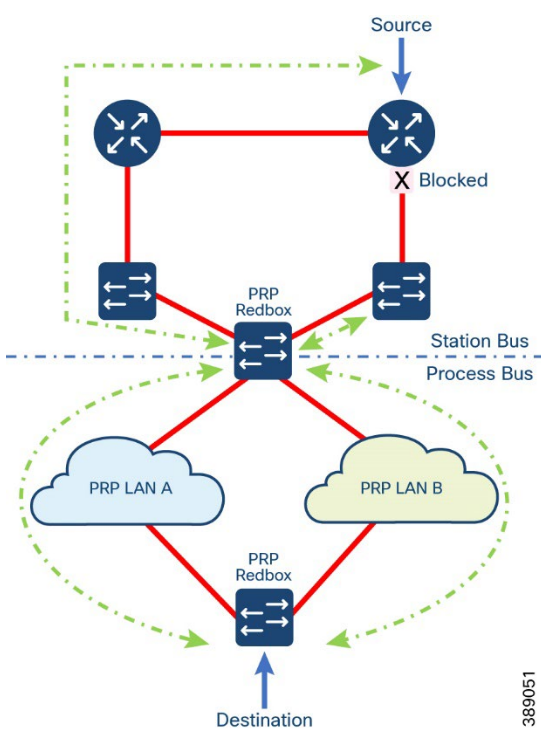
Table 7 Recommendations for design with RSTP for Station Bus and PRP for Process bus

	Station Bus with RSTP	**Process Bus with PRP**
Network Topology	Implement a ring or mesh topology to leverage RSTP's rapid convergence capabilities. Design the network to avoid loops and ensure redundancy.	Use two independent LANs (LAN A and LAN B) to provide seamless redundancy. Ensure both networks are physically separated to avoid common points of failure.
Configuration	Designate a root bridge and configure bridge priorities to ensure predictable network behavior. Set appropriate port roles and states based on the network topology.	Configure devices to support PRP as per IEC 62439-3 standards. Use PRP Redundancy Boxes (RedBoxes) to connect non-PRP devices to the PRP network.
Redundancy and Resilience	Ensure redundant paths are available to avoid single points of failure and implement link aggregation where necessary.	Regularly test PRP failover mechanisms and monitor network traffic on both LANs.
Performance	Monitor network performance and optimize RSTP timers to match the network's specific needs.	Ensure both LANs have similar performance characteristics to avoid asymmetric delays and implement QoS to prioritize critical process data.

By following these recommendations, you can design a robust and resilient network that leverages the strengths of RSTP for the Station bus and PRP for the Process bus, ensuring high availability and reliability in your electrical substation network.

The following section lists the steps to enable RSTP for Station Bus and PRP for Process bus.

Figure 21 RSTP for Station Bus and PRP for Process bus



Steps to Configure

1. Identify the required VLANs and configure them on all the participating switches in the PRP topology and unshut the VLANs configured

   vlan 1-2507,2509-4094

2. Identify the interfaces for the RSTP ring and configure trunk port allowing the identified VLANs on all switches participating in RSTP.

   !

   interface gigabitEthernet 0/1/23

   switchport mode trunk

   switchport trunk allowed vlan 1-2507,2509-4094

   !

3. Identify the root bridge and configure below for identified VLANs.

   spanning-tree vlan 1-2507,2509-4094 root primary

4. On PRP-Redbox, Identify the interfaces for the PRP channel and configure trunk port allowing the identified VLANs. Interfaces GigabitEthernet 1/0/21 and 1/0/22 are used in this sample topology and save the configurations.

   interface gigabitEthernet 1/0/21

   switchport mode trunk

   switchport trunk allowed vlan 1-2507,2509-4094

   end

5. On PRP-Redbox, Configure PRP channel and respective VLANs.

   interface prp-channel 1

   switchport trunk allowed vlan 1-2507,2509-4094

   switchport mode trunk

   !

Verifications

IE9300-004#show spanning-tree vlan 751

VLAN0751
*Spanning tree enabled protocol **rstp***

```
    Root ID    Priority    21231
               Address     cc6a.339c.5700
               Cost        4
               Port        23 (GigabitEthernet1/0/23)
               Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    33519  (priority 32768 sys-id-ext 751)
               Address     b08d.5747.0f00
               Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  300 sec

  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Gi1/0/23            Root FWD 4         128.23   P2p
  Gi1/0/24            Desg FWD 4         128.24   P2p
  Gi1/0/28            Desg FWD 4         128.28   P2p Edge
  PR1                 Desg FWD 3         128.1945 P2p Edge

IE9300-004#show prp channel summary
Flags:  D - down        P - bundled in prp-channel
        R - Layer3      S - Layer2
        U - in use

Number of channel-groups in use: 1
Group  PRP-channel   Ports
------+-------------+-----------------------------------------
1      PR1(SU)       Gi1/0/21(P), Gi1/0/22(P)

IE9300-004#show prp channel 1 detail
PRP-channel: PR1
------------
 Layer type = L2
 Ports: 2      Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/21
   Logical slot/port = 1/21 Port state = Inuse
      Protocol = Enabled
  2) Port: Gi1/0/22
   Logical slot/port = 1/22 Port state = Inuse
      Protocol = Enabled

IE9300-004#show prp channel 1 status
PRP-channel: PR1
------------
 Port state = prp-channel is Inuse
       Protocol = Enabled
```

Best Practices

1. Choose a central, high-performance switch in RSTP ring as the root bridge for predictable and optimized network topology. Also, Lower the bridge priority on the designated root bridge to ensure it remains the root bridge (default priority is 32768, lower it to a value like 4096 or 8192).

2. Protect edge ports with BPDU Guard to automatically shut down the port if a BPDU is received, preventing accidental or malicious loops.

3. Configure bpdufilter on the prp-channel/Edge interfaces. The spanning-tree BPDU filter drops all ingress and egress BPDU traffic. This command is required to create independent spanning-tree domains (zones) in the network.

   ```
   spanning-tree bpdufilter enable
   ```

4. Configure LAN-A/B ports to quickly get to FORWARD mode. This command is optional but highly recommended. It improves the spanning-tree convergence time on PRP RedBoxes and LAN-A and LAN-B switch edge ports. It is also highly recommended to configure this command on the LAN_A/LAN_B ports that are directly connected to a RedBox PRP interface.

   ```
   spanning-tree portfast edge trunk
   !
   interface prp-channel 1
    spanning-tree bpdufilter enable
    spanning-tree portfast trunk
   !
   ```

PRP for Station Bus and PRP for Process Bus

The Parallel Redundancy Protocol (PRP) is a redundancy protocol designed for Ethernet-based networks that demand high availability and minimal switchover time, such as protection systems in electrical substations.
In contrast to traditional redundancy protocols like RSTP (Rapid Spanning Tree Protocol), PRP handles network component failures seamlessly, without any recovery time, and remains transparent to the application.

For networks demanding very high availability with no single point of failure, critical devices should connect to two independent LANs using the Parallel Redundancy Protocol (PRP). Each LAN must meet propagation requirements as if it were the sole network. Non-critical devices can connect to just one LAN. It is possible to connect primary protection to one LAN and backup protection to the other to ensure fail-independence.
This setup combines Station bus and Process bus networks. High availability is maintained by using dual LAN networks for both the Station bus and the Process bus. Adequate multicast filtering in RedBoxes is essential to prevent unnecessary SV traffic from the Process bus entering the Station bus.

- This section lists the steps to configure the use of logical separation for station bus and process bus deployment depicted in the topology.

Steps to Configure

1. Identify the required VLANs and configure them on all the participating switches in the PRP topology and unshut the VLANs configured

   vlan 1-111,301

2. Identify the interfaces for the PRP channel and configure trunk port allowing the identified VLANs. Interfaces GigabitEthernet 0/1/4 and 0/1/5 are used in this sample topology and save the configurations.Also note that the PRP member interfaces from each IR8340-CE router connects to both PRP LANs ,LAN A and LAN B. Gigabithernet0/1/4 from both IR8340-CE routers are connected to PRP LAN A and GigabitEthernet0/1/5 from both IR8340-CE routers are connected to PRP LAN B.

```
!
interface GigabitEthernet0/1/4
switchport trunk allowed vlan 111,301
switchport mode trunk
prp-channel-group 1

!
interface GigabitEthernet0/1/5
switchport trunk allowed vlan 111,301
switchport mode trunk
prp-channel-group 1
!
```

3. Configure PRP channel and respective VLANs on both IR8340-CE routers.

```
!
interface PRP-channel1
switchport
```

```
switchport trunk allowed vlan 111,301

switchport mode trunk

!
```

4. Enable PTP Power Profile if required. Refer to the corresponding section in this document for the step.
5. Ensure the respective VLANs for PRP are configured and enabled on the infrastructure switches that are part of the PRP LANs, PRP LAN A and PRP LAN B. The interfaces on IE9300-004 an infrastructure switch in one of the PRP LANs are set as trunk port with respective VLANs allowed in this example. Repeat this step on appropriate switches part of the PRP LANs.

```
!
interface GigabitEthernet1/0/27
description connected to IR8340-CE-001
switchport trunk allowed vlan 111,301
switchport mode trunk
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!

!
interface GigabitEthernet1/0/28
description connected to IR8340-CE-002
switchport trunk allowed vlan 111,301
switchport mode trunk
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!

!
interface GigabitEthernet1/0/1
Description connected to IE9300-002
switchport trunk allowed vlan 1,111,301
switchport mode trunk
!
```

6. Devices IE9300-001, IE9300-011 and IE9300-012 in the depicted topology are configured as PRP Redboxes so that they provide resiliency between Station BUS and BAY Control devices. These devices also connect as PRP Redbox to two Layer 3 gateways as depicted in the topology through which reachability to Process BUS devices are. These devices help achieve the Logical separation of Station BUS and Process BUS devices and communication as described above.These devices utilize the ability to configure two PRP channels thus able to connect to both Station BUS and Process BUS with one PRP channel each.

```
!
!
interface PRP-channel1
switchport trunk allowed vlan 1,111,301
switchport mode trunk
spanning-tree portfast trunk
spanning-tree bpdufilter enable
!
!
interface GigabitEthernet1/0/21
switchport trunk allowed vlan 1,111,301
switchport mode trunk
prp-channel-group 1
!
!
interface GigabitEthernet1/0/22
switchport trunk allowed vlan 1,111,301
switchport mode trunk
prp-channel-group 1
!
!
interface PRP-channel2
switchport trunk allowed vlan 1,111,301
switchport mode trunk
spanning-tree portfast trunk
spanning-tree bpdufilter enable
!
!
interface GigabitEthernet1/0/23
switchport trunk allowed vlan 1,111,301
switchport mode trunk
prp-channel-group 2
!
interface GigabitEthernet1/0/24
switchport trunk allowed vlan 1,111,301
switchport mode trunk
prp-channel-group 2
!
```

7. PTP Power profile can be transmitted across from Station Bus to Process Bus. This example uses VLAN 301 for the same.

```
!
ptp clock transparent domain 0  profile power
vlan 301
!
```

8. The L3 gateways IE-L3-001, IE-L3-002, IE-L3-003 and IE-L3-004 are L3 switches and enable L3 communication to Process BUS devices using SVI interfaces. These devices also are capable of transmitting PTP Power profile communication with appropriate configuration.

```
!
interface GigabitEthernet1/1
switchport trunk allowed vlan 1,111,301
switchport mode trunk
load-interval 30
media-type sfp
ptp vlan 301
spanning-tree portfast edge trunk
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
!
interface GigabitEthernet1/2
switchport trunk allowed vlan 1,111,301
switchport mode trunk
load-interval 30
media-type sfp
ptp vlan 301
spanning-tree portfast edge trunk
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
ptp profile power
ptp mode p2ptransparent
!
```

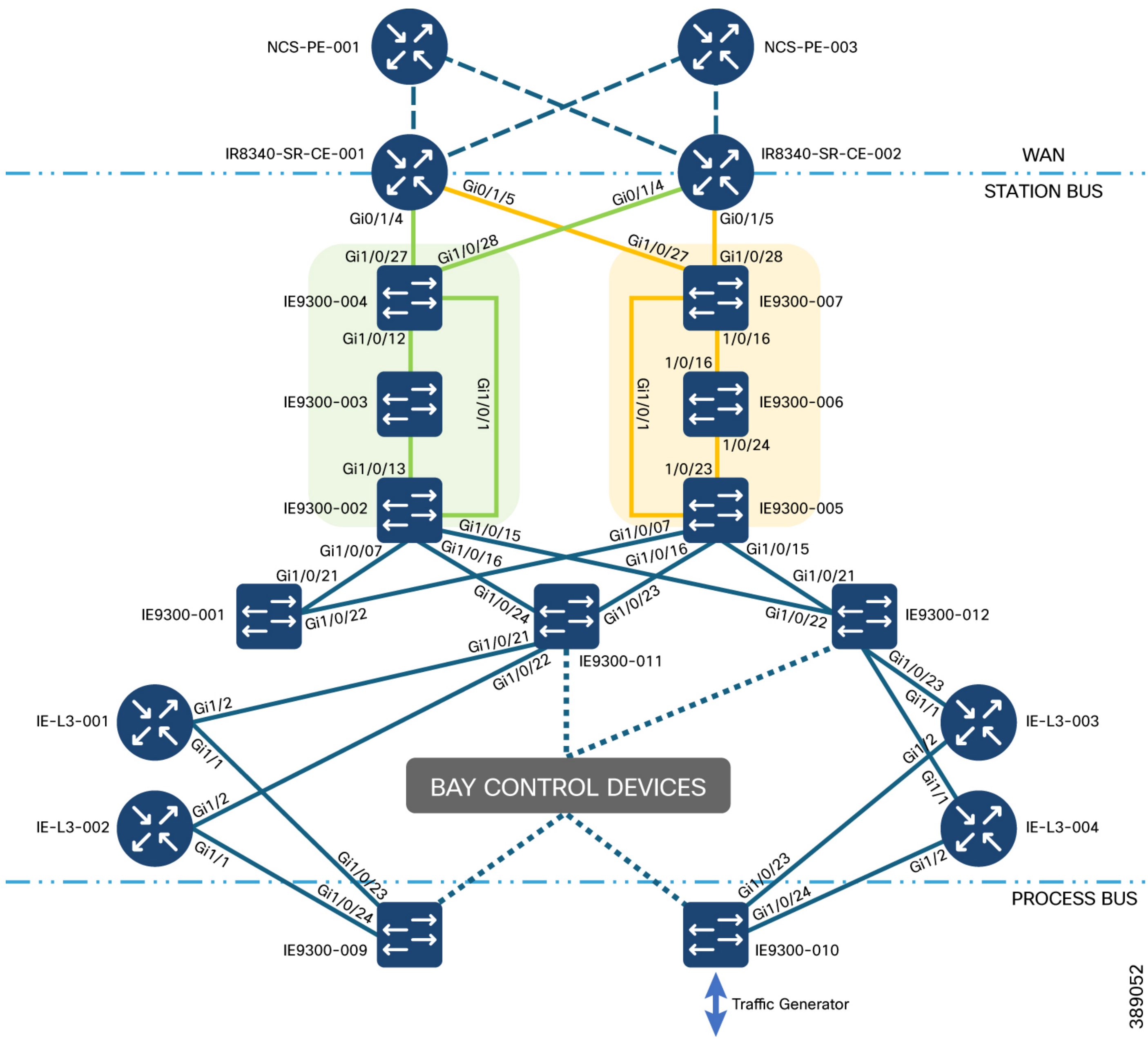
9. The switch IE9300-009 and IE9300-010 helps connect devices in process bus. These switches use PRP Channel to connect to the L3 gateways thus providing resiliency as depicted in the topology.

```
!
interface PRP-channel2
```

```
switchport trunk allowed vlan 1,111,301
switchport mode trunk
spanning-tree portfast trunk
spanning-tree bpdufilter enable
!
!
interface GigabitEthernet1/0/23
switchport trunk allowed vlan 1,111,301
switchport mode trunk
prp-channel-group 2
!
!
interface GigabitEthernet1/0/24
switchport trunk allowed vlan 1,111,301
switchport mode trunk
prp-channel-group 2
```

!

Figure 22 PRP for Station Bus and PRP for Process Bus



Verification

The following commands can be used for verification.

```
IR8340-SR-CE-001#show prp channel summary
Flags:  D - down        P - bundled in prp-channel
        R - Layer3      S - Layer2
        U - in use

Number of channel-groups in use: 2
Group  PRP-channel   Ports
------+-------------+-----------------------------------------
1      PR1(SU)       Gi0/1/4(P), Gi0/1/5(P)
2      PR2(SU)       Gi0/1/6(P), Gi0/1/7(P)
```

```
IR8340-SR-CE-001#show prp channel 1 detail
PRP-channel: PR1
------------
Layer type = L2
Ports: 2      Maxports = 2
Port state = prp-channel is Inuse
Protocol = Enabled
Ports in the group:
  1) Port: Gi0/1/4
   Logical slot/port = 0/4      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi0/1/5
   Logical slot/port = 0/5      Port state = Inuse
        Protocol = Enabled

IR8340-SR-CE-001#show prp statistics egressPacketStatistics
PRP channel-group 1 EGRESS STATS:
   duplicate packet: 345861608
   supervision frame sent: 863198
   packet sent on lan a: 346742768
   packet sent on lan b: 347920182
   byte sent on lan a: 347428762901
   byte sent on lan b: 347508042731
   egress packet receive from switch: 347069611
   overrun pkt: 0
   overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
   duplicate packet: 1321232
   supervision frame sent: 474841
   packet sent on lan a: 1929175
   packet sent on lan b: 1929155
   byte sent on lan a: 305878600
   byte sent on lan b: 147941604
   egress packet receive from switch: 1582086
   overrun pkt: 0
   overrun pkt drop: 0

IR8340-SR-CE-001#show prp statistics ingressPacketStatistics
PRP channel-group 1 INGRESS STATS:
   ingress pkt lan a: 346933751
   ingress pkt lan b: 348111500
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 345520971
   ingress danp pkt dscrd: 345520757
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
```

ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt a: 0
ingress pri over pkt b: 0
ingress oversize pkt a: 0
ingress oversize pkt b: 0
ingress byte lan a: 347462191231
ingress byte lan b: 347541504607
ingress wrong lan id a: 345248489
ingress wrong lan id b: 345248528
ingress warning lan a: 0
ingress warning lan b: 0
ingress warning count lan a: 0
ingress warning count lan b: 7
ingress unique count a: 121
ingress unique count b: 0
ingress duplicate count a: 81746858
ingress duplicate count b: 263773898
ingress multiple count a: 81746858
ingress multiple count b: 263773898

PRP channel-group 2 INGRESS STATS:
ingress pkt lan a: 1897562
ingress pkt lan b: 2068468
ingress crc lan a: 0
ingress crc lan b: 0
ingress danp pkt acpt: 1308752
ingress danp pkt dscrd: 1308752
ingress supfrm rcv a: 0
ingress supfrm rcv b: 0
ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt a: 0
ingress pri over pkt b: 0
ingress oversize pkt a: 0
ingress oversize pkt b: 0
ingress byte lan a: 457687267
ingress byte lan b: 154140668
ingress wrong lan id a: 0
ingress wrong lan id b: 0
ingress warning lan a: 0
ingress warning lan b: 0
ingress warning count lan a: 0
ingress warning count lan b: 0
ingress unique count a: 0
ingress unique count b: 0
ingress duplicate count a: 1305236
ingress duplicate count b: 3516
ingress multiple count a: 1305236

ingress multiple count b: 3516

IR8340-SR-CE-001#

The use of PRP allows for a simple network configuration with independent LANs, maintaining traffic characteristics unaffected by redundancy. Dual Attached Nodes (DANP) and RedBoxes enable seamless failover and redundancy, though this setup requires doubling the network infrastructure and PRP-equipped devices.

Implementing HSR-PRP Dual RedBox

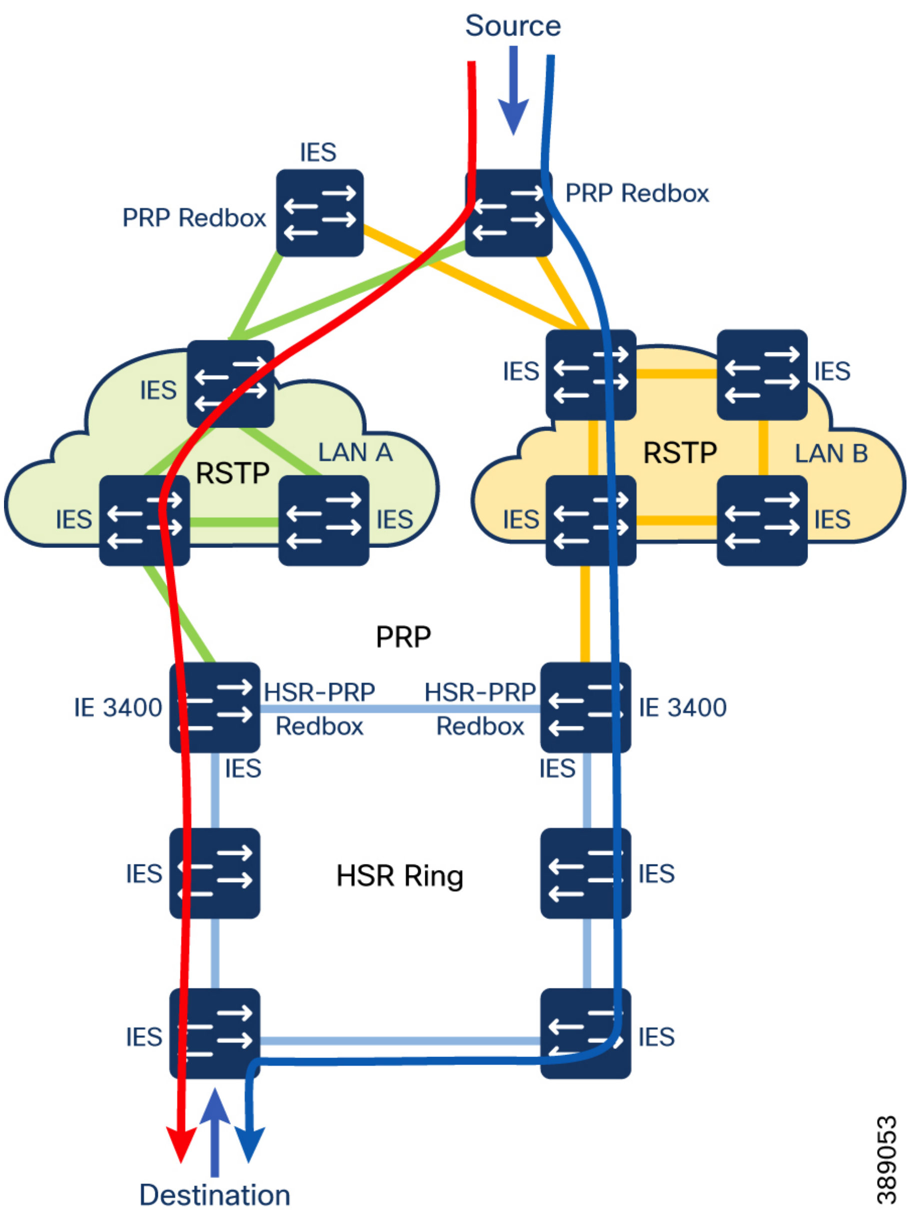
HSR to PRP Dual RedBox is used to connect PRP and HSR networks together. This feature is supported on Cisco IE 3400 switching products. This feature allows HSR + PRP RedBoxes to convert PRP frames to HSR frames and vice versa, all while protecting the network from any loops.

A maximum of 2 ports are configurable for HSR and a maximum of 2 ports are configurable for PRP when enabling HSR to PRP Dual RedBox on the Cisco IE switches. Specific interfaces are reserved for use of the HSR and PRP features. HSR to PRP Dual RedBox is configurable via CLI.

Note: Cisco recommends increasing the MTU size for switch interfaces participating in PRP LAN-A and LAN-B networks to account for the 6-byte PRP trailer added to every packet.

The following topology shows a combination of a station bus and process bus network, but it could also be a second-level station bus. High availability throughout both the station and the process bus network is achieved using a double LAN network on the station bus and an HSR ring of bridging end nodes on the process bus, as shown in figure below.

Figure 23 PRP-Based Station Bus and HSR-Based Process Bus



The redundant LAN networks A and B may be closed into a ring structure using RSTP. They are connected to the rings through redundancy boxes working in PRP LAN-A and LAN-B mode.

Typical deployment of HSR-PRP feature is to use two switches to connect to two different LANs namely LAN-A and LAN-B of a PRP network and HSR network. RedBoxes do not forward duplicate frames in the same direction to avoid loops. RedBoxes convert PRP frames to HSR frames and vice versa.

RedBoxes are configured to support PRP traffic on the interlink ports and HSR traffic on the ring ports. In this example traffic flows between PRP and HSR network through RedBoxes. Traffic in the network consisted of Sample Values, GOOSE and untagged IP packets. To validate the resiliency and the corresponding latency requirements of the network, failures were introduced at different points.

Steps to configure:

Follow these steps to configure HSR-PRP mode on the switch. Enabling HSR-PRP mode creates an HSR ring and a PRP channel.

Before you begin, please note:

- **HSR-PRP RedBox mode uses ports Gi1/1 and Gi1/2 as HSR ring 1 interfaces, and Gi1/3 (for RedBox A) or Gi1/4 (for RedBox B) as PRP channel 1 interfaces. These port assignments are fixed and cannot be changed. Therefore, HSR-PRP Dual RedBox mode is supported only on HSR ring 1.**
- **PRP uplink interfaces can be configured as trunk interfaces allowing VLANs of interest.**
- **PRP Dual Attached Nodes and RedBoxes add a 6-byte PRP trailer to the frame. To help ensure that all packets can flow through the PRP network, increase the MTU size for switches within the PRP LAN-A and LAN-B network to 1506**

1. Identify the required services and relevant VLANs and enable them across the topology as required.
2. Enable HSR PRP Redbox mode as per the device connection based on the PRP LAN it connects to. The following configuration sample shows enablement of HSR-PRP LAN B on an IE3400 thats connected to PRP LAN B segment. Enable option "lan –A" if the node is connected to PRP LAN A segment. Note that the PRP Path ID is set to 4 in the example. Ensure that the same PRP Path ID is used on the HSR-PRP redboxes when configured.

```
IE3400-PRP-HSR-002#config t
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400-PRP-HSR-002(config)#hsr-prp-mode enable ?
  prp-lan-a  Redbox Interlink is connected to lan-A
  prp-lan-b  Redbox Interlink is connected to lan-B
 IE3400-PRP-HSR-002(config)#hsr-prp-mode enable prp-lan-b ?
  <1-6>  PRP Path Id
  <cr>   <cr>

IE3400-PRP-HSR-002(config)#hsr-prp-mode enable prp-lan-b 4
```

3. Interfaces GigabitEthernet1/1 and GigabitEthernet1/2 are internally mapped to HSR Ring as and when HSR-PRP mode is enabled. This does not necessitate the need to attach HSR logical interface to the physical interfaces.

```
!
interface GigabitEthernet1/1
switchport trunk allowed vlan 1-99,101-111,113-2507,2509-4094
switchport mode trunk
!
!
```

```
interface GigabitEthernet1/2
switchport trunk allowed vlan 1-99,101-111,113-2507,2509-4094
switchport mode trunk
!
```

4. Configure HSR interface with the relevant VLANs allowed.

```
!
interface HSR-ring1
switchport trunk allowed vlan 1-99,101-111,113-2507,2509-4094
switchport mode trunk
!
```

5. Note that the remaining interfaces on IE3400 act like a PRP interface. It does not have to be configured to be a PRP channel explicitly unlike other Cisco Industrial Ethernet switches like IE4000 with regards to HSR – PRP mode. Ensure that the relevant VLANs are allowed on the interface. Interfaces other than GigabitEthernet1/1 and GigabitEthernet1/2 can be used as the third port that needs to be connected to a PRP LAN. The following example shows the use of interface GigabitEthernet2/1 as PRP LAN connecting interface.

```
!
interface GigabitEthernet2/1
description connected to PRP-LAN-B
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
!
```

6. Refer to PTP configuration section to configuration PTP on Cisco IE switches that participate in the network.
7. Refer to the HSR-SAN configuration section to configure HSR on Cisco IE switches that participate in the HSR ring.
8. Refer to the PRP RedBox configuration section to configure PRP on Cisco IE switches that participate in the PRP network.
9. Per VLAN Spanning Tree protocol is enabled by default on Cisco Industrial Ethernet switches.

After configuration of the mode, the following commands can be used for verification.

```
show prp statistics ingressPacketStatistics
PRP prp_maxchannel 2 INGRESS STATS:
PRP channel-group 1 INGRESS STATS:
  ingress pkt lan a: 2274884008
  ingress pkt lan b: 2264024229
  ingress crc lan a: 0
  ingress crc lan b: 0
```

```
  ingress danp pkt acpt: 302159955583
  ingress danp pkt dscrd: 290211947168
  ingress supfrm rcv a: 23249837
  ingress supfrm rcv b: 16995811
  ingress supfrm drop a: 0
  ingress supfrm drop b: 0
  ingress over pkt a: 202397706
  ingress over pkt b: 112441721
  ingress pri over pkt a: 0
  ingress pri over pkt b: 0
  ingress oversize pkt a: 0
  ingress oversize pkt b: 0
  ingress byte lan a: 26845590875254
  ingress byte lan b: 26732680591022
  ingress wrong lan id a: 9971181039
  ingress wrong lan id b: 9125419586
  ingress warning lan a: 1
  ingress warning lan b: 1
  ingress warning count lan a: 1
  ingress warning count lan b: 264076
  ingress unique count a: 182821250341
  ingress unique count b: 39580155704
  ingress duplicate count a: 290191970499
  ingress duplicate count b: 290191970499
  ingress multiple count a: 10141395
  ingress multiple count b: 9835039
PRP channel-group 2 INGRESS STATS:
  ingress pkt lan a: 0
  ingress pkt lan b: 0
  ingress crc lan a: 0
  ingress crc lan b: 0
  ingress danp pkt acpt: 0
  ingress danp pkt dscrd: 0
  ingress supfrm rcv a: 0
  ingress supfrm rcv b: 0
  ingress supfrm drop a: 0
  ingress supfrm drop b: 0
  ingress over pkt a: 0
  ingress over pkt b: 0
  ingress pri over pkt a: 0
  ingress pri over pkt b: 0
  ingress oversize pkt a: 0
  ingress oversize pkt b: 0
  ingress byte lan a: 0
  ingress byte lan b: 0
  ingress wrong lan id a: 0
  ingress wrong lan id b: 0
  ingress warning lan a: 0
```

```
    ingress warning lan b: 0
    ingress warning count lan a: 0
    ingress warning count lan b: 0
    ingress unique count a: 0
    ingress unique count b: 0
    ingress duplicate count a: 0
    ingress duplicate count b: 0
    ingress multiple count a: 0
    ingress multiple count b: 0


show prp statistics egressPacketStatistics
PRP channel-group 1 EGRESS STATS:
    duplicate packet: 1583568
    supervision frame sent: 82503
    packet sent on lan a: 2251149698
    packet sent on lan b: 2269842346
    byte sent on lan a: 26336822299655
    byte sent on lan b: 26799189437931
    egress packet receive from switch: 49243584
    overrun pkt: 0
    overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
    duplicate packet: 0
    supervision frame sent: 0
    packet sent on lan a: 0
    packet sent on lan b: 0
    byte sent on lan a: 0
    byte sent on lan b: 0
    egress packet receive from switch: 0
    overrun pkt: 0
    overrun pkt drop: 0

show hsr statistics ingressPacketStatistics
HSR ring 1 INGRESS STATS:
    ingress pkt port A: 300257905247
    ingress pkt port B: 299043985722
    ingress crc port A: 0
    ingress crc port B: 0
    ingress danh pkt portAcpt: 302160822001
    ingress danh pkt dscrd: 290212043493
    ingress supfrm rcv port A: 3049423002
    ingress supfrm rcv port B: 2235098598
    ingress overrun pkt port A: 202397706
    ingress overrun pkt port B: 112441721
    ingress byte port a: 26845633045958
    ingress byte port b: 26732720329413
```

show hsr statistics egressPacketStatistics
HSR ring 1 EGRESS STATS:
duplicate packets: 1583595
supervision frames: 11046825
packets sent on port A: 297221168245
packets sent on port B: 299851708069
byte sent on port a: 26336876852698
byte sent on port b: 26799247178194

Timing Protocols Implementation

NTP

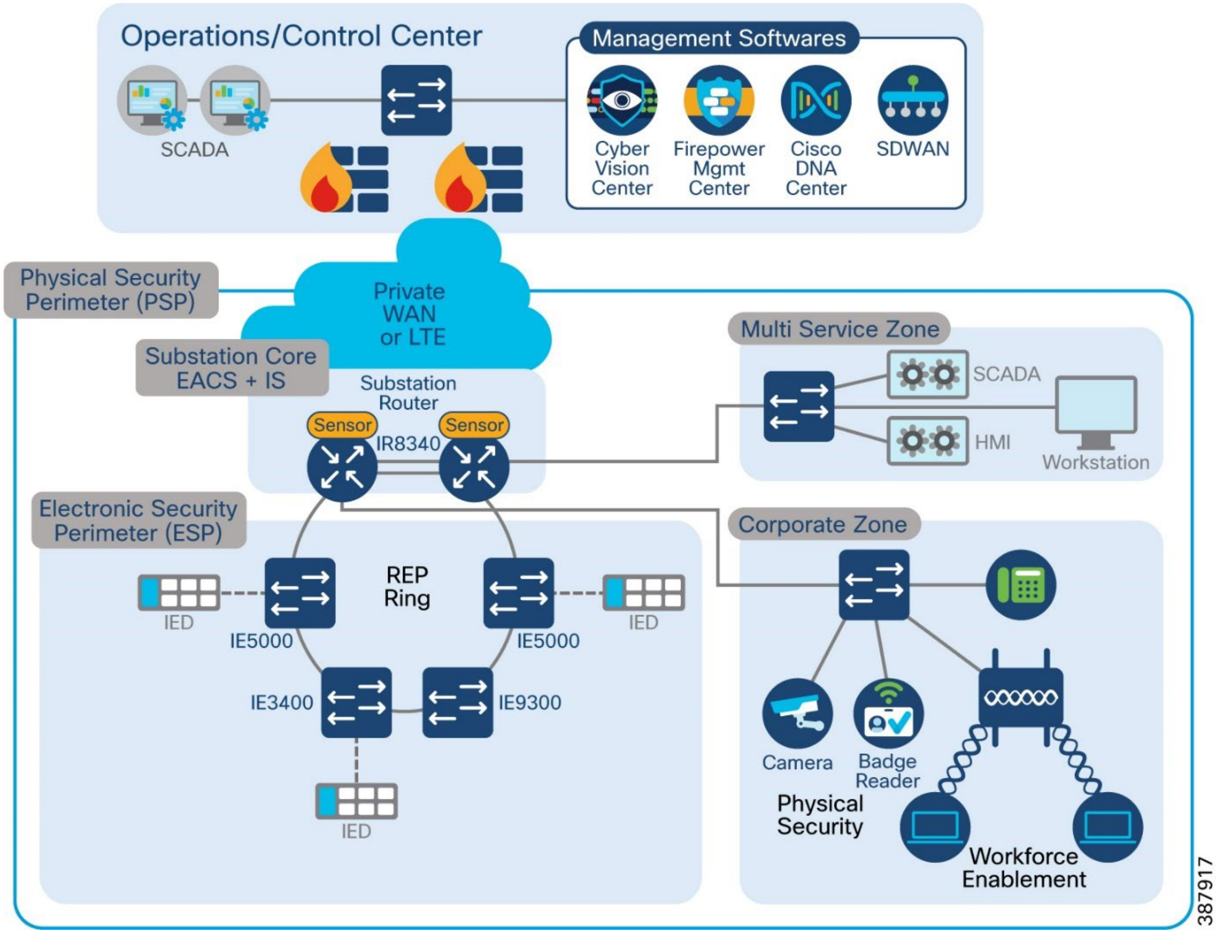
Network Time Protocol (NTP) is a networking protocol for synchronizing clocks across TCP/IP networks. NTP uses a hierarchical system of clocks to synchronize time across disparate hosts on the network.

This solution guide recommends the use of NTP as timing protocol over REP ring. It is to be noted that PTP over REP ring using Cisco IR8340 and IE9300 devices are not supported as of the IOS-XE version that was validated for this solution guide.

The following topology shows a REP ring being aggregated on Cisco IR8340 routers. IR8340 router acts as the NTP parent while the switches in the REP ring and devices that are connected onto the REP ring derive clocking from the IR8340 NTP parent. IR8340 can be configured to derive clock from multiple sources such as:

- PTP as reference clock for NTP.
- From another NTP parent that has better clock quality.

Figure 24 NTP in a Substation



The following section lists the various steps involved in configuring NTP.

Steps to Configure

1. Use the following commands on the device that acts as NTP Parent. This example uses PTP as a reference clock for NTP on the device that acts as NTP Parent. Ensure that PTP is configured and syntonized. Refer relevant section in this guide for PTP configuration steps.

```
!
ptp clock boundary domain 0  profile power
clock-port dynamic1
  transport ethernet multicast interface Gi0/1/4
clock-port dynamic2
  transport ethernet multicast interface Gi0/1/2
  vlan 4001
clock-port dynamic3
  transport ethernet multicast interface Gi0/1/5
clock-port dynamic4
  transport ethernet multicast interface Gi0/1/6
clock-port dynamic5
  transport ethernet multicast interface Gi0/1/8
!

Router#config t
```

Enter configuration commands, one per line. End with CNTL/Z.
ntp master
ntp refclock ptp
end
Router#write

2. Use the following commands to configure on the devices that derive clock from the NTP parent. For e.g., switches and other cisco networking devices that require clocking. We can also have multiple NTP servers to ensure resilience.

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
ntp server 50.1.0.1
ntp source Vlan 501
end
Router#write

Verification

Use the following commands to verify NTP.

On the device acting as NTP parent:

*Router#**show ntp status***
*Clock is **synchronized**, **stratum 1, reference is .PTP.***
*nominal freq is 250.0000 Hz, actual freq is 249.0581 Hz, precision is 2**10*
ntp uptime is 910000 (1/100 of seconds), resolution is 4016
reference time is E6A8847B.FFBE7988 (14:57:23.999 IST Thu Aug 18 2022)
clock offset is 0.9998 msec, root delay is 0.00 msec
root dispersion is 463.52 msec, peer dispersion is 450.92 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000116 s/s
system poll interval is 1024, last update was 709 sec ago.
Router#
*Router#**show ntp associations***

```
  address         ref clock       st   when   poll reach  delay  offset   disp
*~127.127.6.1      .PTP.           0     713   1024    37  0.000   0.999 450.92
 ~127.127.1.1      .LOCL.          7       9     16   377  0.000   0.000  1.204
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router#
```

On the device deriving clock from NTP Parent:

*Switch#**show ntp status***
*Clock is **synchronized**, **stratum 2**, reference is 50.1.0.1*
*nominal freq is 250.0000 Hz, actual freq is 250.0020 Hz, precision is 2**10*
ntp uptime is 8252800 (1/100 of seconds), resolution is 4000

reference time is E6A886ED.91A9FD78 (09:37:49.569 UTC Thu Aug 18 2022)
clock offset is -0.5000 msec, root delay is 1.00 msec
root dispersion is 470.58 msec, peer dispersion is 3.71 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000008011 s/s
system poll interval is 128, last update was 262 sec ago.
Switch#
Switch#show ntp associations

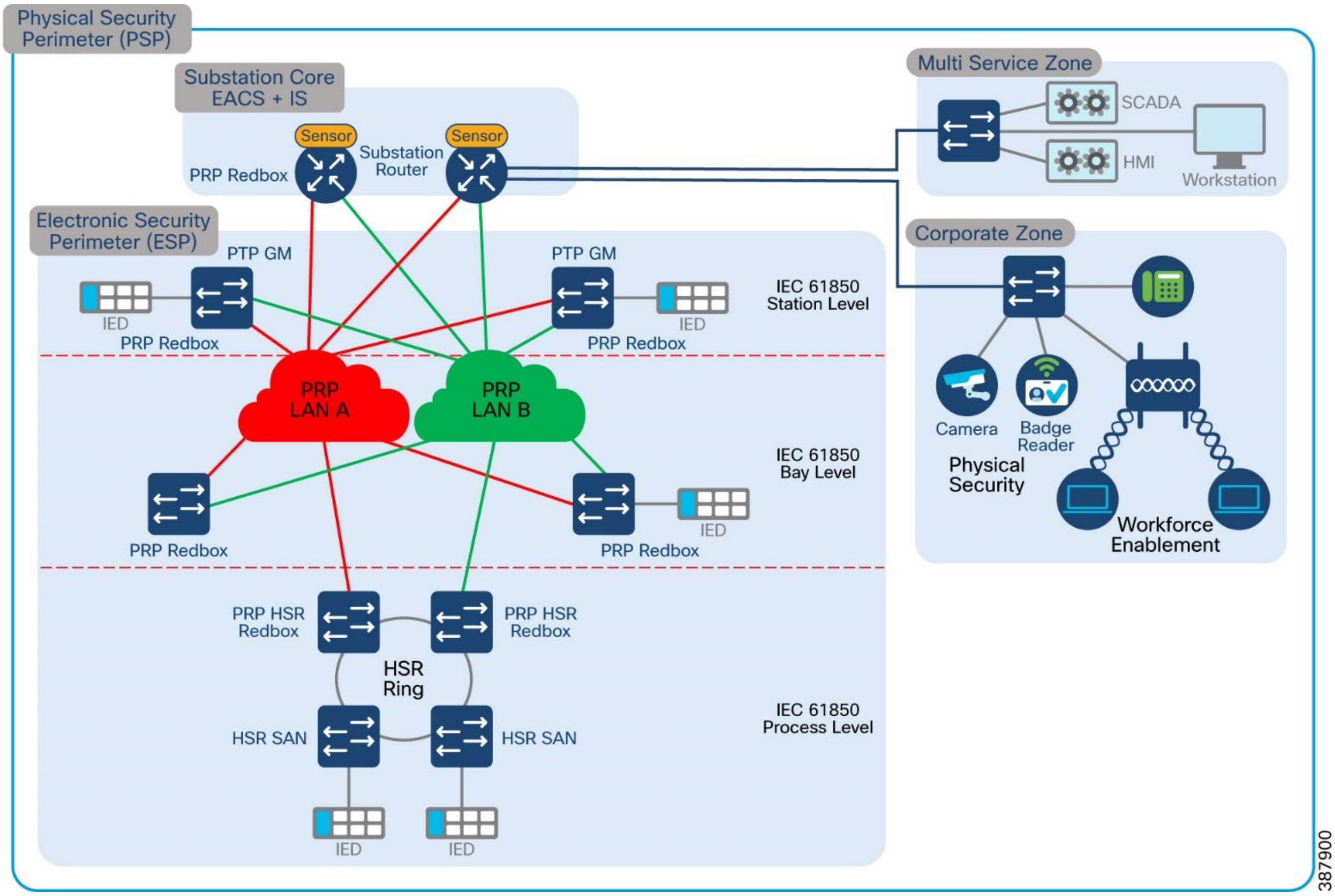
```
  address        ref clock      st   when   poll reach  delay  offset   disp
*~50.1.0.1       .PTP.           1    132    128   377  1.000  -0.500  3.719
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Switch#
Switch#show clock detail
09:42:19.650 UTC Thu Aug 18 2022
Time source is NTP
Switch#
```

PTP

Precision Time Protocol (PTP) is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead. The Power Profile is defined in C37.238-2011 - IEEE Draft Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications. This documentation uses the terms Power Profile mode when referring to this IEEE 1588 profile and its associated configuration values.

The following topology shows IE5000 as PTP Grand Master, Cisco IE9300 as PRP Redbox with PTP. IE5000 supports GNSS connectivity and hence is configured as PTP Grandmaster. Any other PTP Grandmaster can be connected to the topology if required.

Figure 25 PTP in Substation LAN



The following are the steps required to configure GNSS, PTP Grandmaster, PTP Boundary clock and PTP Transparent clocks.

Steps to Configure

1. Connect GNSS Antenna to the GNSS input port on the IE5000. The GNSS feature is supported only on IE 5000 SKUs that have Version ID (VID) v05 or higher and GNSS receiver firmware version 1.04. To verify these details, use the show version command.

2. Wait for the GNSS to synchronize with the GPS satellite. To verify use **show gnss status** command.

3. Configure the switch for grandmaster-boundary clock mode. PTP is not explicitly disabled on the interfaces of the switch. If required enabled PTP on the interfaces to transmit PTP packets.

```
!
ptp profile power
ptp mode gmc-bc pdelay-req
ptp domain 3
ptp priority <priority1>  <priority2>
!
```

4. Cisco IE9300 is configured as PRP Redbox and PTP boundary clock. Cisco IE9300 supports PTP over PRP. Configure the following on Cisco IE9300 for PTP over PRP. Interfaces GigabitEthernet1/0/21 and GigabitEthernet1/0/22 are PRP channel member interfaces. Similarly other interfaces through which PTP packets need to be transmitted can be configured. By default, the switches send PTP packets untagged.If PTP packets need to be tagged with a particular VLAN, ensure that the VLAN is allowed on all the relevant interfaces in the switches and enable under the specific interface.

```
!
ptp clock boundary domain 3 profile power
clock-port dynamic2
  transport ethernet multicast interface Gi1/0/21
clock-port dynamic3
  vlan 1
  transport ethernet multicast interface Gi1/0/22
!
```

5. Other Cisco Industrial Ethernet switches are configured as PTP transparent clocks. As pointed out earlier, the respective VLANs should be enabled and active on the switches involved in transmitting PTP packets.

6. Enable PTP transparent clock using the following commands. Some of the Cisco Industrial Ethernet switches support different versions of PTP Power profile viz (IEEE C37.238-2011 and 2017.) They are backward compatible. Ensure the appropriate version is enabled on the participating devices.

```
!
ptp profile <profile version>
ptp mode p2ptransparent
ptp domain 3
!
```

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

Table 8 PTP Roles, Platforms, and Supported Profile

PTP Role	Platform	Supported Profile
Grand Master	IE5000, IR8340, GT3000	PTP Power profile
PTP Transparent Clock both e2e and p2p	IE9300, IE4000, IE4010, IE3400	PTP Power Profile
PTP Boundary Clock	IE9300, IE4000, IE4010, IE3400	PTP power Profile 2011
PTP Over PRP Redbox	IE5000, IE4000, IE4010, IE3400	
PTP over HSR	IE5000, IE4000, IE4010, IE3400	

Verification

Use the following commands to verify various functions related to PTP.
Note: The following commands are supported on Cisco IE 5000, IE4010, IE3400 and IE4000 running IOS images.

```
IE5000-GM#show gnss status
 GNSS status: Enable
 Constellation: GPS
 Receiver Status: OD
 Survey progress: 100
 Satellite count: 8
 PDOP: 1.00    TDOP: 1.00
 HDOP: 0.00    VDOP: 0.00
 Alarm: None

IE5000-GM#show clock detail
13:25:39.215 IST Tue Aug 23 2022
Time source is GNSS
IE5000-GM#

IE5000-GM#show ptp clock
PTP CLOCK INFO
  PTP Device Type: Grand Master clock - Boundary clock
  PTP Device Profile: Power Profile IEEE-C37.238-2011
  Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Clock Domain: 3
  Number of PTP ports: 28
  PTP Packet priority: 4
  Time Transfer: Linear Filter
  Priority1: 128
  Priority2: 128
  Clock Quality:
      Class: 6
      Accuracy: Within 250ns
      Offset (log variance): N/A
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 0
  Local clock time: 13:26:42 IST Aug 23 2022

IE5000-GM#

IE5000-GM#show ptp parent
PTP PARENT PROPERTIES
  Local Clock:
  Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Local Port Number: 0

  Parent Clock:
  Parent Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
```

```
  Parent Port Number: 0
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Grandmaster Clock Quality:
        Class: 6
        Accuracy: Within 250ns
        Offset (log variance): N/A
        Priority1: 128
        Priority2: 128

IE5000-GM#
```

Note: The following commands are supported on Cisco IE9300 running IOS-XE Polaris images.

```
clarke-002-PRP#show clock detail
*12:59:42.464 IST Tue Aug 23 2022
Time source is PTP
clarke-002-PRP#
clarke-002-PRP#show ptp clock dataset time-properties

CLOCK [Boundary Clock, domain 3]

  Current UTC Offset Valid: FALSE
  Current UTC Offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GPS
clarke-002-PRP#

clarke-002-PRP#show prp control ptpProfile
PRP channel-group 1 PTP PROFILE value is 0x0 (l2-power)
PRP channel-group 2 PTP PROFILE value is 0x0 (l2-power)

clarke-002-PRP#show prp control ptpLanOption
PRP channel-group 1 PTP LAN OPT value is 0x3
PRP channel-group 2 PTP LAN OPT value is 0x0

clarke-002-PRP#
```

The following commands are supported on Cisco IE 5000, IE4010, IE3400 and IE4000 running IOS images.

```
IE4010-005#show ptp clock
PTP CLOCK INFO
  PTP Device Type: Peer to Peer transparent clock
  PTP Device Profile: Power Profile IEEE-C37.238-2017
  Clock Identity: 0x0:BF:77:FF:FE:27:DB:80
  Clock Domain: 3
  Number of PTP ports: 28
  PTP Packet priority: 4
  Delay Mechanism: Peer to Peer
  Local clock time: 11:17:04 IST Aug 23 2022

IE4010-005#show clock detail
11:17:08.545 IST Tue Aug 23 2022
Time source is PTP
IE4010-005#
```

Best Practices

- Cisco recommends that the PTP grandmaster (GM) be connected to both PRP LANs if you want to leverage the PTP over PRP feature. Otherwise, only devices in the single LAN where the PTP GM is connected can be synchronized.
- Disable PTP on interfaces where PTP is not necessary.
- Configure peer-to-peer transparent mode for PTP transparent clocks to reduce jitter and delay accumulation of PTP packets.

  Switch(config)# ptp mode p2ptransparent

- Configure the switch to process a non-compliant PTP grandmaster announce messages without Organization_extension and Alternate_timescale TLVs using the following command:

  Switch(config)# ptp allow-without-tlv

- In interoperability scenarios, it is best to use default PTP domain value, which as per C37.238:2011 standard is 0 (zero). The default PTP domain value on IE switches is set to 0 (zero). It can also be configured using the following command:

  Switch(config)# ptp domain

GT3000 as PTP PowerProfile GrandMaster for Substation LAN

Refer to the following to use GT3000 as PTP Power Profile GrandMaster in a Substation LAN Automation network.

https://www.microchip.com/en-us/products/clock-and-timing/systems/power-utility/gridtime-3000

Refer to the user manuals and other documents from the link above by scrolling to the documentation section in the page.

SCADA Enablement

To ensure the proper functioning of substations and related equipment, most utilities use SCADA systems to automate monitoring and control. New sites typically implement a SCADA system to monitor and control substations and related equipment. However, older facilities can also benefit by adding a

SCADA system or by upgrading an existing SCADA system to take advantage of newer technologies.

SCADA Implementation can be broadly classified by two major methods:

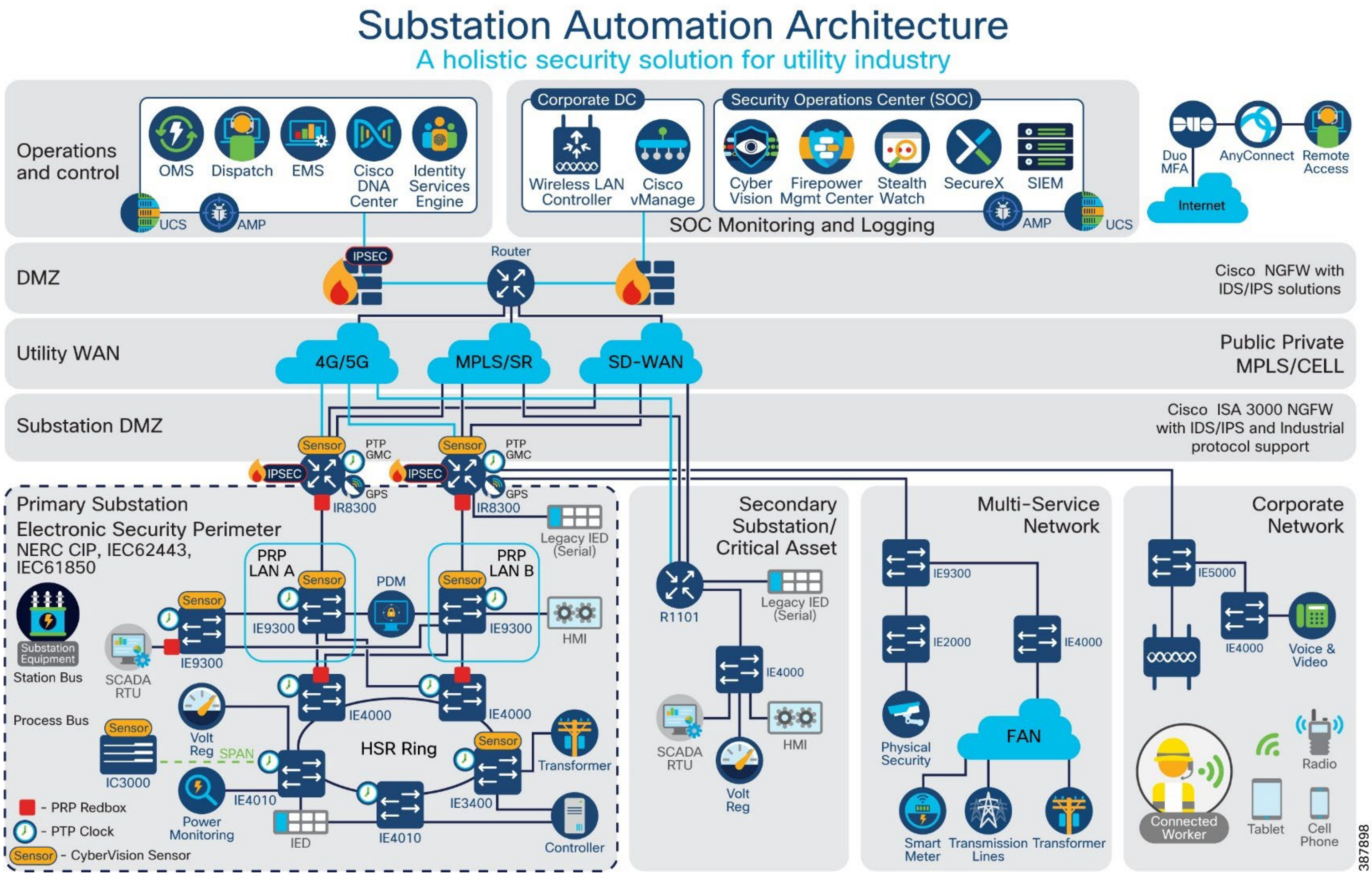
- Ethernet/IP SCADA Implementation which is based on Modbus IP, DNP3/IP, T104 and MMS protocols
- Legacy SCADA Implementation, which is based on Modbus Serial, DNP3 Serial, T101 protocols.

Legacy SCADA is implemented in two ways, either using Raw Socket or by using Protocol Translation.

- Serial based SCADA using Raw Socket
- SCADA Protocol Translation

SCADA validation topology

Figure 26 Substation Automation validation topology with SCADA



SCADA Communication with Serial-based SCADA using Raw Socket

Modbus

Modbus, which was specifically developed for use in electrical utility SCADA applications, is now the dominant protocol in those systems. It is also gaining popularity in other industries, including oil & gas, water, and wastewater. The Modbus specification defines multiple data types. Within each type, variations may be supported. These variations may describe whether the data are sent as 16-bit or 32-bit integral values; 32-bit or 64-bit floating point values.

Reading Data (Inputs)

The Modbus specification supports multiple methods of reading inputs individually or as a group. The FEP station can easily process change event data polled because the report includes the data type and point number, value and (optionally) time stamp.

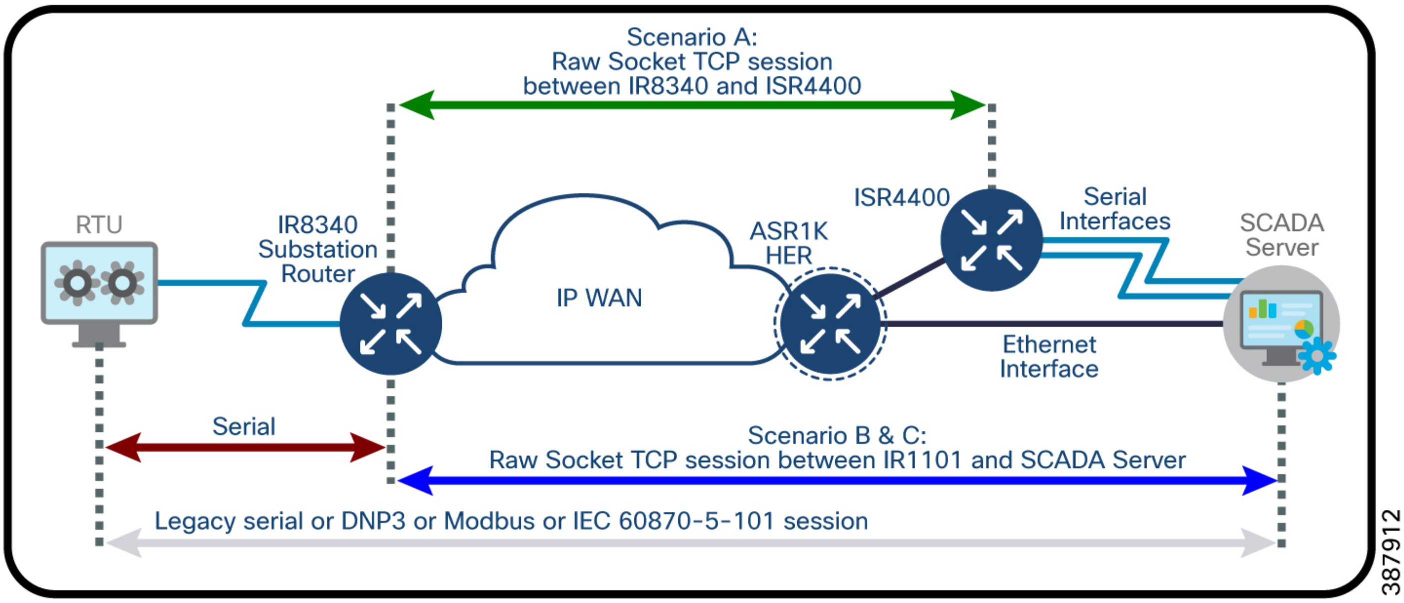
Control Operations (Output)

Modbus supports control operations via Write operation. Modbus output objects are also read/write; reading the output object returns the output stats (that is, the last command that was written). The actual value of the control point can be monitored via a binary or analog input.

Implementation Details

Cisco IR8340 is connected to an actuator or sensor in the Southbound via Serial and uses Modbus as the SCADA communication protocol. The Northbound FEP and Southbound Modbus actuator is simulated using the TMW Distributed Test Manager (DTM) application.

Figure 27 SCADA Raw Socket Implementation diagram



Enabling the IR8340 Serial Port and SCADA Raw Socket

Before you can enable and configure Protocol Translation on the IR8340, you must first enable the serial port on the IR8340 and enable SCADA encapsulation on that port.

You can configure the Modbus serial protocol stacks, which allow end-to-end communication between Control Centers and RTUs within a SCADA system.

```
SUMATRA-CELLULAR#sh running-config interface s 0/3/0
Building configuration...

Current configuration : 89 bytes
!
interface Serial0/3/0
  physical-layer async
  no ip address
  encapsulation raw-tcp
end

SUMATRA-CELLULAR#
```

This example shows how to enable serial port 0/3/0 and how to enable encapsulation on that interface to support SCADA protocols.

Configuring Raw Socket TCP

This example shows how to configure the parameters for raw socket.

```
SUMATRA-CELLULAR#sh running-config | sec line 0/3/0
line 0/3/0
  raw-socket tcp keepalive 10
  raw-socket tcp server 5012 99.99.99.2
  raw-socket special-char 7
  raw-socket packet-timer 1000
  raw-socket packet-length 1400
  stopbits 1
SUMATRA-CELLULAR#
```

Verifying Configuration

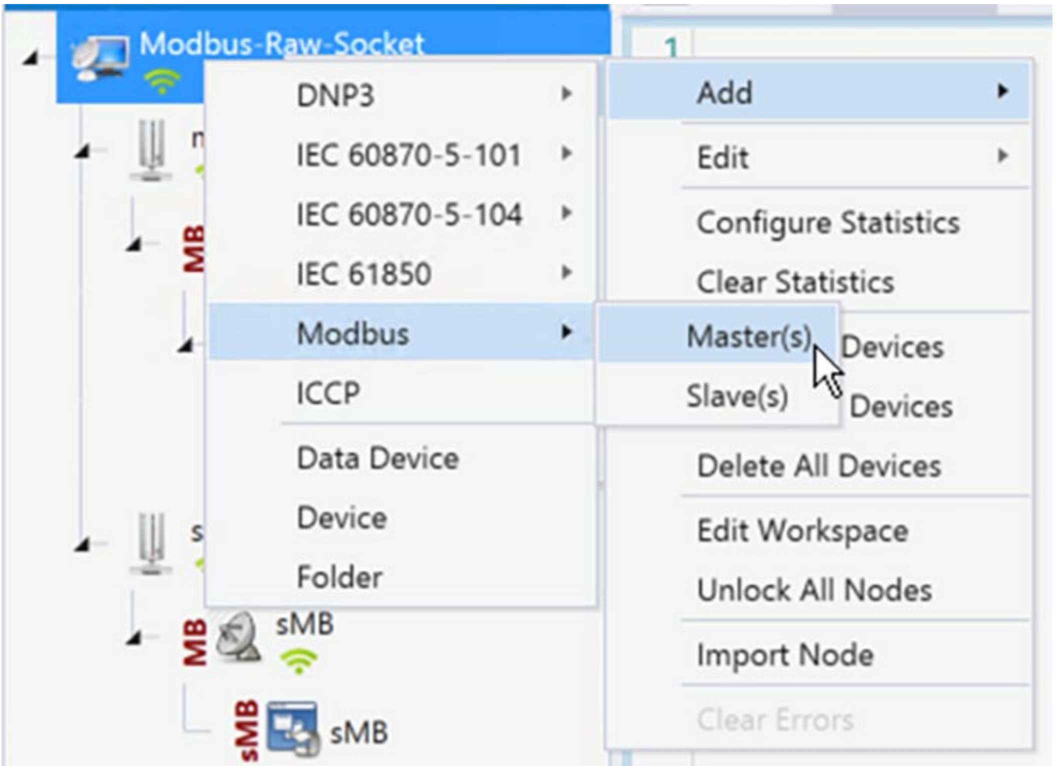
```
SUMATRA-CELLULAR#sh raw-socket tcp sessions
--------------------------------------------------------------------- TCP Sessions ---------------------------------------------------------------------
------
Interface tty             vrf_name            socket   mode    local_ip_addr  local_port    dest_ip_addr  dest_port
up_time      idle_time/timeout
   0/3/0    50                                      0   server      99.99.99.2     5012          listening     ----
--------            --------
   0/3/0    50                                      1   server      99.99.99.2     5012      192.168.4.171    51815
00:01:04      00:01:04/300sec

SUMATRA-CELLULAR#

 SUMATRA-CELLULAR#sh raw-socket tcp statistic
------------------------------------------------------------------ TCP-Serial Statistics------------------------------------------------------------------
Interface  tty              vrf_name             sessions       tcp_in_bytes          tcp_out_bytes
tcp_to_tty_frames     tty_to_tcp_frames
    0/3/0    50                                       1                6856                  5942
858                   857

SUMATRA-CELLULAR#
```

SCADA FEP Configuration

As per the topology, the SCADA FEP resides in the Control Center. The following configuration is required for the SCADA FEP to communicate with the SCADA Outstation/IED. In this implementation, Modbus acted as a SCADA FEP instead of the Modbus Raw Socket Server. The configuration provided below is specific to Modbus.

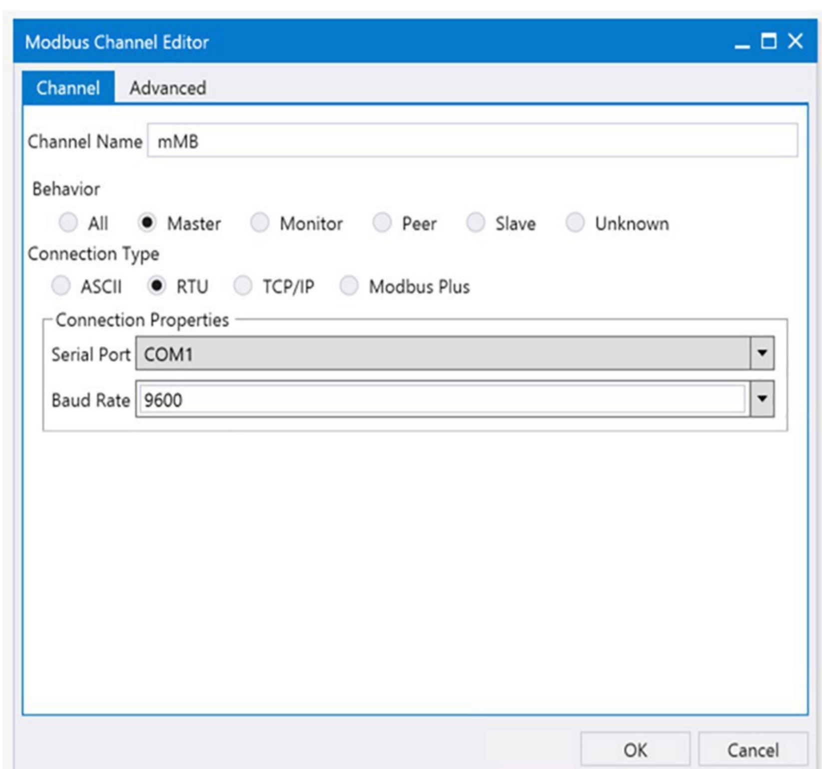
1. Open the SCADA FEP application and click **Add** a new **Modbus Master(s)**.

Figure 28 Modbus FEP Creation



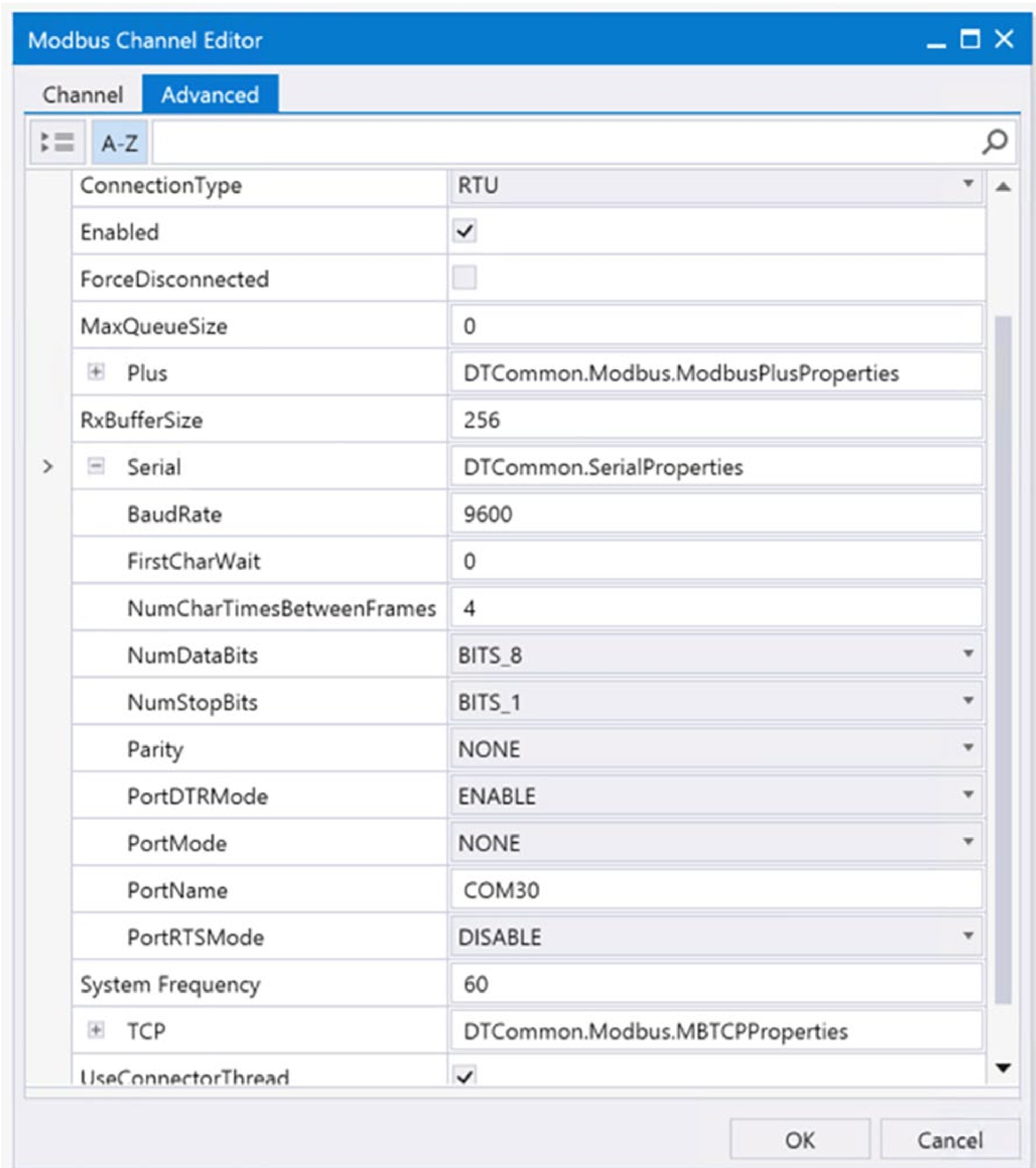
2. Configure the SCADA FEP Modbus Channel as shown in the following figure.

Figure 29 Modbus FEP Channel Configuration



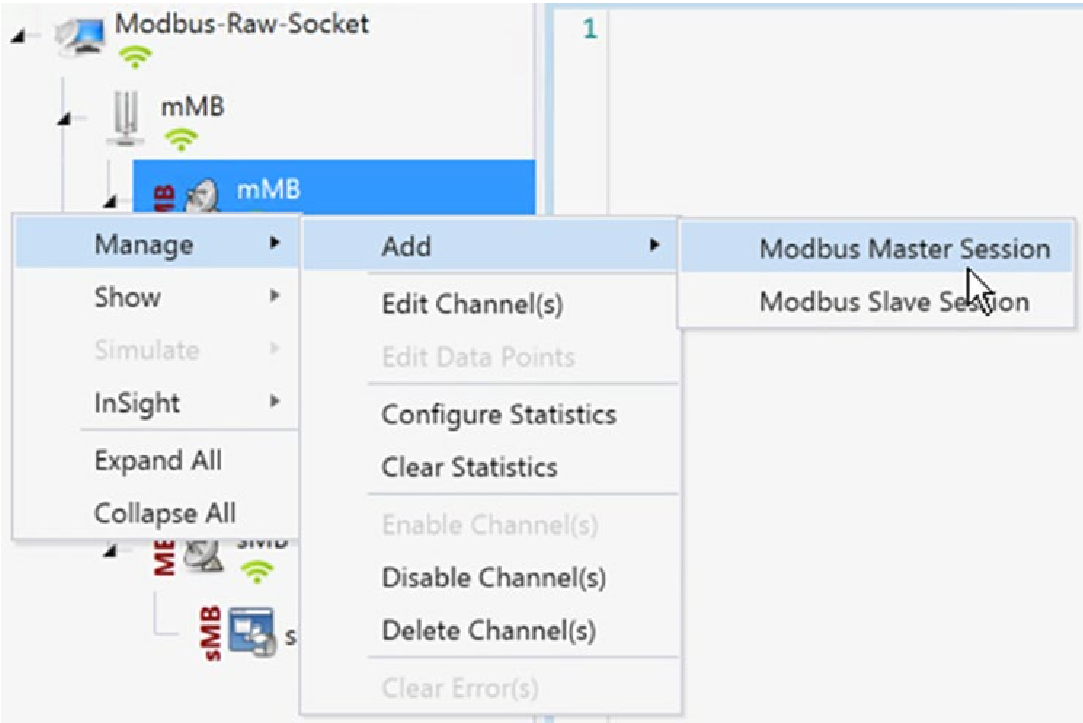
3. Configure the **Advanced** FEP Modbus Channel as shown in the following figure.

Figure 30 Modbus FEP advanced Channel configuration



4. Create Modbus FEP Session from the menu item as shown in the figure that follows.

Figure 31 Modbus FEP Session creation



5. Sample Modbus Data Points Table created by default.

Figure 32 Modbus FEP Data Points table

mMB(0)

Drag a column header and drop it here to group by that column

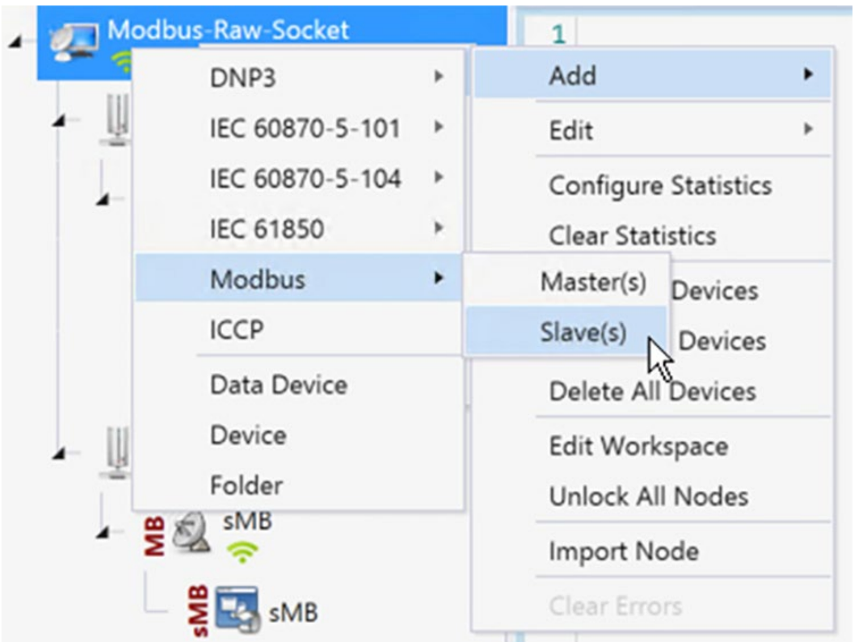
Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2

SCADA Outstation/IED Configuration

As per the topology, the SCADA Outstation/IED resides in the field area. The following configuration is required for the SCADA Outstation/IED to communicate with the SCADA FEP. In this implementation, we used the SCADA DTMW simulator instead of an actual SCADA device.

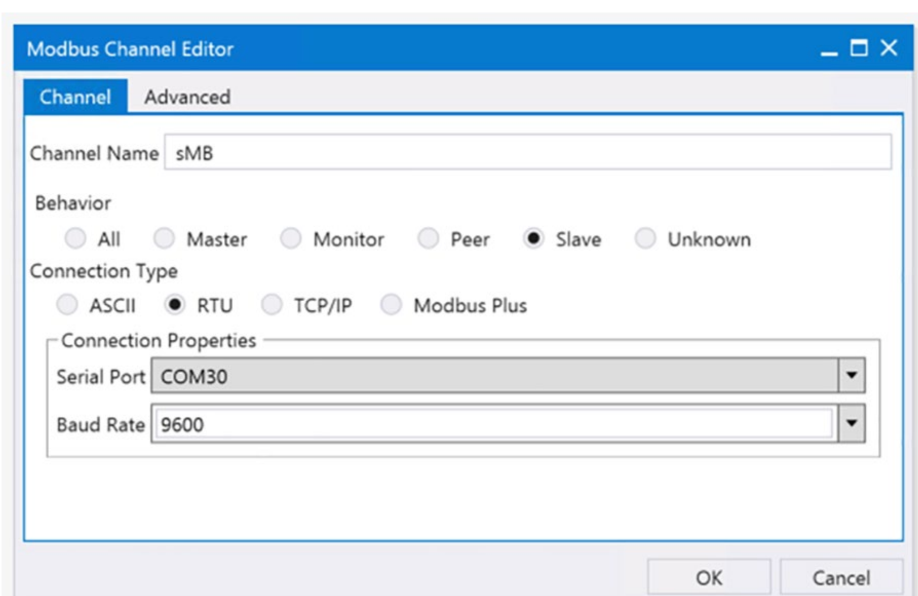
1. Open the SCADA Outstation/IED application and click **Add a new DNP3 Outstation/IED**.
2. From the Channel tab, configure the SCADA FEP as in the following figure.

Figure 33 Modbus IED Creation



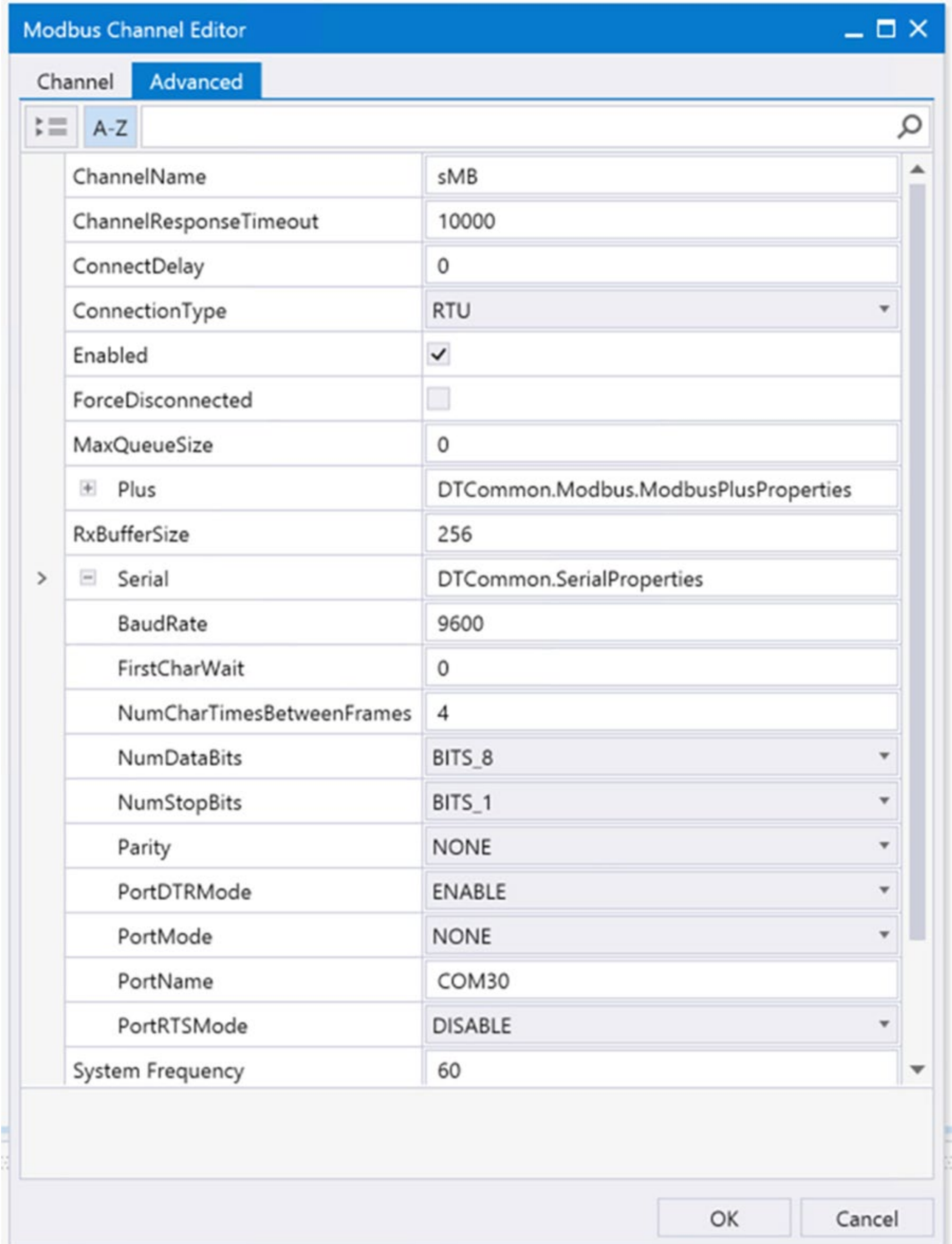
3. Configure the SCADA Outstation Modbus Channel as in the following figure.

Figure 34 Modbus IED Channel configuration



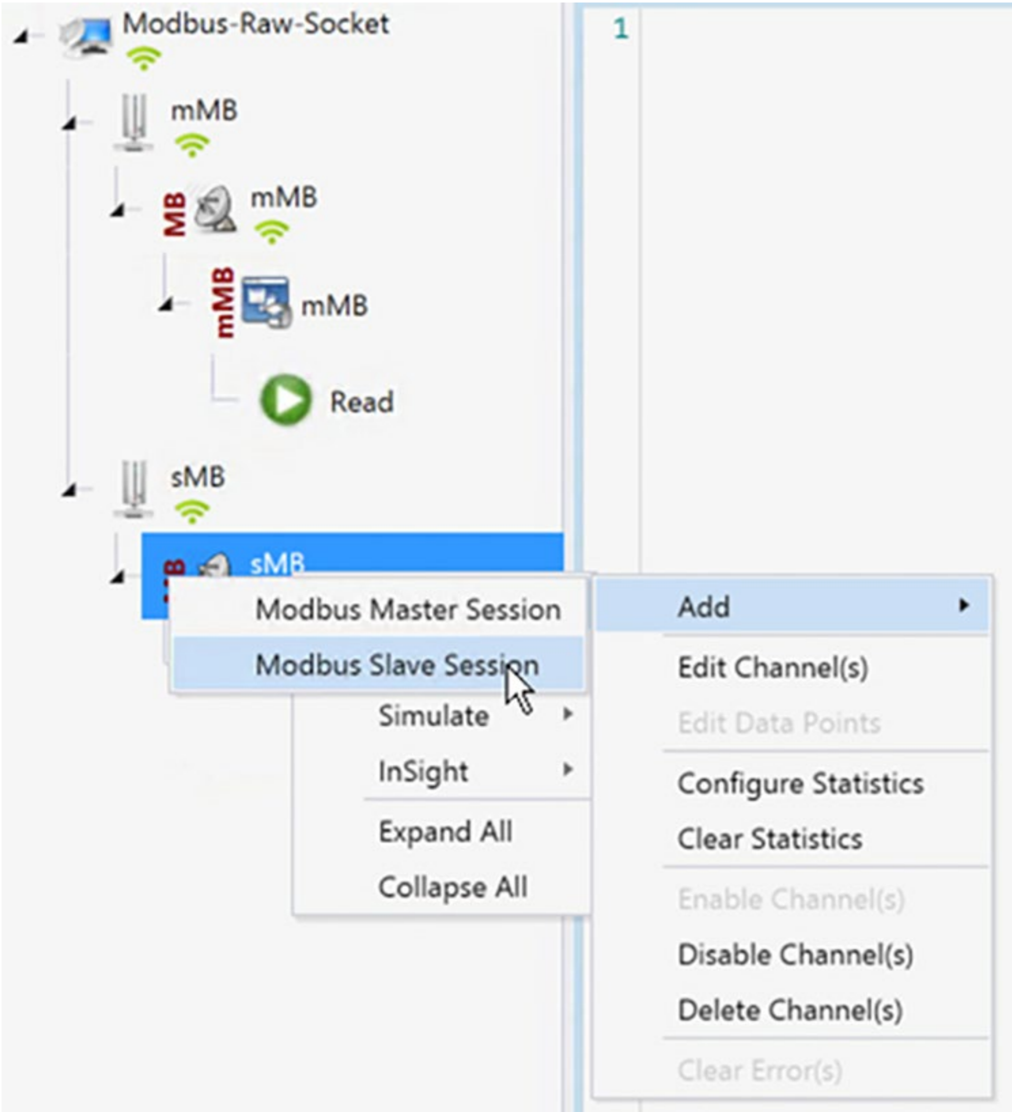
4. Configure the **Advanced Outstation/IED** Modbus Channel as shown in following figure.

Figure 35 Modbus IED Advanced Channel configuration



5. Create Modbus Outstation/IED Session from the menu item as shown in the following figure.

Figure 36 Modbus IED Session creation



SCADA Operations

The FEP and the Outstation/IED can communicate via the network. Poll and Control operations are initiated from the FEP. Unsolicited Reporting is sent to the FEP from the Outstation/IED. Figure 38 and Figure 39 show the Poll operation from the SCADA FEP. Control and Unsolicited Reporting can also be seen on the FEP Analyzer log.

Modbus Polling

The Poll operation is performed by the FEP. The FEP can execute a general Poll in which all the register values are read and sent to the FEP. In Figure 40, we see a general Poll executed on the FEP side.

1. The table that follows shows the SCADA Outstation/IED application initial data points.

Figure 37 Modbus IED Data Points table

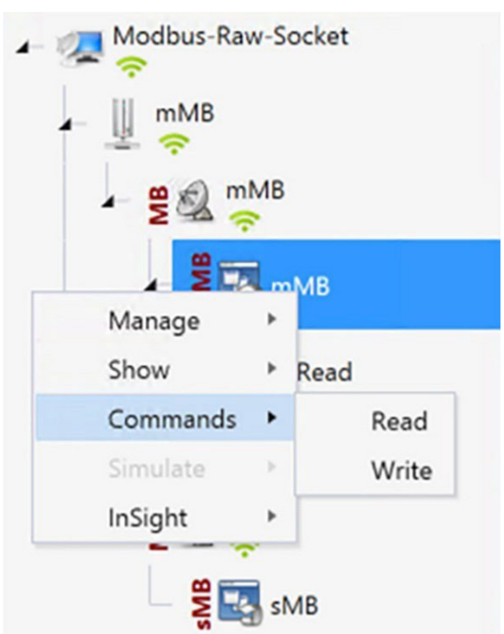
sMB(0)

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3

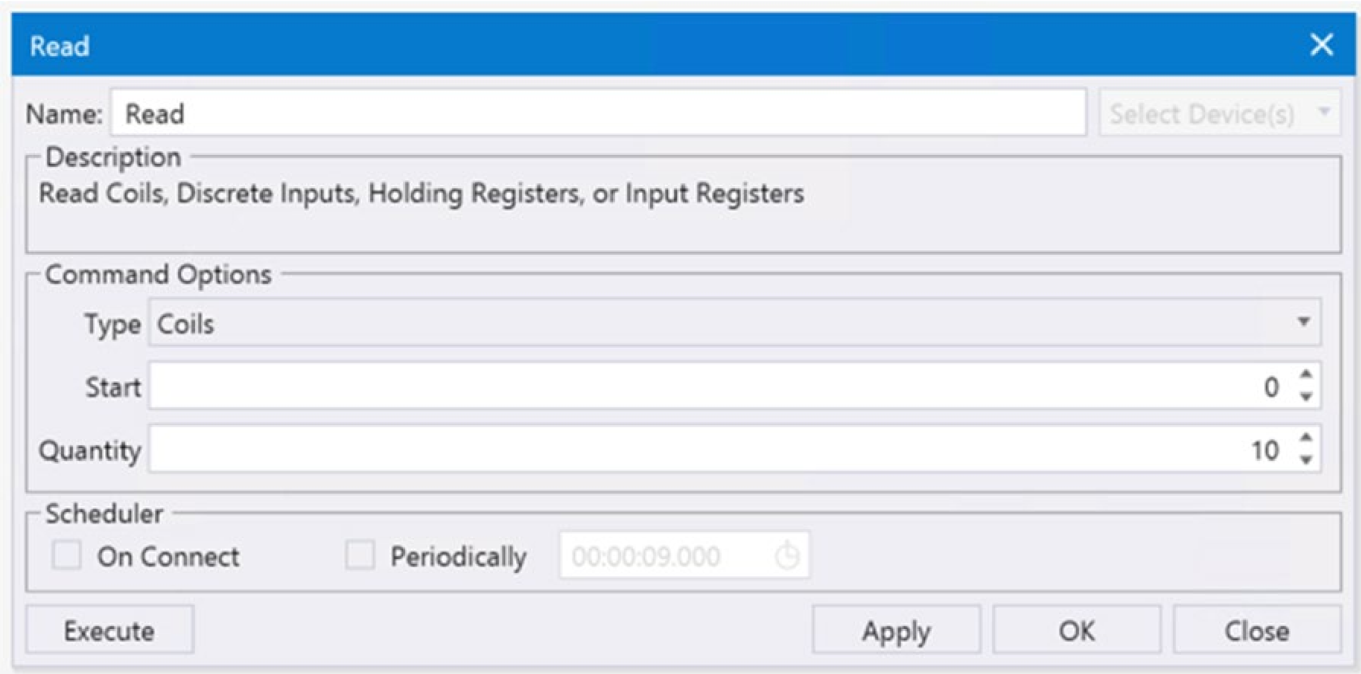
2. Right Click on **FEP** and choose the **Commands** and then the **Read** menu item.

Figure 38 Modbus Read Command



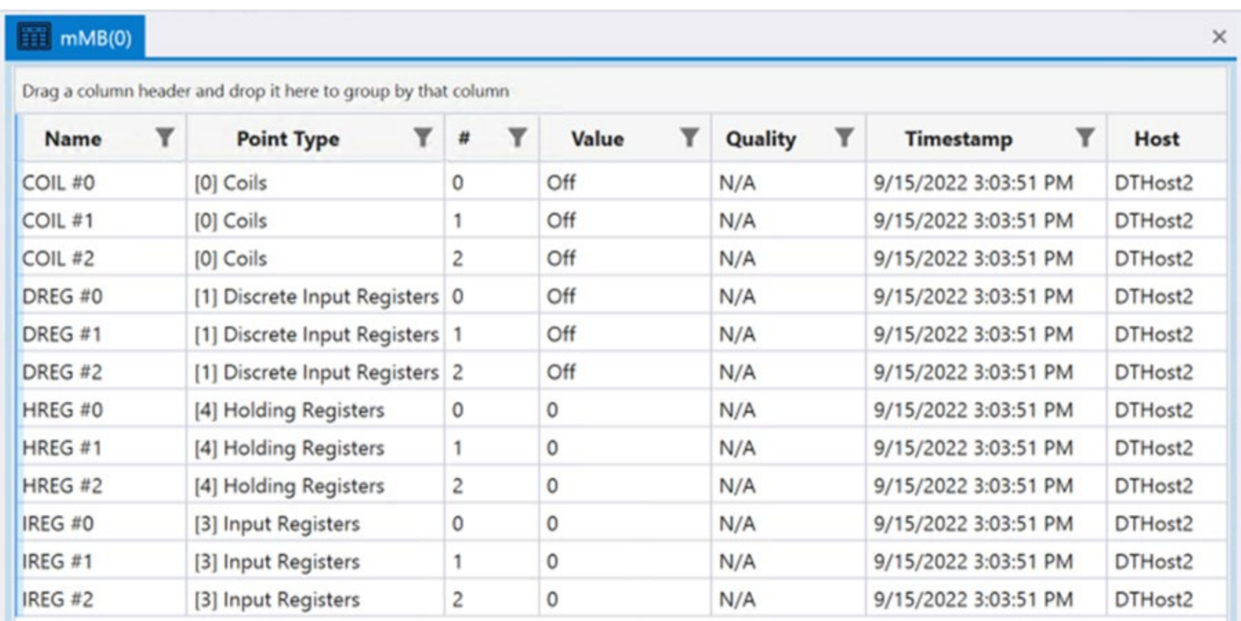
3. Use the Read window to read **COILS** starting from Register value **0.**

Figure 39 Modbus Read command config window



4. On the FEP data table verify the COILS values for the specific Registers are updated as per the values from IED/Outstation register values.

Figure 40 Updated Modbus FEP Data Points table



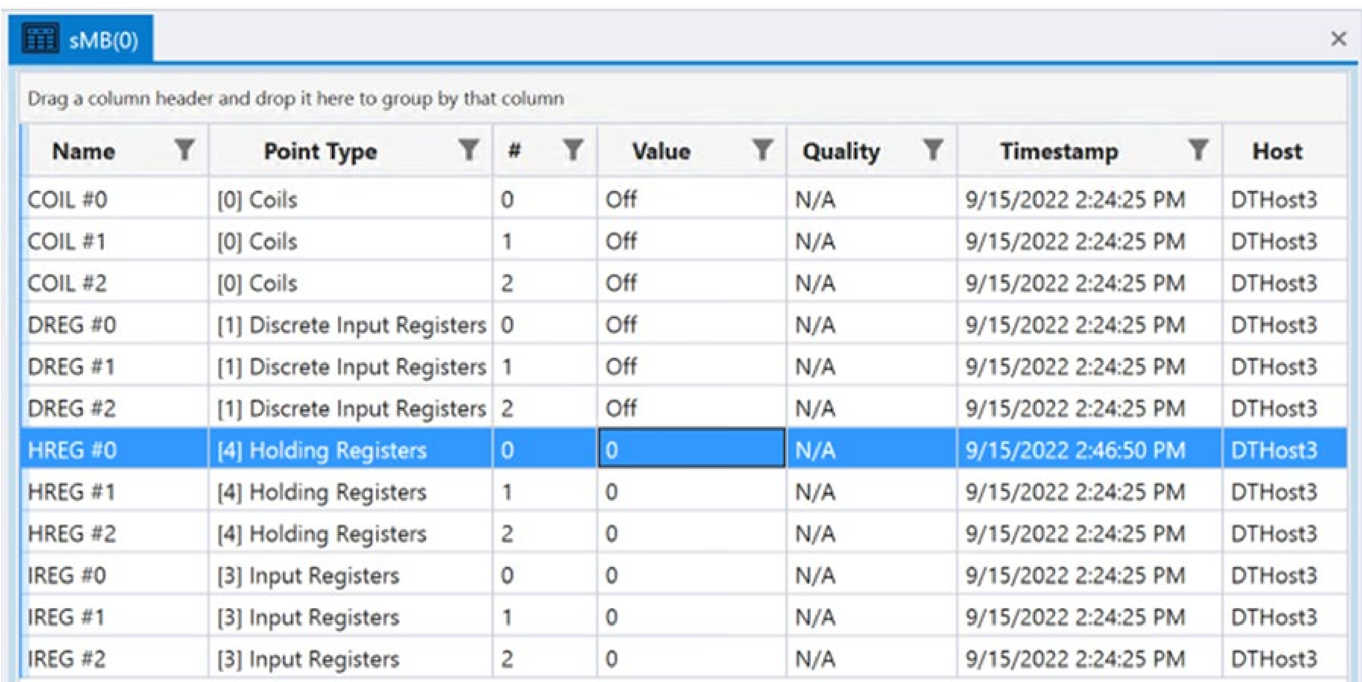
Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2

Modbus Control

The Control operation sends the control command from the SCADA FEP to the SCADA Outstation/IED for the purpose of controlling the operation of end devices. The control command can be executed, and the results can be seen on the analyzer. The value of Control Relay Output is changed and the same is notified to the FEP. SCADA Control operation has been validated in the following sequence of steps:

1. The Initial Holding Registers status would be noted down on SCADA Outstation/IED. Following Figure shows the Holding Register status before sending the control command to the Outstation/IED. Now we will issue a command from the Northbound simulator to change the state of the register to ON.

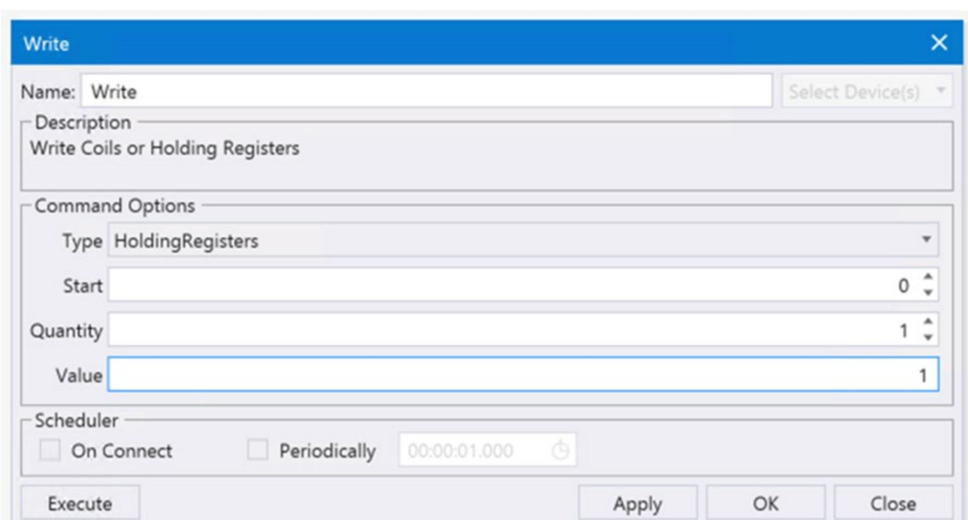
Figure 41 Modbus IED Initial Data Points table



Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 2:46:50 PM	DTHost3
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3

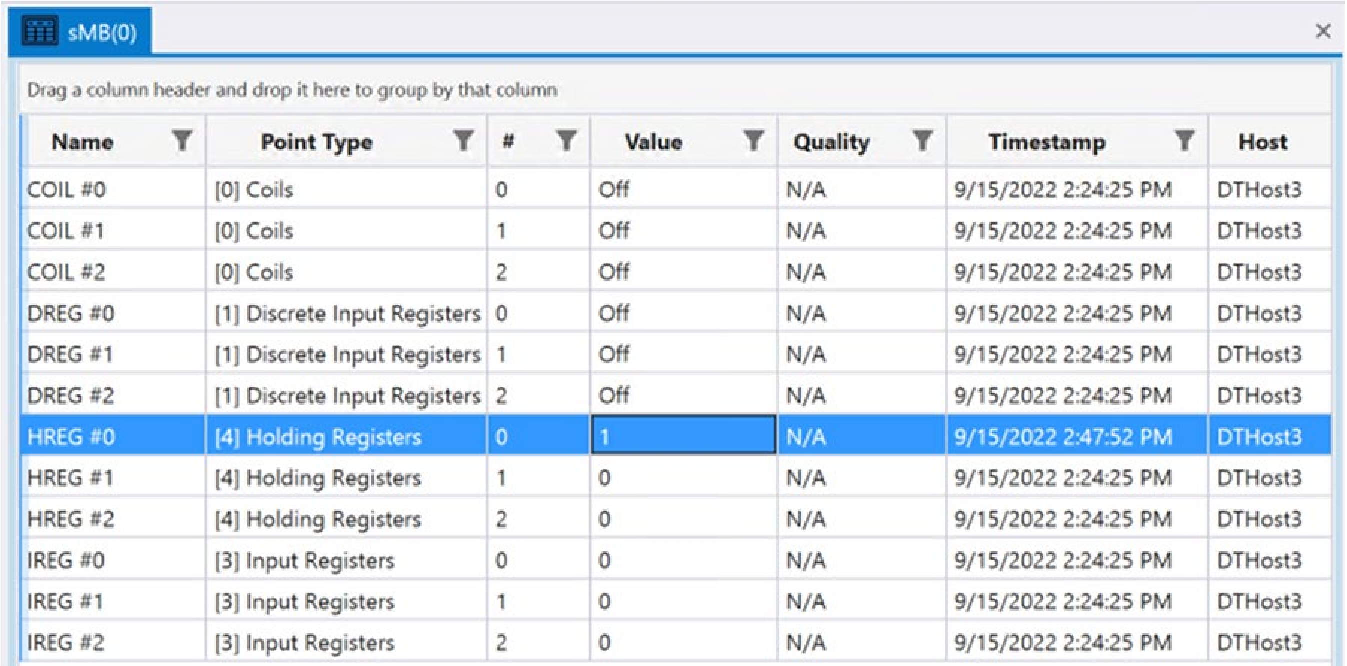
2. Send a **Write** or **Control command** from FEP to the Outstation/IED using the below write window. In this window, the command is written to the **Holding Register** with the starting value of **0** and the value is **1**.

Figure 42 Modbus Control Command config window



3. On the IED data table verify the Holding Register is updated with the values of **Write** or **Control Command** from the previous step.

Figure 43 Modbus IED updated with control command



sMB(0)

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #0	[4] Holding Registers	0	1	N/A	9/15/2022 2:47:52 PM	DTHost3
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3

SCADA Protocol Translation Use Case

The IR8340 performs Protocol Translation for the following protocols:

- IEC 60870 T101 to/from IEC 60870 T104
- DNP3 serial to DNP3 IP

For more details on SCADA, please refer to the Cisco IR8340 SCADA Configuration Guide at the following URL:

https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17_7/m_scada.html

This section provides implementation details for the following SCADA protocol translation scenario.

DNP3 Serial (Southbound) to DNP3 IP (Northbound) Translation Use Case

DNP3

DNP, which was specifically developed for use in electrical utility SCADA applications, is now the dominant protocol in those systems. It is also gaining popularity in other industries, including oil & gas, water, and wastewater. The DNP specification defines a substantial number of data types. Within each type, multiple variations may be supported. These variations may describe whether the data are sent as 16-bit or 32-bit integral values; 32-bit or 64-bit floating point values; with or without timestamps; and with or without quality indicators (flags).

Reading Data (Inputs)

The DNP3 specification supports multiple methods of reading inputs individually or as a group. For example, multiple types of data can be encapsulated in a single message to improve efficiency. Time stamps and data quality information can also be included.

DNP3 also supports change events. By polling for change events, the FEP station can reduce overall traffic on the line, as only values that have changed are reported. This is commonly called Report by Exception (RBE). To further improve efficiency, DNP3 also supports unsolicited reporting. With unsolicited reporting, Outstation/IED devices can send updates as values change, without having to wait for a poll from the FEP.

The FEP station can easily process change event data (polled or unsolicited) because the report includes the data type and variation, point number, value, and (optionally) time stamp and quality indicators.

Control Operations (Output)

DNP3 supports control operations via output object groups (Control Relay Output Blocks or CROBs and Analog Output Blocks). DNP3 output objects are also read/write; reading the output object returns the output stats (that is, the last command that was written). The actual value of the control point can be monitored via a binary or analog input.

DNP3 also supports a variety of functions commonly used on control applications, such as pulsed and paired outputs.

Implementation Details

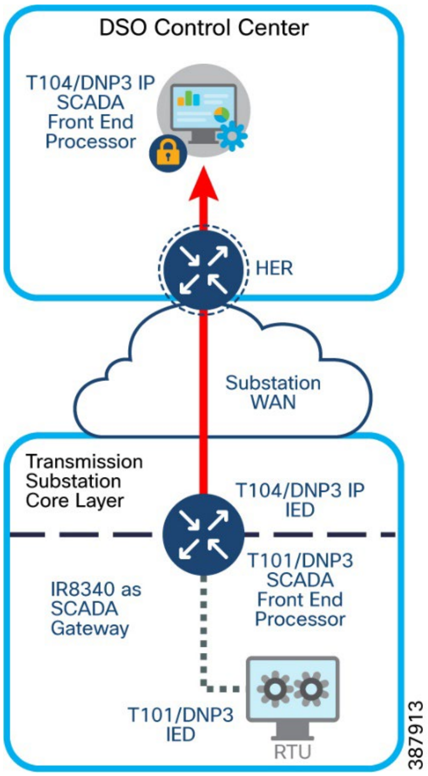
Cisco IR8340 is connected to an actuator or sensor in the Southbound via Serial and uses DNP3 as the SCADA communication protocol. The Southbound DNP3 actuator is simulated using the TMW DTM application. The Northbound DNP3 IP SCADA software is simulated using the TMW Distributed Test Manager (DTM) application.

In the network, the Control Center always serves as the FEP in the network when communicating with the IR8340. The IR8340 serves as a proxy FEP station for the Control Center when it communicates with the RTU.

The IR8340 provides protocol translation to serve as a SCADA gateway to do the following:

1. Receive data from RTUs and relay configuration commands from the Control Center to RTUs.
2. Receive configuration commands from the Control Center and relay RTU data to the Control Center.

Figure 44 Protocol Translation implementation diagram



Enabling the IR8340 Serial Port and SCADA Encapsulation

Before you can enable and configure Protocol Translation on the IR8340, you must first enable the serial port on the IR8340 and enable SCADA encapsulation on that port.

You can configure the DNP3 serial and DNP3 IP protocol stacks, which allow end-to-end communication between Control Centers and RTUs within a SCADA system.

```
SUMATRA-CELLULAR#sh run interface Serial0/3/0
interface Serial0/3/0
physical-layer async
no ip address
encapsulation scada
end
SUMATRA-CELLULAR#
```

The example above shows how to enable serial port 0/3/0 and how to enable encapsulation on that interface to support SCADA protocols.

DPN3-serial

The following example shows how to configure the parameters for the DPN3-serial protocol stack:

```
SUMATRA-CELLULAR#sh run | sec dnp3-serial
scada-gw protocol dnp3-serial
channel serial
```

```
  unsolicited-response enable
  bind-to-interface Serial0/3/0
session serial1
  attach-to-channel serial
SUMATRA-CELLULAR#
```

DNP3 IP

The following example shows how to configure the DNP3 IP parameters:

```
SUMATRA-CELLULAR#sh run | sec dnp3-ip
scada-gw protocol dnp3-ip
channel ip
  link-addr dest 4
  tcp-connection local-port default remote-ip 192.168.4.171/0
session ip1
  attach-to-channel ip
  link-addr source 3
  map-to-session serial1
SUMATRA-CELLULAR#
```

Start or Stop Protocol Translation

To start the protocol translation engine on the router, enter the following commands:

```
SUMATRA-CELLULAR# configure terminal
SUMATRA-CELLULAR(config)#scada-gw enable
```

To stop the protocol translation engine on the router, enter the following commands:

```
SUMATRA-CELLULAR# configure terminal

SUMATRA-CELLULAR(config)# no scada-gw enable
```

Verifying Configuration

```
SUMATRA-CELLULAR#sh scada tcp
DNP3 network channel [ip]: 4 max simultaneous connections
conn: local-ip: 99.99.99.2 local-port 20000    remote-ip 192.168.4.171    data-socket 1
Total:
  1 current client connections
  0 total closed connections
SUMATRA-CELLULAR#

SUMATRA-CELLULAR#sh scada statistics
DNP3 network Channel [ip]:
  210 messages sent, 7 messages received
```

```
  0 timeouts, 0 aborts, 0 rejections

  202 protocol errors, 202 link errors, 0 address errors

DNP3 serial Channel [serial]:


  520 messages sent, 108 messages received

  2 timeouts, 0 aborts, 0 rejections

  0 protocol errors, 8 link errors, 0 address errors
SUMATRA-CELLULAR#
```

```
SUMATRA-CELLULAR#
SUMATRA-CELLULAR#sh line 0/3/0
   Tty Line Typ     Tx/Rx     A Modem  Roty AccO AccI  Uses  Noise Overruns  Int
  0/3/0   50 TTY   9600/9600 -     -      -    -    -     0      0    0/0    Se0/3/0

Line 0/3/0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 1 stopbits, 8 databits
Status: Ready
Capabilities: none
Modem state: Ready
Modem hardware state: noCTS noDSR  DTR noRTS

SUMATRA-CELLULAR#sh run int serial0/3/0
Building configuration...

Current configuration : 87 bytes
!
interface Serial0/3/0
physical-layer async
no ip address
encapsulation scada

end

SUMATRA-CELLULAR#
```

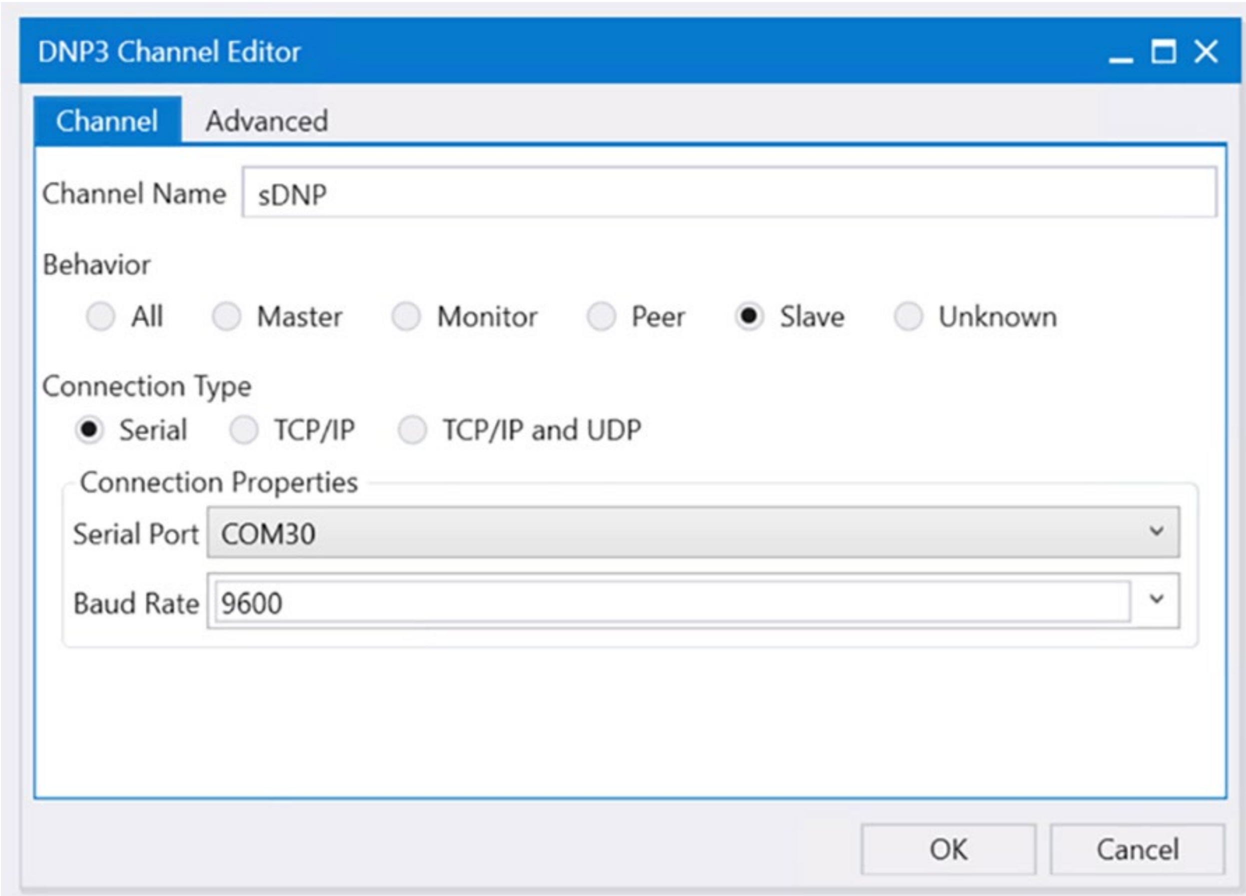
Southbound DNP3 TMW Configuration

Channel Configuration

The Southbound serial IED is simulated using TMW software. In this example, as shown in below Figure, the serial port COM30 with Baud Rate 9600 is connected to Async0 of Cisco IR8340.

1. Create DNP3 IED Channel

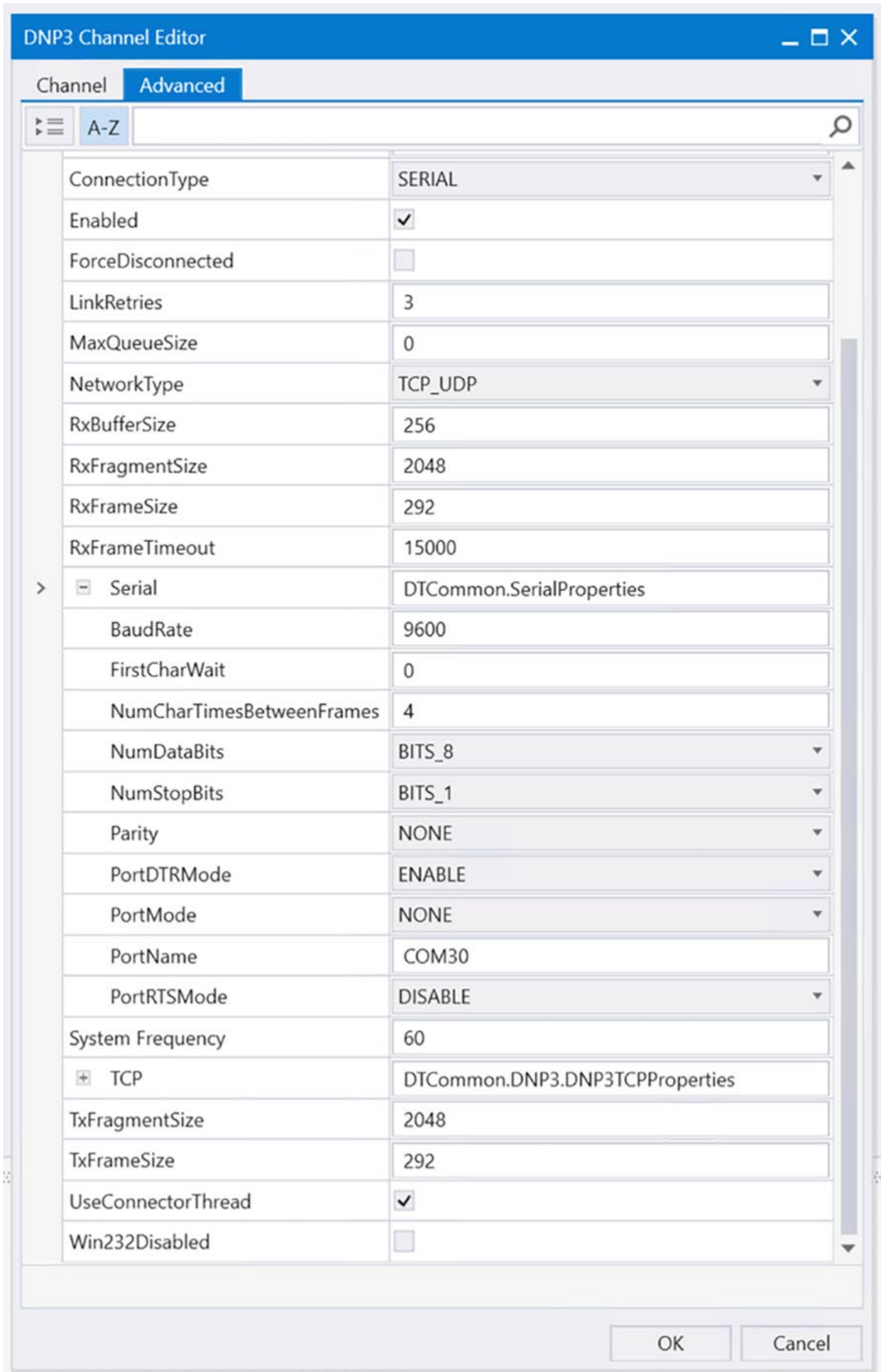
Figure 45 DNP3 IED Channel Configuration



2. Create DNP3 IED Advance Channel configuration

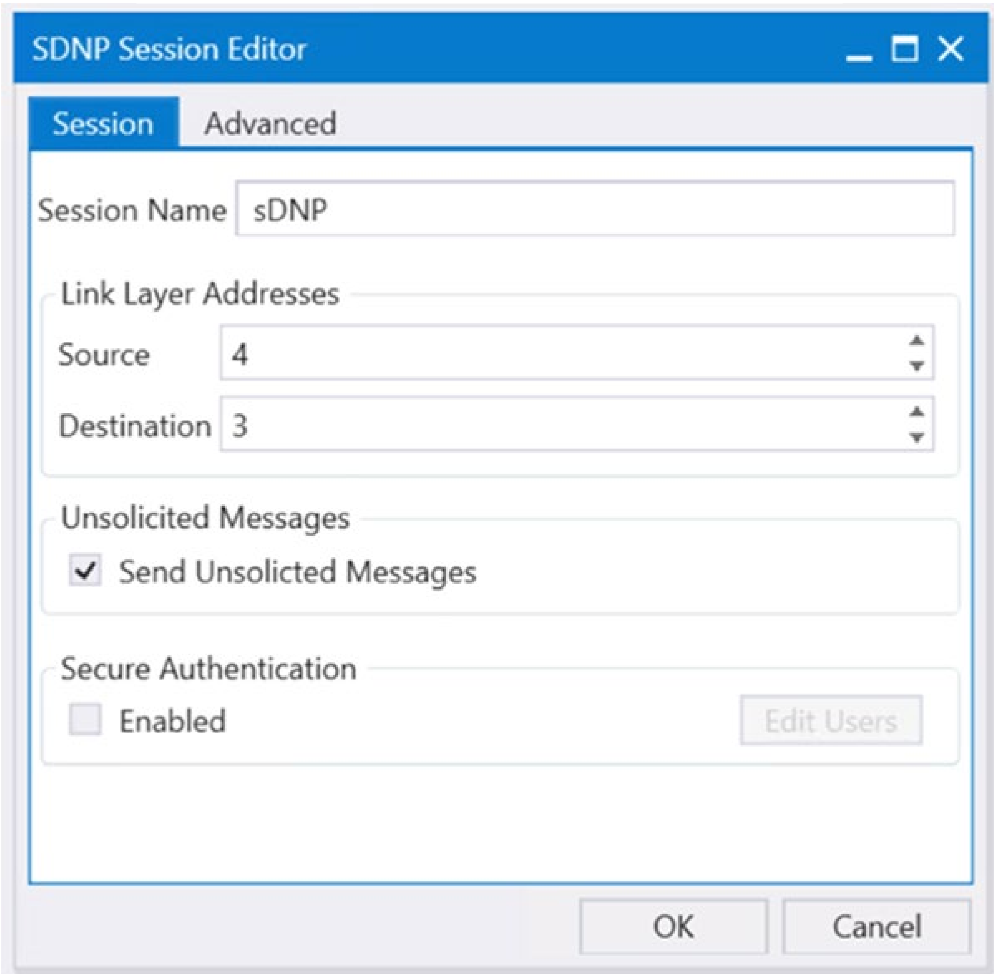
Make sure Parity is set to **None**, port is configured in DTR mode, StopBits is **1**, and DataBits is **8.**

Figure 46 DNP3 IED Advance Channel configuration



3. Create DNP3 IED Sessions, the DNP3 Southbound serial RTU simulator is configured as Outstation/IED and the source and destination layers are configured as 4 and 3 respectively. See below Figure.

Figure 47 DNP3 IED Session creation

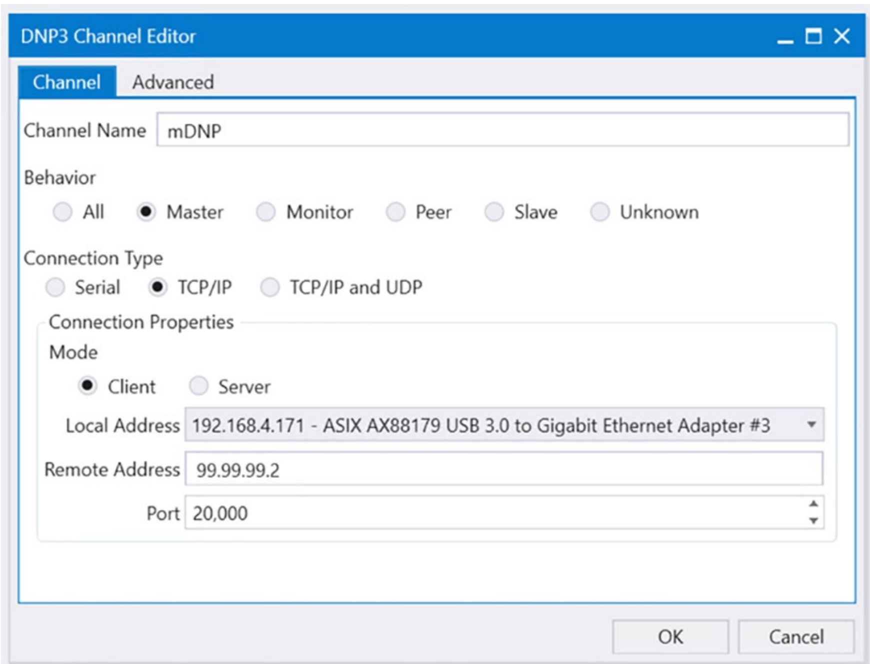


Northbound DNP3 IP TMW Configuration

DNP3 IP Channel Configuration

The TMW DTM software is configured in the DNP3 IP. FEP mode is used to simulate Control Center SCADA software. See the figure that follows.

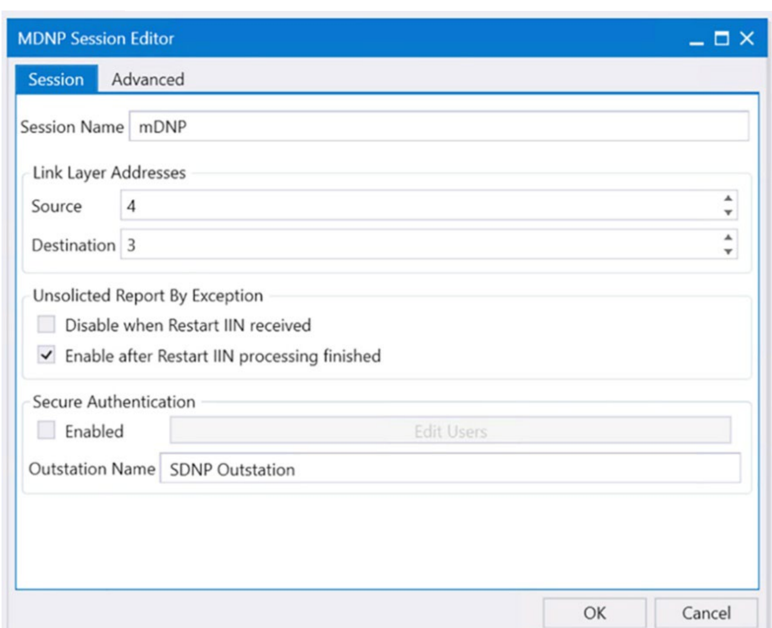
Figure 48 DNP3 FEP Channel configuration



DNP3 IP Session-related Configuration

Configure the DNP3 IP Link layer address 4 and 3. See the figure that follows.

Figure 49 DNP3 FEP session configuration

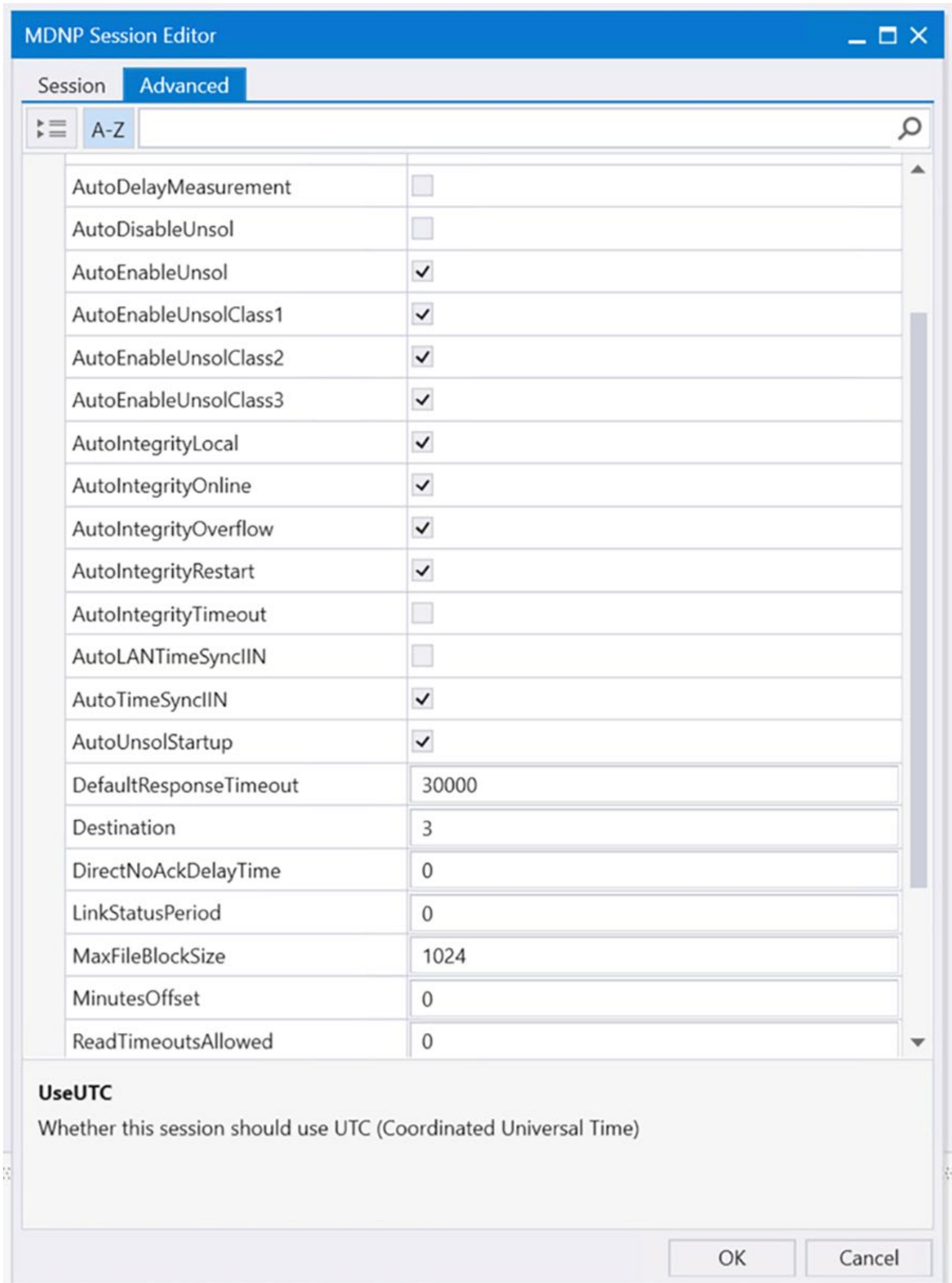


DNP3 IP Advanced Settings

AutoTimeSyncIIN, AutoEnabledUnsol, AutoIntegrityOnline and AutoIntegrityRestart are advanced

Figure 50 DNP3 FEP Advanced session configuration

DNP3 IP settings, which need to be enabled; refer to following Figure for details.



Integrity Poll Use Case

The DNP3 specification supports multiple methods of reading inputs individually or as a group. An integrity poll returns data from Class 0 (known as static data), along with data from Classes 1, 2, and 3 (which will be event data). This may or may not be everything, depending on how the Outstation/IED is configured.

The integrity poll retrieves all events (Class 1, 2, and 3) and static (Class 0) data from the device. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure all data is accurate. This integrity poll is executed in our case from the Northbound DTM application depicted in following Figures.

Figure 51 DNP3 Integrity Data Poll

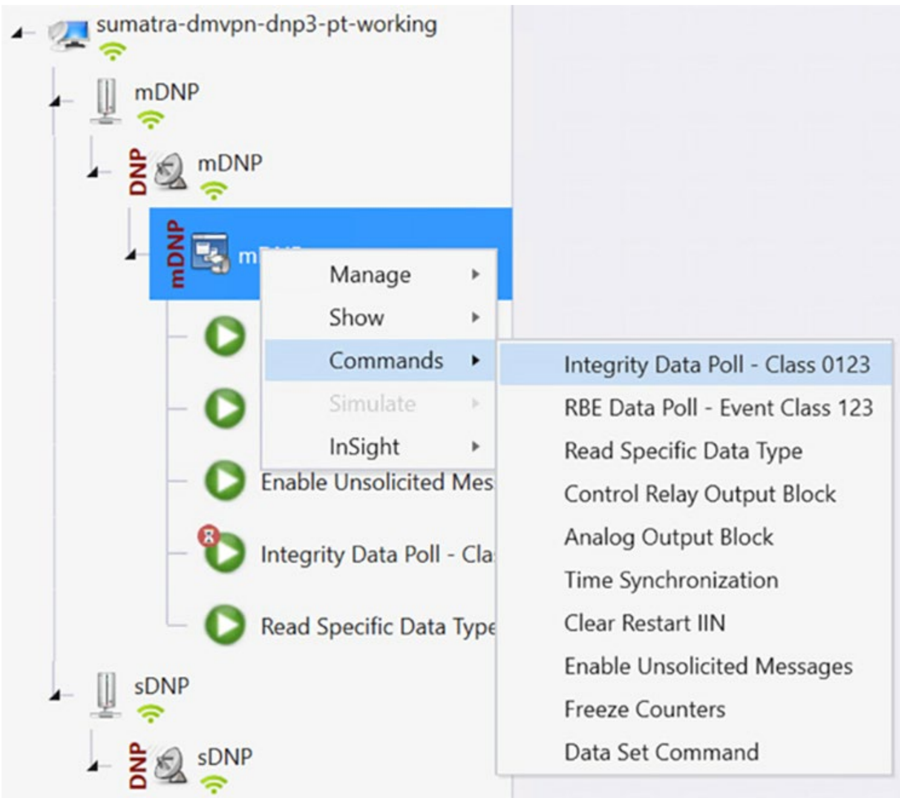
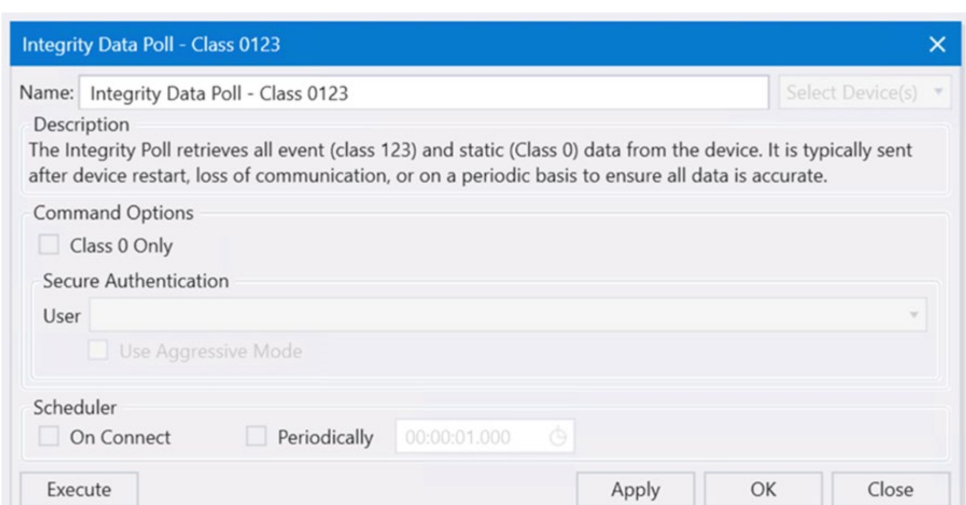


Figure 52 Integrity Data Poll Execute window



Click **Apply** and then click **Execute** to initiate a poll.

Poll results for the Northbound DTM application are shown in the following Figure. Click the **Show Point List** option under the DNP3 IP Session.

Figure 53 DNP3 FEP Data Point list updated after Integrity poll

mDNP(0)

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BO #1	[10] Binary Output Statuses	1	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Offline	9/13/2022 1:42:04 PM	DTHost
CNTR #0	[20] Running Counters	0	0	Offline	9/13/2022 1:42:04 PM	DTHost
CNTR #1	[20] Running Counters	1	0	Offline	9/13/2022 1:42:04 PM	DTHost
CNTR #2	[20] Running Counters	2	0	Offline	9/13/2022 1:42:04 PM	DTHost

In the poll results on the Northbound simulator that are shown above. Four registers values (0, 1 and 2) of binary inputs were received. In the Southbound IED simulator, these are mapped to Binary Input register values (0, 1 and 2).

Figure 54 DNP3 IED Data Points table

sDNP

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #1	[10] Binary Output Statuses	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
CNTR #0	[20] Running Counters	0	0	Online	9/13/2022 2:15:21 PM	DTHost
CNTR #1	[20] Running Counters	1	0	Online	9/13/2022 2:15:21 PM	DTHost
CNTR #2	[20] Running Counters	2	0	Online	9/13/2022 2:15:21 PM	DTHost

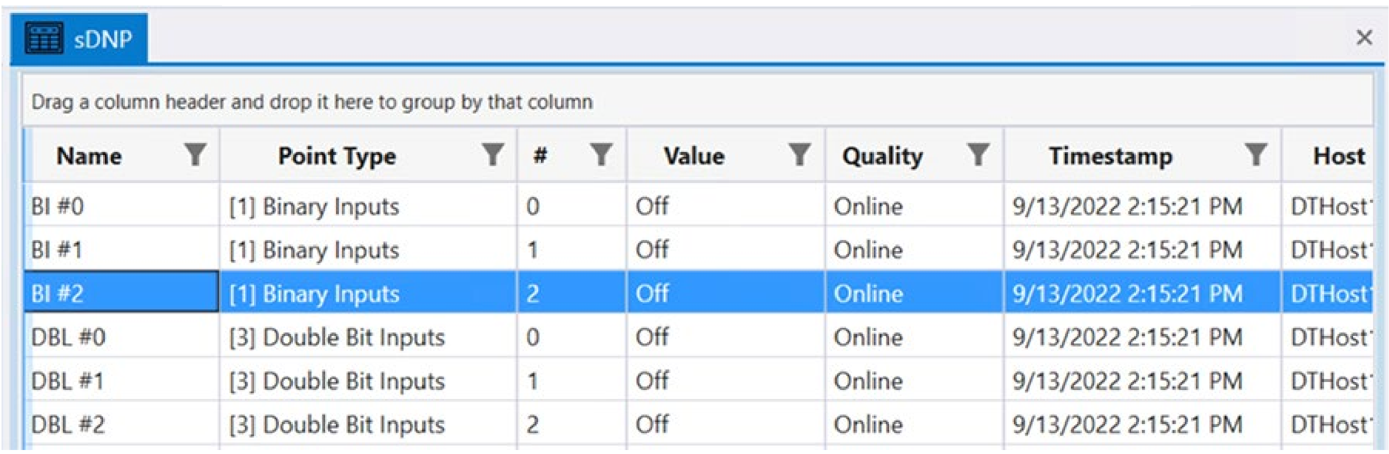
For the purposes of this document, we just discussed Binary Input register values for the Integrity poll.

Unsolicited Reporting

DNP3 supports unsolicited reporting, which means Outstation/IED devices can send updates as values change without having to wait for a poll from the FEP. In our earlier Integrity polling case, we observed that Southbound Input Register #2 is off. Southbound Register #2 is mapped as Register #2 in the Northbound. If we change the state of the Southbound register, the Northbound register state will change automatically.

Check the state check of Input Register #2 value @ Northbound DTM application. In this case, it is **OFF**. See the figure that follows.

Figure 55 DNP3 IED Data Points table with BI register 2

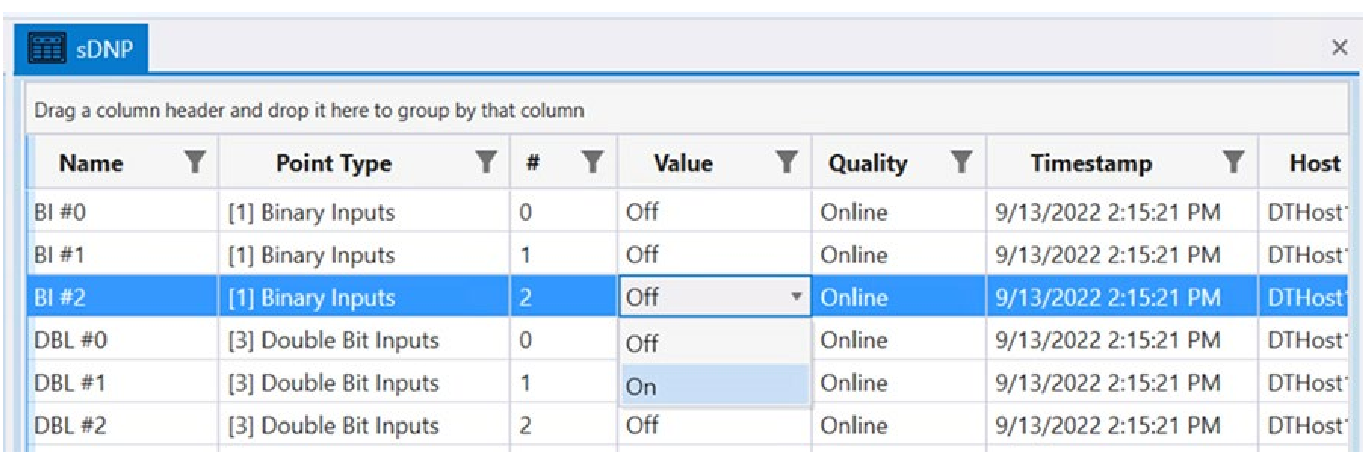


Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

Change the register #2 value to **ON** (right click and toggle) on the Southbound application.

Figure 56 DNP3 IED Binary Input register toggle

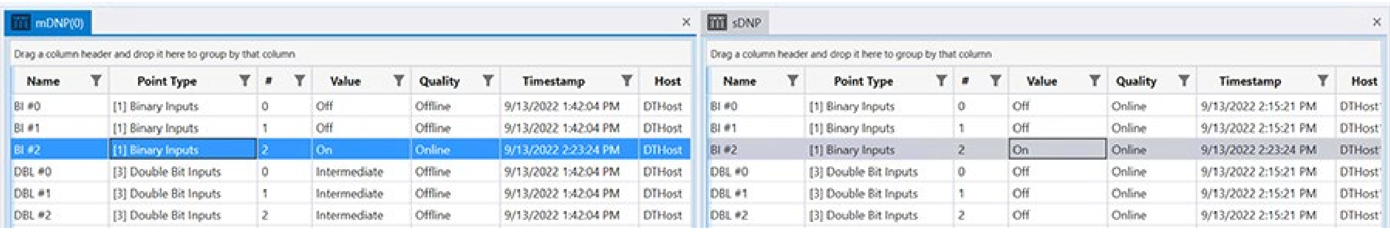
Unsolicited reporting is observed on the Northbound application for Binary Input register value #2.



Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	On	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

Toggle the Binary Input register # 2 values from OFF to ON.

Figure 57 DNP3 FEP Data Point table updated by unsolicited message


mDNP(0)

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost

sDNP

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost'
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost'
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost'
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost'
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost'
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost'

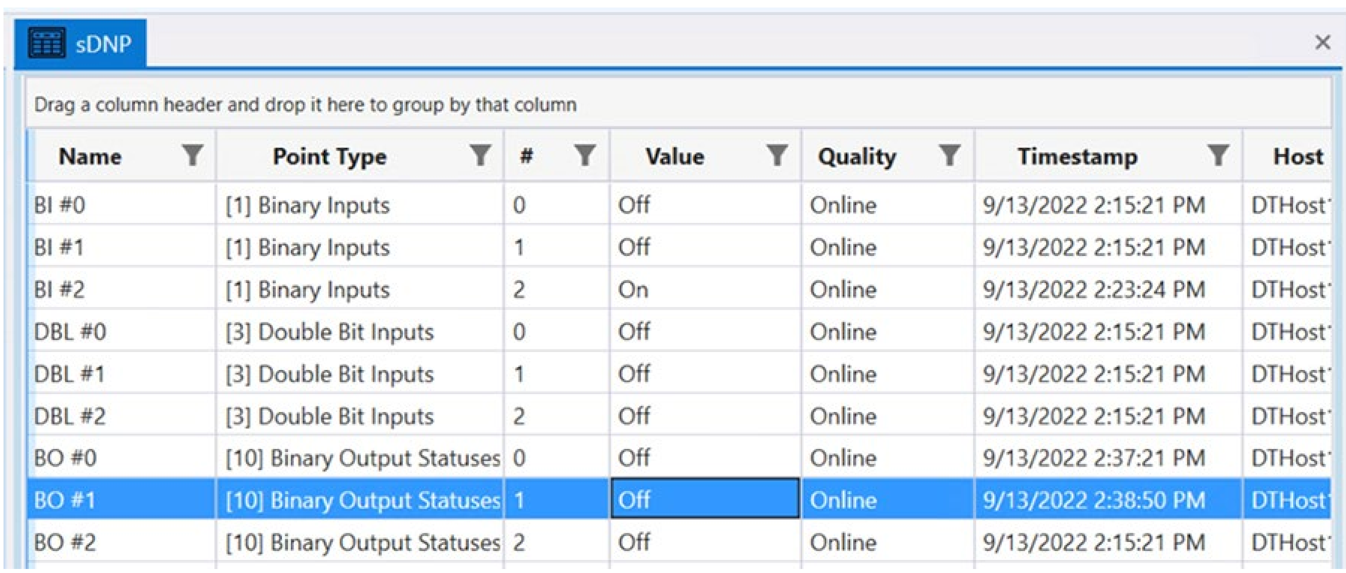
The updated value is **ON**, as shown in above Figure.

Control Command

In DNP3, binary output statues registers are used for control command or write operations. We will try to issue a CROB command from the Northbound DTM application to Register value #1, which will then write on Register #1 in our case. Register Value #1 on the Northbound application is mapped to Register Value #1 in the Southbound application.

1. The status check on the Southbound TMW application binary output statuses Register #1 before issuing a control command from the Northbound. We can see the binary output register #1 status is **OFF** in following Figure.

Figure 58 DNP3 IED Binary Output Register 1


sDNP

Drag a column header and drop it here to group by that column

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost'
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost'
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost'
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost'
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost'
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost'
BO #0	[10] Binary Output Statuses	0	Off	Online	9/13/2022 2:37:21 PM	DTHost'
BO #1	[10] Binary Output Statuses	1	Off	Online	9/13/2022 2:38:50 PM	DTHost'
BO #2	[10] Binary Output Statuses	2	Off	Online	9/13/2022 2:15:21 PM	DTHost'

2. Now we will issue a command from the Northbound simulator to change the state of the register to **ON.** See the following Figure.

Figure 59 DNP3 CROB control command

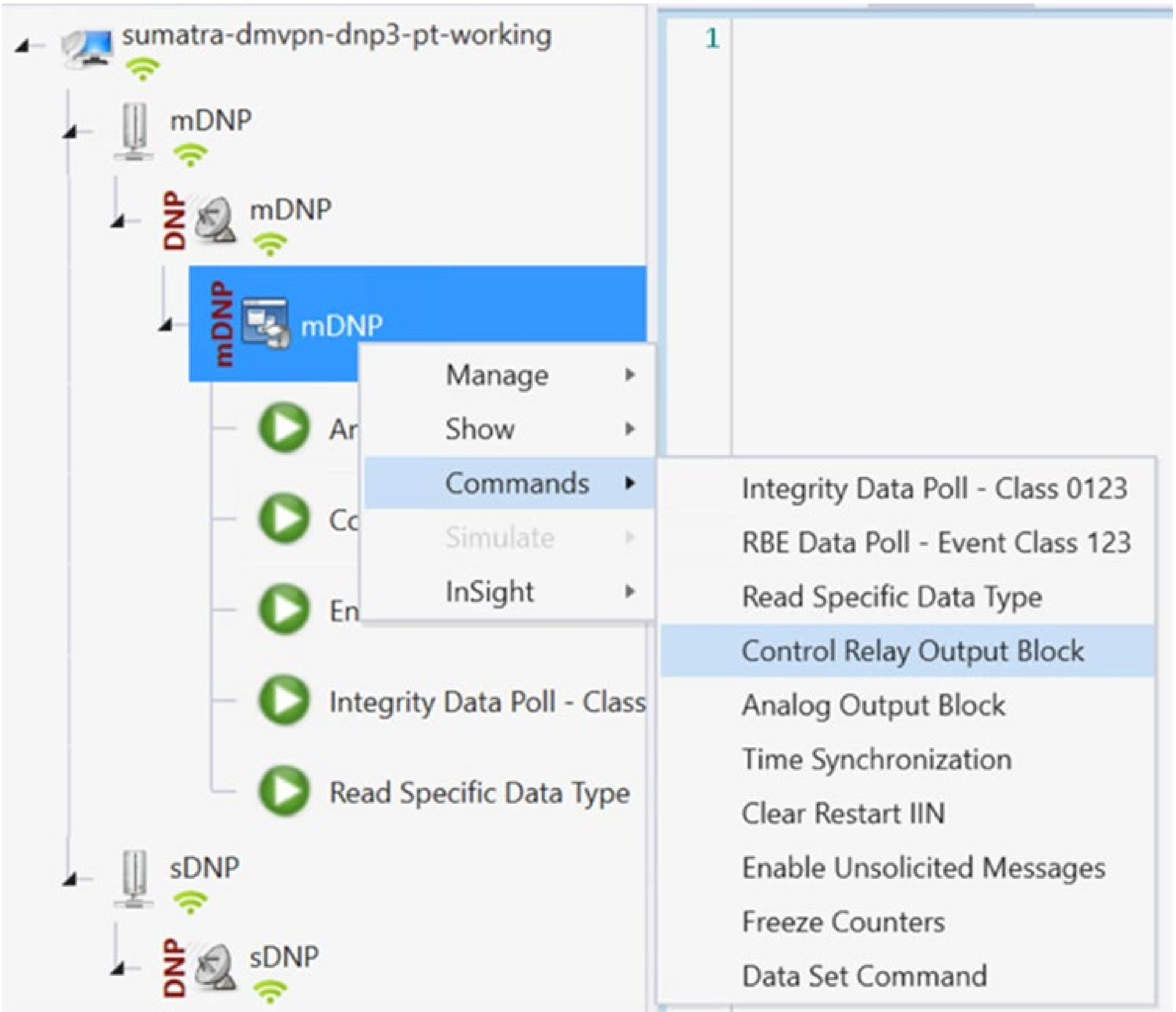
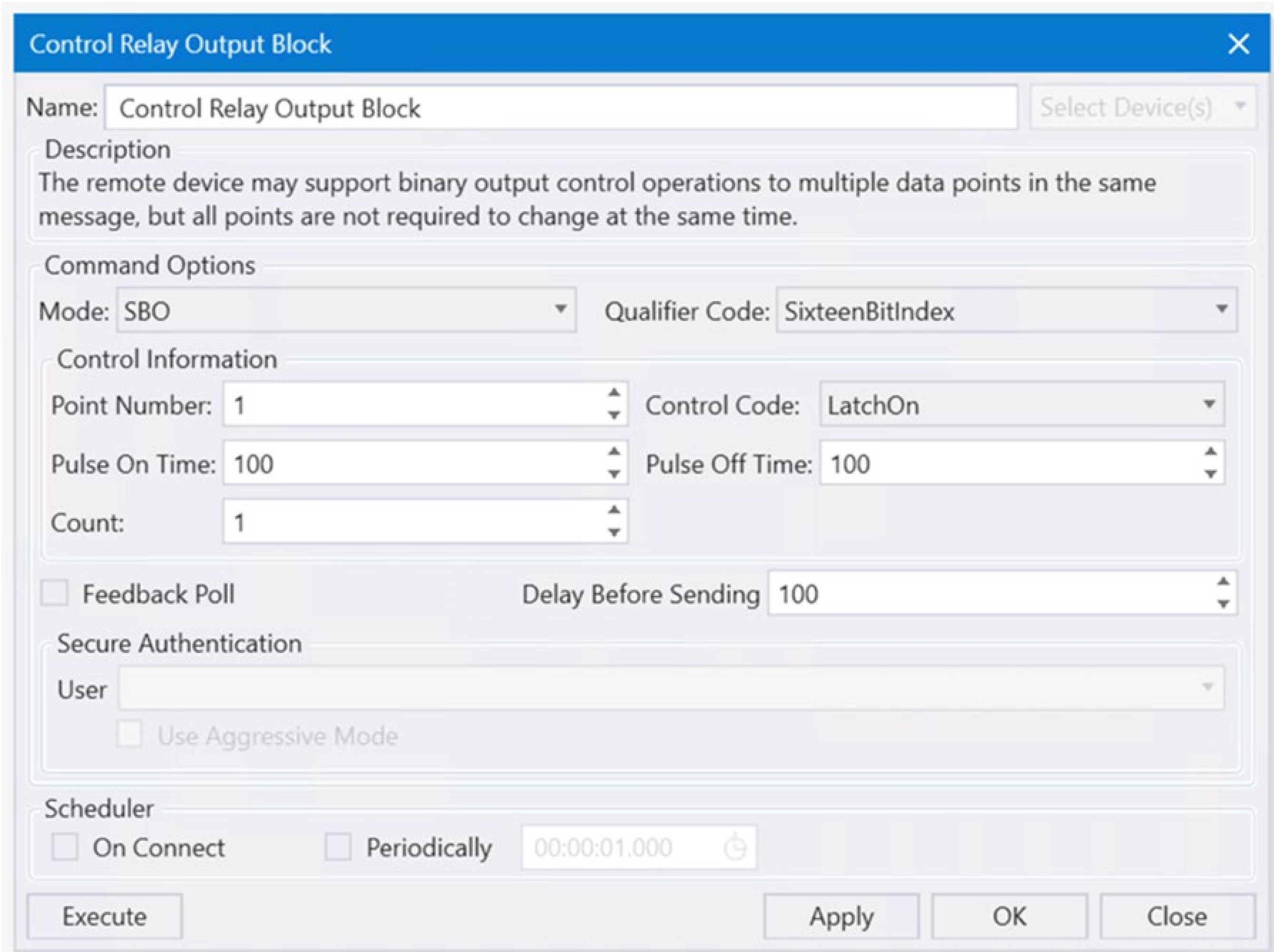


Figure 60 DNP3 CROB config window

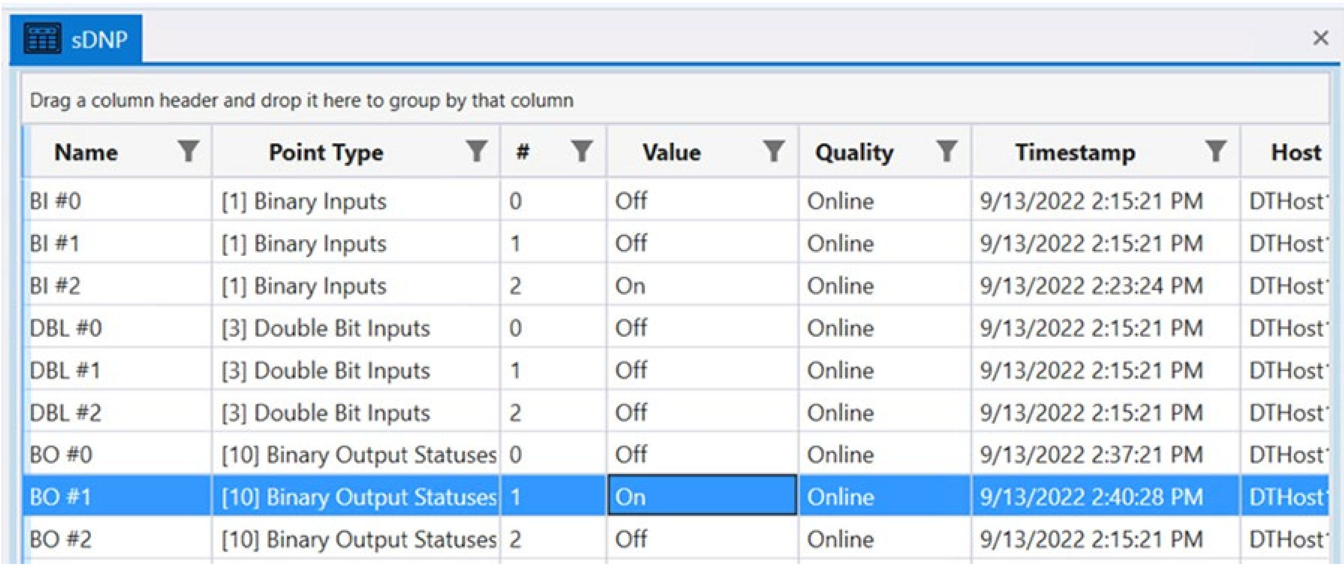


Command LatchOn is executed on Point Number **1** in above Figure. Mode is **SBO**. Control Code is **LatchOn**.

3. Click **Apply** and then click **Execute** to execute the command from the Northbound DTM application.

Binary Output Statuses Register # 1 value on the Southbound TMW application is changed from **OFF** to **ON**, depicted in the following Figure.

Figure 61 DNP3 IED Data Point updated via CROB command



Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Online	9/13/2022 2:37:21 PM	DTHost
BO #1	[10] Binary Output Statuses	1	On	Online	9/13/2022 2:40:28 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

SCADA Ethernet/IP Use Case

The IR8340 supports the following protocols:

- IEC 60870 T104 to/from IEC 60870 T104
- DNP3 IP to DNP3 IP

For more details on SCADA, please refer to the Cisco IR8340 SCADA Configuration Guide at the following URL:

https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17_7/m_scada.html

This section provides implementation details for the following SCADA DNP3 IP scenarios

Southbound DNP3 TMW Configuration

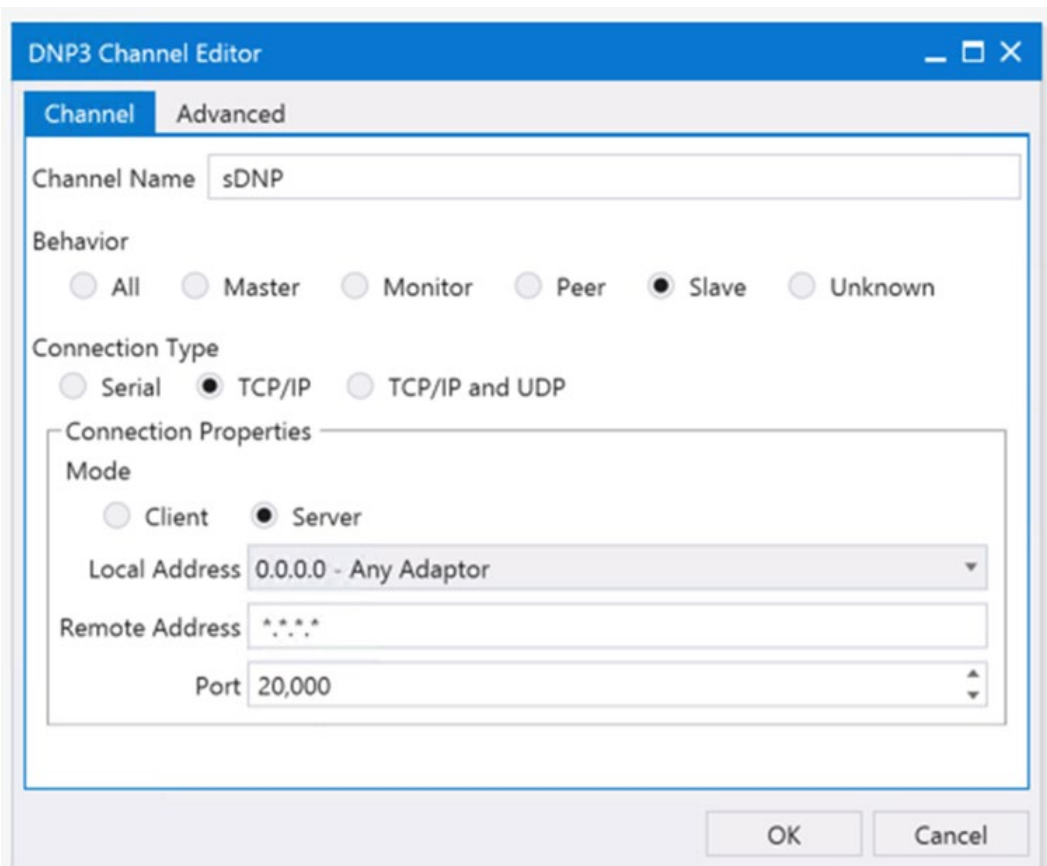
Channel Configuration

The Southbound Ethernet IED is simulated using TMW software. In this example, as shown in Figure 59, the serial port COM30 with Baud Rate 9600 is connected to Async0 of Cisco IR8340.

Complete the following steps:

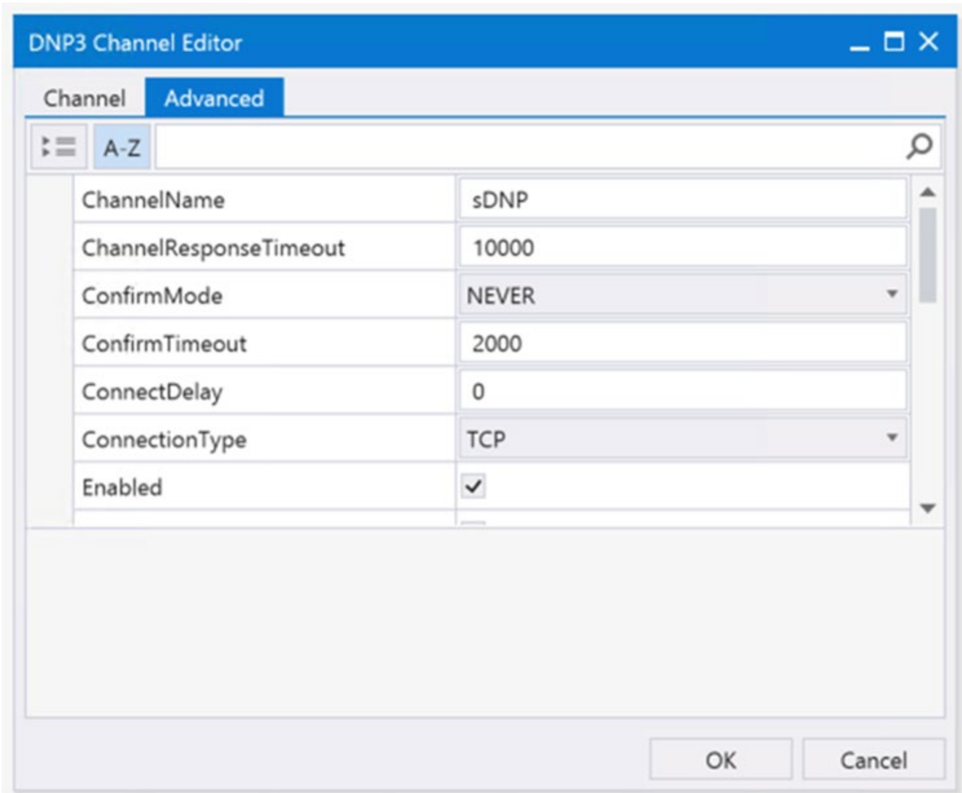
1. Create DNP3 IP IED Channel.

Figure 62 DNP3 IP IED Channel Configuration



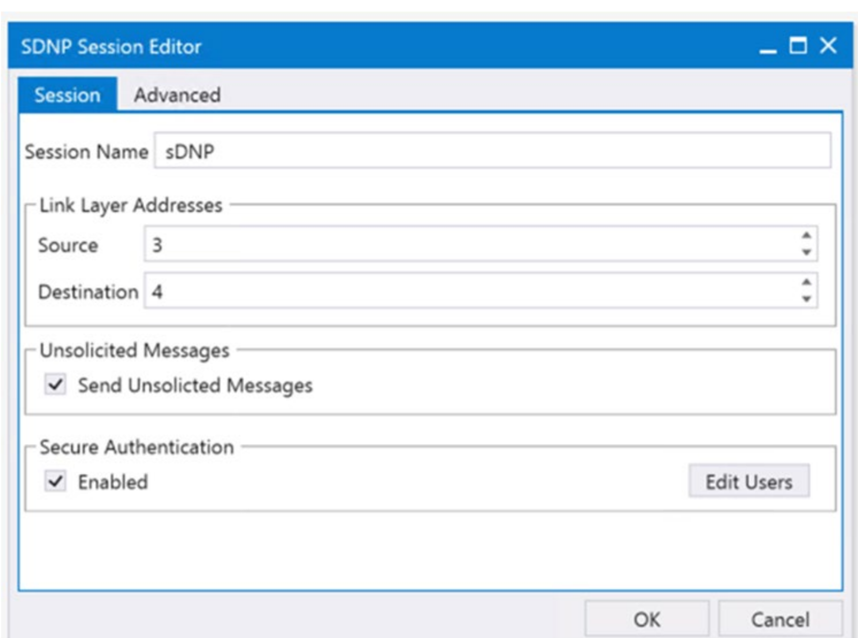
2. Create DNP3 IED Advanced Channel configuration.

Figure 63 DNP3 IP IED Advanced Channel configuration



3. Create DNP3 FEP Sessions, the DNP3 Southbound serial RTU simulator is configured as Outstation/IED and the source and destination layers are configured as 4 and 3 respectively. See the figure that follows.

Figure 64 DNP3 IP IED Session creation



Other configurations of IED and DNP3 IP FEP are all the same as described in Protocol Translation section. Please follow the SCADA operation like unsolicited message, Polling and Control Commands as explained in the Protocol Translation section in this document.

Additional Scada-gw Features

Under global configuration, there are various CLIs available for features on protocol translation. See the following for the cli configuration:

"scada-gw protocol force reset-link".

RTUs require **Reset-Link** message to be sent out along with **Link-status** message to ensure correct initialization of the serial. The feature can be selectively turned on using this new config CLI

Upon adding the new CLI to config, the new initialization sequence will be as follows:

1. Reset Link
2. Link Status
3. Write time
4. Enable unsolicited
5. Class 1/2/3/0

"Scada-gw protocol clock passthru"

When clock passthru is enabled and if the router has not received the timestamp from the DNP3-IP master, the router hardware time will be sent downstream to RTU. Upon receiving a new timestamp from DNP3-IP master, the router will start sending the new timestamp sourced from DNP3-IP master to RTU.

"scada-gw protocol interlock"

This command will be supported on both protocols. The router will disconnect Serial link if the DNP3-IP master is down or unreachable. Similarly, when Serial link to RTU is down, the TCP connection to DNP3-IP master will be untethered.

"Scada-gw protocol ignore direction"

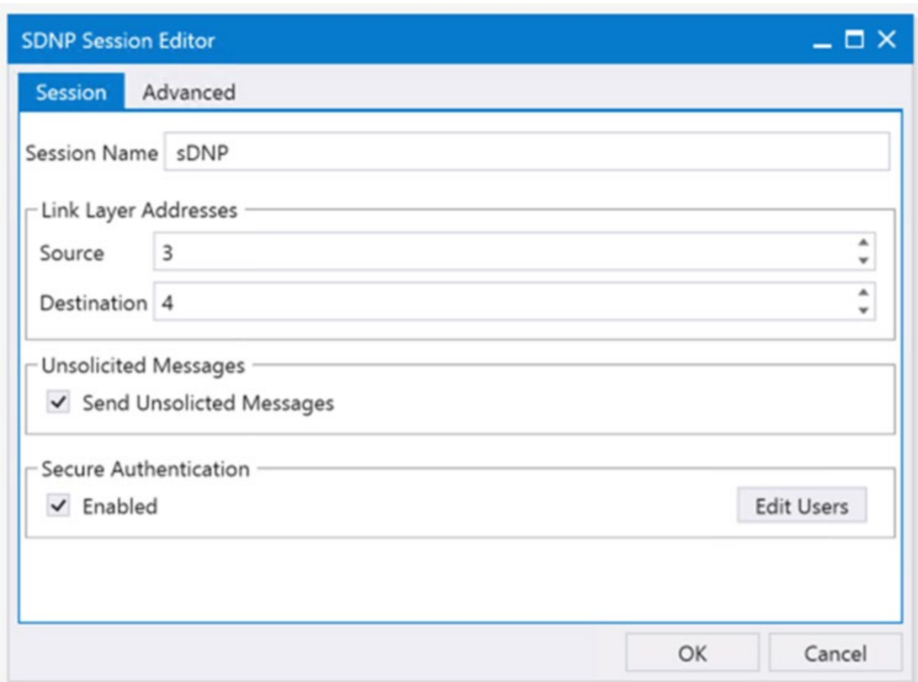
In some cases, older RTUs were previously used in peer-to-peer mode. These RTUs dynamically swapped the roles of DNP3 Serial subordinate and primary by setting the bit DIR=1 in the message header. ASE's SCADA stack used in Cisco routers are always configured to be DNP3 Serial primary. In this case, all the packets received from DNP3 serial with DIR=1 were ignored causing many messages from RTU to be discarded. To handle these scenarios, a new SCADA configuration CLI has been added: Enabling this CLI will allow the router to accept incoming packets from RTU even when DIR=1

Zone Based Firewall Implementation

All traffic originating or passing through from the Substation Router can be protected by enabling IOS zone-based firewall. Zone Based Firewall (ZBFW) IOS feature can be enabled to detect and block unwanted flows.

The ZBFW mainly deals with the security zones, where we can assign the router interfaces to various security zones and control the traffic between the zones, also the traffic will be dynamically inspected as it passes through the zones. Zone based firewall will support Application inspection and control for HTTP, POP3, Sun RPC, IM Applications and P2P File sharing. WAN facing interface like Cellular or Ethernet or FlexVPN tunnel is placed in outside zone and interfaces connected to LAN network devices like IED and other similar endpoints and Edge Compute Application (internal logical interface) are placed on inside zone. Interzone communication is denied, traffic will be denied among the interfaces that are in the different zones unless we specify a firewall policy to allow such traffic if required.

Figure 65 Zone Based Firewall in a Substation



The following firewall policy is defined between outside and inside zones.

- SCADA traffic ports need to be allowed. For example:
  - Modbus Port 502
  - DNP3 port 20000
  - IEC 60870-5-104 port 2404
  - IEC 61850 MMS port 102.
- If Substation Router uses encryption for SCADA traffic, the traffic will be encrypted by IPSEC FlexVPN. So, there is no requirement to open SCADA protocol ports. Allow the following IPSEC FlexVPN ports:
  - ISAKMP - UDP 500
  - ESP - Protocol 50
  - ISAKMP NAT-Traversal - UDP 4500 (NAT-T)

- Open ports required for management applications like FND, Cyber Vision Center and any other similar applications.
- Intra-zone communication is allowed, traffic will flow implicitly among the interfaces that are in the same zone.

The following steps are required to configure zone-based firewall on secondary substation router.

1. Before you create zones, you should group interfaces that are similar when they are viewed from a security perspective. By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. Firewall zones are used for security features.
2. Configure Layer 3 and Layer 4 firewall policies.

```
!
ip access-list extended MISSION-CRITICAL-DATA-IN
    9 permit tcp host 192.168.101.2 eq 20000 host 192.168.4.171
    10 permit tcp host 192.168.101.2 eq 20001 host 192.168.4.171
    11 permit tcp host 192.168.101.2 eq 20002 host 192.168.4.171
    12 permit tcp host 192.168.101.2 eq 20003 host 192.168.4.171
    13 permit tcp host 192.168.101.2 eq 20004 host 192.168.4.171
    14 permit tcp host 192.168.101.2 eq 20005 host 192.168.4.171
    19 permit tcp host 192.168.101.2 eq 20100 host 192.168.4.171
    29 permit tcp host 192.168.101.2 eq 20200 host 192.168.4.171
    39 permit tcp host 192.168.101.2 eq 20300 host 192.168.4.171
    41 permit tcp host 192.168.211.2 host 192.168.2.206 eq 502
    50 permit udp any any
    70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
!

!
ip access-list extended MISSION-CRITICAL-DATA-OUT
    9 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20000
    10 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20001
    11 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20002
    12 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20003
    13 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20004
    14 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20005
    19 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20100
    29 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20200
    39 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20300
    41 permit tcp host 192.168.2.206 host 192.168.211.2 eq 502
    50 permit udp any any
    70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
!

!
ip access-list extended FTP_IN_OUT
```

```
1 permit tcp 192.168.110.0 0.0.0.255 host 192.168.2.176 eq ftp log
2 permit tcp host 192.168.199.2 host 192.168.2.176 eq ftp log
3 permit tcp host 192.168.199.2 host 192.168.2.206 eq ftp
13 permit tcp 50.1.0.0 0.0.0.255 host 192.168.2.176 eq ftp log
!

!
ip access-list extended FTP_OUT_IN
1 permit tcp host 192.168.2.176 192.168.110.0 0.0.0.255 eq ftp
2 permit tcp host 192.168.2.176 host 192.168.199.2 eq ftp
3 permit tcp host 192.168.2.206 host 192.168.199.2 eq ftp
!

!
class-map type inspect match-any IN-IN
        match protocol ssh
        match protocol tcp
        match protocol udp
        match protocol icmp
        match protocol https
        match protocol http
        match protocol login
class-map type inspect match-any OUT-SCADA
        match protocol ntp
        match protocol ssh
        match protocol syslog
        match protocol icmp
        match access-group name MISSION-CRITICAL-DATA-OUT
        match protocol snmp
class-map type inspect match-any SCADA-OUT
        match protocol ntp
        match protocol ssh
        match protocol syslog
        match protocol icmp
        match access-group name MISSION-CRITICAL-DATA-IN
class-map type inspect match-any IN-OUT
        match protocol icmp
        match protocol telnet
        match protocol http
        match protocol https
        match protocol ssh
        match protocol syslog
        match protocol udp
        match access-group name FTP_IN_OUT
        match protocol tcp
        match access-group 102
        match protocol login
```

```
class-map type inspect match-any OUT-IN
 match protocol icmp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
 match protocol syslog
 match access-group name FTP_OUT_IN
 match protocol tcp
 match access-group 102
 match protocol udp
 match protocol snmp
!
```

3. Create security zones and zone pairs.

```
!
zone security INSIDE
zone security OUTSIDE
zone security SCADA
zone-pair security IN-IN-PAIR source INSIDE destination INSIDE
 service-policy type inspect IN-IN
zone-pair security IN-OUT-PAIR source INSIDE destination OUTSIDE
 service-policy type inspect IN-OUT
zone-pair security OUT-IN-PAIR source OUTSIDE destination INSIDE
 service-policy type inspect OUT-IN
zone-pair security OUT-SCADA-PAIR source OUTSIDE destination SCADA
 service-policy type inspect OUT-SCADA
zone-pair security SCADA-OUT-PAIR source SCADA destination OUTSIDE
 service-policy type inspect SCADA-OUT
!
```

4. Assign the interfaces to the respective zones. In this example GigabitEthernet0/0/0 is the OUTSIDE interface. VLAN 101, VLAN 501, VLAN 110 and VLAN201 are INSIDE interfaces.

```
!
interface GigabitEthernet0/0/0
description connected to asr903-003
ip flow monitor StealthWatch_Monitor input
ip address 192.168.100.1 255.255.255.0
zone-member security OUTSIDE
ip ospf network point-to-point
load-interval 30
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
end
!
!
```

```
interface Vlan101
ip address 192.168.101.1 255.255.255.0
zone-member security SCADA
load-interval 30
service-policy input HOST-INPUT-MARKING
end
!
interface Vlan201
ip address 192.168.211.1 255.255.255.0
zone-member security SCADA
load-interval 30
vrrp 1 name MODBUS-IED-1
vrrp 1 ip 192.168.211.100
vrrp 1 timers learn
vrrp 1 priority 200
service-policy input HOST-INPUT-MARKING
end
!
interface Vlan501
description REP-Mgmt
ip address 50.1.0.1 255.255.255.0
zone-member security INSIDE
standby 0 ip 50.1.0.100
standby 0 timers msec 30 msec 120
standby 0 priority 200
standby 0 preempt
load-interval 30
service-policy input TEST_MGMT_TRAFFIC
end
!
interface Vlan1051
description HSRP-GRP-1
ip address 192.168.110.2 255.255.255.0
zone-member security INSIDE
standby 1 ip 192.168.110.1
standby 1 priority 10
standby 1 preempt
standby 1 track 100 decrement 10
bfd interval 999 min_rx 999 multiplier 3

!
```

5. The functioning of the feature can be verified using the following command.

```
Router#show policy-map type inspect zone-pair sessions
 Zone-pair: IN-IN-PAIR
 Service-policy inspect : IN-IN
```

```
    Class-map: IN-IN (match-any)
      Match: protocol ssh
      Match: protocol tcp
      Match: protocol udp
      Match: protocol icmp
      Match: protocol https
      Match: protocol http
      Match: protocol login
      Inspect


    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
  Zone-pair: IN-OUT-PAIR
  Service-policy inspect : IN-OUT

    Class-map: IN-OUT (match-any)
      Match: protocol icmp
      Match: protocol telnet
      Match: protocol http
      Match: protocol https
      Match: protocol ssh
      Match: protocol syslog
      Match: protocol udp
      Match: access-group name FTP_IN_OUT
      Match: protocol tcp
      Match: access-group 102
      Match: protocol login
      Inspect
        Established Sessions
         Session  ID  0x00009B76  (192.168.110.7:8)=>(192.168.2.108:42999)
icmp SIS_OPEN
          Created 00:00:07, Last heard 00:00:07
          Bytes sent (initiator:responder) [36:36]
         Session  ID  0x00009B79  (192.168.110.6:8)=>(192.168.2.176:39395)
icmp SIS_OPEN
          Created 00:00:03, Last heard 00:00:03
          Bytes sent (initiator:responder) [36:36]
         Session  ID  0x00009B7C  (192.168.110.5:8)=>(192.168.2.108:39409)
icmp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [36:36]
         Session  ID  0x00009B70  (192.168.110.8:8)=>(192.168.2.176:48757)
icmp SIS_OPEN
          Created 00:00:28, Last heard 00:00:28
```

Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B5E (50.1.0.2:8)=>(192.168.2.176:45393) icmp/icmp SIS_OPEN
Created 00:01:01, Last heard 00:01:01
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B71 (192.168.110.8:8)=>(192.168.2.108:48758) icmp SIS_OPEN
Created 00:00:28, Last heard 00:00:28
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B63 (192.168.110.51:8)=>(192.168.2.176:39731) icmp SIS_OPEN
Created 00:00:53, Last heard 00:00:53
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B56 (192.168.110.6:8)=>(192.168.2.108:39392) icmp SIS_OPEN
Created 00:01:02, Last heard 00:01:02
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B66 (50.1.0.3:8)=>(192.168.2.176:46126) icmp/icmp SIS_OPEN
Created 00:00:38, Last heard 00:00:38
Bytes sent (initiator:responder) [36:36]
Session ID 0x00000000 (192.168.110.5:54555)=>(192.168.2.206:514) syslog SIS_OPEN
Created 21:33:57, Last heard 00:00:01
Bytes sent (initiator:responder) [427019:0]
Session ID 0x00009B67 (192.168.110.7:8)=>(192.168.2.176:42996) icmp SIS_OPEN
Created 00:00:37, Last heard 00:00:37
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B60 (192.168.110.8:8)=>(192.168.2.108:48756) icmp SIS_OPEN
Created 00:00:58, Last heard 00:00:57
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B75 (192.168.110.7:8)=>(192.168.2.176:42998) icmp SIS_OPEN
Created 00:00:07, Last heard 00:00:07
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B7B (192.168.110.5:8)=>(192.168.2.176:39408) icmp SIS_OPEN
Created 00:00:02, Last heard 00:00:02
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B6C (192.168.110.6:8)=>(192.168.2.108:39394) icmp SIS_OPEN
Created 00:00:33, Last heard 00:00:33
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B6B (192.168.110.6:8)=>(192.168.2.176:39393) icmp SIS_OPEN

Created 00:00:33, Last heard 00:00:33
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B68 (192.168.110.7:8)=>(192.168.2.108:42997) icmp SIS_OPEN
Created 00:00:37, Last heard 00:00:37
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B74 (50.1.0.3:8)=>(192.168.2.176:46127) icmp/icmp SIS_OPEN
Created 00:00:09, Last heard 00:00:09
Bytes sent (initiator:responder) [36:36]
Session ID 0x00000024 (50.1.0.7:53458)=>(192.168.2.211:2055) udp SIS_OPEN
Created 21:32:44, Last heard 00:00:02
Bytes sent (initiator:responder) [260604:0]
Session ID 0x00009B7D (50.1.0.2:8)=>(192.168.2.176:45395) icmp/icmp SIS_OPEN
Created 00:00:01, Last heard 00:00:01
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B6D (192.168.110.5:8)=>(192.168.2.176:39406) icmp SIS_OPEN
Created 00:00:32, Last heard 00:00:32
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B7A (192.168.110.6:8)=>(192.168.2.108:39396) icmp SIS_OPEN
Created 00:00:03, Last heard 00:00:03
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B64 (192.168.110.51:8)=>(192.168.2.108:39732) icmp SIS_OPEN
Created 00:00:53, Last heard 00:00:53
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B5C (192.168.110.5:8)=>(192.168.2.108:39405) icmp SIS_OPEN
Created 00:01:02, Last heard 00:01:02
Bytes sent (initiator:responder) [36:36]
Session ID 0x00000001 (192.168.110.5:50579)=>(192.168.5.11:514) syslog SIS_OPEN
Created 21:33:57, Last heard 00:00:01
Bytes sent (initiator:responder) [427019:0]
Session ID 0x00009B6E (192.168.110.5:8)=>(192.168.2.108:39407) icmp SIS_OPEN
Created 00:00:32, Last heard 00:00:32
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B73 (192.168.110.51:8)=>(192.168.2.108:39734) icmp SIS_OPEN
Created 00:00:24, Last heard 00:00:24
Bytes sent (initiator:responder) [36:36]

```
        Session ID 0x00009B5F (192.168.110.8:8)=>(192.168.2.176:48755)
icmp SIS_OPEN
          Created 00:00:58, Last heard 00:00:58
          Bytes sent (initiator:responder) [36:36]
        Session ID 0x00009B6F (50.1.0.2:8)=>(192.168.2.176:45394)
icmp/icmp SIS_OPEN
          Created 00:00:31, Last heard 00:00:31
          Bytes sent (initiator:responder) [36:36]
        Session ID 0x00009B72 (192.168.110.51:8)=>(192.168.2.176:39733)
icmp SIS_OPEN
          Created 00:00:24, Last heard 00:00:24
          Bytes sent (initiator:responder) [36:36]
        Session ID 0x00009B5B (192.168.110.5:8)=>(192.168.2.176:39404)
icmp SIS_OPEN
          Created 00:01:02, Last heard 00:01:02
          Bytes sent (initiator:responder) [36:36]


    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
  Zone-pair: OUT-IN-PAIR
  Service-policy inspect : OUT-IN

    Class-map: OUT-IN (match-any)
      Match: protocol icmp
      Match: protocol telnet
      Match: protocol http
      Match: protocol https
      Match: protocol ssh
      Match: protocol syslog
      Match: access-group name FTP_OUT_IN
      Match: protocol tcp
      Match: access-group 102
      Match: protocol udp
      Match: protocol snmp
      Inspect
        Established Sessions
        Session ID 0x00009B77 (192.168.2.108:8)=>(50.1.0.2:24433) icmp
SIS_OPEN
          Created 00:00:35, Last heard 00:00:35
       Bytes sent (initiator:responder) [36:36]
        Session ID 0x00009B69 (192.168.2.108:8)=>(50.1.0.3:24429) icmp
SIS_OPEN
          Created 00:01:05, Last heard 00:01:05
          Bytes sent (initiator:responder) [36:36]
```

```
        Session ID 0x0000000D (192.168.2.108:2530)=>(50.1.0.7:2530) udp
SIS_OPEN
          Created 21:33:55, Last heard 00:00:05
          Bytes sent (initiator:responder) [41856:41856]
        Session ID 0x00009B78 (192.168.2.108:8)=>(50.1.0.3:24434) icmp
SIS_OPEN
          Created 00:00:35, Last heard 00:00:35
          Bytes sent (initiator:responder) [36:36]
        Session ID 0x00009B87 (192.168.2.108:8)=>(50.1.0.2:24436) icmp
SIS_OPEN
          Created 00:00:05, Last heard 00:00:05
          Bytes sent (initiator:responder) [36:36]
        Session ID 0x00009B86 (192.168.2.108:8)=>(50.1.0.3:24435) icmp
SIS_OPEN
          Created 00:00:05, Last heard 00:00:05
          Bytes sent (initiator:responder) [36:36]
        Session ID 0x0000000B (192.168.2.108:2530)=>(50.1.0.7:1967) udp
SIS_OPEN
          Created 21:33:55, Last heard 00:00:05
          Bytes sent (initiator:responder) [136292:62784]
        Session ID 0x00009B6A (192.168.2.108:8)=>(50.1.0.2:24430) icmp
SIS_OPEN
          Created 00:01:05, Last heard 00:01:05
          Bytes sent (initiator:responder) [36:36]


    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
  Zone-pair: OUT-SCADA-PAIR
  Service-policy inspect : OUT-SCADA

    Class-map: OUT-SCADA (match-any)
      Match: protocol ntp
      Match: protocol ssh
      Match: protocol syslog
      Match: protocol icmp
      Match: access-group name MISSION-CRITICAL-DATA-OUT
      Match: protocol snmp
      Inspect
        Established Sessions
        Session ID 0x00009B5A
(192.168.4.171:49366)=>(192.168.101.2:20100) tcp SIS_OPEN
          Created 00:01:32, Last heard 00:00:29
          Bytes sent (initiator:responder) [139:1739]
```

```
    Session ID 0x00009B42
(192.168.4.171:49349)=>(192.168.101.2:20002) tcp SIS_OPEN
     Created 00:01:46, Last heard 00:00:41
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B57
(192.168.4.171:49363)=>(192.168.101.2:20005) tcp SIS_OPEN
     Created 00:01:32, Last heard 00:00:29
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B4A
(192.168.4.171:49357)=>(192.168.101.2:20003) tcp SIS_OPEN
     Created 00:01:40, Last heard 00:00:37
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B44
(192.168.4.171:49351)=>(192.168.101.2:20001) tcp SIS_OPEN
     Created 00:01:46, Last heard 00:00:41
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B41
(192.168.4.171:49348)=>(192.168.101.2:20000) tcp SIS_OPEN
     Created 00:01:47, Last heard 00:00:41
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B58
(192.168.4.171:49364)=>(192.168.101.2:20004) tcp SIS_OPEN
     Created 00:01:32, Last heard 00:00:29
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B65
(192.168.4.171:49375)=>(192.168.101.2:20300) tcp SIS_OPEN
     Created 00:01:19, Last heard 00:00:17
     Bytes sent (initiator:responder) [139:1739]
    Session ID 0x00009B61
(192.168.4.171:49368)=>(192.168.101.2:20200) tcp SIS_OPEN
     Created 00:01:26, Last heard 00:00:22
     Bytes sent (initiator:responder) [166:2566]

  Class-map: class-default (match-any)
   Match: any
   Drop (default action)
    0 packets, 0 bytes
 Zone-pair: SCADA-OUT-PAIR
 Service-policy inspect : SCADA-OUT

  Class-map: SCADA-OUT (match-any)
   Match: protocol ntp
   Match: protocol ssh
   Match: protocol syslog
   Match: protocol icmp
   Match: access-group name MISSION-CRITICAL-DATA-IN
   Inspect
```

```
      Class-map: class-default (match-any)
        Match: any
        Drop (default action)
          0 packets, 0 bytes
  Router#
```

QoS Implementation

Quality of Service (QoS) refers to the ability of the network to provide priority service to selected network traffic. Improved and more predictable network service can be offered by:

- Supporting dedicated bandwidth—that is, cellular links have different upload/download bandwidth/throughput
- Reducing loss characteristics—Substation real-time traffic prioritization
- Avoiding and managing network congestion—multi-services traffic
- Setting traffic priorities across the network—multi-services capabilities

QoS is a key feature when designing the multi-services Substation Automation solution since traffic from IEDs, Remote Workforce, and network management use cases must be differentiated and prioritized. Estimated transport losses, delay, and jitter introduced by networking devices must be understood when forwarding sensitive data, particularly when a WAN backhaul link offers a limited amount of bandwidth.

In the case of dual-WAN interfaces with different bandwidth capabilities (that is, cellular), QoS policies must be applied to prioritize the traffic allowed to flow over these limited bandwidth links, to determine which traffic can be dropped, etc.

On a multi-services Substation solution, QoS DiffServ and CoS (IEEE 802.1p) can apply to traffic categorized as:

- IPv4 Traffic—Substation traffic, protocol translation (RTU monitoring), and network management
- Layer 2 Traffic—Substation Automation such as IEC 61850 GOOSE/SV traffic switches between Ethernet interfaces and IEC 61850 traffic bridged over WAN links between substations.

For Substation Lan QoS, refer the following Substation LAN Cisco Validated Design below, https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG/CU-2-3-2-DIG.html#pgfId-234948

Substation Router QoS actions on the Layer 3 (Cellular, Ethernet) interfaces. The sequencing of QoS actions on egress traffic is as follows:

1. Classification
2. Marking
3. Queuing

The following are Configurations required for the QOS implementation on the Substation Solution; DSCP marking and access-list are used to match the traffic for prioritization.

Class-map Configurations,

```
!
class-map match-any MISSION-CRITICAL
 match ip dscp af31  af32  af33  af43
class-map match-all CALL-SIGNALING
 match ip dscp cs3
class-map match-any TRANSACTIONAL
 match ip dscp cs2  af21  af22  af23  cs4  af41  af42
class-map match-all VOICE
 match ip dscp ef
class-map match-any MISSION-CRITICAL-DATA
 match access-group name MISSION-CRITICAL-DATA
!
!
```

Policy-map Configurations,

```
!
policy-map HOST-INPUT-MARKING
 class VOICE
  set dscp ef
 class CALL-SIGNALING
  set dscp cs3
 class MISSION-CRITICAL-DATA
  set dscp af31
 class TRANSACTIONAL
  set dscp af21
 class class-default

policy-map HOST-QUEUE-PACKETS
 class VOICE
  bandwidth remaining percent 30
  queue-limit 96 packets
 class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
 class MISSION-CRITICAL
  priority
 class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
```

The above policy-map can be applied to the WAN(Cellular/Ethernet) interface for egress traffic (Priority Queuing, Classifying)

interface Cellular 0/4/0
service-policy output HOST-QUEUE-PACKETS

The following command can be used to verify the QOS policies applied on the WAN interfaces, this will show the number of packets for the traffic classified based on the class/policy map configurations.

Router#sh policy-map interface g 0/0/0 output
GigabitEthernet0/0/0

Service-policy output: HOST-QUEUE-PACKETS queue stats for all priority classes:
Queueing
queue limit 512 packets
(queue depth/total drops/no-buffer drops) 0/0/0 (pkts output/bytes output) 0/0

Class-map: VOICE (match-all) 634 packets
30 second offered rate 0000 bps, drop rate 0000 bps Match: ip dscp ef (46)
Queueing
queue limit 96 packets
(queue depth/total drops/no-buffer drops) 0/0/0 (pkts output/bytes output) 0/0
bandwidth remaining 30%

Class-map: TRANSACTIONAL (match-any) 125 packets
30 second offered rate 0000 bps, drop rate 0000 bps
Match: ip dscp cs2 (16) af21 (18) af22 (20) af23 (22) cs4 (32) af41 (34) af42 (36)
Queueing queue limit 96 packets
(queue depth/total drops/no-buffer drops) 0/0/0 (pkts output/bytes output) 0/0
bandwidth remaining 20%

Class-map: ***MISSION-CRITICAL*** *(match-any) 1534 packets*
30 second offered rate 0000 bps, drop rate 0000 bps Match: ip dscp af31 (26) af32 (28) af33 (30) af43 (38) Priority: Strict, b/w exceed drops: 0

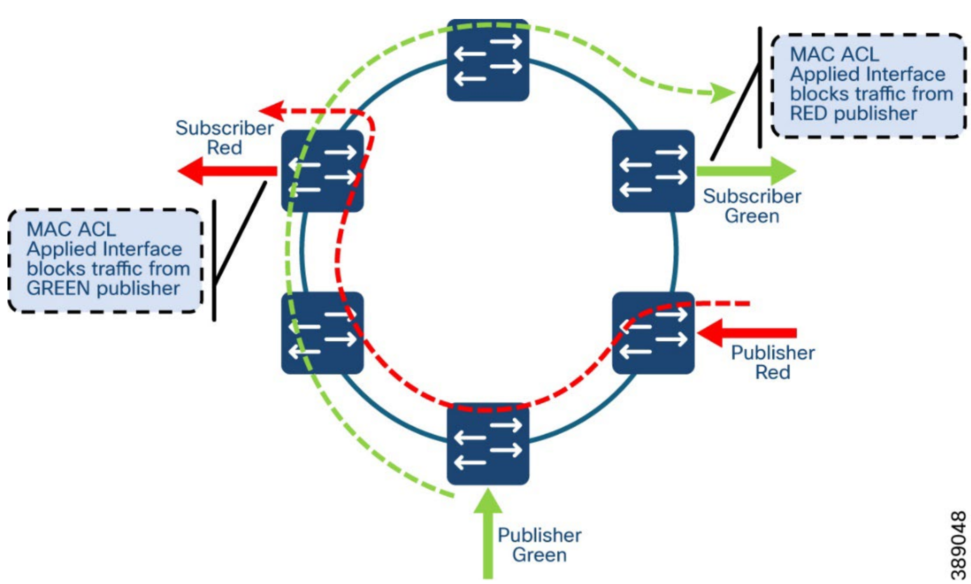
Class-map: class-default (match-any)
24560 packets, 450 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 272 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth remaining 25%

Filtering using MAC ACL Implementation

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

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

Figure 66 Filtering using MAC ACL in Substation LAN networks



The topology depicts two IEC61850 SV flows GREEN and RED published by the respective devices. As the topology depicts the PUBLISHERs and SUBSCRIBERs of the respective traffic are in different points in the network. The L2 SV traffic of both GREEN and RED PUBLISHERs flows through the ring reaches all the devices in the network that may not be interested in. This causes the L2 multicast traffic to flow to all devices in the network and VLAN irrespective of their interest in the traffic.

The following are the configurations that are required to implement filtering of IEC61850 SV traffic using MAC ACL.

Identify the traffic stream that a device is interested in receiving and not receiving. The destination mac address of the IEC61850 SV flow is usually chosen to help identify the flows. The following configuration example depicts an ACL that is configured to block a flow and allow the remaining *traffic.*

```
!
mac access-list extended SV_BLOCK_PERMIT_REST
deny   any host 010c.cd04.0000
permit any any

!
```

After configuring the MAC ACL, identify the interface of interest and apply the MAC ACL in the egress direction to ensure that the specified traffic is appropriately dropped.

```
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 552
switchport mode trunk
load-interval 30
mac access-group SV_BLOCK_PERMIT_REST out
!
```

Use the following command to check the applied ACL on the interface.

```
show mac access-group interface gigabitEthernet 1/0/2
Interface GigabitEthernet1/0/2:
  Inbound access-list is not set
  Outbound access-list is SV_BLOCK_PERMIT_REST
```

Network Management

IR8340 Management using Cisco Catalyst SDWAN

The Cisco Catalyst SD-WAN for a Substation Automation LAN deployment is based on the Cisco Catalyst SD-WAN End-to-End Deployment Guide and expands its scope to using Cisco IR8340 as the SD-WAN edge router. This implementation supports controllers running on the Cisco cloud-managed service.

Prerequisites

- This guide assumes that the user has already installed Cisco Catalyst SD-WAN controllers. For more details on installation see the following resources:

- On-premises deployments: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html
- Cloud deployments: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/knowledge-base/cloudops.html

▪ Data center and enterprise branch sites are already configured per Cisco Catalyst SD-WAN End-to-End Deployment Guide.

▪ Cisco WAN Edge routers are installed and ready to be configured. The IOS XE SD-WAN routers should already be converted from IOS XE to SD-WAN code.

▪ Devices adjacent to the Cisco WAN Edge routers are configured.

▪ vBond IP address or hostname must be configured under the WAN Manager administration settings.

- vSmart is attached to a template.
- SDWAN image may not support all modules from day 0. Refer the respective platform guide for supported modules.

Onboarding IR8340

Bringing up a router to connect to SD-WAN network can be done by three methods:

- PnP for zero touch deployment.
- Bootstrap, for devices that cannot get Internet connectivity without additional configuration, such as devices connected to transport with a static IP configuration or non-default cellular profiles.
- CLI, adding manual configuration via the console.

These methods are explained below.

Before Onboarding

For the WAN Edge devices to join and be active in the overlay, a valid, authorized serial number file must be uploaded to vManage. This authorized serial number file lists the serial and chassis numbers for all WAN Edge routers allowed in the network. vManage will send this file to the controllers, and only devices that match serial numbers on this list will be validated and authenticated successfully by the controllers.

The authorized serial number for IOS XE SD-WAN routers is obtained from Plug and Play (PnP) Connect portal. PnP Connect portal is also used to automate onboarding of network devices and apply configuration settings without manual intervention.

This guide will provide the required steps to add a device on PnP Connect using a smart account and associate it to a vBond profile. Refer to the following link for deeper understanding on PnP connect:

https://www.cisco.com/c/en/us/products/collateral/software/smart-accounts/guide-c07-744931.html#4Deploymentoptions

Adding a device on PnP Connect

A device can be added to PnP Connect automatically if the smart account and virtual account are added to the order on Cisco Commerce Workspace.
If the device is not added through the procurement process, follow these steps:

1. Get serial number and certificate serial number from the device using the show crypto pki certificates CISCO_IDEVID_SUDI command:

```
Router# show crypto pki certificates CISCO_IDEVID_SUDI
Certificate
  Status: Available
  Certificate Serial Number (hex): XXXXXXXXX
  Certificate Usage: General Purpose
  Issuer:
    o=Cisco
    cn=High Assurance SUDI CA
  Subject:
    Name: IR8340-K9
    Serial Number: PID:IR8340-K9 SN:XXXXXXXXX
    cn=IR8340-K9
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:IR8340-K9 SN: XXXXXXXXX
  Validity Date:
    start date: 10:11:36 UTC Feb 8 2021
    end  date: 20:58:26 UTC Aug 9 2099
  Associated Trustpoints: CISCO_IDEVID_SUDI
```

2. Navigate to *https://software.cisco.com*.
3. Under the Network Plug and Play section, click the **Plug and Play Connect** link.
4. Ensure the correct virtual account is chosen in the top right corner.
5. Click **Add Devices** button.
6. Select **Enter Device Info Manually** radio button. Alternatively, you could upload a Comma Separated Values (CSV) file.
7. Click **Next**.
8. Click **Identify Device** button.
9. Fill out the serial number obtained in Step 1, base PID (IR8340-K9), and the selected

bond controller profile.

10. Click **Save**. On the wizard screen, click **Next**.
11. On Review & Submit, click **Submit**.
12. Click **Done**.
13. After the router is added, a list of devices displays. Select the recently added device and then click **Edit Selected**.
14. Click the space under the Certificate Serial Number column for the device and enter the information from Step 1.
15. Click **Submit**.
16. The device will show in yellow status showing Pending (Redirection). If the device is onboarded using the PnP automatic onboarding process, this state will change to Redirect Successful; otherwise, it will stay in its current state.

Load authorized WAN edge serial numbers to vManage

There are two methods to upload the authorized devices to vManage.

Method 1: Sync to the Smart Account

1. In the vManage GUI, go to **Configuration > Devices**.
2. Ensure that WAN Edge List tab is selected.
3. Click **Sync Smart Account.** A window opens to prompt you for your Username and Password.
4. Enter your username and password for the Cisco website. The check box which validates the uploaded list is checked by default.
5. Click **Sync**. Wait for status to show success.

Note: You must re-sync vManage with the Smart Account/Virtual Account for any new devices added to the PNP portal.

Method 2: Upload File Manually

1. Navigate to [*https://software.cisco.com*](https://software.cisco.com).
2. Under the Network Plug and Play section, click the **Plug and Play Connect** link.
3. Ensure the correct virtual account is chosen in the top right corner.
4. Click **Controller Profiles** text.
5. Next to the correct controller profile, click **Provisioning File** text.
6. In the pop-up window, select the controller versions from the drop-down list. Choose **18.3 and newer**. Click **Download** button and save the file to your computer.
7. In the vManage GUI, go to **Configuration > Devices** on the left panel.
8. Ensure that WAN Edge List tab is selected.

9. Click the **Upload WAN Edge List** button. A pop-up window displays. Choose file.
10. Check the check box to validate the list and send it to the controllers. Click **Upload**. If you do not select Validate, then all the devices will show up as invalid, and you will need to individually change them to valid if you want to bring them up on the network and participate in the overlay.
11. Select **OK** in the confirmation box that appears.

12. A pop-up window displays to inform you that the list uploaded successfully and informs you of the number of routers that were uploaded successfully. Select **OK**. A page will indicate that the list has been successfully pushed out to the vBond and vSmart controllers.

Attach device to template

Attaching the device to a device template will associate the configuration to the device. During this process, all variables on the templates need to be assigned to a value.

1. Go to **Configuration** > **Templates**.
2. In the Device tab, identify the template you want to use.
3. Click the more actions (**…**) icon to the right of the row and then click **Attach Devices**. The Attach Devices dialog box opens.
4. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the Selected Devices column on the right.

6. Click **Attach**.
7. Before the full configurations can be built and pushed out, you need to first define all variables associated with the feature templates attached to the device template. There are two ways to do this: either by entering the values of the variables manually within the GUI, or by uploading a CSV file with a list of the variables and their values. Detailed steps for each option are provided at the end of this section.
8. Click the **Next** button. The next screen will indicate that the configure action will be applied to the devices attached to the template.
9. (Optional) Select a device on the left side to show the configuration that will be pushed to the IOS XE SD-WAN router on the Config Preview tab.
10. (Optional) Select the **Config Diff** tab at the top of the screen to see the difference in the current local configuration versus the new configuration which is about to be pushed.
11. (Optional) You may select the **Configure Device Rollback Timer** text in the lower left corner to view or change the rollback timer. Rollback timer is a protection mechanism; if the router is unreachable after a configuration change it rolls back to the previous configuration. You can configure the timer to any value between 6 and 15 minutes. It is not recommended to disable it. Click **Save** or **Cancel** to go back to main window.
12. Select **Configure Devices**. If configuring more than one device, a pop-up window warns of committing changes to multiple devices. Check the check box to Confirm configuration changes on the devices. Select **OK**. The configuration then gets pushed out to the devices. When complete, vManage should show the Done-Scheduled status, indicating the device is offline but template is scheduled to be pushed when connectivity is established.
13. (Optional) To view devices attached to a device template, go to **Configuration > Templates**. From the Device tab, identify the template and click the **Device Attached** column that indicates how many devices are attached. The pop out window will show attached devices.

Generate Bootstrap Configuration File

This step is only needed if onboarding devices using the bootstrap method described in the next section.

1. On vManage, navigate to **Configuration > Devices**.
2. Click the More Actions icon (**…**) to the right of the row for the applicable device and choose **Generate Bootstrap Configuration**.
3. In the dialog box that opens, make sure that the Cloud-init radio button is selected, and then click **OK**.
4. The system generates a file and displays its contents in a pop-up window.
5. Click **Download**.
6. Rename the file to ciscosdwan.cfg (case sensitive).
7. Copy the ciscosdwan.cfg file to a bootable USB drive or to the bootflash of the device. The file must be named exactly as shown or the device will not read it.

Method - Plug and Play

When a device meets the requirements stated below, it boots and reaches PNP Connect portal to get the vBond IP address. The router establishes a secure tunnel to vBond, and after authentication vBond sends the vManage IP address to the Cisco IOS XE router. The router contacts vManage over a secure tunnel and vManage sends the full configuration to the Cisco IOS XE router. Finally, the router contacts vSmart over a secure tunnel; after authentication, it will join the SD-WAN fabric. This process does not require any manual intervention or configuration.

Prerequisites

- Device is connected to a network.
- Device can get a DHCP IP address and reach PnP portal and vBond.
- Device does not have any configuration.
- Device is imported to vManage as valid or staging.
- Device is assigned to a device template.

Method – Bootstrap

If the device meets prerequisites mentioned below, when the device boots, it reads the configuration file from the USB drive from or the bootflash and uses the configuration information to join the network. The configuration will enable network connectivity as well as provide system parameters and vBond address. Once the device is authenticated by vBond, it gets vManage information. The router establishes communication with vManage and joins the overlay network. It is recommended to copy the configuration file on bootflash before performing IOS XE SD-WAN installation. After IOS XE SD-WAN installation is completed the default one-time user admin is deleted, and the default password can be used once and then must be changed.

Prerequisites

- Device is connected to a network.
- SD-WAN controllers should be reachable on the network.
- Bootstrap configuration is loaded on bootflash of the device or on a bootable USB drive plugged to the device.
- Device is imported to vManage as valid or staging.
- Device is assigned to a device template.

Method - Manual Configuration

Complete the following step for manual onboarding of the router onto SD-WAN network.

1. Login onto vManage GUI using the credentials provided.
2. Logon to the IR8340 router using the console.
3. Make the necessary connections to ensure that the IR8340 Cisco Edge router is reachable to the cloud infra.
4. Check the rom version and the IOS-XE version that's running on the router. Ensure that they are the latest recommended version supporting SDWAN. If required, kindly upgrade rommon and IOS-XE. With later releases of IOS-XE, there's no need to load a separate SDWAN image onto the router.
5. Ensure that the router to which the Cisco Edge device is connected to reach the SDWAN Cloud infra is configured to provide ip address, default gateway and dns server addresses to the Cisco Edge router as it boots up. In this scenario, SA-HER is the dhcp server and assigns the parameters to IR8340 Cisco Edge router.
6. If the asr1002-HX has the latest IOS-XE image:
    - Take a backup of the running configuration.
    - issue "controller-mode enable"
    - The router will be reloaded with a warning message saying, "No day 0 Bootstrap configuration available". Proceed with reload.
    - As the router reloads, the interface would get a dhcp assigned ip address, default route and dns servers.
        - Static ip addressing and default route can also be provisioned instead of dhcp.
    - The router initiates the PNP process. Use "pnpa service discovery stop" command to stop the PNP registration process.
    - Check the reachability to the cloud infra from the Cisco Edge router using ping.
        - Gather the output of "show sdwan certificate serial" command.

Chassis number: IR8340-K9-FDO2506J99H Board ID serial number: XXXXXXXX Subject S/N: XXXXXXXX

- Fill these details in CSV Format file.

 # Format - chassis number, product id, cert serial number, sudi serial

- cert serial number is the same as Board Serial number
- Sudi serial number is the same as Subject S/N.
- From the vManage page, navigate to Devices Menu. Click on the top left corner → Configuration → Devices.
- Select WAN Edge list option and upload the CSV file with the appropriate details.
- From the main menu, navigate to Administration→ Settings.

- Write down the Organization name and vBOND details.
  - Create and apply the following configuration on the router. system-ip , domain-id and site-id are important attributes.

```
Router#config-transcation
!
system
system-ip 192.168.60.100
domain-id 1
site-id 2001
admin-tech-on-failure
sp-organization-name "IOT-BU - 238964"
organization-name "IOT-BU - 238964"
vbond vbondviptela.net port 12346          <<<<<< VBOND Detail
!
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet0/0/0    <<<<<<< Interface through which internet is
reachable for the  topology.
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet0/0/0
cIStunnel-interface
encapsulation ipsec
exit
hostname IR8340-vEDGE-001
commit
exit
!
```

Device Management

Software Upgrade

When upgrading using Cisco Catalyst SD-WAN Manager, you can upgrade using a code image that is directly loaded onto vManage or a remote Cisco Catalyst SD-WAN Manager, and you can also upgrade using a code image located on a remote file server. In this procedure, software for any device is uploaded to the vManage software repository.

Uploading Images on Cisco Catalyst SD-WAN Manager

1. Go to **Maintenance > Software Repository**. The repository stores the image locally on Cisco Catalyst SD-WAN Manager, a remote file server, or remote Cisco Catalyst SD-WAN Manager.
2. Click **Add New Software** and choose **vManage** from the drop-down list.
3. A dialog box will appear prompting you to drop an image file or browse for an image on the local computer.
4. Load the desired images and click the **Upload** button. A window will indicate that the images are being loaded to the Cisco Catalyst SD-WAN Manager. Once completed, a message will indicate the images were uploaded successfully, and the version, software location (Cisco Catalyst SD-WAN Manager), and available files will be added to the repository.

Device Upgrade

1. Confirm there is enough space on the device for an image download using the dir bootflash: command. Free space is shown at the bottom. Remove files if needed.
2. Go to **Maintenance > Software Upgrade** to check the code versions under the Current Version column.
3. If an upgrade is needed, check the check boxes next to the routers you want to upgrade and click the **Upgrade** button. A dialog box will appear.
4. Verify that vManage is selected. Choose the new code version from the drop-down list.
5. Check the Activate and Reboot check box and then click **Upgrade**. The device will retrieve the software, install it, and then reboot in order to activate it. Optionally you can leave the box unchecked and activate the image later.

Activate an Image

For images already installed but not activated follow these steps:

1. Go to **Maintenance > Software Upgrade** to check the code versions under the Current Version column.
2. Check the check boxes next to the routers you want to activate and click **Activate**. A dialog box will appear.
3. If there is an image installed ready to activate it will show in the Version drop-down menu. Select the version and click **Activate**. The router will reboot with the new version.

Best Practices

- Break up the routers into different upgrade groups. You can identify them with a tag in the device-groups field in the system template. Target a test site or multiple test sites and put those routers into the first upgrade group.
- In dual-router sites, put each router into a different upgrade group and do not upgrade either of them at the same time.
- All routers in an upgrade group can be upgraded in parallel (up to 32 WAN Edge routers), however, consider the ability for vManage or a remote file server to be able to handle the concurrent file transfers to the routers.
- Upgrade the first upgrade group and let the code run stable for a predetermined amount of time, then proceed to upgrade the additional upgrade groups.
- To keep the disk from getting full, clean up older versions using vManage. To delete older versions, go to **Maintenance > Software Upgrade**, select the device you want to clear and select Delete Available Software. On the dialog box select the images you want to delete and then click **Delete**.

Reboot a Device

Reboot a router by going into **Maintenance > Device Reboot**. Make sure you are on the WAN Edge tab. Select the device to reboot and click **Reboot**. Confirm the action on the pop out window.

Connect to the Device Terminal

Go to **Tools > SSH terminal**. Choose the device you want to connect on the left panel. A terminal window to the device will be displayed. Provide device credentials.

Refer to the list of documents in the following table for other scenarios that were also validated as part of the solution.

Table 9 SDWAN Templates and Configurations

Template	Reference
Device Template	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/configure-devices.html
VPN Interface using SVI	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/configure-interfaces.html#c-VPN_Interface_SVI-12319

Configure VPN	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/segmentation/vEdge-20-x/segmentation-book/segmentation.html#d221e494a1635
Centralized Policy for Hub and Spoke	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/centralized-policy.html
Zone Based Firewall	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security-book/m-firewall-17.html#c_Zone_Based_Firewall_Configuration_Examples_12252.xml

IR8340 Management using Cisco Catalyst Center

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

Administration

Installation

For information on installing the Cisco Catalyst Center appliance, refer to: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html.

Licensing

For this implementation the Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) tool was used for Cisco Catalyst Center licensing. For Cisco SSM On-Prem installation, see: https://www.cisco.com/web/software/286285517/152313/Smart_Software_Manager_On-Prem_8-202006_Installation_Guide.pdf.

Upgrade

Information for upgrading Cisco Catalyst Center can be found at: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide.html.

Substation Router Discovery

Cisco Catalyst Center can discover network devices and add them to the managed inventory, which can help administrators maintain and monitor the environment from a central viewpoint. The Device Controllability feature can be added to the discovery process to prepare devices for management through Cisco Catalyst Center when subsequent provisioning configuration or inventory changes are made. To discover devices, do the following:

Prerequisites before discovering in DNA

For the Network devices to be discovered by the Cisco Catalyst Center, CLI and SNMP credentials should be configured on the devices as configured at the Cisco Catalyst Center in the previous section. The example configuration used network devices in this implementation is:

1. Configure CLI SSH user credentials on the network device. Example configuration on Cisco Catalyst 9300 Switch Stack:

```
username <username> privilege 15 password 7 <password>enable secret
<password>
```

2. Configure SNNMPv3 credentials on the network device. Example configuration on Cisco Catalyst 9300 Switch Stack:

```
snmp-server group default v3 priv
snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None
snmp-server view SNMPv3All iso included
snmp-server view SNMPv3None iso excluded
snmp-server community <CommunityString> RWsnmp-server user <username>
default v3 auth md5 <password> priv aes 128 <password>
```

3. Enable SSH Version 2 access on the network device. Example configuration on Cisco Catalyst 9300 Switch Stack:

```
ip ssh source-interface Loopback0
crypto key generate rsa modulus 2048
ip ssh version 2
!
line vty 0 4
login local
transport preferred ssh
transport input all
line vty 5 15
login local
transport preferred ssh
transport input all
!
```

1. From the Cisco Catalyst Center web interface, navigate to **Tools > Discovery**.

2. Click the **Add Discovery** button.

   - Note at the bottom if Device Controllability is enabled (it is enabled by default). If enabled, Cisco Catalyst Center will configure SNMP or NETCONF credentials on the device during Discovery (it will not overwrite existing SNMP or NETCONF configuration). We recommend using Device Controllability to make use of the Cisco Catalyst Center monitoring capabilities.

     Note: Currently Cisco IE switches can be discovered via NETCONF however there are no additional capabilities from it in the current release. If you do not want any configuration changes made to the device(s), click the **Disable** link.

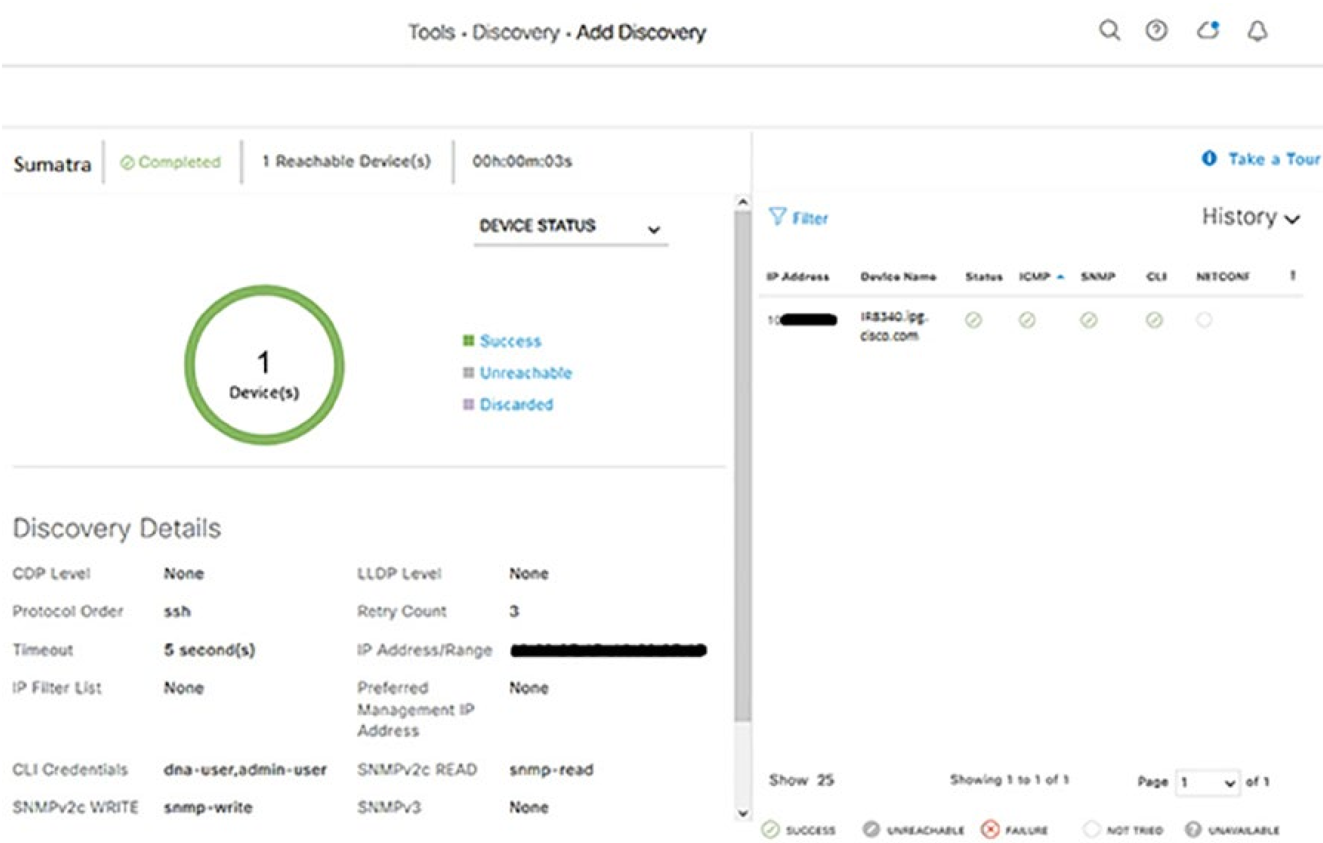
   - In the **Discovery Name** field, enter a name for the relevant device(s) being discovered.

   - Under **IP Address/Range**, choose the appropriate **Discovery Type**:
     - For **CDP**, enter the **IP Address** of a device to be discovered. You can change the **CDP Level** to something other than the default to detect more or fewer neighboring devices to the original device.
     - For **IP Address/Range**, in the **From** field enter the lowest IP address to be scanned. In the **To** field, enter the highest IP address to be scanned. If only one device is being discovered, enter the same IP address in both fields. The IP address method is recommended for discovering devices.
     - For **LLDP**, enter the **IP Address** of a device to be discovered. You can change the **LLDP Level** to something other than the default to detect more or fewer neighboring devices to the original device.

3. Under **Credentials**, click the toggle buttons of the necessary entities under **CLI, SNMPv2c Read, SNMPv2c Write**, and so on. The device being discovered must accept at least one form of these credentials for discovery to be successful and CLI credentials are mandatory.

4. Click the **Discover** button. The Discovery process will begin and show progress on the Discovery page with automatic refreshing to display the current status. When the process is finished, it will display success or failure results and add the discovered device to Inventory.

Figure 67 Catalyst Center discovery of substation router



After discovery, assign the device to a Site and Provision, which can be done individually or in the same step.
Assign to Site only:

1. Navigate to **Provision** > **Network Devices** > **Inventory**.
2. From the left Hierarchy, choose **Global** > **Unassigned Devices**.
3. Locate the newly discovered device in the list and check the checkbox. From the Actions drop-down list, choose **Provision** > **Assign Device to Site**.
   a. On the Assign Device to Site slide-in pane, click the **Choose a Site** link. Click the desired site from the hierarchy then click the **Save** button. Click the **Next** button.
   b. Review the settings that will be deployed, then click the **Next** button.
   c. Click the **Now** radio button to make the change immediately (if scheduling the assignment for a future date and time, click the **Later** radio button and specify the date and time).
   d. Click the **Assign** button.

After the device has been assigned, it will be in the device list of the specified Site. Note that when Device Controllability is enabled, assigning the device to a Site will trigger the following configurations (where applicable):

- Controller certificates
- SNMP trap server definitions
- Syslog server definitions
- NetFlow server definitions
- IPDT enablement

Assign to Site and Provision:
1. Navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose **Global > Unassigned Devices**.
3. Locate the newly discovered device in the list and check the checkbox. From the Actions drop-down list, choose **Provision > Provision device**.
   a. On the Assign Site step, click the **Choose a site link** and choose the desired Site. Click the **Save** button, then click the **Next** button. (Note that if Site assignment was done previously no action is needed here).
   b. On the Advanced Configuration step, choose the device from the Devices list if there are any template settings to be configured. When finished, or if no template is applied, click the **Next** button.
   c. On the Summary step, review the configuration to be added to the device. Click the **Deploy** button.

After the device has been provisioned, it will be in the device list of the specified Site.

Note: For Cisco Catalyst Center release 2.2.3.3:
- Provisioning a device that has already been configured with AAA before being discovered will fail. Remove any AAA configuration before pushing AAA using Cisco DNA Center.

Inventory

Cisco Catalyst Center Inventory has a wide variety of capabilities to manage devices. Once a device has been discovered or added to inventory through PnP, it can be provisioned, which adds the specified Network Settings to devices. In addition, after devices are fully managed, Inventory can provide compliance and software verification, as well as options to change device settings or initiate device replacement. The following section details some of the monitoring and management capabilities in Inventory.

Image Repository

Cisco Catalyst Center communicates with Cisco.com to retrieve available software images for the suite of supported devices, whether directly or through a proxy. Similar to Network Settings, software versions can be specified on a per-Site basis to ensure consistent operation across devices. After devices have been discovered and added to Sites, you can change the Golden Image in Image Repository for each device type by doing the following:

1. From the Cisco Catalyst Center web interface, navigate to **Design > Image Repository**.
2. Choose the desired Site from the left hierarchy.
3. From the Devices list, expand each device to see all available software images. Click the arrow button in the Golden Image column to download the relevant image, and in the subsequent Download Image dialogue box, check the Mark the image as golden after download checkbox to set that image as the Golden Image for that specific device type.
4. Repeat for other devices and Sites as necessary.

Software Image Management

Devices can be upgraded automatically through Cisco Catalyst Center, which downloads the image from Cisco.com, pushes the image to the device, and performs the upgrade. In addition, you have the option of uploading a desired image to Cisco Catalyst Center and upgrades can be scheduled in advance. After ensuring the image is set as Golden (see the Image Repository section), update a device software image by doing the following:

1. From the Cisco Catalyst Center web interface, navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose the Site with the device to be upgraded.
3. Check the checkbox next to the device to be upgraded and from the Actions drop-down list choose **Software Image > Update Image**.
4. From the Image Upgrade slide-in pane, check the checkbox of the device to be upgraded and click the **Next** button.
5. Under Software Distribution, click the **Now** radio button (if scheduling an upgrade for a future date and time, click the Later radio button and specify the date and time). Click the **Next** button.
6. Under Software Activation, check the Initiate Image Activation after Image Distribution is finished checkbox. If you just want to push the image to the device and not launch the upgrade, leave the box unchecked and either specify the start date and time or click the **Skip Activation** link at the bottom. You also have the option of checking the Initiate Flash Cleanup after Activation checkbox, which will automatically remove unused software image files from the device after the upgrade. Click the **Next** button.
7. On the Summary step, review the upgrade details and then click the **Submit** button.

Notes on software image management:

- Cisco Catalyst Center will give priority to installing and running the image on sdflash if it is present. If the software is running in Install mode from flash with sdflash present, the upgrade will fail.
- If the image is running on sdflash and it is formatted as vfat the upgrade will be successful. If it is formatted in ext4 only (for Cisco Cyber Vision) the upgrade will fail. See IOS XE Devices with Cisco Cyber Vision for details on partitioning sdflash, which allows the software image and iox applications to run concurrently from sdflash.
- The update process will trigger a reload on the device which will impact network connectivity for the device and any connected endpoints.
  On the Inventory page, you can review the status of the update by choosing Software Image > Image Update Status from the Actions drop-down list. In addition, from Inventory you can review which devices are not running the specified Golden Image with the Compliance status column or choosing Software Images from the Focus drop-down list.

Templates

Cisco Catalyst Center Templates can be used to automate any configuration on discovered or managed devices, whether they are new or have existing configurations. See the Appendix for examples and tips on using templates. To create a template, do the following:

1. From the Cisco Catalyst Center web interface, navigate to **Tools > Template Editor**.
2. Click the **Plus** button and choose **Create Template**.
   a. Under Template Type, click the **Regular Template** radio button.
   b. Under Template Language, click the **Velocity** radio button. The Jinja option can be used as well; for more details refer to Cisco DNA Center Documentation:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3.html.

c. Under Name, enter a name for the template.

d. From the Project Name drop-down list, choose the relevant project. For example, choose **Onboarding Configuration** to create a template to be used for initial configuration of a new device during Plug and Play.

- Click the **Edit** link under Device Type(s).
- Navigate through the expandable lists to check the boxes for all relevant devices.

e. At the top, click the **Back** to Add New Template link.

f. From the Software Type drop-down list, choose the appropriate Cisco software type.

g. Click the **Add** button.

h. The Template Editor pane will display, allowing you to enter CLI commands for configuration. Note that variables may be used by denoting a dollar sign with the argument; for example:

```
ip address $address 255.255.255.0
```

i. After adding all desired configuration, from the Actions drop-down list choose **Save** and then choose **Commit**.

Note: Any changes to existing templates do not trigger a configuration change on associated devices until they are provisioned again.

Network Profiles

Cisco Catalyst Center Network Profiles allow you to attach templates to Sites so that when a device is added to the Site, Cisco Catalyst Center will automatically apply the configuration specified in the template. To create a Network Profile, do the following:

1. From the Cisco Catalyst Center web interface, navigate to **Design > Network Profiles**.
2. From the Add Profile drop-down list, choose the appropriate device type.

a. For the Profile Name field, enter a name.

b. Choose the OnBoarding Template(s) tab to attach any templates to be used during Plug and Play for unconfigured devices or the Day-N Template(s) tab to attach any templates for additional configuration to be pushed during provisioning.

c. Click the **Add Template** button.

- On the Add Template slide-in pane, choose the relevant template from the Templates list.
- Click the **Add** button.

d. Click the **Save** button.

Note: Adding a template to a Network Profile will not trigger a configuration change on applicable existing devices until they are provisioned again.

For Assurance, Device Health and DNA security, see the following Cisco Validated Document for more details. https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Networking/DNA_Center_IA_IG.html

Network Management of PE and core NCS devices with Crosswork Network Controller

Cisco Crosswork Network Controller (CNC) automation suite offers a unified platform for seamlessly deploying, managing, and monitoring end-to-end transport networks with real-time visibility and control. Crosswork enhances customer experience by enabling real-time visualization of networks, and GUI-driven deployment of policies, VPN services, and traffic engineering with advanced SLAs over multi-vendor & multi-domain transport networks. Crosswork Infrastructure is a microservices-based platform, leveraging a cluster architecture to provide scalability and high availability (HA). CNC 6.0 has been leveraged for the CVD. Please refer the Cisco CNC Installation Guide 6.0 (https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/InstallGuide/b_cisco_crosswork_6_0_install_guide.html) for detailed instructions on installing CNC 6.0.

Prerequisites

- This guide assumes that the user has already installed Cisco Crosswork Network Controller (CNC), Cisco Crosswork Data Gateway (CDG), and Cisco Network Services Orchestrator (NSO).
  - Crosswork Network Controller
    https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/InstallGuide/b_cisco_crosswork_6_0_install_guide.html

  - Crosswork Data Gateway
    https://www.cisco.com/c/en/us/td/docs/net_mgmt/crosswork_data_gateway/6-0-1-Cloud/InstallConfigGuide/bk-cdg-6-0-1-installation-configuration-guide-for-cloud/m_cdg_overview_cloud.html

  - Network Services Orchestrator
    https://developer.cisco.com/docs/nso-guides-6.1/installation/
    https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/InstallGuide/b_cisco_crosswork_6_0_install_guide/m_cw-5-0-integrate-nso.html

- Routers have base configurations (SSH, Netconf, SNMP, IGP, BGP etc.) to reach Crosswork Data Gateway, Crosswork VMs, NSO and SR-PCE
  - Configure CLI SSH user credentials on the network device. Example configuration on Cisco NCS540 router:

```
username <username>
 group root-lr
 group cisco-support
 secret 10 <password>
!
```

  - Configure SSH Version 2 on the network device. Example configuration on Cisco NCS540 router:

```
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
```

- Configure Netconf and SNMP on the network device. Example configuration on Cisco NCS540 router:

```
netconf agent tty
!
netconf-yang agent
ssh
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
snmp-server packetsize 4096
```

- Configure NTP settings ensure that Crosswork receives the correct timestamps for events. Example configuration on Cisco NCS540 router:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server <NTP_Server>
update-calendar
```

- Configure IGP and BGP on the network device.

  Refer to "*IR8340 Substation Router as PE over SR*" for configuration examples.

Onboarding Devices

- The NSO and SR-PCE provider are added as per the Installation Guide (https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/InstallGuide/b_cisco_crosswork_6_0_install_guide.html)

- The network devices are onboarded onto CNC as per the User Guide.(https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/AdminGuide/b_CiscoCrossworkAdminGuide_6_0/m_onboarding.html#id_103026)

- Attach the added devices to Cisco Crosswork Data Gateway by referring to steps in below link: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/AdminGuide/b_CiscoCrossworkAdminGuide_6_0/m-crosswork-data-gateway.html#id_126373

- Once the devices are onboarded and attached to CDG, You can view the network devices and their connections in different ways on the topology map. Please refer below link for more information: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/6-0/AdminGuide/b_CiscoCrossworkAdminGuide_6_0/Set-Up-and-Use-Your-Topology-Map-for-Network-Visualization.html

  Note: Visualization of VPN Services (L3VPN/L2VPN) is supported only when they are provisioned in Crossworks. Steps for provisioning the use cases mentioned in this document have been added in following sections.

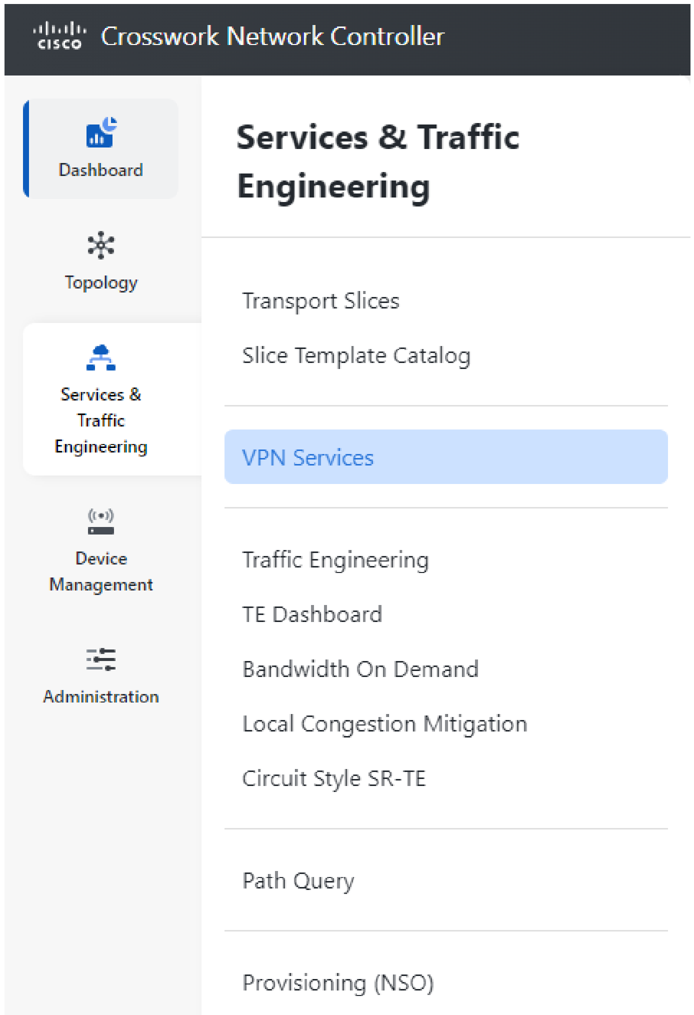
Provisioning L3VPN Services for SCADA

This section lists the various steps to successfully configure L3VPN service between two endpoints. SR-MPLS is the transport enabled with Topology-Independent Loop-Free Alternate (TI-LFA) Fast Reroute (FRR) that enforces the activation of a pre-calculated backup path within 50 milliseconds of path failure. "Cisco Crosswork Optimization Engine" helps in provisioning/monitoring the above. Please refer to the link below for more details: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-optimization-engine/6-0/UserGuide/b_cisco-crosswork-coe-6-0/m2-about-crosswork-optimization-engine.html

Steps to configure:

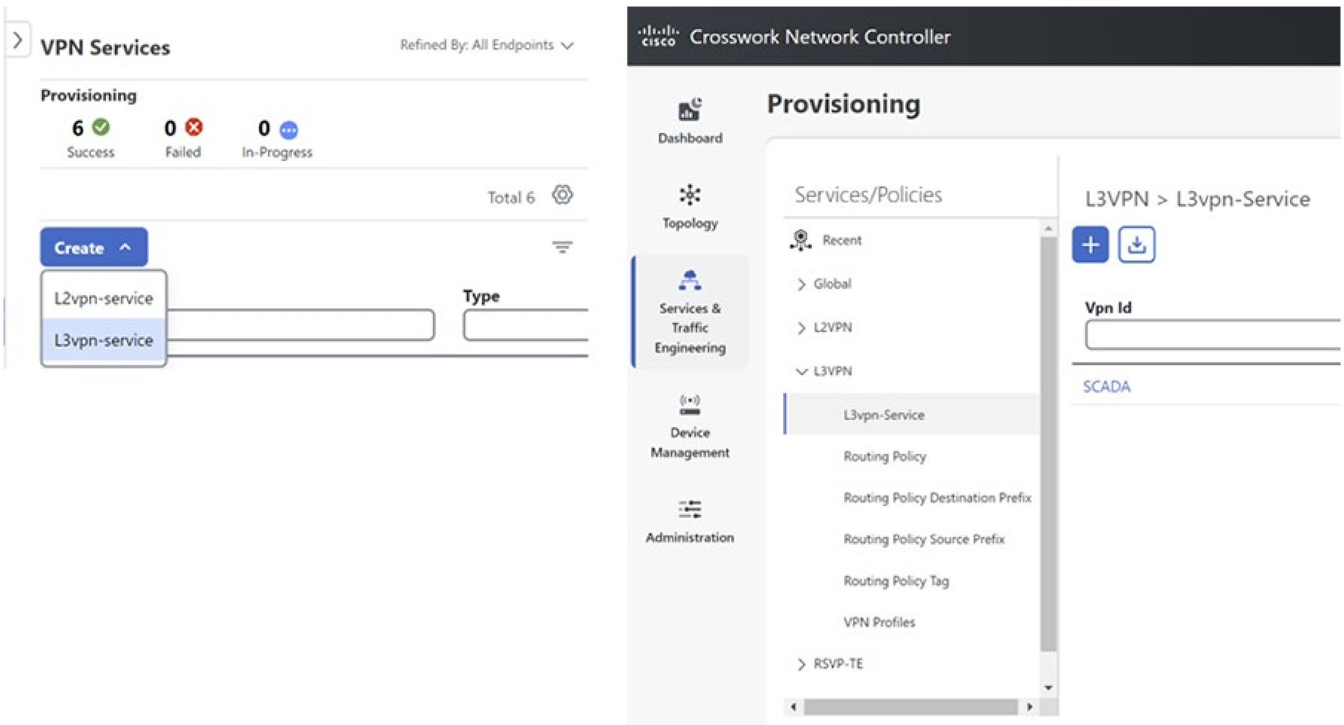
1. From the CNC UI, navigate to **Services & Traffic Engineering -> VPN services**.

Figure 68 VPN Services accessibility from CNC Dashboard



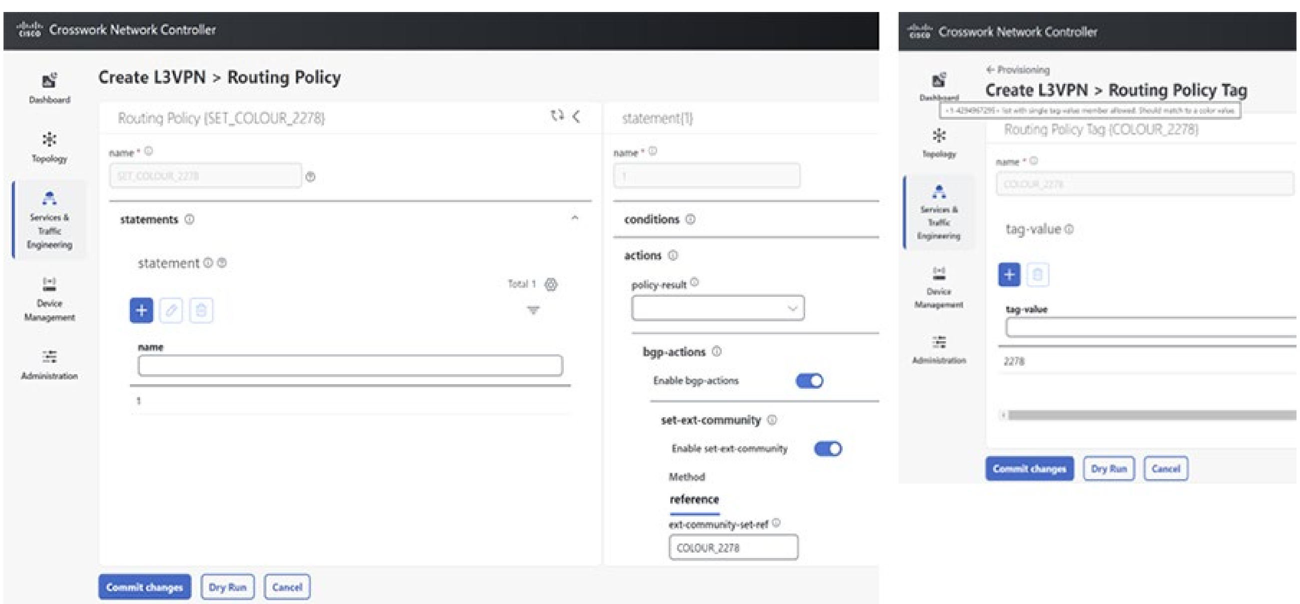
2. As a first step to provision L3VPN service, under **VPN services**, click on **L3VPN** and this will redirect to the L3VPN Provisioning UI.

Figure 69 L3VPN service initiation



3. Under **Routing Policy**, set the BGP extended community color for advertising specific routes. The color has been defined under **Routing Policy Tag**.

Figure 70 L3VPN Routing Policy BGP actions



4. Then under **L3vpn-Service**, the L3VPN service details are entered. Firstly, a VPN identifier/name and VPN instance profile identifier is provided.

Figure 71 L3VPN service parameters' overview

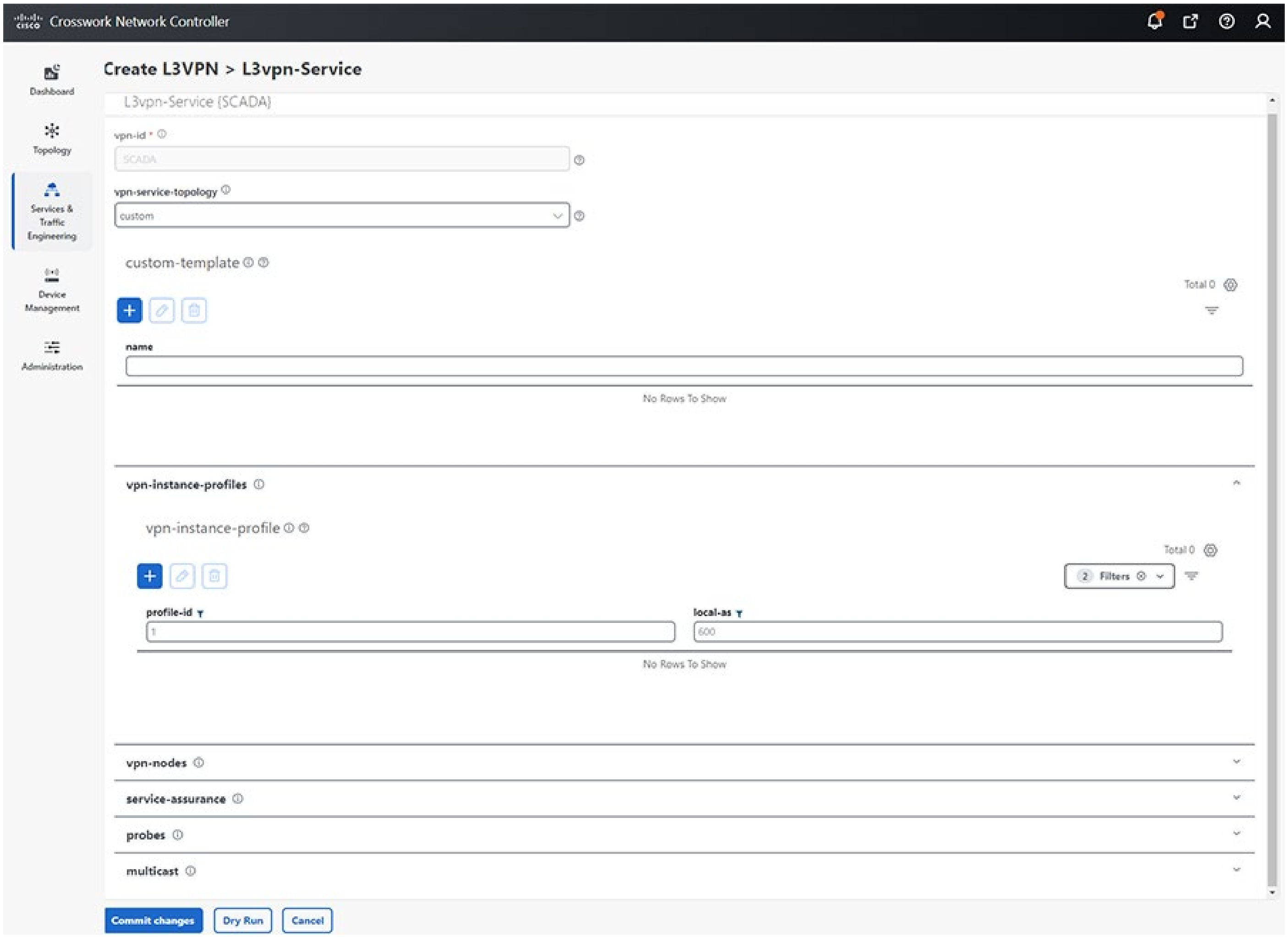
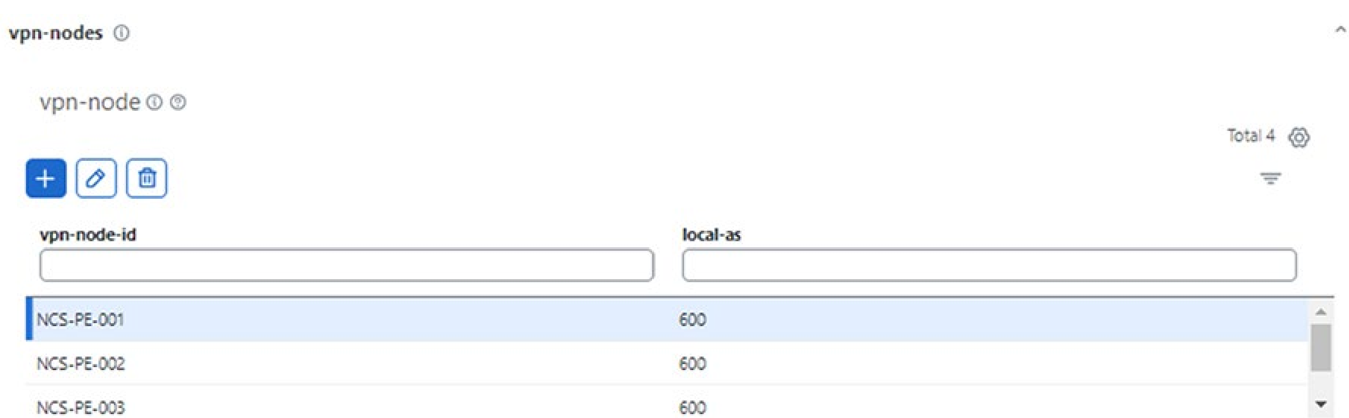


Figure 72 L3VPN endpoint nodes entered under vpn-node

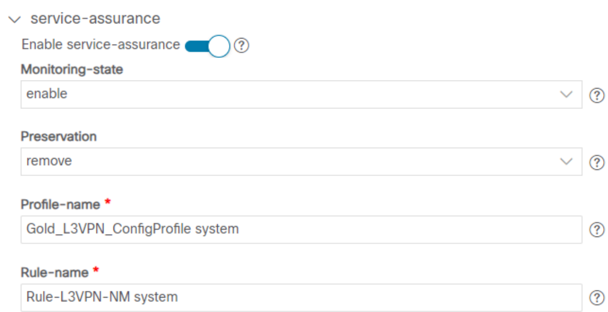


5. Service Assurance can be implemented optionally from the same UI. Firstly, the service assurance monitoring state is enabled. Then one can choose to preserve or remove all assurance related historical data.

   The the profile and rule names are provided. The definition is provided via the IETF-L3VPN-NM service

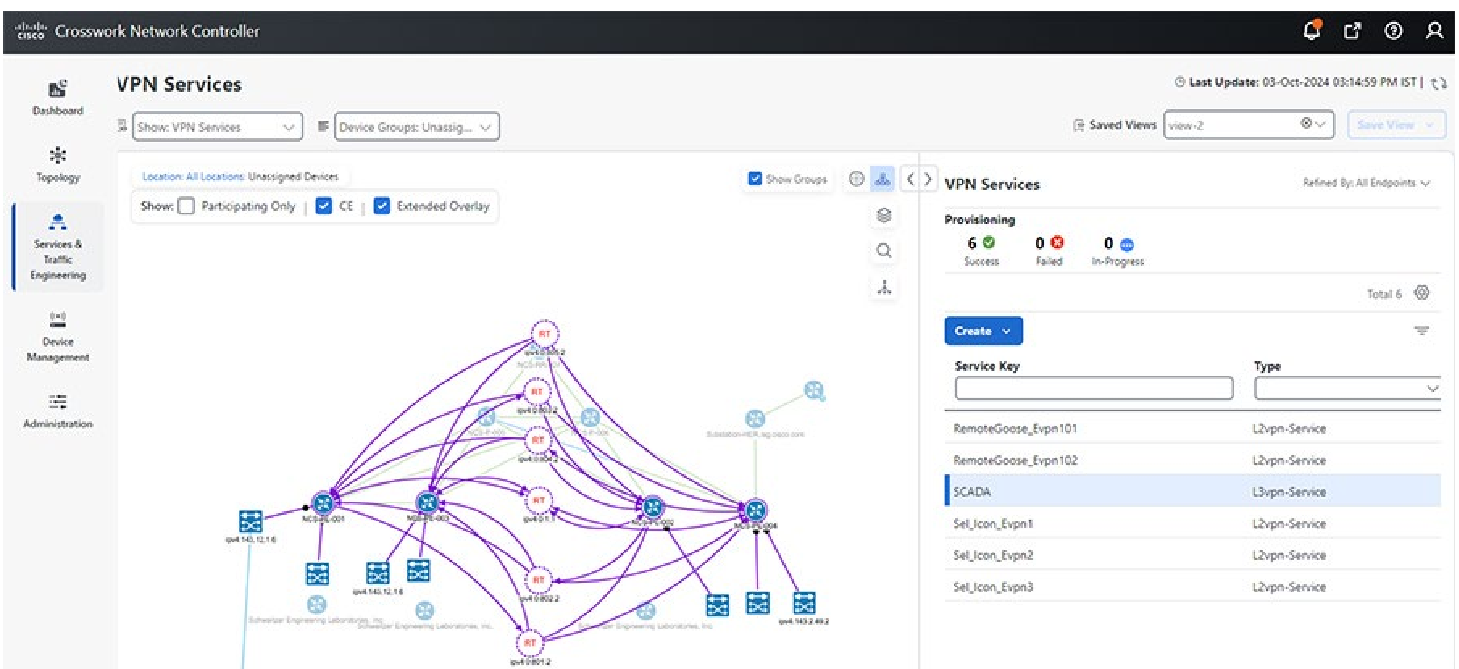
YANG model from Cisco Transport SDN (T-SDN) NSO function pack. Please refer to [NSO T-SDN Function Pack](https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/NSO-CFPs/6-0/Cisco_NSO_Transport_SDN_Function_Pack_Bundle_User_Guide_6_0_0.pdf) User Guide (https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/NSO-CFPs/6-0/Cisco_NSO_Transport_SDN_Function_Pack_Bundle_User_Guide_6_0_0.pdf) for more details.

Figure 73 L3VPN service assurance



After the above steps are completed, the L3VPN service is provisioned, the following figure displays.

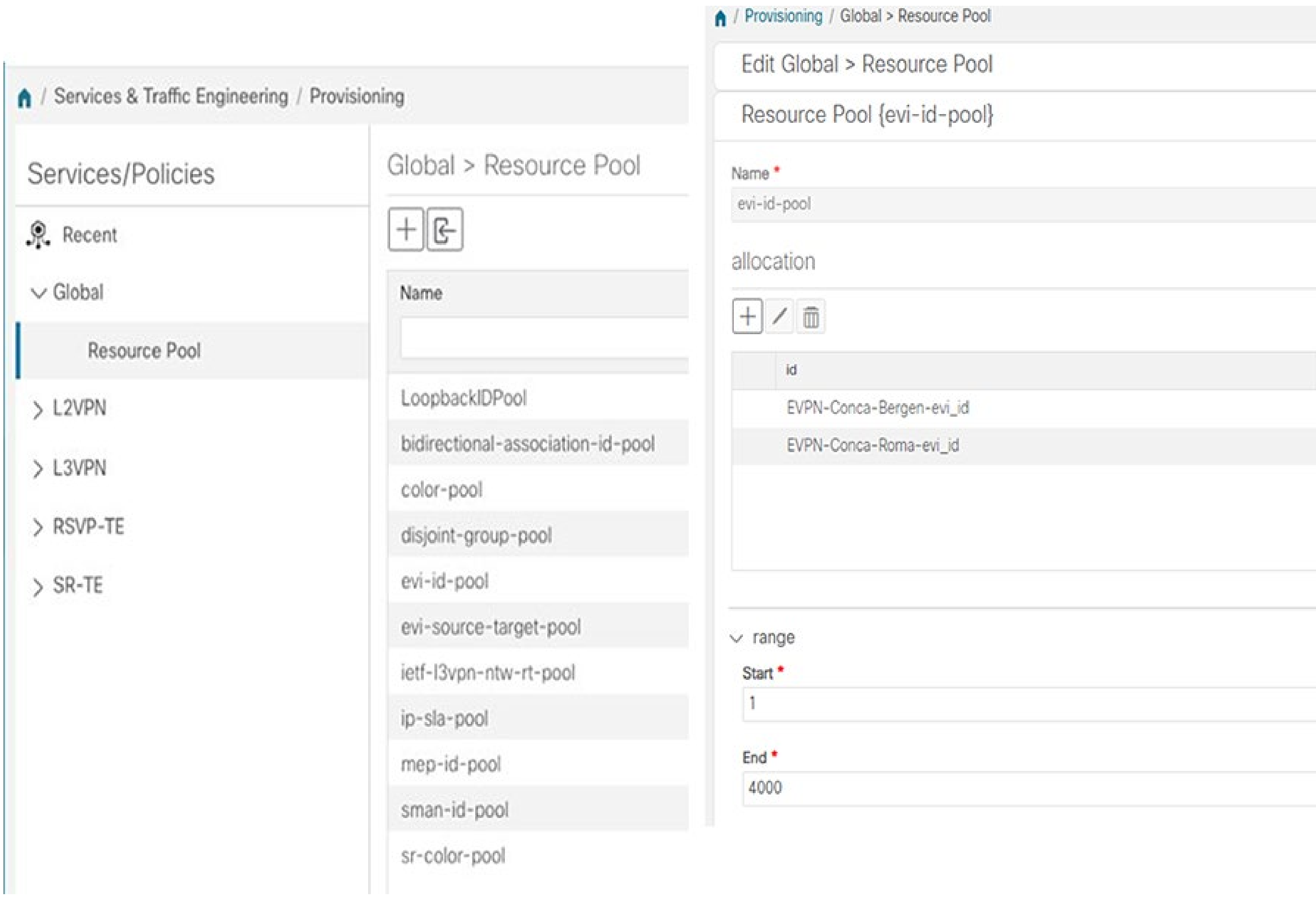
Figure 74 Visualization of the L3VPN service



Provisioning L2VPN Services for Teleprotection

This section lists the steps to provision an L2VPN service. Utility WAN Layer 2 Teleprotection services demand path predictability with bidirectional co-routed path behavior. Herein, a circuit-style segment routing traffic engineering (CS SR-TE) policy is stitched to an L2VPN service. CS SR-TE provides bidirectional co-routed working & protect paths with sub-50-ms switching times.

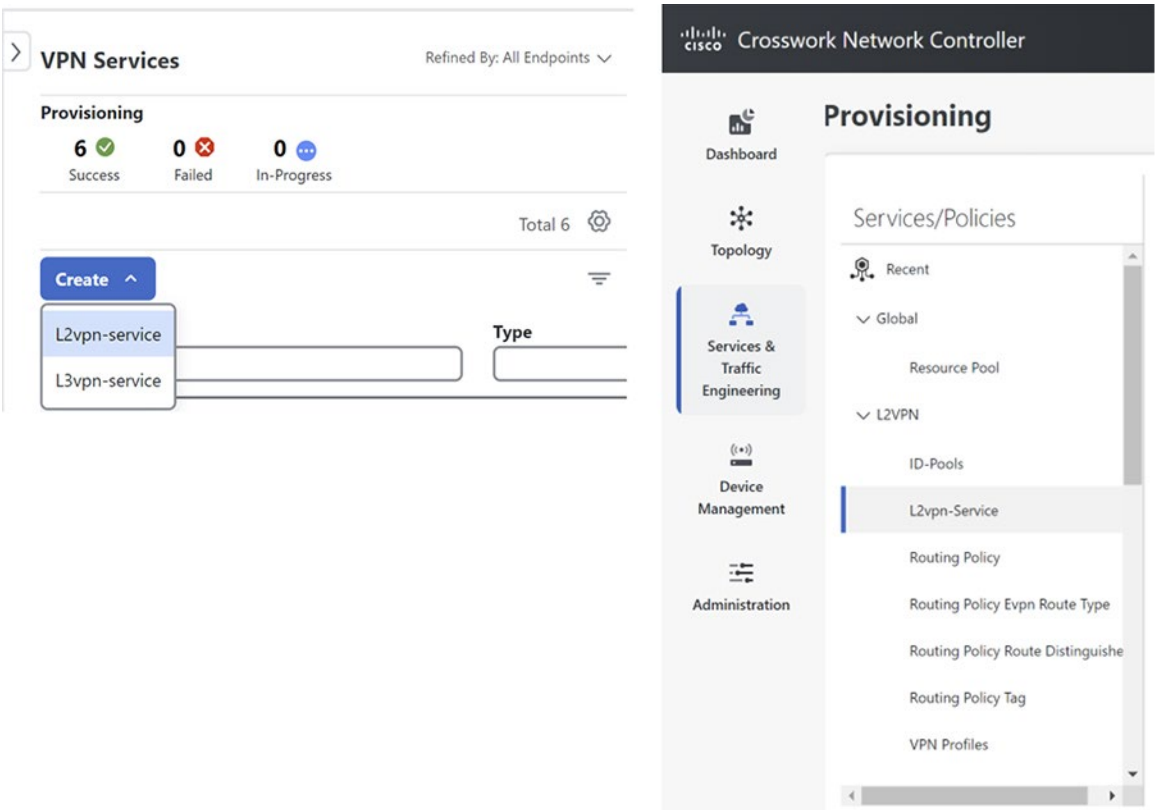
Figure 75 Service/Policy Global Resource Pool overview with example EVI ID definition



Prior to initiating the workflow to provision an L2VPN service, let us briefly look at the facility CNC offers to assign resource pools to global identifiers. One can configure the range for the diverse identifiers required for provisioning VPN service/SR policy. For example, one can allocate the range for the unique EVPN identifier evi, as shown in the figure that follows.

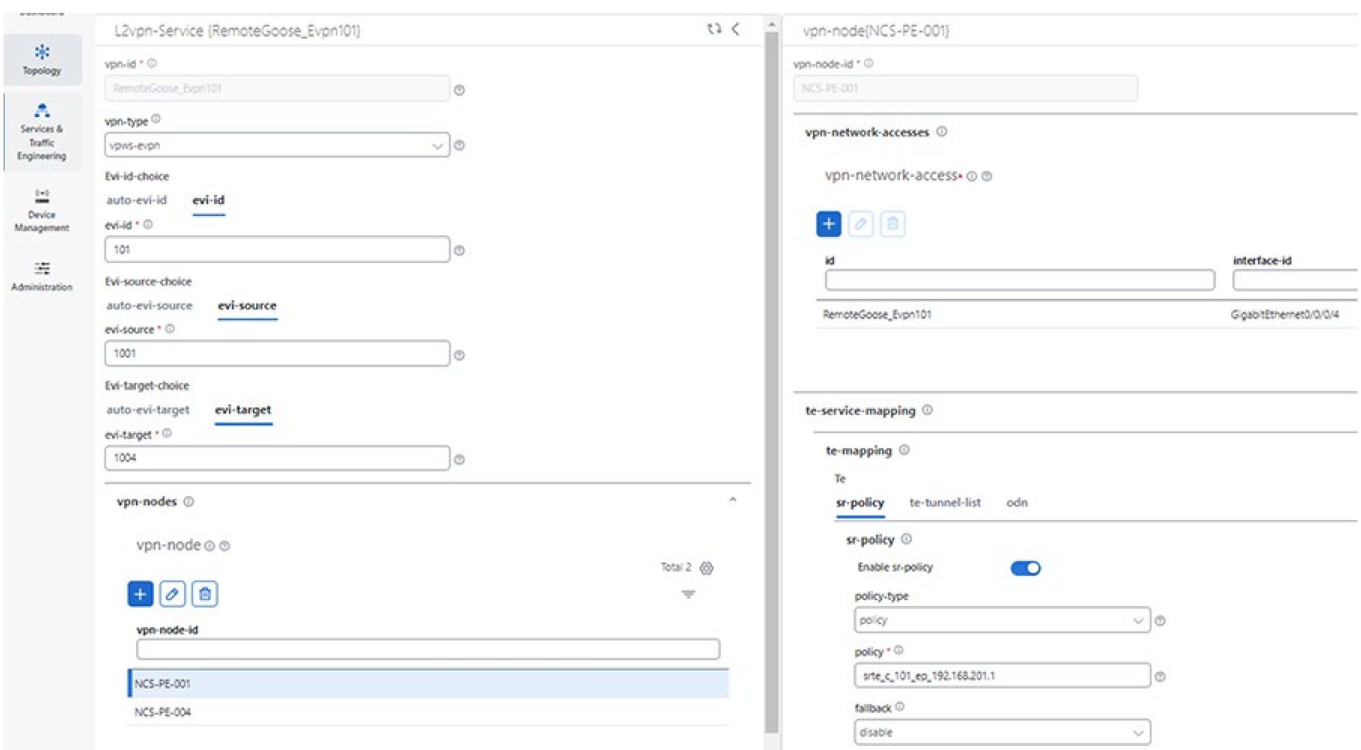
1. Under VPN services, click L2VPN. The figure that follows displays the L2VPN Provisioning UI.

Figure 76 L2VPN service provisioning initiation



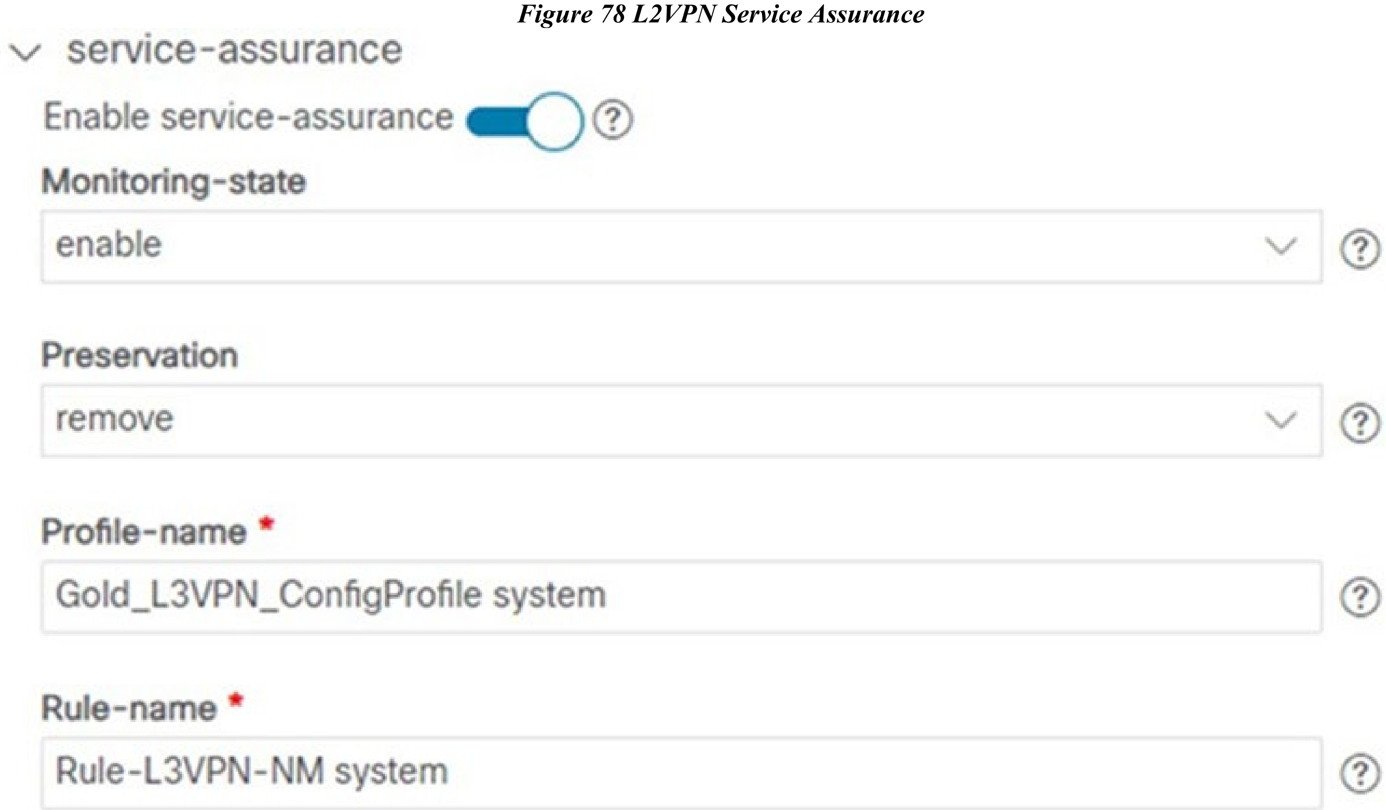
2. Select the L2VPN type. As part of the CVD, EVPN-VPWS service has been provisioned. The VPN name Vpn-id, the unique EVPN identifier evi, source/target identifier that denotes the local/remote attachment circuit ID are entered. One can choose the auto assignment from the global resource pool definition as explained earlier, or manually enter these fields.

Figure 77 L2VPN service parameter overview



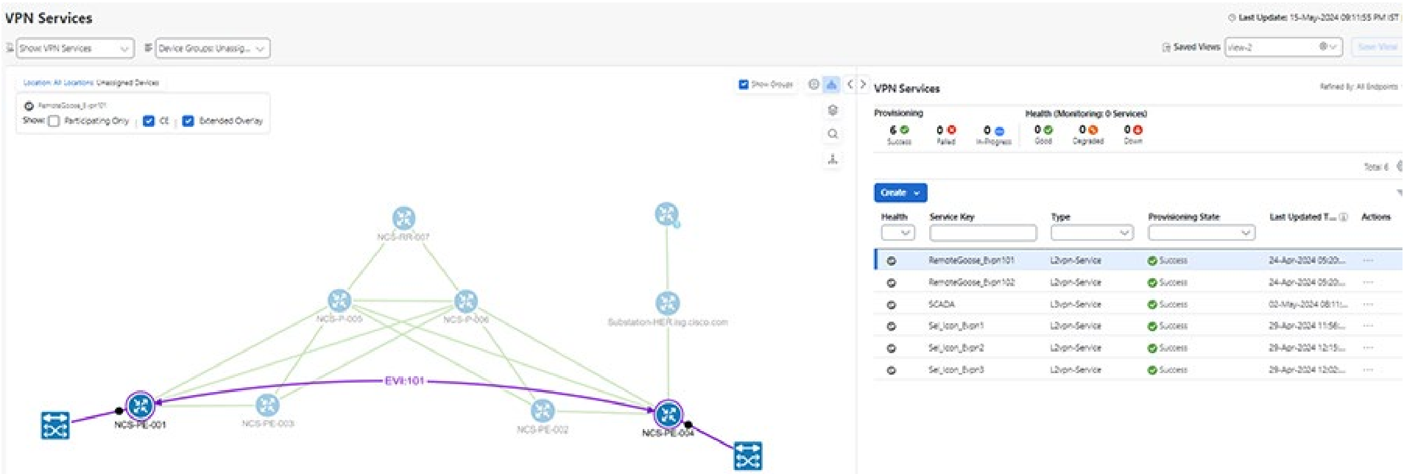
3. Similar to L3VPN, Service Assurance can be implemented. The definition is provided via the IETF-L2VPN-NM service YANG model from T-SDN NSO function pack. Please refer to [NSO T-SDN Function Pack User Guide](https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/NSO-CFPs/6-0/Cisco_NSO_Transport_SDN_Function_Pack_Bundle_User_Guide_6_0_0.pdf) (https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-infrastructure/NSO-CFPs/6-0/Cisco_NSO_Transport_SDN_Function_Pack_Bundle_User_Guide_6_0_0.pdf) for more details.

Figure 78 L2VPN Service Assurance



After these steps are completed, the EVPN-VPWS service is provisioned. Please note that this EVPN-VPWS policy is stitched to a circuit-style SR-TE policy that must be pre-configured, the details for which are provided in the following sections.

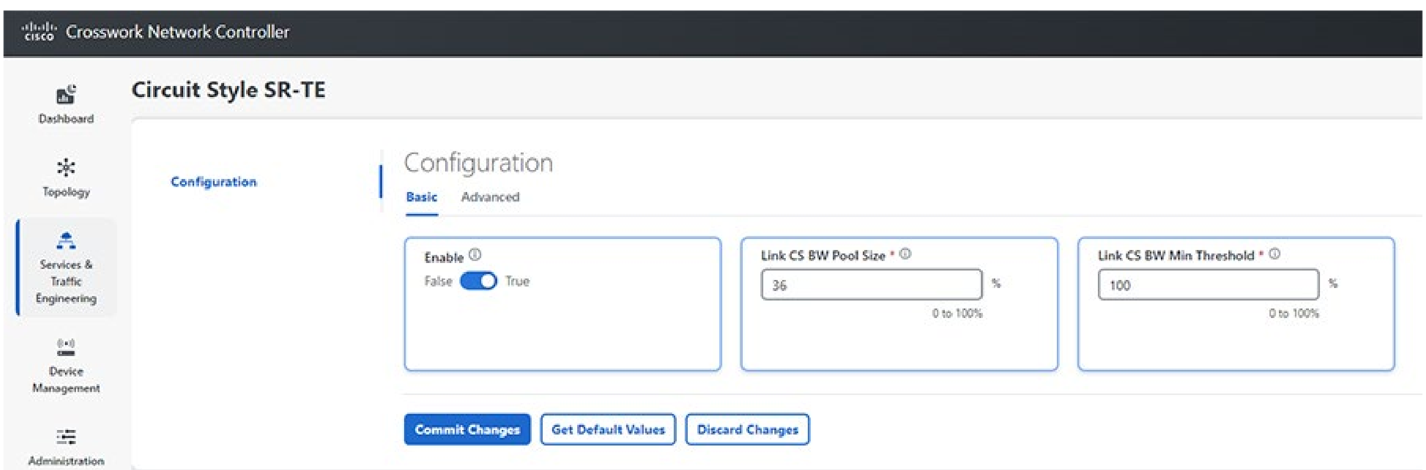
Figure 79 Visualization of the EVPN-VPWS service



To provision circuit-style (CS) SR-TE policy, complete the steps that follow.

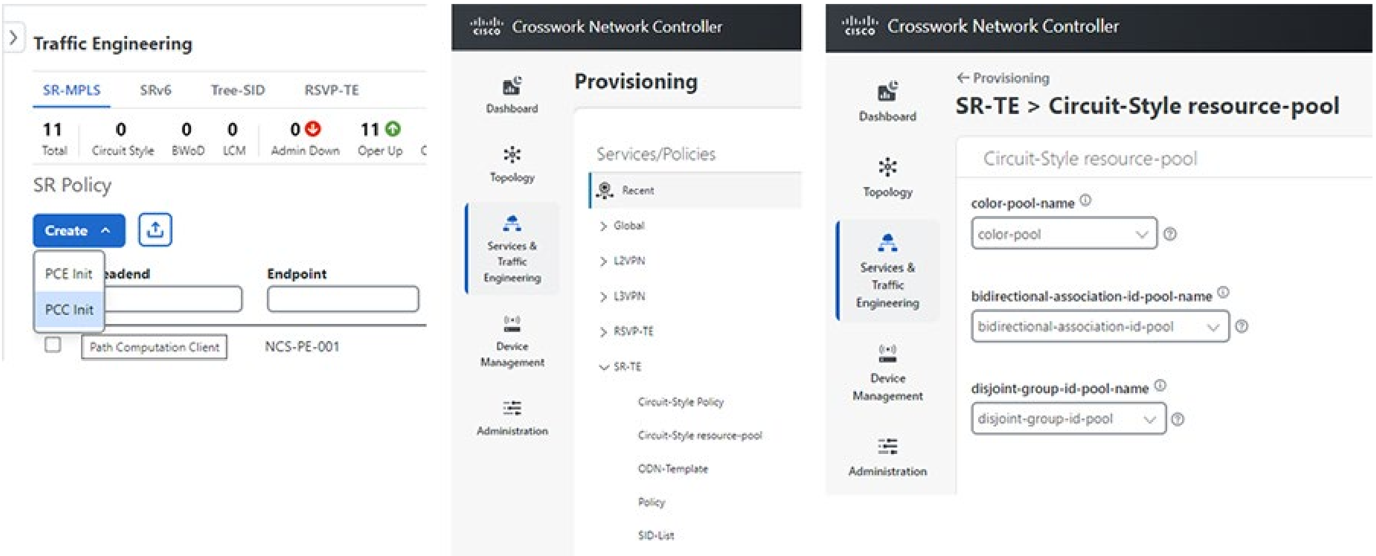
1. Under Services & Traffic Engineering -> Circuit-Style SR-TE, basic configuration is entered including Link CS bandwidth pool size. That is, the percentage of link bandwidth assigned to CS, and CS bandwidth pool utilization threshold beyond which notification will be generated. There is an Advanced configuration, not described here for simplicity.

Figure 80 CS SR-TE bandwidth settings



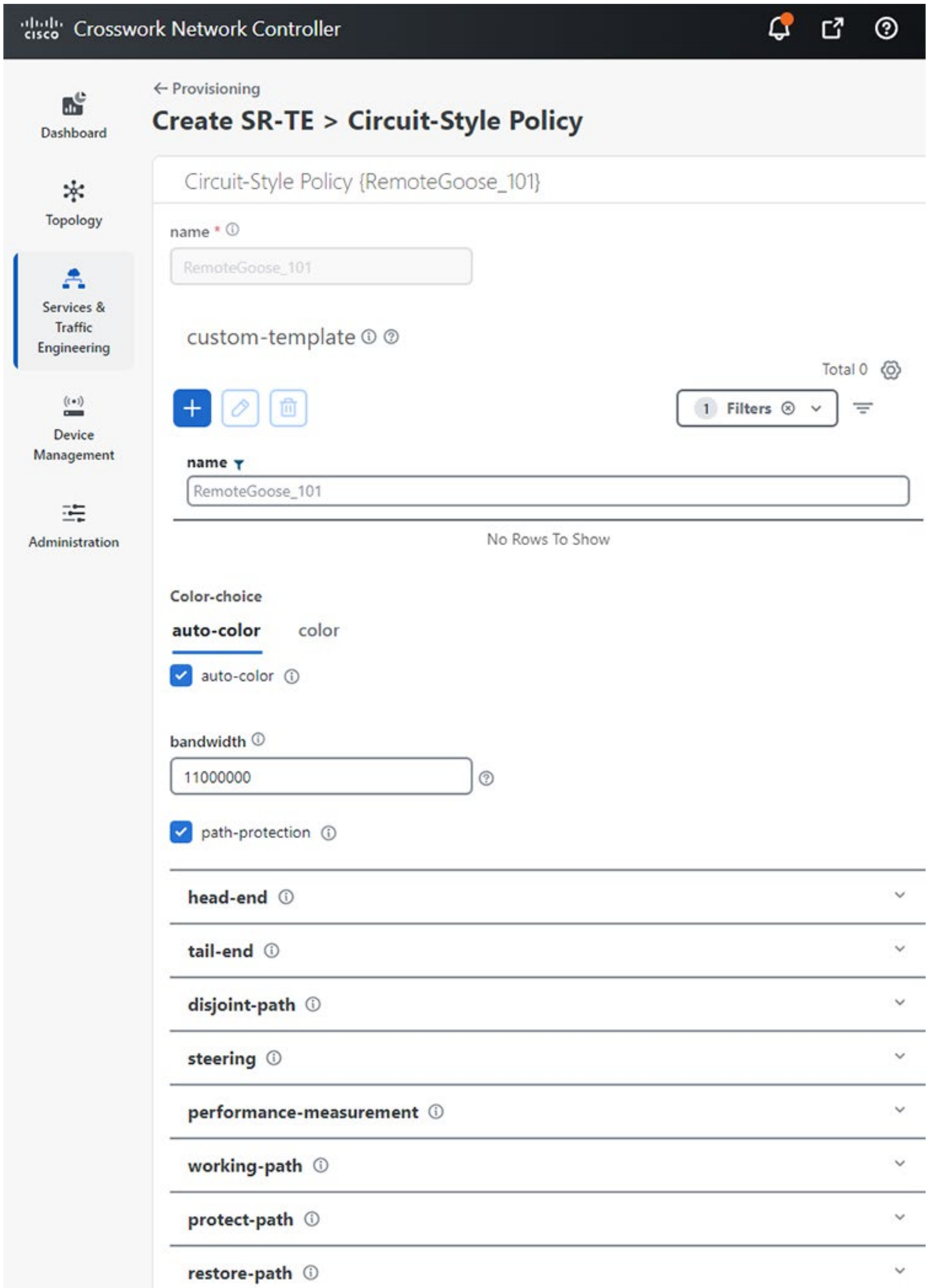
2. Then, under Services & Traffic Engineering -> Traffic Engineering, create an SR policy initiated by PCC (Path Computation Client for example, the headend nodes; not delving into protocol level details for the benefit of simplicity). This leads to the Provisioning window, wherein firstly one defines the Circuit-Style resource-pool to allocate Color, bi-directional ID, and disjoint group, the ranges having already been defined under Global Resource Pool. This step is optional if user wants to explicitly allocate the IDs while configuring SR-TE policies.

Figure 81 CS SR-TE policy initiation; CS resource-pool definition



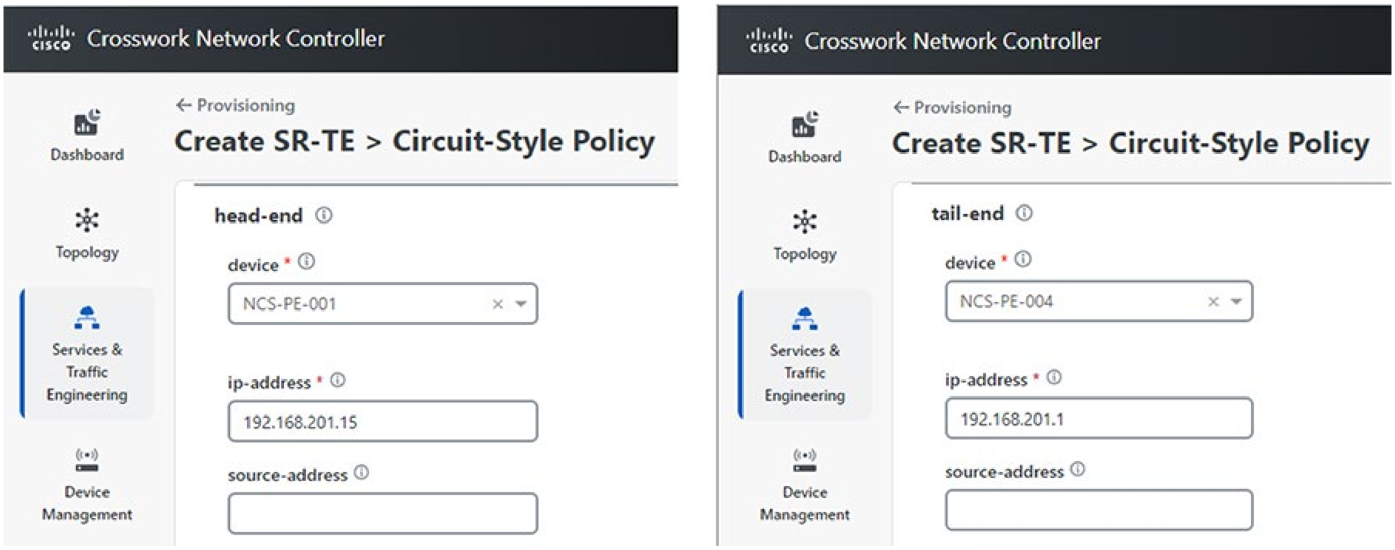
The next image provides the overview of CS SR-TE policy to be provisioned. Under SR-TE->Circuit- Style Policy in the Provisioning window, input the name of the policy color (selection of auto-color enforces automatic assignment from the global Resource pool, as described earlier) and requested bandwidth (in kbps) and enable path protection.

Figure 82 CS SR-TE policy parameters overview



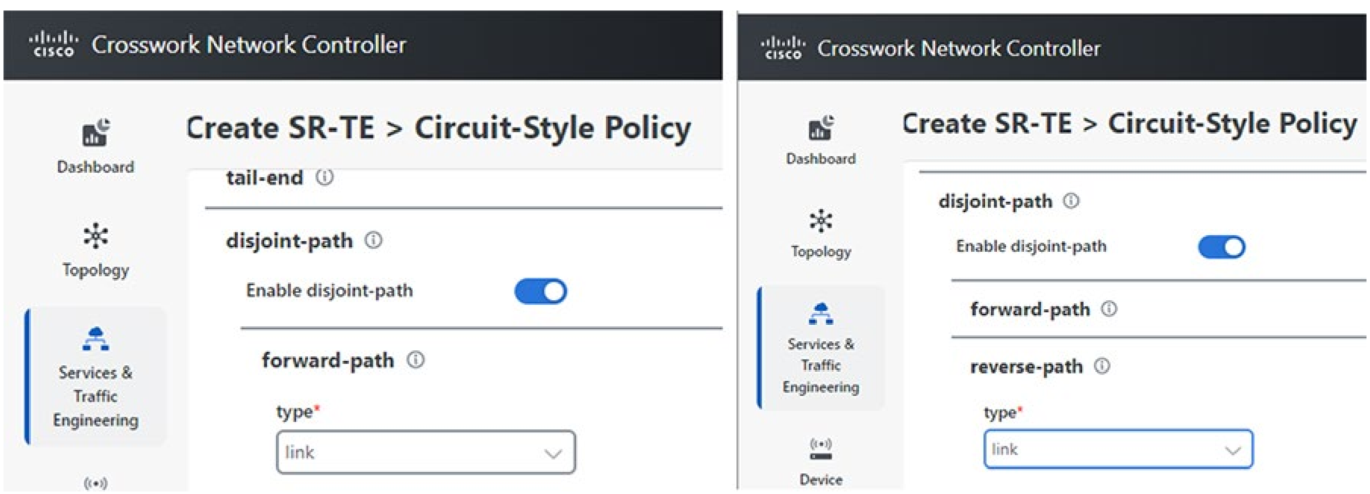
3. Enter headend device name/IP address, tailend device name/IP address for the CS SR-TE policy, considering one direction.

Figure 83 CS SR-TE policy endpoints



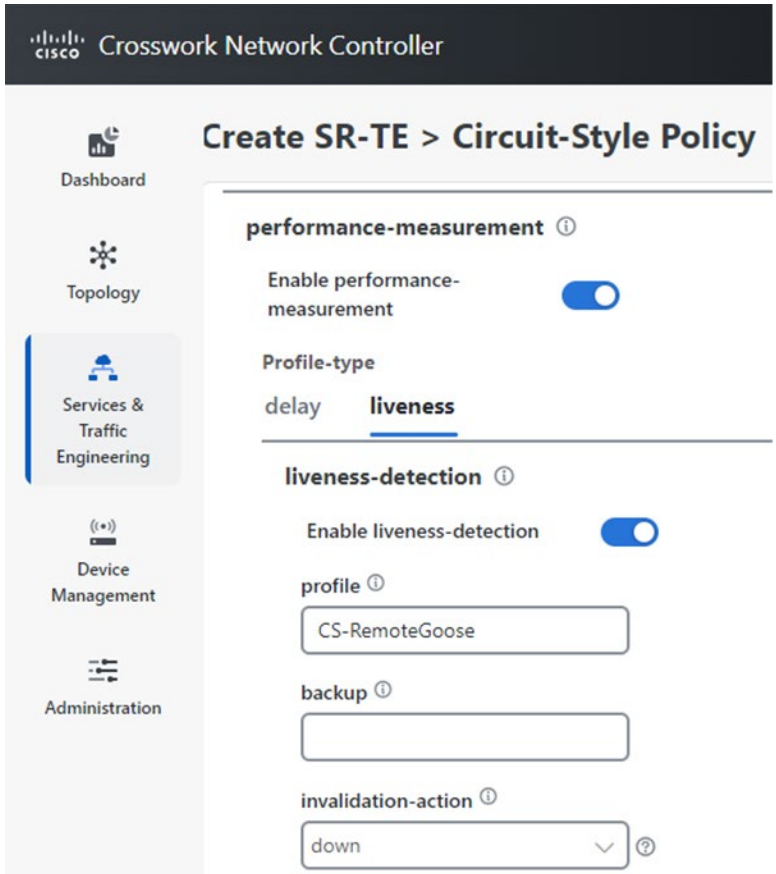
4. Enter the type of disjointedness: for example, link/node, to ensure that the working path is disjoint from the protect path. The forward/reverse of working and protect paths under the CS SR-TE policy are configured with the same disjointedness type. The disjointedness constraint must be the same in both directions.

Figure 84 CS SR-TE disjointedness definition for working and protect path



5. Enable performance-measurement via end-to-end SR policy liveness detection for all segment-lists of the active and standby candidate-path. Liveness profile and Invalidation action are defined. The liveness profile for example, CS_PLE is configured via T-SDN NSO function pack. For example, the probe packet interval to check the liveness of the path can be defined to be as low as 3.3 ms, wherein the liveness-check functionality is offloaded from software to hardware. This guarantees failure detection at ~10ms upon 3 probe packet misses, thereby enforcing the sub-50 ms path switching time, required in L2 Teleprotection use cases in Utility WAN. The default setting for invalidation action is "down," which ensures that when the PM liveness session goes down, the candidate path is immediately operationally brought down.

Figure 85 SR Performance Measurement definition with liveness-detection

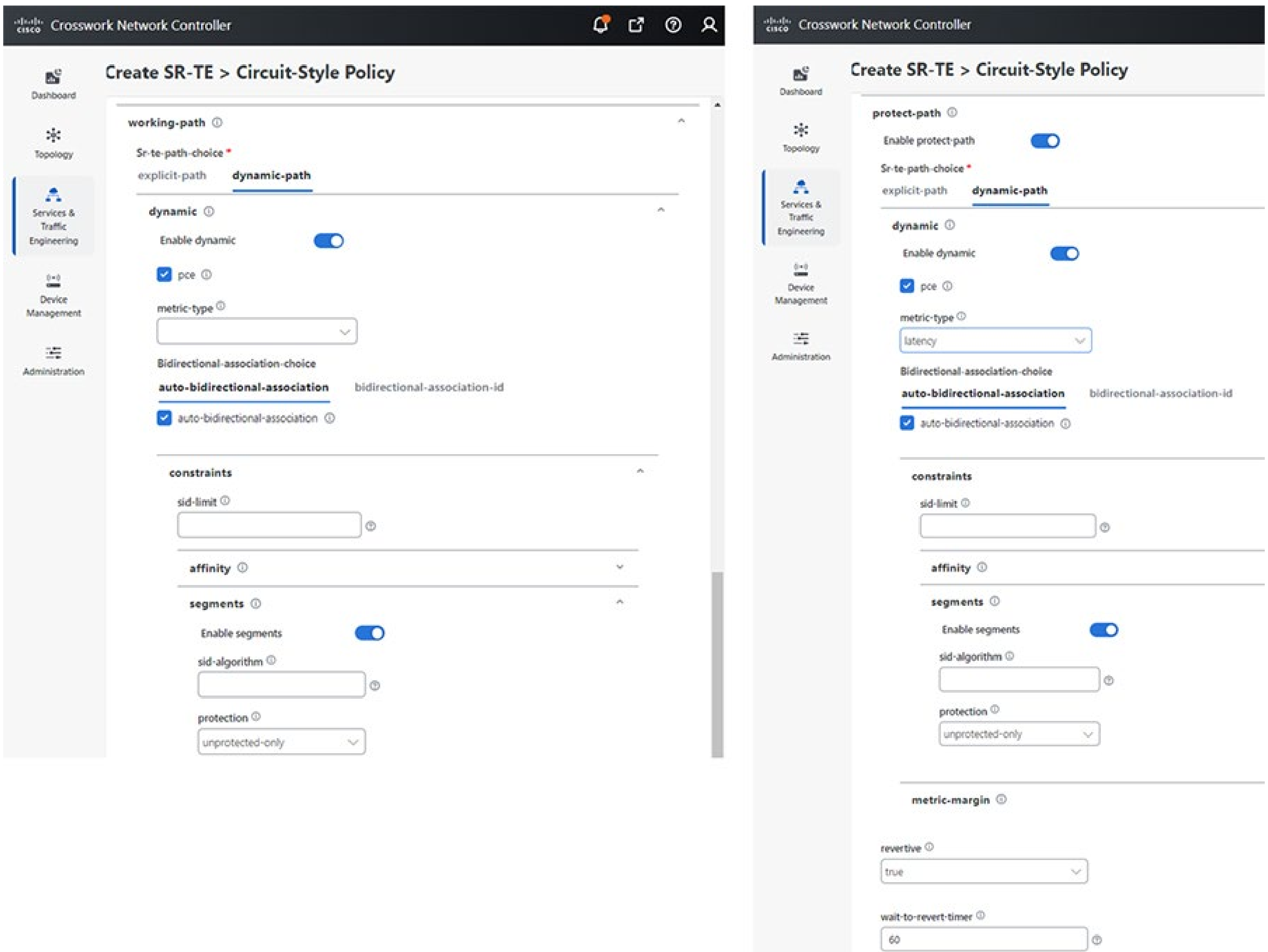


There are two ways to define working/protect/restore paths. One can define the path manually by specifying explicit paths wherein the path computation and bandwidth management needs to be handled by the user. The recommended way is to provision the paths dynamically. Herein, CNC offers the CS SR-TE Feature Pack that provides a bandwidth-aware Path Computation Element (PCE) for computing CS SR-TE policy.

6. Select dynamic-path under SR-TE-path-choice, as shown in the two images that follow.
7. Select PCE. The Metric-type is provided as IGP/latency/te/hopcount.
8. Auto-assignment of bi-directional association ID is enabled and the constraint segment type is provided. All Working, protect, and restore paths must be configured with unprotected-only segment type constraint.

In addition, you can define revertive path behavior for protect and restore path upon recovery of working and protect path respectively. Parameters for configuring restore path are like that of Protect path.

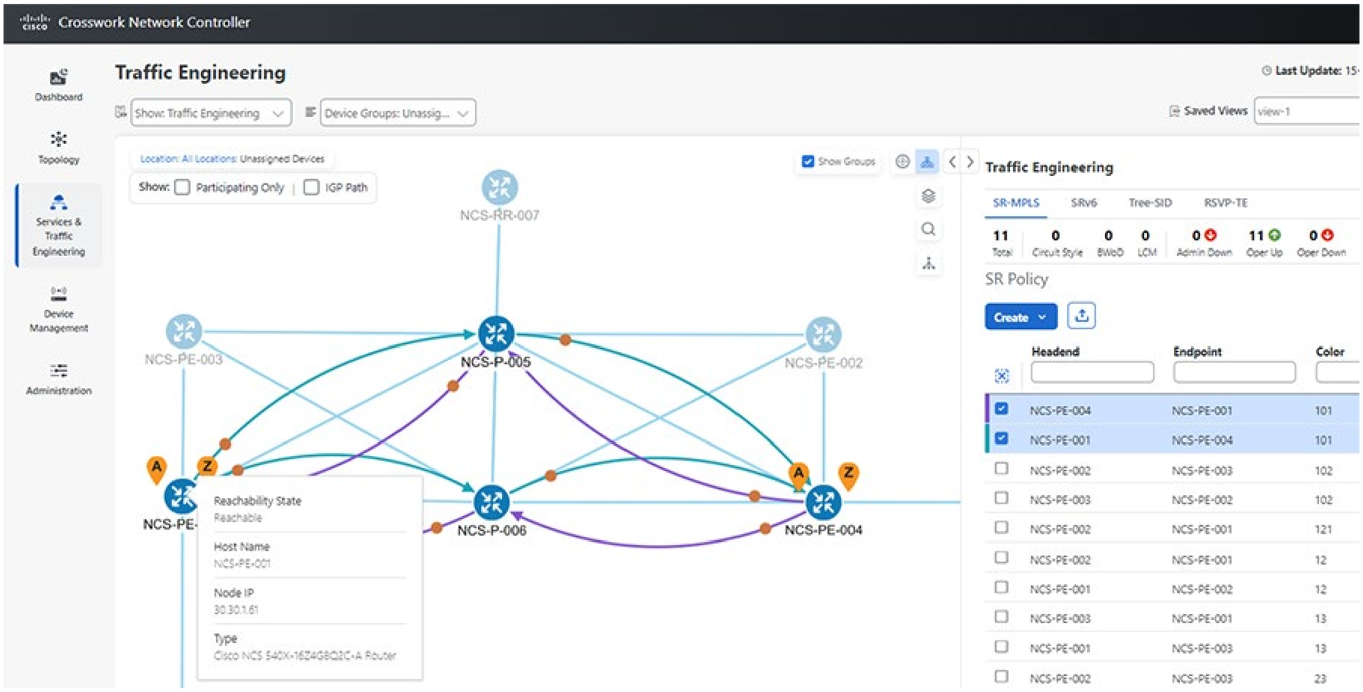
Figure 86 Working and Protect path definition



After committing the changes, the bi-directional CS SR-TE policy is provisioned between the endpoints.

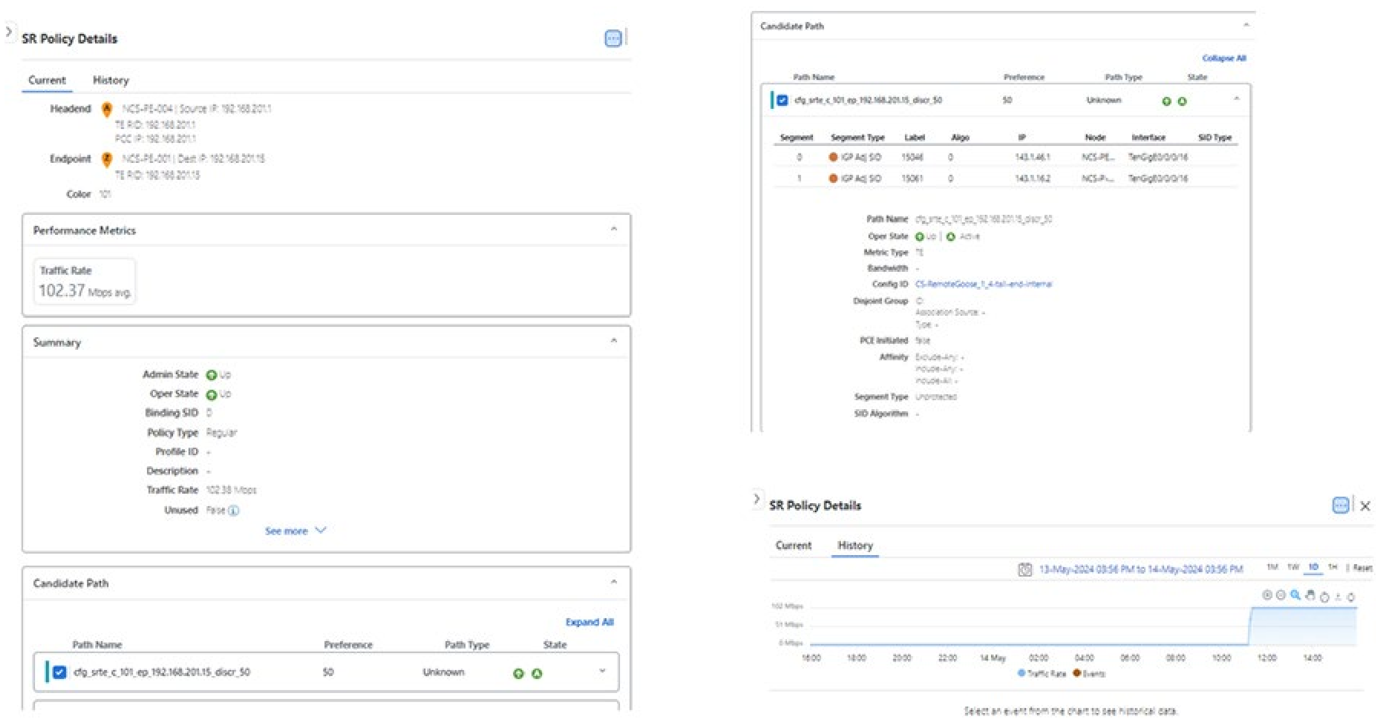
The following two images showcase the bi-directional nature of CS SR-TE policies between the endpoints: for example, NCS-PE-001 (headend A) to NCS-PE-004 (tailend Z) marked in purple and NCS-PE-004 (headend A) to NCS-PE-001 (tailend Z) marked in blue. The endpoints are NCS devices running IOS XR.
To view this topology, Under Services & Traffic Engineering -> Traffic Engineering -> Select the checkboxes of SR-TE policies to be viewed. To view the details of the device (Reachability state, Hostname, Node IP, Device Type), hover the cursor over device Icon.

Figure 87 Bi-directional CS SR-TE policy with NCS endpoint



Click the **Actions** button adjacent to the Policy and then click **View Details** to see more details on the configured Service.

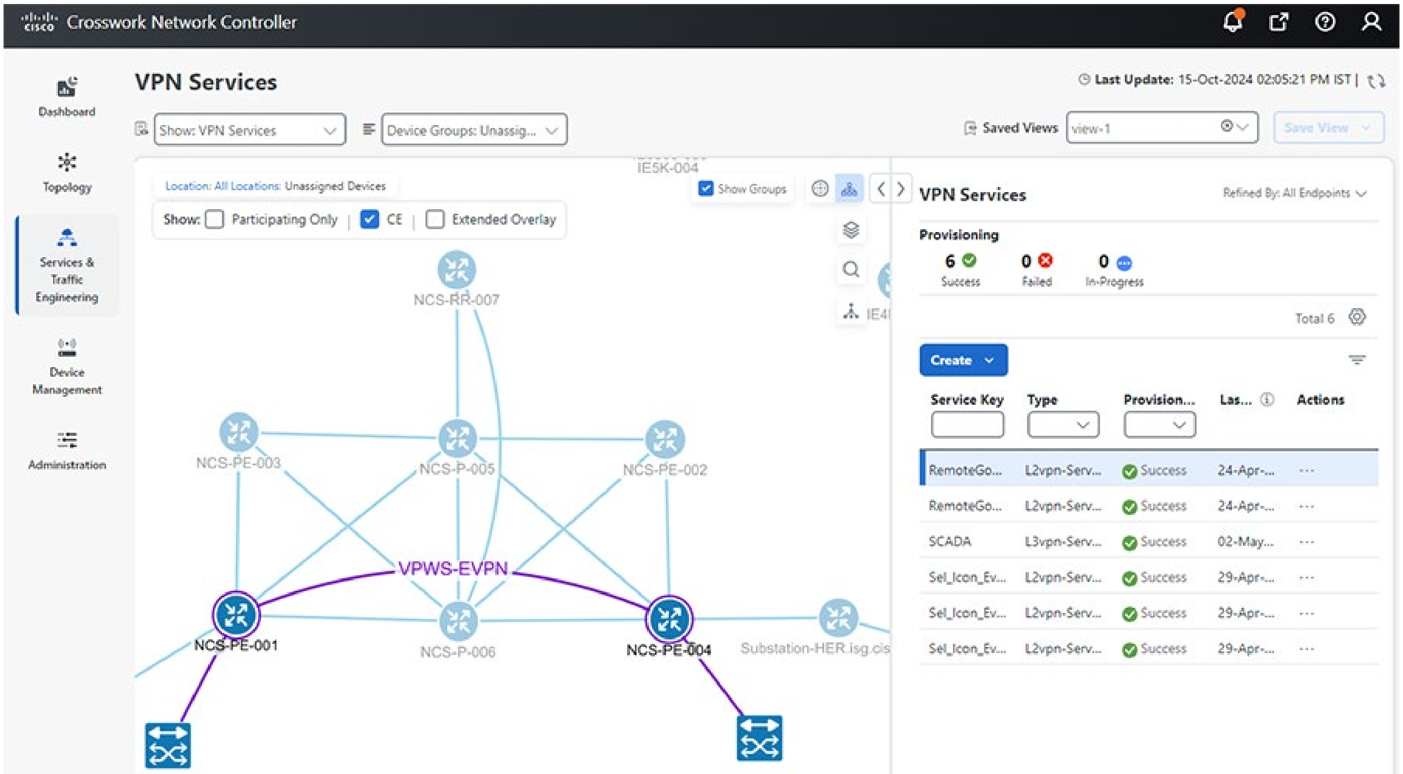
Figure 88 CS SR-TE policy Details



Details of both working path or protect path can be viewed.

The image that follows shows that the EVPN-VPWS service is stitched to the bi-directional CS SR-TE policy in the VPN Services window (Services & Traffic Engineering -> VPN Services -> Select the service to be viewed).

Figure 89 Visualization of EVPN-VPWS service



Click the **Actions** button adjacent to the Service and click **View Details** to see more details on the configured Service. The "Transport" tab in Service details page displays the CS SR-TE Policies stitched to the VPN Service.

The next two images show CNC Traffic Engineering per Link with **Circuit-Style Bandwidth Pool** monitoring between endpoints on the Working Path and Protect Path respectively. Crosswork tracks the bandwidth Used by the policy and the remaining available bandwidth that can be allocated to further policies.

Figure 90 Bandwidth monitoring on the Working Path

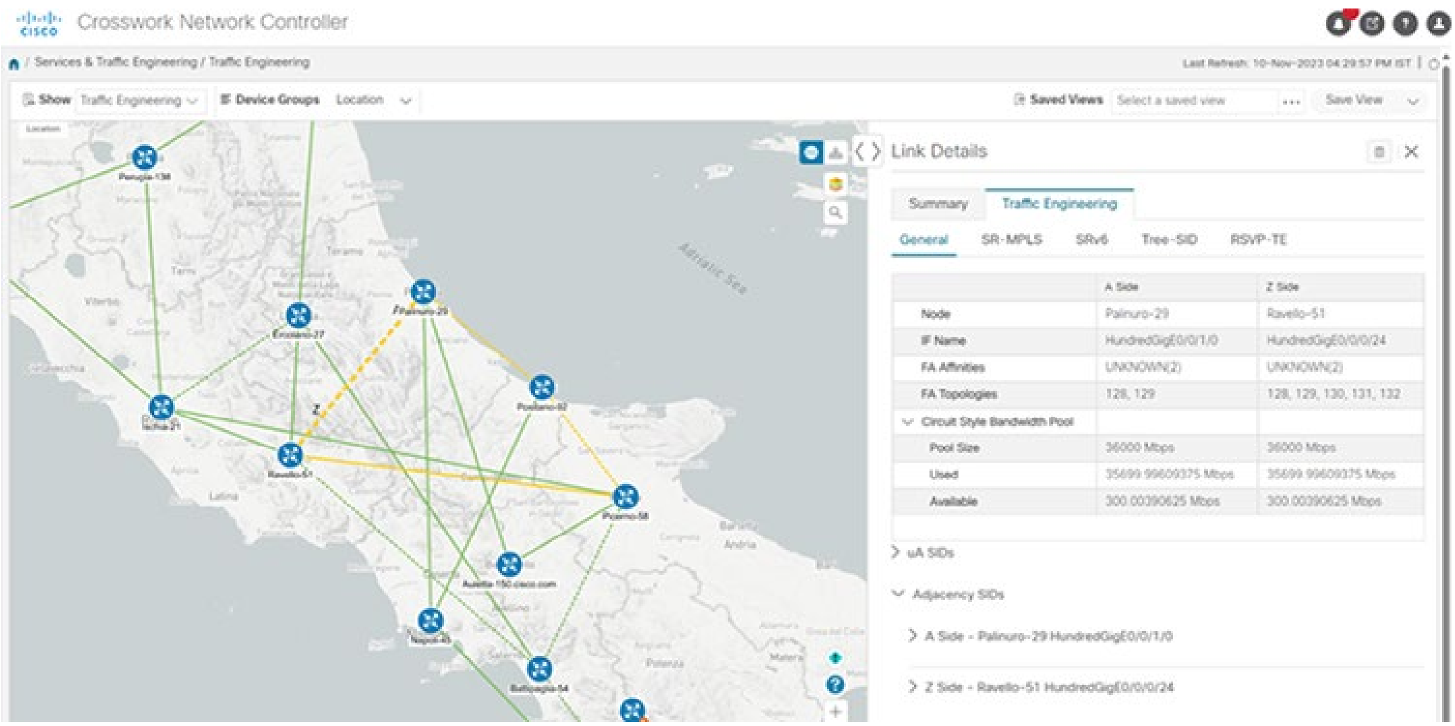
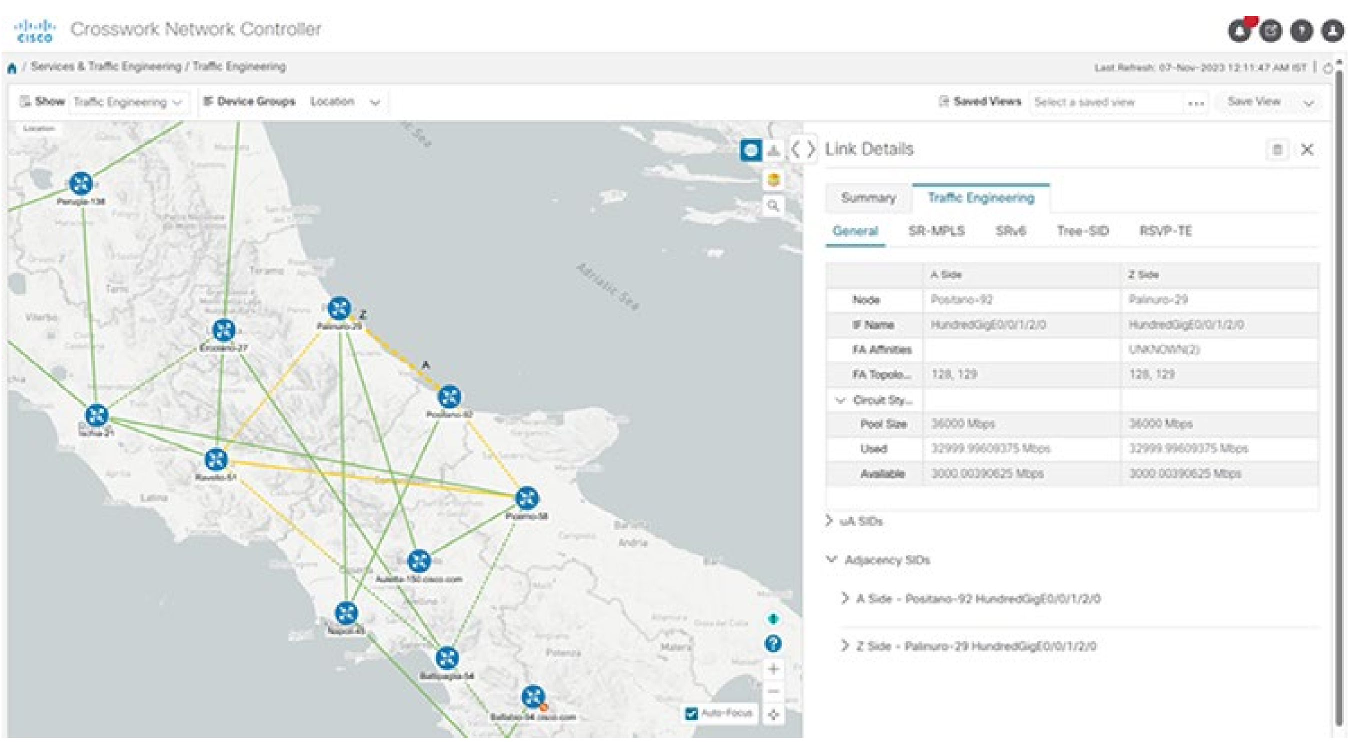


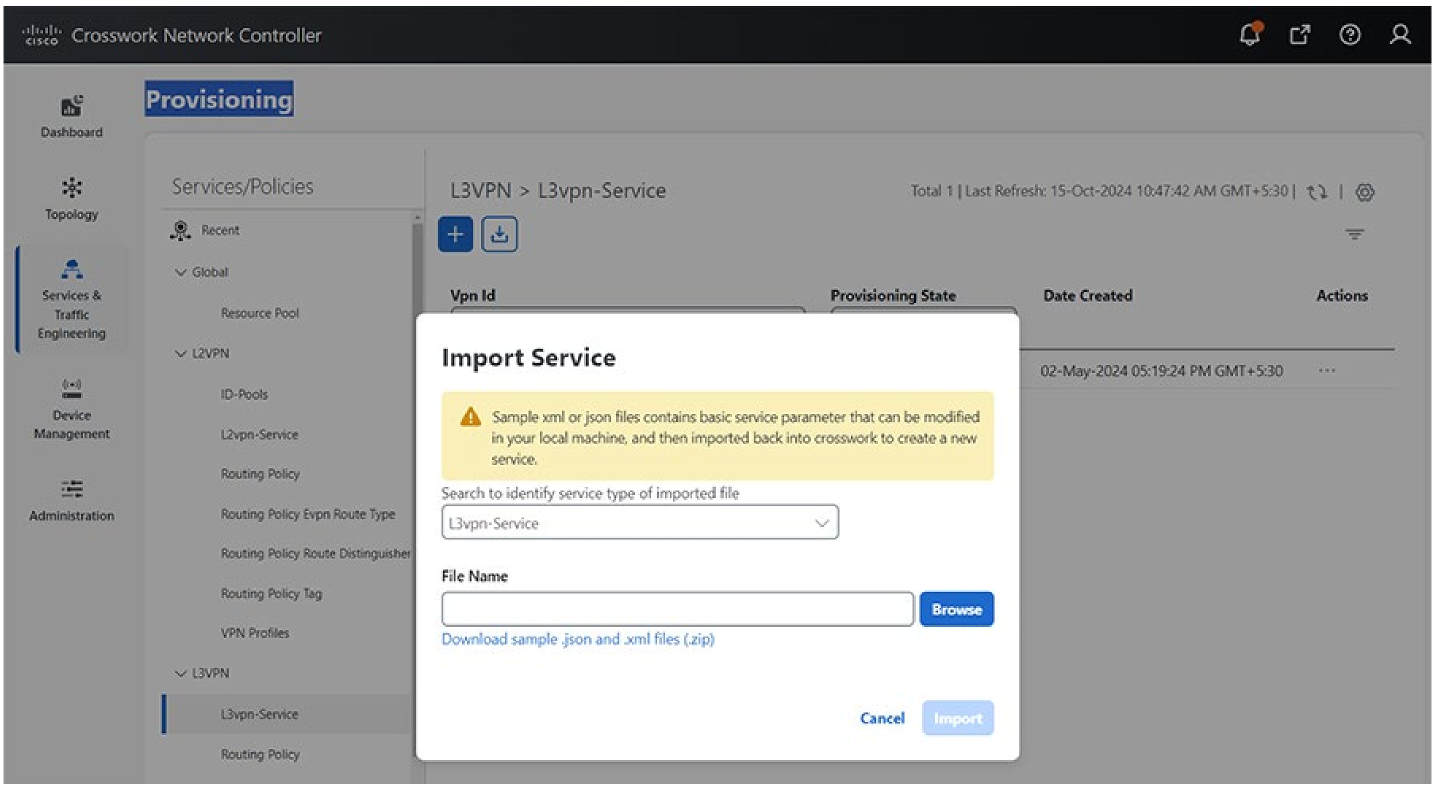
Figure 91 Bandwidth monitoring on the Protect Path



Note:
Users can streamline the configuration process in Crosswork by importing parameters via a JSON file instead of entering each parameter manually through the GUI. Follow the steps below to use this feature:

1. Under Services & Traffic Engineering -> Provisioning (NSO) -> Click on the service to be configured. Then click the **Import Service** button.

Figure 92 Import Service for Provisioning



2. Download sample XML or JSON files containing basic service parameters from the provisioning page.

3. Modify these files on your local machine to include the desired configuration parameters. Below is an example that shows CS Policy configuration with explicit SID List.

Figure 93 JSON file example for importing the service


```json
{
    "cisco-cs-sr-te-cfp:cs-sr-te-policy": {
        "name": "RemoteGoose_1_4",
        "head-end": {
            "device": "NCS-PE-001",
            "ip-address": "192.168.201.15"
        },
        "tail-end": {
            "device": "NCS-PE-004",
            "ip-address": "192.168.201.1"
        },
        "color": 101,
        "path-protection": "",
        "working-path": {
            "explicit": {
                "forward-sid-list-name": "cs-rg-14-working-fwd",
                "reverse-sid-list-name": "cs-rg-14-working-bck"
            }
        },
        "protect-path": {
            "explicit": {
                "forward-sid-list-name": "cs-rg-14-protect-fwd",
                "reverse-sid-list-name": "cs-rg-14-protect-bck"
            },
            "revertive": true,
            "wait-to-revert-timer": 30
        },
        "restore-path": {
            "explicit": {
                "forward-sid-list-name": "cs-rg-14-restore-fwd",
                "reverse-sid-list-name": "cs-rg-14-restore-bck"
            },
            "revertive": true,
            "wait-to-revert-timer": 30
        }
    }
}
```


4. Import the modified files back into Crosswork to create a new service.

Appendix – Running Configuration

HER

```
Substation-HER#show running-config
Building configuration...

Current configuration : 33102 bytes
!
! Last configuration change at 10:41:10 IST Thu Sep 15 2022 by admin
! NVRAM config last updated at 10:41:10 IST Thu Sep 15 2022 by admin
!
version 17.3
service timestamps debug uptime
service timestamps log uptime
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform hardware crypto-throughput level 8-25g
!
hostname Substation-HER
!
boot-start-marker
boot system bootflash:asr1000-universalk9.17.03.04a.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition VRF_BUSINESS
rd 199:104
route-target export 199:104
route-target import 199:104
!
address-family ipv4
exit-address-family
!
vrf definition VRF_GRIDMON
rd 199:102
route-target export 199:102
route-target import 199:102
!
address-family ipv4
exit-address-family
```

```
!
vrf definition VRF_MGMT
rd 199:101
route-target export 199:101
route-target import 199:101
!
address-family ipv4
exit-address-family
!
vrf definition VRF_PLANTLINK
rd 199:105
route-target export 199:105
route-target import 199:105
!
address-family ipv4
exit-address-family
!
vrf definition VRF_SCADA
rd 199:111
route-target export 199:111
route-target import 199:111
route-target import 101:111
!
address-family ipv4
  route-target export 199:111
  route-target import 199:111
  route-target import 101:111
exit-address-family
!
vrf definition VRF_TSCADA
rd 199:103
route-target export 199:103
route-target import 199:103
!
address-family ipv4
exit-address-family
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
!
aaa session-id common
```

```
clock timezone IST 5 30
clock calendar-valid
!
!
!
!
!
!
!
ip name-server xx.xx.xx.xx
ip domain name isg.cisco.com
!
ip dhcp pool ASR1002-HX-DHCP
network 192.168.60.0 255.255.255.0
default-router 192.168.60.1
dns-server xx.xx.xx.xx
!
ip dhcp pool SUMATRA-vEDGE-001
network 192.168.66.0 255.255.255.0
default-router 192.168.66.1
dns-server xx.xx.xx.xx
!
ip dhcp pool ASR1002-HX-MPLS-POOL
network 192.168.6.0 255.255.255.0
dns-server xx.xx.xx.xx
!
ip dhcp pool SUMATRA-vEDGE-001-MPLS
network 192.168.7.0 255.255.255.0
default-router 192.168.7.1
dns-server xx.xx.xx.xx
!
ip dhcp pool CSR1000vEdge-001
network 192.168.85.0 255.255.255.0
dns-server xx.xx.xx.xx
default-router 192.168.85.1
!
ip dhcp pool IR1101-cEDGE
network 192.168.8.0 255.255.255.0
dns-server xx.xx.xx.xx
default-router 192.168.8.1
!
!
!
login on-success log
ipv6 unicast-routing
l2tp-class L2TP_TUNNEL_TEST
hidden
authentication
digest secret 0 xxxxxxxx hash SHA1
hello 100
hostname Substation-HER
```

```
password xxxxxxxx
receive-window 50
retransmit retries 10
timeout setup 400
!
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
mpls label protocol ldp
mpls ldp igp sync holddown 1
mpls traffic-eng tunnels
multilink bundle-name authenticated
!
!
!
key chain DMVPN
key 1
  key-string dmvpn
!
!
!
!
!
!
!
!
!
!
!
license udi pid ASR1002-HX sn XXXXXXXX
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
license boot level adventerprise
license solution level appxk9
license solution level securityk9
memory free low-watermark processor 991004
!
!
spanning-tree extend system-id
```

```
diagnostic bootup level minimal
!
username cisco privilege 15 password 0 xxxxxxxx
username admin privilege 15 password 0 xxxxxxxx
!
redundancy
mode none
!
bridge-domain 1
member vni 6001
member GigabitEthernet0/2/15 service-instance 1
!
bridge-domain 601
no mac learning
!
bridge-domain 1000
crypto ikev2 authorization policy default_No_cert
route set interface
route set access-list FLEX_ACL
!
no crypto ikev2 authorization policy default
!
crypto ikev2 redirect gateway init
! (IKEv2 Cluster load-balancer is not enabled)
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_No_cert
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_No_cert
proposal FlexVPN_IKEv2_Proposal_No_cert
!
crypto ikev2 keyring ANY
peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key sentryo
!
!
!
crypto ikev2 profile FLEX_SERVER_PROF_No_cert_1
match identity remote address 0.0.0.0
match identity remote fqdn domain isg.cisco.com
identity local address 89.89.89.1
authentication remote pre-share
authentication local pre-share
keyring local ANY
aaa authorization group psk list FlexVPN_Author default_No_cert
virtual-template 4
!
crypto ikev2 fragmentation
!
```

```
!
cdp run
!
lldp run
pseudowire-class L2TP_PW_TEST
encapsulation l2tpv3
sequencing both
protocol l2tpv3 L2TP_TUNNEL_TEST
ip local interface Loopback1
ip pmtu
ip dfbit set
ip tos reflect
ip ttl 100
!
!
class-map match-any TRANSACTIONAL
match ip dscp cs2  af21  af22  af23  cs4  af41  af42
class-map match-all VOICE
match ip dscp ef
class-map match-any MISSION-CRITICAL-DATA
match access-group name MISSION-CRITICAL-DATA
class-map match-any MISSION-CRITICAL
match ip dscp cs3  af31  af32  af33  cs6
class-map match-all CALL-SIGNALING
match ip dscp cs3
!
policy-map HOST-INPUT-MARKING
class VOICE
  set dscp ef
class CALL-SIGNALING
  set dscp cs3
class MISSION-CRITICAL-DATA
  set dscp af31
class class-default
policy-map HOST-QUEUE-PACKETS
class VOICE
  priority
class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets
class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map UPLINK-QUEUE-PACKETS
class VOICE
  priority
class MISSION-CRITICAL
  bandwidth remaining percent 30
```

```
  queue-limit 96 packets
class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
!
!
!
!
!
!
!
crypto isakmp invalid-spi-recovery
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_No_cert esp-aes esp-sha256-hmac
mode transport
crypto ipsec fragmentation after-encryption
crypto ipsec df-bit clear
!
!
crypto ipsec profile default_No_cert_1
set transform-set FlexVPN_IPsec_Transform_Set_No_cert
set pfs group14
set ikev2-profile FLEX_SERVER_PROF_No_cert_1
!
!
!
!
!
!
!
!
!
interface Loopback0
ip address 192.168.201.6 255.255.255.255
!
interface Loopback1
ip address 192.168.200.1 255.255.255.255
!
interface Loopback12
ip address 12.12.12.1 255.255.255.255
ip ospf network point-to-point
ip ospf 12 area 0
!
interface Loopback99
ip address 192.168.13.1 255.255.255.255
```

```
!
interface Loopback100
ip address 10.60.60.1 255.255.255.255
bfd interval 50 min_rx 50 multiplier 3
!
interface Loopback101
ip address 10.70.70.1 255.255.255.255
!
interface Loopback111
ip address 192.168.220.4 255.255.255.255
!
interface Loopback200
ip address 192.168.117.1 255.255.255.255
!
interface Tunnel100
no ip address
!
interface GigabitEthernet0/0/0
description connected to DMZ switch
ip address xx.xx.xx.xx xx.xx.xx.xx
ip nat outside
negotiation auto
!
interface GigabitEthernet0/0/1
description connected to asr920-001
ip dhcp relay information trusted
ip dhcp relay information option-insert
ip dhcp relay information check-reply
ip address 192.168.69.1 255.255.255.0
ip nat inside
ip ospf network point-to-point
ip ospf 1 area 0
load-interval 30
negotiation auto
cdp enable
mpls ip
mpls ldp discovery transport-address 192.168.201.6
mpls traffic-eng tunnels
bfd interval 200 min_rx 200 multiplier 3
service-policy output UPLINK-QUEUE-PACKETS
!
interface GigabitEthernet0/0/2
description connected to ixia card 2 por 1
mtu 9216
no ip address
load-interval 30
negotiation auto
!
interface GigabitEthernet0/0/2.1201
encapsulation dot1Q 1201
vrf forwarding VRF_SCADA
```

```
ip address 12.0.1.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1202
encapsulation dot1Q 1202
vrf forwarding VRF_TSCADA
ip address 12.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1203
encapsulation dot1Q 1203
vrf forwarding VRF_PLANTLINK
ip address 12.0.3.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1204
encapsulation dot1Q 1204
vrf forwarding VRF_MGMT
ip address 12.0.4.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1205
encapsulation dot1Q 1205
vrf forwarding VRF_GRIDMON
ip address 12.0.5.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1206
encapsulation dot1Q 1206
vrf forwarding VRF_BUSINESS
ip address 12.0.6.1 255.255.255.0
!
interface GigabitEthernet0/0/2.3001
encapsulation dot1Q 3001
ip address 30.1.0.1 255.255.255.0
!
interface GigabitEthernet0/0/2.3002
encapsulation dot1Q 3002
ip address 30.2.0.1 255.255.255.0
!
interface GigabitEthernet0/0/3
description connected to ixia card 2 port 2
mtu 9216
no ip address
load-interval 30
negotiation auto
service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  bridge-domain 601
!
service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1000
!
```

```
!
interface GigabitEthernet0/0/3.140
encapsulation dot1Q 140
ip address 140.140.140.1 255.255.255.0
!
interface GigabitEthernet0/0/3.799
encapsulation dot1Q 799
xconnect 192.168.199.1 799 encapsulation mpls
!
interface GigabitEthernet0/0/4
ip address 99.99.99.100 255.255.255.0
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/5
description connected to xx.xx.xx.xx PC ethernet - asr G5
ip address 192.168.228.1 255.255.255.252
negotiation auto
!
interface GigabitEthernet0/0/6
description Phy_Loop
no ip address
negotiation auto
service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 601 split-horizon group 0
!
service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 1000
!
service instance 998 ethernet
  encapsulation dot1q 998
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 1000
!
service instance 1001 ethernet
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 1000
!
```

```
service instance 1002 ethernet
 encapsulation dot1q 1002
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1000
!
service instance 1052 ethernet
 encapsulation dot1q 1052
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1000
!
service instance 1053 ethernet
 encapsulation dot1q 1053
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1000
!
service instance 1054 ethernet
 encapsulation dot1q 1054
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1000
!
service instance 1055 ethernet
 encapsulation dot1q 1055
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1000
!
service instance 1056 ethernet
 encapsulation dot1q 1056
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1056
!
service instance 1057 ethernet
 encapsulation dot1q 1057
 rewrite ingress tag pop 1 symmetric
 l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
 bridge-domain 1000
!
service instance 1058 ethernet
 encapsulation dot1q 1058
```

```
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 1000
!
service instance 2502 ethernet
  encapsulation dot1q 2502
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 601 split-horizon group 1
!
!
interface GigabitEthernet0/0/7
description Phy_Loop
no ip address
load-interval 30
negotiation auto
!
interface GigabitEthernet0/0/7.989
encapsulation dot1Q 989
xconnect 192.168.205.2 989 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.990
encapsulation dot1Q 990
xconnect 192.168.220.3 990 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.991
encapsulation dot1Q 991
xconnect 192.168.205.2 991 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.992
encapsulation dot1Q 992
xconnect 192.168.205.2 992 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.993
encapsulation dot1Q 993
xconnect 192.168.223.1 993 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.994
encapsulation dot1Q 994
xconnect 192.168.223.1 994 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.995
encapsulation dot1Q 995
xconnect 192.168.223.1 995 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.996
encapsulation dot1Q 996
xconnect 192.168.223.1 996 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
```

```
interface GigabitEthernet0/0/7.997
encapsulation dot1Q 997
xconnect 192.168.223.1 997 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.998
encapsulation dot1Q 998
xconnect 192.168.202.2 998 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.1001
encapsulation dot1Q 1001
xconnect 192.168.199.2 1001 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2502
encapsulation dot1Q 2502
xconnect 192.168.199.2 2502 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2503
encapsulation dot1Q 2503
xconnect 192.168.199.2 2503 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2504
encapsulation dot1Q 2504
xconnect 192.168.199.2 2504 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2505
encapsulation dot1Q 2505
xconnect 192.168.199.2 2505 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2506
encapsulation dot1Q 2506
xconnect 192.168.199.2 2506 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2507
encapsulation dot1Q 2507
xconnect 192.168.199.2 2507 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2508
encapsulation dot1Q 2508
xconnect 192.168.199.2 2508 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2509
encapsulation dot1Q 2509
xconnect 192.168.199.2 2509 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2560
encapsulation dot1Q 2560
xconnect 192.168.199.2 2560 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface TenGigabitEthernet0/1/0
description connected to FPR4010 port 8
ip address 192.168.70.2 255.255.255.0
```

```
service-policy input HOST-INPUT-MARKING
!
interface TenGigabitEthernet0/1/1
no ip address
!
interface TenGigabitEthernet0/1/2
no ip address
!
interface TenGigabitEthernet0/1/3
no ip address
shutdown
!
interface TenGigabitEthernet0/1/4
no ip address
!
interface TenGigabitEthernet0/1/5
no ip address
!
interface TenGigabitEthernet0/1/6
no ip address
!
interface TenGigabitEthernet0/1/7
no ip address
!
interface GigabitEthernet0/2/0
description connected to ixia 10.64.66.36 card 1 port 14
no ip address
negotiation auto
!
interface GigabitEthernet0/2/0.143
encapsulation dot1Q 143
ip address 143.143.143.1 255.255.255.0
!
interface GigabitEthernet0/2/1
description connected to Laptop SCADA FEP
ip address 192.168.189.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/2
description connected to ixia card 1 port 10
ip address 171.171.171.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/3
description connected to gig0/0/0 SUMATRA-P3-01
ip address 192.168.66.1 255.255.255.0
ip nat inside
negotiation auto
cdp enable
!
interface GigabitEthernet0/2/4
```

```
ip address 90.90.90.1 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet0/2/5
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/2/6
description connected to sumatra-pp-2 on G0/0/0
ip address 89.89.89.1 255.255.255.0
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/2/7
no ip address
speed 1000
no negotiation auto
!
interface GigabitEthernet0/2/7.152
encapsulation dot1Q 152
ip address 152.152.152.1 255.255.255.0
!
interface GigabitEthernet0/2/8
no ip address
negotiation auto
!
interface GigabitEthernet0/2/9
description connected to SA-1002HX-002 gi0/0/0
ip address 192.168.60.1 255.255.255.0
ip nat inside
negotiation auto
mpls ip
mpls label protocol ldp
!
interface GigabitEthernet0/2/10
description connected to UCS xx.xx.xx.xx on VMNIC 8
ip address 192.168.85.1 255.255.255.0
ip nat inside
negotiation auto
cdp enable
!
interface GigabitEthernet0/2/11
description connected to SA-1002HX-002 gi0/0/1
ip address 192.168.6.1 255.255.255.0
ip nat inside
ip ospf network point-to-point
ip ospf 1 area 0
negotiation auto
cdp enable
```

```
mpls ip
mpls label protocol ldp
!
interface GigabitEthernet0/2/12
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/2/13
no ip address
negotiation auto
!
interface GigabitEthernet0/2/14
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/2/15
description connected to IXIA card 2 port 13
no ip address
negotiation auto
service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
!
!
interface GigabitEthernet0/2/16
description connected to IR1101
ip address 69.69.69.1 255.255.255.0
ip ospf network point-to-point
ip ospf 12 area 0
negotiation auto
!
interface GigabitEthernet0/2/17
description connected to IR1101-cEDGE-002
ip address 192.168.8.1 255.255.255.0
ip nat inside
negotiation auto
cdp enable
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
!
interface Virtual-Template4 type tunnel
bandwidth 1000000
ip unnumbered Loopback100
tunnel source GigabitEthernet0/2/6
tunnel bandwidth transmit 1000000
```

```
tunnel bandwidth receive 1000000
tunnel protection ipsec profile default_No_cert_1
!
interface nve1
no ip address
source-interface Loopback12
member vni 6001
  ingress-replication 12.12.12.2
!
!
!
router eigrp 99
bfd interface GigabitEthernet0/0/4
bfd interface GigabitEthernet0/2/6
network 10.0.0.0
network 89.89.89.0 0.0.0.255
network 99.99.99.0 0.0.0.255
network 140.140.140.0 0.0.0.255
network 143.143.143.0 0.0.0.255
network 152.152.0.0
network 192.168.2.0
network 192.168.4.0
network 192.168.13.0
network 192.168.89.0
network 192.168.200.0
network 192.168.201.0
network 192.168.228.0
redistribute bgp 200 metric 100 1 255 1 1500
eigrp router-id 10.60.60.1
!
router ospf 1
router-id 192.168.201.6
network 192.168.201.6 0.0.0.0 area 0
bfd all-interfaces
mpls ldp sync
!
router ospf 12
router-id 12.12.12.1
network 12.12.12.1 0.0.0.0 area 0
bfd all-interfaces
!
router bgp 200
bgp router-id interface Loopback0
bgp log-neighbor-changes
neighbor 192.168.60.2 remote-as 2001
neighbor 192.168.60.2 shutdown
neighbor 192.168.60.2 ebgp-multihop 255
neighbor 192.168.70.1 remote-as 1001
neighbor 192.168.70.1 ebgp-multihop 255
neighbor 192.168.70.1 update-source Loopback0
neighbor 192.168.111.1 remote-as 200
```

```
neighbor 192.168.111.1 ebgp-multihop 255
neighbor 192.168.111.1 update-source Loopback0
neighbor 192.168.113.1 remote-as 200
neighbor 192.168.113.1 ebgp-multihop 255
neighbor 192.168.113.1 update-source Loopback0
neighbor 192.168.198.1 remote-as 200
neighbor 192.168.198.1 update-source Loopback0
neighbor 192.168.198.1 fall-over
neighbor 192.168.198.1 fall-over bfd
neighbor 192.168.199.1 remote-as 200
neighbor 192.168.199.1 update-source Loopback0
neighbor 192.168.199.1 fall-over
neighbor 192.168.199.1 fall-over bfd multi-hop
neighbor 192.168.201.4 remote-as 200
neighbor 192.168.201.4 shutdown
neighbor 192.168.201.4 update-source Loopback0
neighbor 192.168.201.10 remote-as 200
neighbor 192.168.201.10 update-source Loopback0
neighbor 192.168.202.1 remote-as 101
neighbor 192.168.202.1 ebgp-multihop 255
neighbor 192.168.202.1 update-source Loopback0
neighbor 192.168.203.1 remote-as 200
neighbor 192.168.203.1 update-source Loopback0
neighbor 192.168.220.2 remote-as 102
neighbor 192.168.220.2 ebgp-multihop 255
neighbor 192.168.220.2 update-source Loopback0
!
address-family ipv4
 bgp additional-paths install
 bgp nexthop trigger delay 1
 network 30.1.0.0 mask 255.255.255.0
 network 30.2.0.0 mask 255.255.255.0
 network 140.140.140.0 mask 255.255.255.0
 network 141.141.141.0 mask 255.255.255.0
 network 192.168.189.0
 network 192.168.200.1 mask 255.255.255.255
 network 192.168.205.2 mask 255.255.255.255
 network 192.168.205.4 mask 255.255.255.255
 network 192.168.220.2 mask 255.255.255.255
 network 192.168.223.1 mask 255.255.255.255
 redistribute connected
 redistribute eigrp 99
 neighbor 192.168.60.2 activate
 neighbor 192.168.60.2 next-hop-self
 neighbor 192.168.60.2 send-label
 neighbor 192.168.70.1 activate
 neighbor 192.168.70.1 next-hop-self
 neighbor 192.168.70.1 send-label
 neighbor 192.168.111.1 activate
 neighbor 192.168.111.1 send-community extended
 neighbor 192.168.111.1 next-hop-self
```

```
  neighbor 192.168.113.1 activate
  neighbor 192.168.113.1 send-community extended
  neighbor 192.168.113.1 next-hop-self
  neighbor 192.168.198.1 activate
  neighbor 192.168.198.1 next-hop-self
  neighbor 192.168.198.1 soft-reconfiguration inbound
  neighbor 192.168.198.1 send-label
  neighbor 192.168.199.1 activate
  neighbor 192.168.199.1 weight 40000
  neighbor 192.168.199.1 next-hop-self
  neighbor 192.168.199.1 soft-reconfiguration inbound
  neighbor 192.168.199.1 send-label
  neighbor 192.168.201.4 activate
  neighbor 192.168.201.4 next-hop-self
  neighbor 192.168.201.4 soft-reconfiguration inbound
  neighbor 192.168.201.4 send-label
  neighbor 192.168.201.10 activate
  neighbor 192.168.201.10 next-hop-self
  neighbor 192.168.201.10 soft-reconfiguration inbound
  neighbor 192.168.201.10 send-label
  neighbor 192.168.202.1 activate
  neighbor 192.168.202.1 next-hop-self
  neighbor 192.168.202.1 soft-reconfiguration inbound
  neighbor 192.168.202.1 send-label
  neighbor 192.168.203.1 activate
  neighbor 192.168.203.1 next-hop-self
  neighbor 192.168.203.1 soft-reconfiguration inbound
  neighbor 192.168.203.1 send-label
  neighbor 192.168.220.2 activate
  neighbor 192.168.220.2 next-hop-self
  neighbor 192.168.220.2 send-label
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.70.1 activate
  neighbor 192.168.70.1 send-community extended
  neighbor 192.168.70.1 next-hop-self
  neighbor 192.168.198.1 activate
  neighbor 192.168.198.1 send-community extended
  neighbor 192.168.198.1 next-hop-self
  neighbor 192.168.199.1 activate
  neighbor 192.168.199.1 send-community extended
  neighbor 192.168.199.1 next-hop-self
  neighbor 192.168.201.4 activate
  neighbor 192.168.201.4 send-community extended
  neighbor 192.168.201.4 next-hop-self
  neighbor 192.168.201.10 activate
  neighbor 192.168.201.10 send-community extended
  neighbor 192.168.201.10 next-hop-self
 exit-address-family
 !
```

```
address-family ipv4 vrf VRF_BUSINESS
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_PLANTLINK
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_TSCADA
 redistribute connected
exit-address-family
!
ip tcp path-mtu-discovery
ip telnet source-interface GigabitEthernet0/0/0
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip ftp source-interface Loopback1
ip ftp username xxxxxxxx
ip ftp password xxxxxxxxxx
ip tftp source-interface GigabitEthernet0/2/9
ip dns server
ip pim rp-address 12.12.12.1
ip nat inside source static tcp 192.168.205.2 22 interface GigabitEthernet0/2/4 43
ip nat inside source list NAT_INSIDE_POOL interface GigabitEthernet0/0/0 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
ip route 192.168.21.0 255.255.255.0 192.168.70.1
ip route 192.168.220.2 255.255.255.255 99.99.99.2 255
ip ssh source-interface GigabitEthernet0/0/0
ip ssh version 2
!
ip access-list standard FLEX_ACL
13 permit 89.89.89.0
14 permit 99.99.99.0
15 permit 192.168.169.1
10 permit 10.60.60.0 0.0.0.255
11 permit 192.168.220.0 0.0.0.255
```

```
16 permit 140.140.140.0 0.0.0.255
20 permit 192.168.2.0 0.0.0.255
30 permit 192.168.4.0 0.0.0.255
40 permit 192.168.5.0 0.0.0.255
50 permit 192.168.199.0 0.0.0.255
60 permit 192.168.200.0 0.0.0.255
80 permit 192.168.202.0 0.0.0.255
90 permit 192.168.203.0 0.0.0.255
100 permit 192.168.204.0 0.0.0.255
110 permit 192.168.210.0 0.0.0.255
!
ip access-list extended MISSION-CRITICAL-DATA
10 permit tcp any eq 20000 any
20 permit tcp any eq 20100 any
30 permit tcp any eq 20101 any
40 permit tcp any eq 20102 any
50 permit udp any eq 1234 any
60 permit udp any eq 1235 any
ip access-list extended NAT_INSIDE_POOL
10 permit ip 192.168.60.0 0.0.0.255 any
11 permit ip 192.168.85.0 0.0.0.255 any
12 permit tcp 192.168.85.0 0.0.0.255 any
13 permit udp 192.168.85.0 0.0.0.255 any
14 permit icmp 192.168.85.0 0.0.0.255 any
15 permit esp 192.168.85.0 0.0.0.255 any
16 permit ahp 192.168.85.0 0.0.0.255 any
20 permit tcp 192.168.60.0 0.0.0.255 any
30 permit udp 192.168.60.0 0.0.0.255 any
40 permit icmp 192.168.60.0 0.0.0.255 any
50 permit esp 192.168.60.0 0.0.0.255 any
60 permit ahp 192.168.60.0 0.0.0.255 any
71 permit ip 192.168.66.0 0.0.0.255 any
72 permit tcp 192.168.66.0 0.0.0.255 any
73 permit udp 192.168.66.0 0.0.0.255 any
74 permit icmp 192.168.66.0 0.0.0.255 any
75 permit esp 192.168.66.0 0.0.0.255 any
76 permit ahp 192.168.66.0 0.0.0.255 any
77 permit ip any any
78 permit gre any any
81 permit ip 192.168.6.0 0.0.0.255 any
82 permit tcp 192.168.6.0 0.0.0.255 any
83 permit udp 192.168.6.0 0.0.0.255 any
84 permit icmp 192.168.6.0 0.0.0.255 any
85 permit esp 192.168.6.0 0.0.0.255 any
86 permit ahp 192.168.6.0 0.0.0.255 any
91 permit ip 192.168.7.0 0.0.0.255 any
92 permit tcp 192.168.7.0 0.0.0.255 any
93 permit udp 192.168.7.0 0.0.0.255 any
94 permit icmp 192.168.7.0 0.0.0.255 any
95 permit esp 192.168.7.0 0.0.0.255 any
96 permit ahp 192.168.7.0 0.0.0.255 any
```

```
101 permit ip 192.168.8.0 0.0.0.255 any
102 permit tcp 192.168.8.0 0.0.0.255 any
103 permit udp 192.168.8.0 0.0.0.255 any
104 permit icmp 192.168.8.0 0.0.0.255 any
105 permit esp 192.168.8.0 0.0.0.255 any
106 permit ahp 192.168.8.0 0.0.0.255 any
!
!
!
snmp-server community public RO
snmp-server trap link ietf
snmp-server trap link switchover
snmp-server location SA-HER
snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp ifmib ifindex persist
!
tftp-server bootflash:ASR1002-HX-JAE225206QL.cfg
tftp-server bootflash:ciscosdwan.cfg
!
!
!
!
control-plane
!
!
!
!
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
transport input all
transport output all
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
ntp master
ntp server xx.xx.xx.xx
ntp server xx.xx.xx.xx
!
```

```
!
!
!
!
end
```

IE9300-PRP :

```
clarke-002-PRP#show running-config
Building configuration...

Current configuration : 21708 bytes
!
! Last configuration change at 17:34:23 IST Wed Sep 21 2022 by admin
!
version 17.10
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
platform punt-keepalive disable-kernel-core
!
hostname clarke-002-PRP
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
logging userinfo
no logging console
aaa new-model
!
!
aaa group server radius AAASERVER
 server name CISCOISE
!
aaa authentication login default local
aaa authentication dot1x default group AAASERVER
aaa authorization exec default local
aaa authorization network default group radius
aaa authorization network SGLIST group AAASERVER
aaa authorization auth-proxy default group AAASERVER
aaa authorization configuration default group AAASERVER
aaa accounting auth-proxy default start-stop group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
```

```
aaa accounting exec default start-stop group AAASERVER
aaa accounting network default start-stop group AAASERVER
!
!
aaa server radius policy-device
 key xxxxxxx
!
aaa server radius dynamic-author
 client 192.168.2.202 server-key xxxxxx
 server-key xxxxxx
!
aaa session-id common
!
!
!
clock timezone IST 5 30
boot system switch all
sdflash:ie9k_iosxe.BLD_V1710_THROTTLE_LATEST_20220913_143247_V17_10_0_41.SSA.bin
switch 1 provision ie-9320-26s2c
!
!
!
!
ip routing
!
!
!
!
login on-success log
!
!
!
!
!
!
flow record StealthWatch_Record
 description NetFlow record format to send to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
!
!
flow exporter StealthWatch_Exporter
```

```
 description StealthWatch Flow Exporter
 destination 192.168.2.211
 source Vlan111
 transport udp 2055
 option application-table
!
!
flow monitor StealthWatch_Monitor
 description StealthWatch Flow Monitor
 exporter StealthWatch_Exporter
 cache timeout active 60
 cache timeout update 5
 record StealthWatch_Record
!
!
table-map policed-dscp
 map from  0 to 8
 map from  10 to 8
 map from  18 to 8
 map from  24 to 8
 map from  46 to 8
 default copy
table-map AutoQos-4.0-Trust-Cos-Table
 default copy
!
!
dot1x system-auth-control
memory free low-watermark processor 84281
!
!
mac access-list extended TEST_MAC_ACL
 permit any any 0x88B8 0x0
mac access-list extended TEST_MAC_SV
 permit any any 0x88BA 0x0
mac access-list extended TEST_PTP_POWER
 permit any any 0x88F7 0x0
diagnostic bootup level minimal
dying-gasp primary syslog secondary snmp-trap
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
alarm facility sd-card enable
alarm facility sd-card syslog
```

```
alarm facility sd-card notifies
alarm facility power-supply relay major
alarm facility power-supply notifies
alarm facility power-supply disable
!
enable password xxxxxx
!
username admin privilege 15 password 0 xxxxxx
!
redundancy
 mode sso
crypto engine compliance shield disable
!
!
!
!
!
vlan 2508,4040
!
lldp run
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
class-map match-any AutoQos-4.0-Output-Multimedia-Conf-Queue
 match dscp af41  af42  af43
 match cos  4
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any AutoQos-4.0-Bulk-Data-Class
 match access-group name AutoQos-4.0-Acl-Bulk-Data
class-map match-any AutoQos-4.0-Output-Bulk-Data-Queue
match dscp af11  af12  af13
 match cos  1
class-map match-any system-cpp-default
  description EWLC data, Inter FED Traffic
class-map match-any AutoQos-4.0-Multimedia-Conf-Class
 match access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
class-map match-all TEST_COS_52_ADV_UI_CLASS
  description TEST_COS_52_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match cos  5
class-map match-all NETWORK_MGMT
match access-group name NETWORK_MGMT
class-map match-all TEST_DSCP_33
 match dscp 33
class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-all TEST_COS_51_ADV_UI_CLASS
  description TEST_COS_51_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match cos  4
```

```
class-map match-all TEST_DSCP_23
 match dscp 23
class-map match-any AutoQos-4.0-Output-Priority-Queue
 match dscp cs4  cs5  ef
 match cos  5
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any AutoQos-4.0-Output-Multimedia-Strm-Queue
 match dscp af31  af32  af33
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any AutoQos-4.0-Voip-Data-CiscoPhone-Class
 match cos  5
class-map match-all COS_6
 match cos  6
class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description MCAST Data
class-map match-any AutoQos-4.0-Voip-Signal-CiscoPhone-Class
 match cos  3
class-map match-all QOS_GRP_4
 match qos-group 4
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
description Stackwise Virtual OOB
class-map match-any non-client-nrt-class
class-map match-any AutoQos-4.0-Default-Class
match access-group name AutoQos-4.0-Acl-Default
class-map match-any system-cpp-police-routing-control
description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
class-map match-any AutoQos-4.0-Output-Trans-Data-Queue
 match dscp af21  af22  af23
 match cos  2
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
class-map match-any AutoQos-4.0-Transaction-Class
 match access-group name AutoQos-4.0-Acl-Transactional-Data
class-map match-any system-cpp-police-ios-routing
  description L2 control, Topology control, Routing control, Low Latency
```

```
class-map match-all class_test_CRITICAL
 match ip precedence 5
class-map match-any AutoQos-4.0-Scavanger-Class
match access-group name AutoQos-4.0-Acl-Scavanger
class-map match-any system-cpp-police-system-critical
description System Critical and Gold Pkt
class-map match-all TEST_GOOSE2_ADV_UI_CLASS
  description TEST_GOOSE2_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match access-group name TEST_MAC_SV
class-map match-all TEST_GOOSE3_ADV_UI_CLASS
  description TEST_GOOSE3_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match access-group name TEST_PTP_POWER
class-map match-any AutoQos-4.0-Signaling-Class
match access-group name AutoQos-4.0-Acl-Signaling
class-map match-all TEST_GOOSE1_ADV_UI_CLASS
  description TEST_GOOSE1_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match access-group name TEST_MAC_ACL
class-map match-any AutoQos-4.0-Output-Scavenger-Queue
 match dscp cs1
class-map match-all TEST_COS_3
 match cos  3
class-map match-any system-cpp-police-ios-feature
  description
ICMPGEN,BROADCAST,ICMP,L2LVXCntrl,ProtoSnoop,PuntWebauth,MCASTData,Transit,DOT1XAuth,Swf
wd,LOGGING,L2LVXData,ForusTraffic,ForusARP,McastEndStn,Openflow,Exception,EGRExcption,NflSample
d,RpfFailed
class-map match-all TEST_COS_5
 match cos  5
class-map match-any AutoQos-4.0-Output-Control-Mgmt-Queue
 match dscp cs2  cs3  cs6  cs7
 match cos  3
!
policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Output-Priority-Queue
 priority level 1 percent 30
 class AutoQos-4.0-Output-Control-Mgmt-Queue
  bandwidth remaining percent 10
  queue-limit dscp cs2 percent 80
  queue-limit dscp cs3 percent 90
  queue-limit dscp cs6 percent 100
  queue-limit dscp cs7 percent 100
  queue-buffers ratio 10
 class AutoQos-4.0-Output-Multimedia-Conf-Queue
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class AutoQos-4.0-Output-Trans-Data-Queue
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class AutoQos-4.0-Output-Bulk-Data-Queue
  bandwidth remaining percent 4
  queue-buffers ratio 10
```

```
 class AutoQos-4.0-Output-Scavenger-Queue
  bandwidth remaining percent 1
  queue-buffers ratio 10
 class AutoQos-4.0-Output-Multimedia-Strm-Queue
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
policy-map TEST_COS_5
 class TEST_COS_51_ADV_UI_CLASS
class  TEST_COS_52_ADV_UI_CLASS
policy-map pp2
 class NETWORK_MGMT
policy-map AutoQos-4.0-Trust-Cos-Input-Policy
 class class-default
  set cos cos table AutoQos-4.0-Trust-Cos-Table
policy-map system-cpp-policy
policy-map TEST_RADIUS_DSCP
 class TEST_DSCP_23
  set ip precedence 2
 class TEST_DSCP_33
 set ip precedence 2
 class QOS_GRP_4
 police cir 8000
   exceed-action drop
policy-map TEST_OUTSTATION_MARKING
 class class_test_CRITICAL
  set cos 5
policy-map TEST_GOOSE
 class TEST_GOOSE1_ADV_UI_CLASS
  set cos 4
  police cir 10000000
   exceed-action drop
 class TEST_GOOSE2_ADV_UI_CLASS
  set cos 4
  police cir 10000000
   exceed-action drop
 class TEST_GOOSE3_ADV_UI_CLASS
  set qos-group 4
policy-map TEST_DSCP_MARKING
 class TEST_COS_5
  set dscp ef
 class TEST_COS_3
  set dscp af43
policy-map AutoQos-4.0-Classify-Input-Policy
 class AutoQos-4.0-Multimedia-Conf-Class
  set dscp af41
 class AutoQos-4.0-Bulk-Data-Class
  set dscp af11
 class AutoQos-4.0-Transaction-Class
```

```
  set dscp af21
 class AutoQos-4.0-Scavanger-Class
  set dscp cs1
 class AutoQos-4.0-Signaling-Class
  set dscp cs3
 class AutoQos-4.0-Default-Class
  set dscp default
policy-map AutoQos-4.0-CiscoPhone-Input-Policy
 class AutoQos-4.0-Voip-Data-CiscoPhone-Class
 set dscp ef
  police cir 128000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
  set dscp cs3
  police cir 32000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Default-Class
  set dscp default
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
 description connected to clarke001 gi1/0/2
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 service-policy output TEST_RADIUS_DSCP
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
!
```

```
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
 description connected Ixia 1/11
 switchport trunk allowed vlan 1,111
 switchport mode trunk
 load-interval 30
 authentication event fail action next-method
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast trunk
!
interface GigabitEthernet1/0/12
 description Test_MAB
 switchport access vlan 111
 switchport mode access
 switchport voice vlan dot1p
 ip flow monitor StealthWatch_Monitor input
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 service-policy output pp2
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
```

```
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 prp-channel-group 1
 service-policy input TEST_GOOSE
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 prp-channel-group 1
 service-policy input TEST_GOOSE
!
interface GigabitEthernet1/0/23
 shutdown
!
interface GigabitEthernet1/0/24
 shutdown
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface AppGigabitEthernet1/0/1
 switchport voice vlan dot1p
!
interface Vlan1
 no ip address
!
interface Vlan111
 ip address 192.168.21.52 255.255.255.0
```

```
!
interface Vlan177
 ip address 177.177.177.3 255.255.255.0
!
interface Vlan751
 ip address 192.168.177.5 255.255.255.0
!
ip tcp selective-ack
ip tcp mss 1460
ip tcp window-size 131072
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip ftp source-interface Vlan111
ip ftp username xxxxxxx
ip ftp password xxxxxxx
ip route 192.168.2.0 255.255.255.0 192.168.21.99
ip ssh bulk-mode 131072
!
ip access-list extended AutoQos-4.0-Acl-Bulk-Data
 10 permit tcp any any eq 22
 20 permit tcp any any eq 465
 30 permit tcp any any eq 143
 40 permit tcp any any eq 993
 50 permit tcp any any eq 995
 60 permit tcp any any eq 1914
 70 permit tcp any any eq ftp
 80 permit tcp any any eq ftp-data
 90 permit tcp any any eq smtp
 100 permit tcp any any eq pop3
ip access-list extended AutoQos-4.0-Acl-Default
 10 permit ip any any
ip access-list extended AutoQos-4.0-Acl-MultiEnhanced-Conf
 10 permit udp any any range 16384 32767
 20 permit tcp any any range 50000 59999
ip access-list extended AutoQos-4.0-Acl-Scavanger
 10 permit tcp any any range 2300 2400
 20 permit udp any any range 2300 2400
 30 permit tcp any any range 6881 6999
 40 permit tcp any any range 28800 29100
 50 permit tcp any any eq 1214
 60 permit udp any any eq 1214
 70 permit tcp any any eq 3689
 80 permit udp any any eq 3689
 90 permit tcp any any eq 11999
ip access-list extended AutoQos-4.0-Acl-Signaling
 10 permit tcp any any range 2000 2002
 20 permit tcp any any range 5060 5061
 30 permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-Acl-Transactional-Data
```

```
 10 permit tcp any any eq 443
 20 permit tcp any any eq 1521
 30 permit udp any any eq 1521
 40 permit tcp any any eq 1526
 50 permit udp any any eq 1526
 60 permit tcp any any eq 1575
 70 permit udp any any eq 1575
 80 permit tcp any any eq 1630
 90 permit udp any any eq 1630
 100 permit tcp any any eq 1527
 110 permit tcp any any eq 6200
 120 permit tcp any any eq 3389
 130 permit tcp any any eq 5985
 140 permit tcp any any eq 8080
ip access-list extended NETWORK_MGMT
 10 permit ip any host 192.168.2.176
 20 permit tcp any host 192.168.2.176
 30 permit udp any host 192.168.2.108
 40 permit 22 any any
 50 permit 21 any any
!
ip radius source-interface Vlan111
ip sla responder
ip sla responder udp-echo ipaddress 192.168.2.108 port 2526
logging alarm informational
logging origin-id ip
logging host 192.168.5.11
logging host 192.168.2.206
!
snmp-server community public RO
snmp-server trap link ietf
snmp-server trap link switchover
snmp-server location CLARKE-002
snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp-server manager
snmp ifmib ifindex persist
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute nas-port-id include circuit-id
radius-server dscp auth 33 acct 23
!
radius server CISCOISE
 address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
 pac key xxxxxx
!
!
!
control-plane
 service-policy input system-cpp-policy
```

```
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 length 0
 transport input all
line vty 5 15
transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
!
ptp clock boundary domain 3  profile power
 clock-port dynamic1
  transport ethernet multicast interface Gi1/0/2
 clock-port dynamic2
  transport ethernet multicast interface Gi1/0/21
 clock-port dynamic3
  transport ethernet multicast interface Gi1/0/22
 clock-port dynamic4
  transport ethernet multicast interface Gi1/0/12
 clock-port dynamic5
  transport ethernet multicast interface Gi1/0/11
!
!
!
!
!
!
!
end
```

IR8340

```
Sumatra-001#show running-config
Building configuration...

Current configuration : 43642 bytes
!
! Last configuration change at 14:52:59 IST Wed Sep 21 2022 by admin
!
```

```
version 17.11
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year
service internal
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform hardware throughput crypto T0
!
hostname Sumatra-001
!
boot-start-marker
boot system flash:ir8340-universalk9.SSA.bin
boot-end-marker
!
!
vrf definition VRF_BUSINESS
 rd 199:104
 route-target export 199:104
 route-target import 199:104
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_GRIDMON
 rd 199:102
 route-target export 199:102
 route-target import 199:102
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_MGMT
 rd 199:101
 route-target export 199:101
 route-target import 199:101
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_PLANTLINK
 rd 199:105
 route-target export 199:105
 route-target import 199:105
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_SCADA
 rd 199:111
 route-target export 199:111
```

```
 route-target import 199:111
 route-target import 101:111
 !
 address-family ipv4
  route-target export 199:111
  route-target import 199:111
  route-target import 101:111
 exit-address-family
!
vrf definition VRF_TSCADA
 rd 199:103
 route-target export 199:103
 route-target import 199:103
 !
 address-family ipv4
 exit-address-family
!
card type t1 0 2
logging userinfo
no logging console
aaa new-model
!
!
aaa group server radius AAASERVER
 server name CISCOISE
!
aaa authentication login default local
aaa authentication dot1x default group AAASERVER
aaa authorization exec default local
aaa authorization network default group AAASERVER group radius
aaa authorization network SGLIST group AAASERVER
aaa authorization auth-proxy default group AAASERVER
aaa authorization configuration default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
!
!
aaa server radius policy-device
 key xxxxx
!
aaa server radius dynamic-author
 client 192.168.2.202 server-key xxxxxx
 server-key xxxxxx
!
aaa session-id common
ethernet cfm ieee
ethernet cfm global
clock timezone IST 5 30
rep admin vlan 1991 segment 2
rep multicast-fast-convergence
!
!
```

```
!
!
!
no ip nbar classification dns learning cache-ttl-zero
!
!
!
!
no ip domain lookup
ip domain name sumatra-001.cisco.com
!
ip dhcp pool TEST_POOL
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
!
!
!
login on-success log
l2tp-class L2TP_TUNNEL_TEST
 hidden
 authentication
 digest secret 0 xxxxxx hash SHA1
 hello 100
 hostname Sumatra-001
 password xxxxxx
 receive-window 50
 retransmit retries 10
 timeout setup 400
!
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
vtp mode off
!
mpls ldp igp sync holddown 1
multilink bundle-name authenticated
!
flow record StealthWatch_Record
 description NetFlow record format to send to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
```

```
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport tcp flags
 collect interface input
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter StealthWatch_Exporter
 description StealthWatch Flow Exporter
 destination 192.168.2.211
 source Loopback1
 transport udp 2055
 option application-table
!
!
flow monitor StealthWatch_Monitor
 description StealthWatch Flow Monitor
 exporter StealthWatch_Exporter
 cache timeout active 60
 cache timeout update 5
 record StealthWatch_Record
!
ptp clock forward-mode
!
!
!
!
!
cts sxp enable
no license feature hseck9
license udi pid IR8340-K9 sn FDO2551J707
license boot level network-advantage
license smart url https://smartreceiver-stage.cisco.com/licservice/license
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
license smart transport smart
archive
 log config
  logging enable
  logging size 500
 path ftp://192.168.2.176/sumatra-001
 write-memory
memory free low-watermark processor 67541
!
```

```
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1,201,501,1501 priority 4096
!
mac access-list extended GOOSE
 permit any any 0x88B8 0x0
mac access-list extended PTP
permit any any 0x88F7 0x0
mac access-list extended SV
permit any any 0x88BA 0x0
dot1x system-auth-control
geo database
no power main redundant
!
!
enable password xxxxxxxx
!
username admin privilege 15 password 0 xxxxxxxx
!
redundancy
 mode none
bfd fast-timers-on-slow-interface
!
!
!
!
controller T1 0/2/0
 framing esf
 clock source internal
 linecode b8zs
 cablelength long 0db
 channel-group 2 timeslots 1-24
 description connected to t1 0/2/2 on asr903
!
controller T1 0/2/1
 framing esf
 clock source internal
 linecode b8zs
 cablelength long 0db
 channel-group 1 timeslots 1-24
 description connected to T10/2/3 on asr903
!
!
vlan internal allocation policy ascending
!
vlan 55,101,119,177,201,210,500-501,997-998,1001
!
vlan 1051
 name HSRP-GRP-1
```

```
!
vlan 1052-1060
!
vlan 1501
 remote-span
!
vlan 1990-1991,2340,4001
!
track 1 ip sla 1 reachability
 delay down 5 up 5
!
track 100 ip route 192.168.201.4 255.255.255.255 reachability
!
track 200 ip route 192.168.201.6 255.255.255.255 reachability
!
lldp run
!
class-map match-any MGMT_TRAFFIC
 match protocol ftp
 match  protocol  ssh
 match  protocol  ntp
 match  protocol  http
 match protocol https
class-map match-any PREC_ROUTINE
 match precedence 0
class-map match-any DSCP_af21_af22
 match ip dscp af21
 match ip dscp af22
 match dscp af21
 match dscp af22
 match dscp af23
 match dscp af12
 match dscp af11
class-map type ngsw-qos match-any SCADA_PTP_NGSW
 match access-group name GOOSE
 match access-group name SV
match access-group name PTP
class-map match-any SCADA_SV
match access-group name SV
class-map match-all TEST_DSCP_af11
 match dscp af11
class-map match-all TEST_DSCP_af22
 match dscp af22
class-map match-all TEST_DSCP_af12
 match dscp af12
class-map match-all TEST_DSCP_af21
 match dscp af21
class-map match-any EXP_2
 match mpls experimental topmost 2
class-map match-any EXP_3
 match mpls experimental topmost 3
```

```
class-map match-any EXP_0
 match mpls experimental topmost 0
class-map match-any EXP_1
 match mpls experimental topmost 1
class-map match-any EXP_4
 match mpls experimental topmost 4
class-map match-any EXP_5
 match mpls experimental topmost 5
class-map type ngsw-qos match-any TEST_COS_3_NGSW
 match cos  3
class-map type ngsw-qos match-any TEST_COS_2_NGSW
 match cos  2
class-map type ngsw-qos match-any TEST_COS_1_NGSW
 match cos  1
class-map type inspect match-any IN-IN
 match protocol ssh
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol https
 match protocol http
 match protocol login
class-map match-all COPP-MONITORING
 match access-group name coppacl-monitor
class-map type ngsw-qos match-any TEST_COS_5_NGSW
 match cos  5
class-map type ngsw-qos match-any TEST_COS_4_NGSW
 match cos  4
class-map match-all COPP-MANAGEMENT
 match access-group name coppacl-mgmt
class-map type inspect match-any OUT-SCADA
 match protocol ntp
 match protocol ssh
 match protocol syslog
 match protocol icmp
 match access-group name MISSION-CRITICAL-DATA-OUT
 match protocol snmp
class-map type inspect match-any SCADA-OUT
 match protocol ntp
 match protocol ssh
 match protocol syslog
 match protocol icmp
 match access-group name MISSION-CRITICAL-DATA-IN
class-map match-any QOS_GRP_6
 match qos-group 6
class-map match-any QOS_GRP_7
 match qos-group 7
class-map match-all COPP-CRITICAL-APP
match access-group name coppacl-critical-app
class-map match-any TRANSACTIONAL
 match ip dscp cs2  af21  af22  af23  cs4  af41  af42
```

```
class-map match-all COPP-REMAINING-IP
match access-group name coppacl-classification
class-map match-all VOICE
 match ip dscp ef
class-map match-any MISSION-CRITICAL-DATA
 match access-group name MISSION-CRITICAL-DATA-IN
class-map match-any SCADA_GOOSE
 match access-group name GOOSE
class-map match-any PREC_CRITIC
match precedence 5
class-map match-any SCADA_PTP
match access-group name PTP
class-map match-all COPP-ARP
match protocol arp
class-map type inspect match-any IN-OUT
 match protocol icmp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
 match protocol syslog
 match protocol udp
 match access-group name FTP_IN_OUT
 match protocol tcp
 match access-group 102
 match protocol login
class-map type inspect match-any OUT-IN
 match protocol icmp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
 match protocol syslog
 match access-group name FTP_OUT_IN
 match protocol tcp
 match access-group 102
 match protocol udp
 match protocol snmp
class-map match-any PREC_3
 match ip precedence 3
class-map match-any PREC_2
 match ip precedence 2
class-map match-any MISSION-CRITICAL
match ip dscp cs3  af31  af32  af33  cs6
class-map match-any PREC_1
 match ip precedence 1
class-map match-any PREC_0
 match ip precedence 0
class-map type ngsw-qos match-any NGSW_QOS_GRP_7
 match qos-group 7
class-map match-any PREC_5
```

```
 match ip precedence 5
class-map match-any PREC_4
 match ip precedence 4
class-map match-all CALL-SIGNALING
 match ip dscp cs3
class-map match-all COPP-FRAGMENTS
match access-group name coppacl-frag
class-map match-all COPP-BGP
 match access-group name coppacl-bgp
class-map match-all COPP-UNDESIRABLE
match access-group name coppacl-drop
class-map match-all COPP-IGP
 match access-group name coppacl-igp
!
policy-map TEST_EXP_CLASS
 class EXP_0
  shape average 10000000
 class EXP_1
  shape average 10000000
 class EXP_2
  shape average 10000000
 class EXP_3
  shape average 10000000
 class EXP_4
  shape average 10000000
 class EXP_5
  shape average 10000000
policy-map TEST_MGMT_TRAFFIC
 class MGMT_TRAFFIC
  police cir 100000000
   conform-action transmit
   exceed-action transmit
policy-map type inspect SCADA-OUT
 class type inspect SCADA-OUT
 inspect
 class class-default
policy-map HOST-INPUT-MARKING
 class VOICE
  set dscp ef
 class CALL-SIGNALING
  set dscp cs3
 class MISSION-CRITICAL-DATA
  set dscp af31
 class class-default
policy-map HOST-QUEUE-PACKETS
 class VOICE
  priority
 class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets
 class TRANSACTIONAL
```

```
  bandwidth remaining percent 20
  queue-limit 96 packets
 class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map TEST_INPUT
 class PREC_CRITIC
  set precedence 5
 class PREC_ROUTINE
  set precedence 0
policy-map PARENT
 class class-default
  shape average 1000000000
   service-policy TEST_INPUT
policy-map type inspect IN-IN
 class type inspect IN-IN
 inspect
 class class-default
policy-map TEST_QOS_OUT
 class QOS_GRP_7
  priority 1
 class QOS_GRP_6
  priority 2
policy-map TEST_OUT_DSCP
 class DSCP_af21_af22
policy-map type inspect OUT-IN
 class type inspect OUT-IN
 inspect
 class class-default
policy-map UPLINK-QUEUE-PACKETS
 class VOICE
  priority level 1
 class MISSION-CRITICAL
  priority level 2
 class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
 class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map TEST_RADIUS_DSCP
 class TEST_DSCP_af11
  set dscp af11
 class TEST_DSCP_af12
  set dscp af12
 class TEST_DSCP_af21
  set dscp af21
 class TEST_DSCP_af22
  set dscp af22
policy-map type ngsw-qos TEST_COS_CLASS_NGSW
 class TEST_COS_1_NGSW
```

```
  set mpls experimental imposition 1
 class TEST_COS_2_NGSW
  set mpls experimental imposition 2
 class TEST_COS_3_NGSW
  set mpls experimental imposition 3
 class TEST_COS_4_NGSW
  set mpls experimental imposition 4
 class TEST_COS_5_NGSW
  set mpls experimental imposition 5
 class SCADA_PTP_NGSW
  set qos-group 7
policy-map type ngsw-qos TEST_COS_PRIORITY
 class TEST_COS_1_NGSW
  set qos-group 7
policy-map type ngsw-qos TEST_OUTPUT
 class NGSW_QOS_GRP_7
  priority level 1
  set cos 7
  police cir 100000000
   conform-action transmit
   exceed-action drop
policy-map COPP
 class COPP-FRAGMENTS
  police 32000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-UNDESIRABLE
  police 8000 1500 1500 conform-action drop  exceed-action drop
 class COPP-BGP
  police 125000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-IGP
  police 125000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-MANAGEMENT
  police 192000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-MONITORING
  police 64000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-CRITICAL-APP
  police 50000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-ARP
  police 32000 1500 1500 conform-action transmit  exceed-action transmit
 class COPP-REMAINING-IP
  police 8000 1500 1500 conform-action transmit  exceed-action transmit
 class class-default
  police 8000 1500 1500 conform-action transmit  exceed-action transmit
policy-map type inspect IN-OUT
 class type inspect IN-OUT
  inspect
 class class-default
policy-map type inspect OUT-SCADA
 class type inspect OUT-SCADA
 inspect
 class class-default
policy-map type ngsw-qos SCADA_IN
```

```
 class SCADA_PTP_NGSW
  priority level 1
!
pseudowire-class L2TP_PW_TEST
 encapsulation l2tpv3
 sequencing both
 protocol l2tpv3 L2TP_TUNNEL_TEST
 status control-plane route-watch
 ip local interface Loopback1
 ip pmtu
 ip dfbit set
 ip tos reflect
 ip ttl 100
!
!
zone security INSIDE
zone security OUTSIDE
zone security SCADA
zone-pair security IN-IN-PAIR source INSIDE destination INSIDE
 service-policy type inspect IN-IN
zone-pair security IN-OUT-PAIR source INSIDE destination OUTSIDE
 service-policy type inspect IN-OUT
zone-pair security OUT-IN-PAIR source OUTSIDE destination INSIDE
 service-policy type inspect OUT-IN
zone-pair security OUT-SCADA-PAIR source OUTSIDE destination SCADA
 service-policy type inspect OUT-SCADA
zone-pair security SCADA-OUT-PAIR source SCADA destination OUTSIDE
 service-policy type inspect SCADA-OUT
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip flow monitor StealthWatch_Monitor input
 ip address 192.168.199.1 255.255.255.255
!
interface Loopback1
```

```
 ip address 192.168.199.2 255.255.255.255
 ip nat outside
 zone-member security INSIDE
!
interface Port-channel1
 ip flow monitor StealthWatch_Monitor output
 ip address 192.168.100.1 255.255.255.0
 no ip redirects
 zone-member security OUTSIDE
 ip ospf network point-to-point
 load-interval 30
 negotiation auto
 mpls ip
 bfd interval 200 min_rx 200 multiplier 3
 lacp max-bundle 2
!
interface Multilink1
 ip address 3.3.3.2 255.255.255.0
 zone-member security OUTSIDE
 load-interval 30
 mpls ip
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string mlp1
 service-policy output UPLINK-QUEUE-PACKETS
!
interface Multilink2
 ip address 5.5.5.2 255.255.255.0
 shutdown
 mpls ip
 ppp multilink
 ppp multilink group 2
 ppp multilink endpoint string mlp2
!
interface Multilink100
 no ip address
 ppp multilink
 ppp multilink group 100
!
interface VirtualPortGroup0
 description Routing Port pkt capture
 ip address 136.1.2.1 255.255.255.0
 no mop enabled
 no mop sysid
!
interface VirtualPortGroup1
 ip address 137.1.2.1 255.255.255.0
 ip mtu 1200
 zone-member security INSIDE
 ip tcp adjust-mss 1160
 no mop enabled
```

```
 no mop sysid
!
interface GigabitEthernet0/0/0
 description connected to asr903-003
 ip flow monitor StealthWatch_Monitor input
 no ip address
 zone-member security OUTSIDE
 ip ospf network point-to-point
 load-interval 30
 negotiation auto
 bfd interval 50 min_rx 50 multiplier 3
 channel-group 1 mode active
!
interface GigabitEthernet0/0/1
 description connected to asr903-003
 ip flow monitor StealthWatch_Monitor input
 no ip address
 load-interval 30
 shutdown
 negotiation auto
 service-policy output UPLINK-QUEUE-PACKETS
!
interface GigabitEthernet0/0/1.1101
 encapsulation dot1Q 1101
 vrf forwarding VRF_SCADA
 ip address 15.1.0.2 255.255.255.0
 ip ospf network point-to-point
 ip ospf 101 area 0
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1102
 encapsulation dot1Q 1102
 vrf forwarding VRF_TSCADA
 ip address 16.1.0.2 255.255.255.0
 ip ospf network point-to-point
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1103
 encapsulation dot1Q 1103
 vrf forwarding VRF_PLANTLINK
 ip address 17.1.0.2 255.255.255.0
 ip ospf network point-to-point
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1104
 encapsulation dot1Q 1104
 vrf forwarding VRF_MGMT
 ip address 18.1.0.2 255.255.255.0
 ip ospf network point-to-point
 bfd interval 50 min_rx 50 multiplier 3
!
```

```
interface GigabitEthernet0/0/1.1105
 encapsulation dot1Q 1105
 vrf forwarding VRF_GRIDMON
 ip address 19.1.0.2 255.255.255.0
 ip ospf network point-to-point
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1106
 encapsulation dot1Q 1106
 vrf forwarding VRF_BUSINESS
 ip address 20.1.0.2 255.255.255.0
 ip ospf network point-to-point
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/1/0
 switchport access vlan 500
 switchport mode access
!
interface GigabitEthernet0/1/1
 description connected to TGN card 2 port 4
 switchport access vlan 2502
 switchport trunk allowed vlan 1-500,502-4094
 switchport mode access
 mtu 9216
 load-interval 30
!
interface GigabitEthernet0/1/2
 description connected to IE3400-SA02-01
 switchport trunk allowed vlan 1,201,204,210,4001
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 spanning-tree portfast trunk
!
interface GigabitEthernet0/1/3
 description connected to PD6500-Camera
 switchport access vlan 500
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
 authentication event fail action next-method
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
!
interface GigabitEthernet0/1/4
 description connected to IE3400-SA02-005
 switchport trunk allowed vlan 1,1001,1051-1062,3001-3006
```

```
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 carrier-delay msec 1
 media-type rj45
!
interface GigabitEthernet0/1/5
 description connected gi0/1/7 sumatra-pp-1
 switchport trunk allowed vlan 1,201,501,1501
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 rep segment 1 edge
 rep lsl-retries 3
 rep lsl-age-timer 3000
 service-policy input TEST_COS_CLASS_NGSW
!
interface GigabitEthernet0/1/6
 description REP-Ring connected to IE2KU-REP001
 switchport trunk allowed vlan 1,201,501,1501
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 rep segment 1 edge primary
 rep preempt delay 15
 rep lsl-retries 3
 rep lsl-age-timer 3000
 service-policy input TEST_COS_CLASS_NGSW
!
interface GigabitEthernet0/1/7
 description connected to .148 PC
 switchport access vlan 101
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky xxxx.xxxx.xxxx
 switchport port-security
!
interface GigabitEthernet0/1/8
 description connected Ixia
 switchport trunk allowed vlan 1,501
 switchport mode trunk
 spanning-tree portfast trunk
 service-policy input TEST_COS_CLASS_NGSW
!
interface GigabitEthernet0/1/9
 switchport trunk allowed vlan 1990,1991
 switchport mode trunk
 shutdown
 rep segment 2 edge primary
!
interface GigabitEthernet0/1/10
```

```
 switchport trunk allowed vlan 1990,1991
 switchport mode trunk
 shutdown
 rep segment 2 edge
!
interface GigabitEthernet0/1/11
 switchport mode trunk
!
interface AppGigabitEthernet0/1/1
 switchport trunk allowed vlan 2340
 switchport mode trunk
!
interface Serial0/2/0:2
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial0/2/1:1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial0/3/1
 no ip address
 shutdown
!
interface Serial0/3/2
 no ip address
 shutdown
!
interface Serial0/3/3
 no ip address
 shutdown
!
interface Serial0/3/4
 no ip address
 shutdown
!
interface Serial0/3/5
 no ip address
 shutdown
!
interface Serial0/3/6
 no ip address
 shutdown
!
interface Serial0/3/7
 no ip address
 shutdown
```

```
!
interface Serial0/3/0
 physical-layer async
 no ip address
 encapsulation scada
!
interface Vlan1
 no ip address
!
interface Vlan55
 description Jumbo-Fragmentation
 mtu 9216
 ip address 192.168.155.1 255.255.255.0
 zone-member security INSIDE
!
interface Vlan101
 ip address 192.168.101.1 255.255.255.0
 zone-member security SCADA
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
interface Vlan119
 ip address 11.9.0.1 255.255.255.0
!
interface Vlan177
 ip address 177.177.177.1 255.255.255.0
 zone-member security INSIDE
!
interface Vlan201
 ip address 192.168.211.1 255.255.255.0
 zone-member security SCADA
 load-interval 30
 vrrp 1 name MODBUS-IED-1
 vrrp 1 ip 192.168.211.100
 vrrp 1 timers learn
 vrrp 1 priority 200
 service-policy input HOST-INPUT-MARKING
!
interface Vlan210
 ip address 192.168.210.1 255.255.255.0
 ip nat outside
 zone-member security INSIDE
!
interface Vlan500
 description Cisco IP Camera
 ip address 192.168.0.1 255.255.255.0
 zone-member security INSIDE
 load-interval 30
!
interface Vlan501
 description REP-Mgmt
```

```
 ip address 50.1.0.1 255.255.255.0
 zone-member security INSIDE
 standby 0 ip 50.1.0.100
 standby 0 timers msec 30 msec 120
 standby 0 priority 200
 standby 0 preempt
 load-interval 30
 service-policy input TEST_MGMT_TRAFFIC
!
interface Vlan1001
 no ip address
 xconnect 192.168.200.1 1001 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan1051
 description HSRP-GRP-1
 ip address 192.168.110.2 255.255.255.0
 zone-member security INSIDE
 standby 1 ip 192.168.110.1
 standby 1 priority 10
 standby 1 preempt
 standby 1 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
!
interface Vlan1052
 ip address 192.168.111.2 255.255.255.0
 zone-member security INSIDE
 standby 1 track 100 decrement 10
 standby 2 ip 192.168.111.1
 standby 2 priority 10
 standby 2 preempt
 bfd interval 999 min_rx 999 multiplier 3
!
interface Vlan1053
 ip address 192.168.53.2 255.255.255.0
 zone-member security INSIDE
 standby 3 ip 192.168.53.1
 standby 3 priority 10
 standby 3 preempt
 standby 3 track 100 decrement 10
 standby 4 priority 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1054
 ip address 192.168.54.2 255.255.255.0
 zone-member security INSIDE
 standby 4 ip 192.168.54.1
 standby 4 priority 10
 standby 4 preempt
 standby 4 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
```

```
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1055
 ip address 192.168.55.2 255.255.255.0
 zone-member security INSIDE
 standby 5 ip 192.168.55.1
 standby 5 priority 10
 standby 5 preempt
 standby 5 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1056
 ip address 192.168.56.2 255.255.255.0
 zone-member security INSIDE
 standby 6 ip 192.168.56.1
 standby 6 priority 10
 standby 6 preempt
 standby 6 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1057
 ip address 192.168.57.2 255.255.255.0
 zone-member security INSIDE
 standby 7 ip 192.168.57.1
 standby 7 priority 10
 standby 7 preempt
 standby 7 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1058
 ip address 192.168.58.2 255.255.255.0
 zone-member security INSIDE
 standby 8 ip 192.168.58.1
 standby 8 priority 10
 standby 8 preempt
 standby 8 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1059
 ip address 192.168.59.2 255.255.255.0
 zone-member security INSIDE
 standby 9 ip 192.168.59.1
 standby 9 priority 10
 standby 9 preempt
 standby 9 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
```

```
!
interface Vlan1060
 ip address 192.168.60.2 255.255.255.0
 zone-member security INSIDE
 standby 10 ip 192.168.60.1
 standby 10 priority 10
 standby 10 preempt
 standby 10 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1061
 ip address 192.168.61.2 255.255.255.0
!
interface Vlan1062
 ip address 192.168.62.2 255.255.255.0
!
interface Vlan1101
 no ip address
!
interface Vlan1990
 ip address 19.90.0.1 255.255.255.0
 zone-member security INSIDE
 vrrp 11 ip 19.90.0.100
 vrrp 11 timers learn
 vrrp 11 priority 50
!
interface Vlan2002
 ip address 20.2.0.1 255.255.255.0
!
interface Vlan2340
 description LAN port pkt capture
 ip address 136.1.1.1 255.255.255.0
!
interface Vlan2501
 no ip address
 xconnect 192.168.223.1 2501 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2502
 no ip address
 zone-member security INSIDE
 load-interval 30
 xconnect 192.168.200.1 2502 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2503
 no ip address
 xconnect 192.168.200.1 2503 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2504
 no ip address
 xconnect 192.168.200.1 2504 encapsulation l2tpv3 pw-class L2TP_PW_TEST
```

```
!
interface Vlan2505
 no ip address
 xconnect 192.168.200.1 2505 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2506
 no ip address
 xconnect 192.168.200.1 2506 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2507
 no ip address
 xconnect 192.168.200.1 2507 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2508
 no ip address
 xconnect 192.168.200.1 2508 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2509
 no ip address
 xconnect 192.168.200.1 2509 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2560
 no ip address
 xconnect 192.168.200.1 2560 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan3001
 vrf forwarding VRF_SCADA
 ip address 30.0.1.1 255.255.255.0
 ip access-group VRF_SCADA out
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
interface Vlan3002
 vrf forwarding VRF_TSCADA
 ip address 30.0.2.1 255.255.255.0
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
interface Vlan3003
 vrf forwarding VRF_PLANTLINK
 ip address 30.0.3.1 255.255.255.0
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
interface Vlan3004
 vrf forwarding VRF_MGMT
 ip address 30.0.4.1 255.255.255.0
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
interface Vlan3005
```

```
 vrf forwarding VRF_GRIDMON
 ip address 30.0.5.1 255.255.255.0
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
interface Vlan3006
 vrf forwarding VRF_BUSINESS
 ip address 30.0.6.1 255.255.255.0
 load-interval 30
 service-policy input HOST-INPUT-MARKING
!
!
router eigrp 1
 bfd interface GigabitEthernet0/0/0
 bfd interface GigabitEthernet0/0/1
 bfd interface Port-channel1
 bfd interface Multilink1
 bfd interface Multilink2
 network 3.3.3.0 0.0.0.255
 network 5.5.5.0 0.0.0.255
 network 192.168.0.0
 network 192.168.75.0
 network 192.168.76.0
 network 192.168.100.0
 network 192.168.199.1 0.0.0.0
 shutdown
!
router ospf 101 vrf VRF_SCADA
 shutdown
 network 15.1.0.0 0.0.0.255 area 0
 network 30.0.1.0 0.0.0.255 area 0
 bfd all-interfaces
!
router ospf 102 vrf VRF_TSCADA
 shutdown
 network 16.1.0.0 0.0.0.255 area 0
 network 30.0.2.0 0.0.0.255 area 0
 bfd all-interfaces
!
router ospf 103 vrf VRF_PLANTLINK
 shutdown
 network 17.1.0.0 0.0.0.255 area 0
 network 30.0.3.0 0.0.0.255 area 0
 bfd all-interfaces
!
router ospf 104 vrf VRF_MGMT
 shutdown
 network 18.1.0.0 0.0.0.255 area 0
 network 30.0.4.0 0.0.0.255 area 0
 bfd all-interfaces
!
```

```
router ospf 105 vrf VRF_GRIDMON
 shutdown
 network 19.1.0.0 0.0.0.255 area 0
 network 30.0.5.0 0.0.0.255 area 0
 bfd all-interfaces
!
router ospf 106 vrf VRF_BUSINESS
 shutdown
 network 20.1.0.0 0.0.0.255 area 0
 network 30.0.6.0 0.0.0.255 area 0
 bfd all-interfaces
!
router ospf 1
 router-id 192.168.199.1
 network 3.3.3.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
 network 192.168.199.1 0.0.0.0 area 0
 bfd all-interfaces
!
router bgp 200
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor 192.168.201.6 remote-as 200
 neighbor 192.168.201.6 update-source Loopback0
 neighbor 192.168.201.6 fall-over bfd multi-hop
 !
 address-family ipv4
  network 11.9.0.0 mask 255.255.255.0
  network 19.90.0.0 mask 255.255.255.0
  network 20.1.0.0 mask 255.255.255.0
  network 20.2.0.0 mask 255.255.255.0
  network 50.1.0.0 mask 255.255.255.0
  network 137.1.2.0 mask 255.255.255.0
  network 177.177.177.0 mask 255.255.255.0
  network 192.168.0.0
  network 192.168.53.0
  network 192.168.54.0
  network 192.168.55.0
  network 192.168.56.0
  network 192.168.57.0
  network 192.168.58.0
  network 192.168.59.0
  network 192.168.60.0
  network 192.168.101.0
  network 192.168.110.0
  network 192.168.155.0
  network 192.168.199.2 mask 255.255.255.255
  network 192.168.210.0
  network 192.168.211.0
  neighbor 192.168.201.6 activate
  neighbor 192.168.201.6 send-community extended
```

```
  neighbor 192.168.201.6 next-hop-self
  neighbor 192.168.201.6 send-label
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.201.6 activate
  neighbor 192.168.201.6 send-community extended
  neighbor 192.168.201.6 next-hop-self
 exit-address-family
 !
 address-family ipv4 vrf VRF_BUSINESS
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_GRIDMON
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_MGMT
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_PLANTLINK
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_SCADA
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_TSCADA
  redistribute connected
 exit-address-family
!
!
virtual-service
 signing level unsigned
!
!
!
iox
ip tcp selective-ack
ip tcp mss 1460
ip tcp window-size 131072
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip ftp source-interface Loopback1
ip ftp username xxxxxxxx
ip ftp password xxxxxxxx
```

```
ip tftp source-interface Loopback1
ip nat inside source list NAT_ACL interface Port-channel1 overload
ip route 192.168.221.1 255.255.255.255 Port-channel1
ip route 192.168.222.1 255.255.255.255 Port-channel1
ip route vrf VRF_BUSINESS 0.0.0.0 0.0.0.0 20.1.0.1
ip route vrf VRF_GRIDMON 0.0.0.0 0.0.0.0 19.1.0.1
ip route vrf VRF_MGMT 0.0.0.0 0.0.0.0 18.1.0.1
ip route vrf VRF_PLANTLINK 0.0.0.0 0.0.0.0 17.1.0.1
ip route vrf VRF_SCADA 0.0.0.0 0.0.0.0 15.1.0.1
ip route vrf VRF_TSCADA 0.0.0.0 0.0.0.0 16.1.0.1
ip ssh bulk-mode 131072
ip ssh source-interface Loopback1
!
!
ip access-list standard CVPOOL
 10 permit 169.254.0.0 0.0.0.255
ip access-list standard NAT_ACL
 10 permit 169.254.0.0 0.0.0.3
 20 permit 50.1.0.0 0.0.0.255
!
ip access-list extended FTP_IN_OUT
 1 permit tcp 192.168.110.0 0.0.0.255 host 192.168.2.176 eq ftp log
 2 permit tcp host 192.168.199.2 host 192.168.2.176 eq ftp log
 3 permit tcp host 192.168.199.2 host 192.168.2.206 eq ftp
 13 permit tcp 50.1.0.0 0.0.0.255 host 192.168.2.176 eq ftp log
ip access-list extended FTP_OUT_IN
 1 permit tcp host 192.168.2.176 192.168.110.0 0.0.0.255 eq ftp
 2 permit tcp host 192.168.2.176 host 192.168.199.2 eq ftp
 3 permit tcp host 192.168.2.206 host 192.168.199.2 eq ftp
ip access-list extended MISSION-CRITICAL-DATA
 10 permit tcp any eq 20000 any
 11 permit tcp any eq 20001 any
 12 permit tcp any eq 20002 any
 13 permit tcp any eq 20003 any
 14 permit tcp any eq 20004 any
 15 permit tcp any eq 20005 any
 20 permit tcp any eq 20100 any
 30 permit tcp any eq 20101 any
 40 permit tcp any eq 20102 any
 50 permit udp any eq 1234 any
 60 permit udp any eq 1235 any
 70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
ip access-list extended MISSION-CRITICAL-DATA-IN
 9 permit tcp host 192.168.101.2 eq 20000 host 192.168.4.171
 10 permit tcp host 192.168.101.2 eq 20001 host 192.168.4.171
 11 permit tcp host 192.168.101.2 eq 20002 host 192.168.4.171
 12 permit tcp host 192.168.101.2 eq 20003 host 192.168.4.171
 13 permit tcp host 192.168.101.2 eq 20004 host 192.168.4.171
 14 permit tcp host 192.168.101.2 eq 20005 host 192.168.4.171
 19 permit tcp host 192.168.101.2 eq 20100 host 192.168.4.171
 29 permit tcp host 192.168.101.2 eq 20200 host 192.168.4.171
```

```
 39 permit tcp host 192.168.101.2 eq 20300 host 192.168.4.171
 41 permit tcp host 192.168.211.2 host 192.168.2.206 eq 502
 50 permit udp any any
 70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
ip access-list extended MISSION-CRITICAL-DATA-OUT
 9 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20000
 10 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20001
 11 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20002
 12 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20003
 13 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20004
 14 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20005
 19 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20100
 29 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20200
 39 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20300
 41 permit tcp host 192.168.2.206 host 192.168.211.2 eq 502
 50 permit udp any any
 70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
ip access-list extended VRF_SCADA
 1 deny ip 3.0.1.0 0.0.0.255 any log
 2 deny ip 4.0.1.0 0.0.0.255 any log
 3 deny ip 5.0.1.0 0.0.0.255 any log
 4 deny ip 6.0.1.0 0.0.0.255 any log
 5 deny ip 7.0.1.0 0.0.0.255 any log
 6 deny ip 8.0.1.0 0.0.0.255 any log
 7 deny ip 9.0.1.0 0.0.0.255 any log
 8 deny ip 10.0.1.0 0.0.0.255 any log
 9 deny ip 11.0.1.0 0.0.0.255 any log
 10 permit ip 12.0.1.0 0.0.0.255 host 30.0.1.2 log
ip access-list extended coppacl-bgp
 10 permit tcp any any eq bgp
 20 permit tcp any eq bgp any
ip access-list extended coppacl-classification
 10 permit tcp any any eq www
 20 permit tcp any any lt 1024
 30 permit tcp any any gt 1024
 40 permit udp any any lt isakmp
 50 permit udp any any gt 1000
 60 permit ip any any
ip access-list extended coppacl-critical-app
 10 permit ip any host 224.0.0.2
 20 permit ip any host 224.0.0.102
 30 permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
 40 permit udp any eq bootps any eq bootps
ip access-list extended coppacl-drop
 10 permit udp any any eq 1434
 20 permit udp any any eq 1975
ip access-list extended coppacl-frag
 10 permit tcp any any fragments
 20 permit udp any any fragments
 30 permit icmp any any fragments
 40 permit ip any any fragments
```

```
ip access-list extended coppacl-igp
 10 permit ospf any host 224.0.0.5
 20 permit ospf any host 224.0.0.6
 30 permit ospf any any
 40 permit eigrp any any
 50 permit pim any any
ip access-list extended coppacl-mgmt
 10 permit tcp any any established
 20 permit tcp any any eq telnet
 30 permit tcp any any eq 22
 40 permit udp any any eq snmp
 50 permit udp any any eq ntp
 60 permit tcp any any eq tacacs
 70 permit udp any any eq syslog
ip access-list extended coppacl-monitor
 10 permit icmp any any ttl-exceeded
 20 permit icmp any any port-unreachable
 30 permit icmp any any echo-reply
 40 permit icmp any any echo
 50 permit icmp any any packet-too-big
!
ip radius source-interface Loopback1
ip sla 1
 icmp-echo 192.168.2.108 source-interface Loopback1
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo 192.168.2.176 source-interface Loopback1
  frequency 5
ip sla schedule 2 life forever start-time now
ip sla 2006
 udp-echo 177.177.177.2 2525 source-ip 177.177.177.1 source-port 2525
  frequency 5
ip sla schedule 2006 life forever start-time now
ip sla 2007
 udp-echo 177.177.177.3 2526 source-ip 177.177.177.1 source-port 2526
  frequency 5
ip sla schedule 2007 life forever start-time now
logging origin-id hostname
logging source-interface Loopback1
logging host 192.168.5.11
logging host 192.168.2.206
ip access-list extended 101
 1 deny udp any eq syslog host 192.168.2.206 log
ip access-list extended 102
 10 permit ip any any
arp 169.254.2.2 5254.dd42.d460 ARPA
arp 136.1.1.3 5254.dd05.96c9 ARPA
!
mpls ldp router-id Loopback0
snmp-server community public RO
snmp-server trap link ietf
```

```
snmp-server trap link switchover
snmp-server location SUMATRA_001
snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp ifmib ifindex persist
!
tftp-server bootflash:xxxxxxxxx_20210614221401703.lic
!
!
!
radius server CISCOISE
 address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
 pac key xxxxxx
!
!
control-plane
 service-policy input COPP
!
scada-gw protocol dnp3-serial
 channel serial
  unsolicited-response enable
 session serial
  attach-to-channel serial
scada-gw protocol dnp3-ip
channel ip
  tcp-connection local-port 23000 remote-ip 192.168.4.171/0
 session ip
  attach-to-channel ip
  map-to-session serial
!
!
!
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line 0/3/0
line vty 0 4
 logging synchronous
 login authentication local
 history size 50
 transport input all
line vty 5 15
 logging synchronous
 login authentication local
 history size 50
 transport input all
!
!
```

```
monitor session 1 type erspan-source
 source interface Gi0/1/0 - 11
 destination
  erspan-id 1
  mtu 1464
  ip address 136.1.1.3
  origin ip address 136.1.1.1
!
!
monitor session 5 type erspan-source
 source interface Po1
 source interface Vl101
 destination
  erspan-id 5
  mtu 1464
  ip address 136.1.2.3
  origin ip address 136.1.2.1
!
!
monitor session 20 source vlan 1
monitor session 20 destination remote vlan 1501
network-clock synchronization automatic
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
ntp master
ntp refclock ptp
!
ptp clock boundary domain 0  profile power
 clock-port dynamic1
  transport ethernet multicast interface Gi0/1/4
 clock-port dynamic2
  transport ethernet multicast interface Gi0/1/2
  vlan 4001
 clock-port dynamic3
  transport ethernet multicast interface Gi0/1/5
 clock-port dynamic4
  transport ethernet multicast interface Gi0/1/6
 clock-port dynamic5
  transport ethernet multicast interface Gi0/1/8
!
!
!
!
!
!
```

```
!
app-hosting appid sensor3
 app-vnic AppGigabitEthernet trunk
  vlan 2340 guest-interface 3
   guest-ipaddress 136.1.1.3 netmask 255.255.255.0
 app-vnic gateway0 virtualportgroup 1 guest-interface 0
  guest-ipaddress 137.1.2.3 netmask 255.255.255.0
 app-vnic gateway1 virtualportgroup 0 guest-interface 1
  guest-ipaddress 136.1.2.3 netmask 255.255.255.0
 app-default-gateway 137.1.2.1 guest-interface 0
 app-resource docker
  run-opts 1 --rm
 app-resource profile custom
  cpu 1155
  memory 2048
  persist-disk 8192
  vcpu 2
end
```