\€

Distribution Automation

Direct Transfer Trip over Cellular

Design and Implementation Guide

September 2024

Table of Contents

1 Introduction

1.1 Direct Transfer Trip over Cellular

Traditionally Direct Transfer Trip Signals (DTT) were sent between substations and remote Distributed Generation (DG) site using leased telephone lines. DTT systems are traditionally installed for critical high-speed tripping of circuit breakers on either side of a feeder interconnecting substations or between the substation breaker and a DG site station equipment.

To ease the deployment and make it flexible for the utility customers, Cisco undertook work to design and validate key use cases over Cellular backhaul technology, an easy to deploy connectivity solution for the various distribution grid use cases, especially in providing connectivity to the various Distributed Energy Resources (DER) assets and the local distribution substations. Today cellular networks are reliable and low cost to deploy compared to dedicated fiber. This solution uses the Catalyst IR1101 rugged router, used widely in distribution automation networks today with plugin cellular modules to support the various commercial and private spectrum bands.

The focus was on leveraging standards-based and scalable communication technologies to provide encrypted connectivity between sites while supporting the transport of layer 2 multicast non routable IEC61850 GOOSE messaging in secure peer-to-peer topologies. Plus, the same solution will natively allow SCADA data also to be transported within the encrypted tunnels.

DTT is an additional use case that could be deployed on existing Cisco IR1101 platforms. Adding the DTT use case can be done centrally via templated configuration on Cisco Field Network Director management platform, thus providing an optional capability that can be provisioned into the network where required.

Entire solution is encrypted at various layers (MACSEC between SEL recloser and Cisco IR1101, IPSEC encrypted tunnels between Cisco IR1101s, IPSEC encrypted tunnels between Cisco IR1101 and Headend Router Cluster, https between Cisco IR1101 and Cisco FND, and so on). Thus, all communications used in this solution are over secure transport.

2 DESIGN SECTION

2.1 Use Cases Covered

Vertical Use cases:

1. Direct Transfer Trip use case
2. SCADA use case
3. Engineering Access use case for remote management of grid devices

Horizontal use cases:

4. Service Isolation use case
5. Last mile security using MACSEC
6. Cisco IR1101 management use case

End to End secure communication with IPSEC:

All the above-mentioned use cases require communication with Control Center (hosting SCADA, Engineering Access UI), substation sites (hosting SEL RTAC), distribution sites (also known in this document as DA site or midpoint recloser site), distributed generation site (also known in this document as DER site or point of interconnect recloser site) and Network Operations Centre (hosting FND/NMS). **The communications between these various locations are designed and validated over secure transport, protected with IPSEC/Flex-VPN**. Last mile security is provided with the help of MACSEC feature.

Terminology references in this document:

Substation site: A secondary substation site.

DA site: A distribution site, located along the distribution feeder lines. It's also known in this document as midpoint recloser site.

DER site: A distributed energy resource site, also known in this document as distributed generation site (DG site) or point of interconnect (POI) recloser site.

Recloser: In the context of this document, any reference to recloser (with communication context) refers to recloser controller, as the communication aspect is handled by the controller device, and not recloser by itself.

2.1.1 Use case actors:

Use Case	Actors Involved	Communication Flow	VRF used on Cisco IR1101
Direct Transfer Trip	SEL RTAC in Substation SEL 651RA in DER site (POI recloser controller) SEL 651RA in DA sites (Midpoint recloser controller) Cisco IR1101 in all sites (Substation, DA, DER)	IED to IED (peer to peer layer2 multicast communication) IEC 61850 Layer2 GOOSE messages are sent over emulated Layer2 network.	DTT_VRF
SCADA	SCADA, HER cluster in DSO control center SEL RTAC in substation site SEL 651RA in DER/DA sites Cisco IR1101 in all sites (Substation, DA, DER)	a. SCADA to RTU b. SCADA to IED SCADA <-> RTU/IED communication using Layer3 Unicast.	SCADA_VRF
Engineering Access – Direct access, Substation RTAC as proxy	SEL Engineering Access software in DSO control center. SEL RTAC in substation site SEL 651RA in DER/DA sites HER cluster in DSO control center Cisco IR1101 in each site (Substation, DA site, DER site)	Method1 – Direct access: Control Center to RTAC/IED (or) Method2 – Engineering Access using substation RTAC as proxy: 1. Control Center to Substation RTAC 2. Substation RTAC to IED	SCADA_VRF
Cisco IR1101 device management	Cisco IR1101, Cisco Field Network Director, HER cluster in NOC Headend	NOC Headend to Cisco IIOT Cellular Gateways (IR1101)	MGMNT_VRF

2.1.2 Direct Transfer Trip use case:

This use case validates transmission of “Direct Transfer Trip” message using IEC-61850 GOOSE messaging from substation RTAC (or) distribution sites recloser controller to DER site recloser controller.

For additional details, please refer to Direct Transfer Trip (DTT) use case.

2.1.3 SCADA use case:

This “Supervisory Control and Data Acquisition” use case validates monitoring and control operations of various Utility controller devices, RTACs remotely from the Utility Control Center

premise. These utility controller devices could be located along the distribution feeders or at the distributed generation sites. RTAC is in the substation premise.

For additional details, refer to SCADA communication between Control Center and Reclosers/IEDs:

2.1.4 Engineering Access use case for remote management of grid devices

This "Engineering Access" use case enables in band remote management of the grid devices (for example, Recloser controllers) and the substation RTAC. Engineering Access allows the utility controller devices to be managed remotely.

For additional details, refer to Engineering Access to SEL Reclosers, RTACs:

2.1.5 Service Isolation use case

"Direct Transfer Trip" communication is isolated from SCADA & engineering access.
Cisco management communication of IR1101s is isolated from DTT, SCADA and engineering access.

For additional details, refer to "DTT Service Isolation from SCADA and other services:"

2.1.6 Last Mile security using MACSEC

Securing the "Last Foot" could be achieved with the help of Layer2 MACSEC between the IED and the Cisco IR1101 gateways. Vendor IEDs must be capable of supporting MACSEC.

For additional details, refer to "Securing the "Last Foot" with Layer2 MACSEC:"

2.1.7 Cisco IR1101 management use case

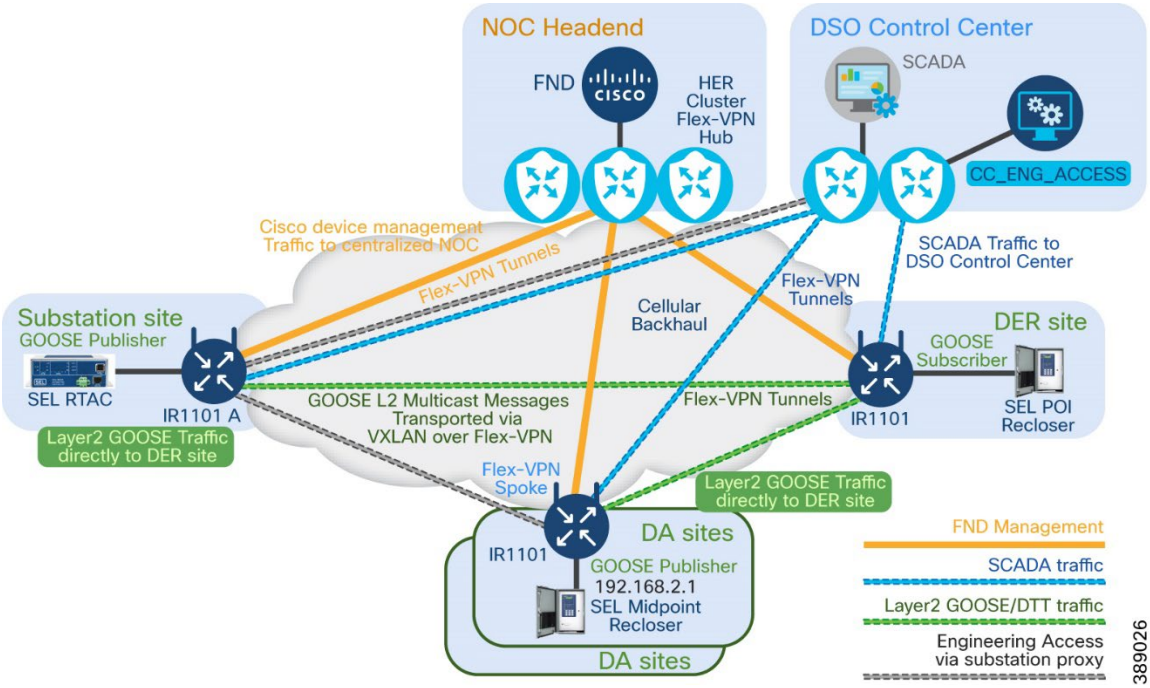
Cisco IR1101s could be onboarded with the help of Plug and Play (PnP) and Zero Touch Deployment (ZTD) using Cisco Field Network Director as NMS. This use case validates the Day N operations (like configuration management, device monitoring and management, firmware upgrade) over a service isolated "MGMNT_VRF". This use case traffic is isolated from the rest of the use case traffic that includes DTT, SCADA & Engineering Access.

For further details, refer to Management of Cisco IR1101s using Field Network Director:

2.2 Multi Service Architecture with SERVICE ISOLATION

This solution is built on top of existing Distribution Automation solution CVD for Secondary Substation.

Figure 1. Multi-Service Architecture



In the above figure:

Separate (green) tunnels are established between the Substation site/DA sites and the DER site. These tunnels facilitate the communication of “Direct Transfer Trip” message using Layer2 GOOSE.
Blue tunnels are established between DSO control center and Substation/DA/DER sites, for the purpose of SCADA communication.
Orange tunnels are established between NOC headend and Substation/DA/DER sites, for the purpose of Cisco IR1101 device management.

2.2.1 Places in the Network:

- DSO Control center: It hosts SCADA, Engineering Access UI/Software
- DER site: Point of Interconnect (POI) recloser controller is in this Distributed Generation site
- Substation site: SEL RTAC is in this site.
- DA sites: Mid-Point recloser controllers are located along the distribution feeders.
- NOC Headend: It hosts Cisco Field Network Director, the NMS software.

Cisco IIoT gateway provides secure communication infrastructure for multi service use cases including DTT, SCADA, Engineering Access, and so on.

2.2.2 Hardware Software Matrix:

Device	Device Type	Role	Firmware
SEL 651RA	Recloser Controller	Midpoint Recloser controller at DA sites	SEL-651RA-R106-VO-Z006001-D20230130
	Recloser Controller	Point of Interconnect Recloser controller at DER site	SEL-651RA-R106-VO-Z006001-D20230130
SEL 3530	SEL RTAC device	Substation RTAC	SEL-3530-R151-V3-Z000148-D20230522
SEL 3505	SEL RTAC device	Control Centre SCADA	SEL-3530-R151-V3-Z000148-D20230522
Cisco IR1101	Cisco IIoT Cellular Gateway	Secondary Substation Router	17.13.1
Cisco IR1101	Cisco IIoT Cellular Gateway	DA site gateway	17.13.1
Cisco IR1101	Cisco IIoT Cellular Gateway	DER site gateway	17.13.1
Cisco Catalyst 8000	Cisco Head End Router	HER router at Network Operations Center (NOC)	17.14.1a
Cisco Catalyst 8000	Cisco Head End Router	HER router at Control Centre/SCADA	17.14.1a
Cisco Field Network Director (FND)	Network Management Server	To support with Cisco IR1101 device management use case	4.11.0-69

2.2.3 Security Considerations:

Communication between	Description	Applicable use case traffic
Cisco IR1101 to Cisco IR1101	WAN communication protected with secure Flex-VPN Tunnels (IPSec/IKEv2)	1. Direct Transfer Trip use case traffic 2. Engineering Access use case traffic.
Cisco IR1101 to Cisco Cat8000	WAN communication protected with secure Flex-VPN Tunnels (IPSec/IKEv2)	1. SCADA use case traffic 2. Engineering Access use case traffic. 3. Cisco IIoT cellular gateway management traffic from NMS
SEL 651RA to Cisco IR1101 (Last mile protection)	Last mile LAN communication with IED, protected with MACSEC.	All communication between Cisco IR1101 and SEL 651 RA over Ethernet last mile connection.
FND to Cisco IR1101	https using TLS/SSL with certificate-based security	Cisco IIoT cellular gateway management traffic from NMS

2.2.4 ICT Technology Considerations:

Device	Served by
Layer3 Security	Flex-VPN Tunnels (IPSEC, IKEv2)
Layer2 Security	MACSEC
Layer2 bridge emulation over Layer3 network (for Direct Transfer Trip)	VXLAN over Flex-VPN Tunnel, PIM, IKEv2 prefix injection for control plane (BGP not used for control plane)
Route exchange between IR1101, Head End Router cluster	IKEv2 prefix injection (BGP or routing protocol not required)

2.3 Direct Transfer Trip (DTT) use case

2.3.1 Direct Transfer Trip - An overview:

It is vital to quickly disconnect the DER whenever the feeder protection switch that the DTT is configured to monitor opens.

In the Direct Transfer Trip use case, the DER site waits for communication from the upstream reclosers and substation RTAC for an Open signal. Once the “Direct Transfer Trip” is received, the DER site disconnects itself from the power grid. The entire communication happens over secure a communication network (using IPSec encryption). Even the last 'foot’ ethernet connectivity with the actual recloser is secured with the use of MACSEC encryption. So, the connection is truly secured end to end.

Figure 2. Direct Transfer Trip: sent by DTT transmitter to DTT receiver

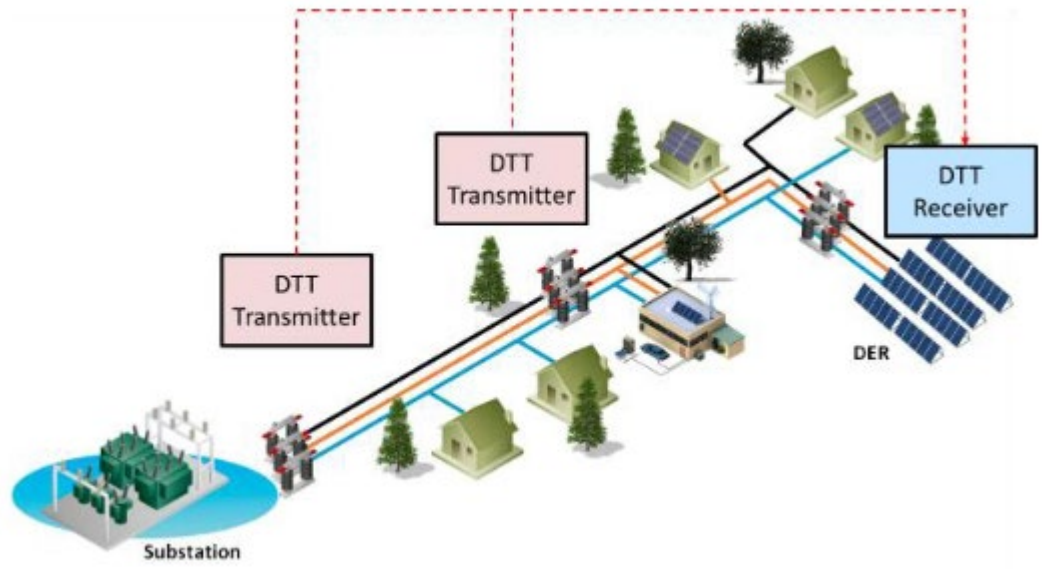


Image courtesy: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9938886

2.3.2 Direct Transfer Trip use case – Actors:

Actors of this "Direct Transfer Trip" use case include:

1. Point of Interconnect (POI) recloser controller, connected to Distributed Energy Resource (DER) site.
2. Midpoint recloser controller, connected along the distribution feeders.
3. Substation RTAC, connected to substation site.

Note: All these participating actors must be Time synchronised. As part of this validation effort, **SEL devices were time synchronized using IRIG-B input.**

Midpoint recloser controller and Substation RTAC are the generators of the "DTT message". They are DTT Transmitters.
Point of Interconnect recloser controller connected to DER site, acts as receiver of DTT message (sent by any of the DTT transmitters). This relationship is referred to as Publisher and Subscriber.

The Trip message is transferred from either the RTAC (or) Midpoint recloser controllers, directly to the POI recloser controller using IEC 61850 layer2 GOOSE messages. The DA sites and DER sites are located along the feeder lines and at the distributed generation site, respectively. These sites typically are remote and may not have the Fiber connectivity, thus making Cellular a good connectivity option. To transfer this DTT command using Layer2 multicast GOOSE message, an emulated layer2 network is needed between the actors located in the Substation, DA sites and the DER sites over the Layer3 cellular network.

2.3.3 Direct Transfer Trip use case - Application Traffic Flow:

This use case requires a unidirectional flow of "Direct Transfer Trip" messages from the DTT transmitter (any of substation RTAC or Midpoint recloser controllers) to the DTT receiver (DER site).

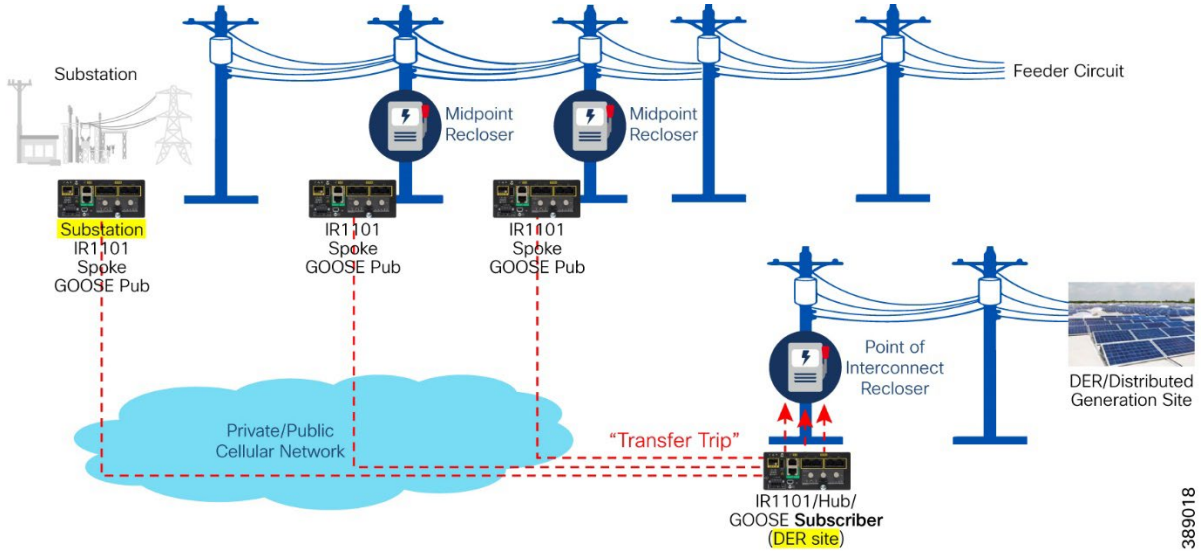
- DTT transmitter side serves as publisher of GOOSE message.
- DTT receiver side serve as subscriber of GOOSE message.

Hub & Spoke Topology for sending "Direct Transfer Trip" message:

Traffic flow between the DTT transmitter sites & DTT receiver site would be achieved with the use of a Hub & Spoke design.

- DER site (positioned as Hub) acts as GOOSE subscriber.
- Each participating upstream DTT transmitter (Spoke) acts as GOOSE publisher.

Figure 3. Direct Transfer Trip Overview



The Hub used in this "Direct Transfer Trip" use case is positioned in the DER site. At the same time, the same DER site also acts as a spoke with respect to the HER cluster (Hub) located in the control centre.

Direct Transfer Trip is the primary use case of this document. The other use cases implicitly covered in this document are SCADA, Engineering Access, along with network management of Cisco IR1101s.

Cisco IR1101 based on positioning of the device could play multiple roles, as follows:

- Secondary Substation Router: Cisco IR1101 when positioned in substation location.
- DA site Gateway: Cisco IR1101 when positioned along the feeder lines (in DA sites)
- DER site Gateway: Cisco IR1101 when positioned at the DER site (Distributed Generation site)

The reader of this document must learn to differentiate between the multiple Hub & Spoke designs used in the solution.

- First H&S design is between the HER cluster (as Hub) and the IR1101s positioned in DA site, DER sites, substation, and so on. This is primarily used for management of IR1101s using FND (Cisco device management use case).
- Second H&S design is between the IR1101s in the field:
    a. IR1101 located in DER site (as Hub)
    b. IR1101s located in DA site/substation (as spokes).
    c. This Hub & Spoke design of Tunnels between the Cisco IR1101s is dedicated for transmission of layer2 GOOSE message from the DTT transmission site(s) to the DTT receiving DER site.
    d. This is used for the Direct Transfer Trip use case.
- Third H&S design is between the IR1101s in the field:
    a. IR1101 located in DA sites (as Spokes)
    b. IR1101s located in substation (as Hub).
    c. This Hub & Spoke design of Tunnels between the Cisco IR1101s is dedicated for transmission of peer-to-peer layer3 communication between the substation RTAC and the DA sites.
    d. This is used for Engineering Access use case.

2.3.4 Direct Transfer Trip message to POI recloser using Layer2 GOOSE:

Point of Interconnect (POI) recloser controller located in DER site is the receiver of "Direct Transfer Trip" message sent by Substation RTAC or Midpoint recloser controllers.

The POI recloser controller, upon receiving the “Trip” message, isolates the DER site from the electrical grid.

Within the substation network, RTAC would usually be connected to the Breaker relay over the serial connection. Usage of serial connection between the SEL-RTAC and the Breaker relay is for these reasons:

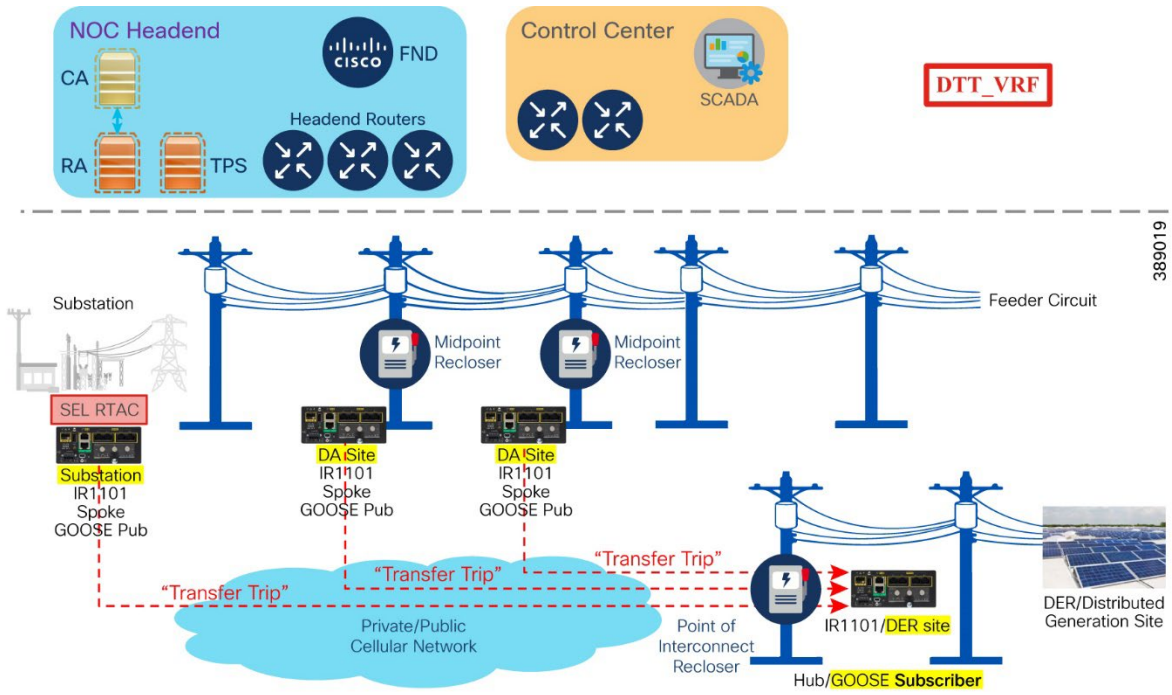
- It provides speed and simplicity in communication.
- Creates a protocol break (from routable protocols)
- It helps isolates the Feeder facing “Transfer Trip” routable network from the substation routable network.

The communication between the RTAC and Breaker relay could be using standard/proprietary protocol. Based on the “breaker status” information received from Breaker relay, the RTAC then converts the received information to GOOSE messaging for sending the “Transfer Trip” message to the POI recloser. In other words, based on the system event initiated by the feeder breaker, the RTAC generates the “Transfer Trip” message to POI recloser.

The Midpoint recloser controllers, based on its own status information could also generate the “Transfer Trip” message to the POI recloser controller.

The POI recloser controller, upon receiving the “Transfer Trip” message executes a Trip operation de-energising the grid, thus achieving the desired goal.

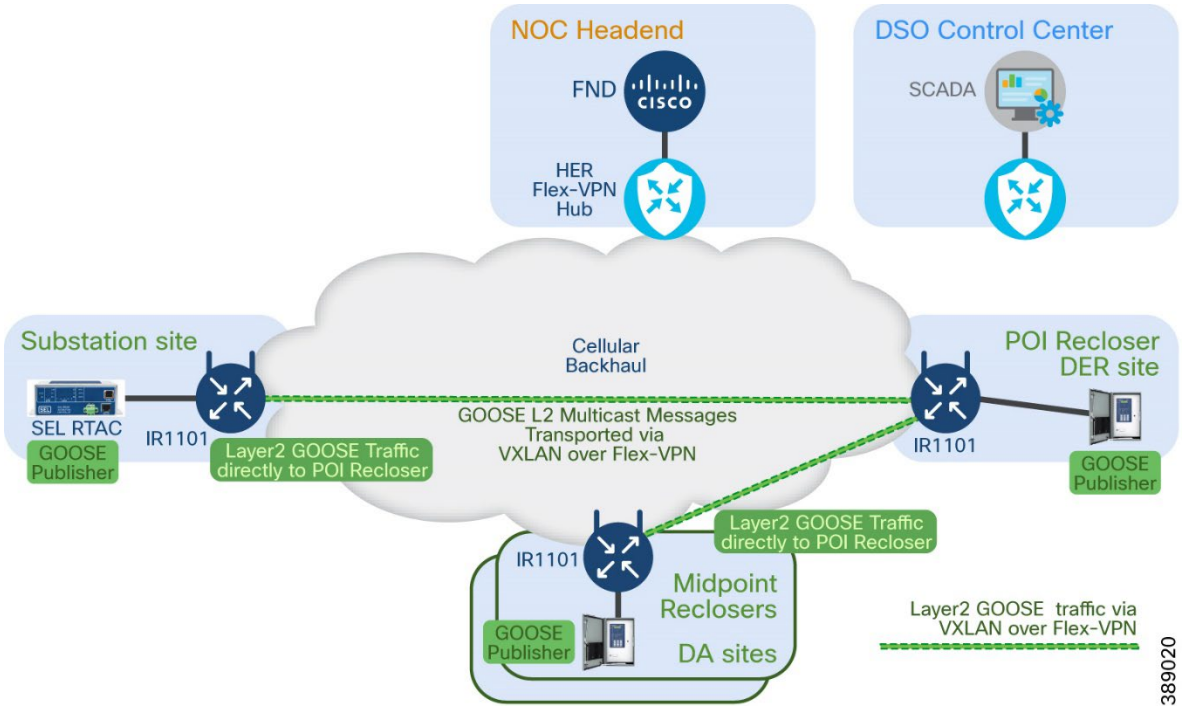
Figure 4. Transfer Trip message sent to POI Recloser



Above figure shows the GOOSE subscriber (DER site) receiving “Transfer Trip” message from any of the GOOSE publishers, which could be Substation RTAC or Midpoint Reclosers from the feeders.

Tunnel architecture (as shown in figure below) would be used to enable secure communication of Layer2 GOOSE messages between the “DTT Transmitters” (aka GOOSE publishers) and “DTT receiver” (aka GOOSE subscriber).

Figure 5. Tunnel Architecture for SECURE communication of Layer 2 GOOSE message



In the above figure, secure Cisco Flex-VPN communication is established between Spoke-IR1101s (located in substation and DA sites) and the Hub-IR1101 (located in the DER site). For Example, it could be Tunnel15 on spoke-IR1101s and Virtual-Template15 on the Hub-IR1101. This is a secure peer-to-peer layer3 communication path established between the Substation/DA site and the DER site using Flex-VPN tunnel over the Cellular backhaul. On Cisco spoke-IR1101s, the Tunnel15 is part of “DTT_VRF”. On Cisco Hub-IR1101, the Virtual-Template15 will be part of “DTT_VRF”.

Inside the Flex-VPN tunnel, VXLAN overlay in conjunction with PIM multicast is used to emulate the Layer2 network. VXLAN is used to extend the layer2 network across a Layer3 network. The IEC 61850 GOOSE messaging capable IEDs could send out a 802.1q tagged ethernet frame to the Cisco IR1101. This tagged GOOSE frame is transported by Cisco IR1101 across the L3 network using VXLAN technology and delivered on the POI recloser controller connected interface with the original 802.1q tagged frame. For VXLAN, IKEv2 based prefix injection is used for advertising the routes required. This design doesn’t require any additional routing protocols like BGP, OSPF for VXLAN operation. VXLAN operates in a 'Flood & Learn' method to keep the configuration simple. The number of reclosers and hence tunnels required for the DTT overlay is minimal. Hence the Flood & Learn method is seen as sufficient.

Flood and Learn: In a VXLAN environment, a technique called “Flood and Learn” is used to handle unknown destination MAC addresses. When a VTEP receives a unicast frame with an unknown destination MAC address, it floods the frame to all other VTEPs within the same VXLAN segment. The destination VTEP that owns the recloser/IED with the corresponding MAC address learns the association between the MAC address and the VNI, thus providing layer 2 connectivity.

IEC 61850 GOOSE messaging capable IEDs that require layer2 connectivity between themselves, but are located distantly across a layer3 network (for example, Cellular network) could be enabled for layer2 connectivity between themselves with the help of Cisco IR1101 gateways (Zero Touch).

The layer2 GOOSE messages (carrying the “Transfer Trip”) flows directly from any of the GOOSE publisher(s) to the GOOSE subscriber over this secure layer2 network. As this layer2 GOOSE communication is the payload for the peer-to-peer secure layer3 Flex-VPN tunnel, this “Direct Transfer Trip” message is also secured/encrypted between the Cisco IR1101s.

Thus, a seamless layer2 network is provided between midpoint recloser controllers/substation-RTAC and the POI recloser controller.

2.3.5 DTT Service Isolation from SCADA and other services:

The “Direct Transfer Trip” service could be isolated and segregated from other services like SCADA service, Cisco IR1101 management service (by NMS), Engineering Access of IEDs by utilities, and so on.

Various services used in the solution are:

- Direct Transfer Trip message to POI recloser using Layer2 GOOSE.
- SCADA communication between Control Centre and Reclosers/IEDs
- Engineering Access to all the Reclosers/IEDs from the Control Centre
- Engineering Access to all the Reclosers/IEDs from the Control Centre using Substation RTAC as proxy
- Additional layer of Last mile data security between the IEDs and the Cisco IR1101 using MACSEC
- Management of the Cisco IR1101s from NOC using FND.

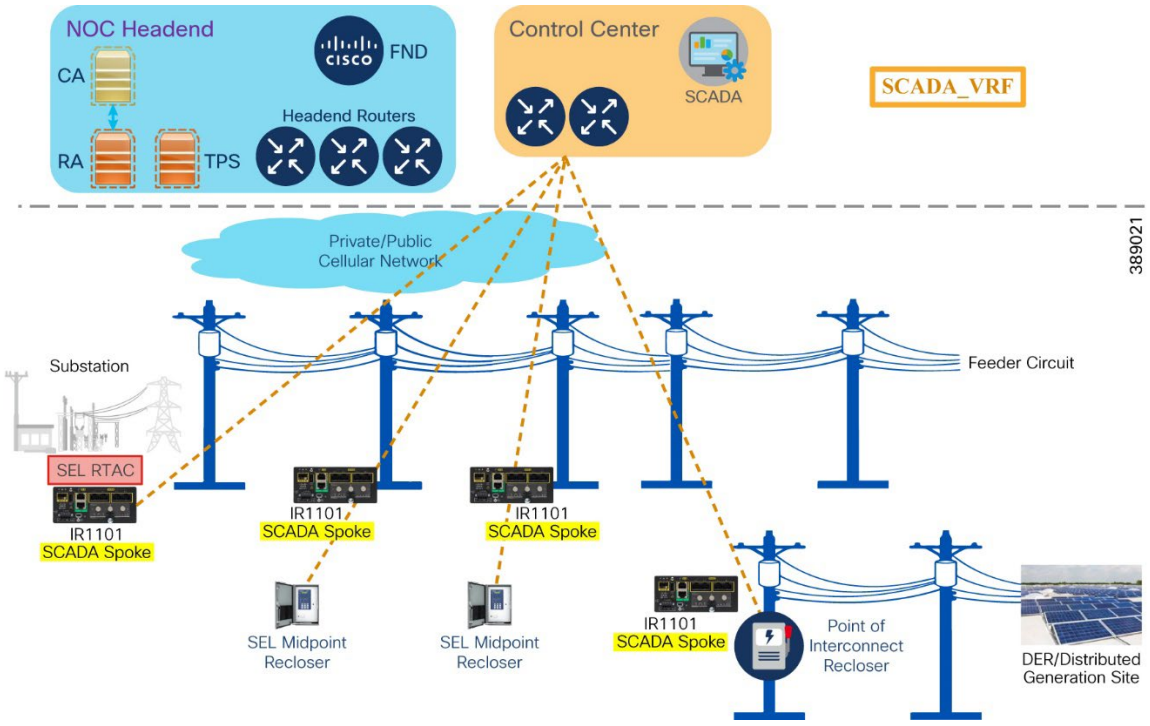
This service isolation requirement aims at grouping and isolating the services on the Cisco IR1101, so that the services are isolated into respective VRFs like “MGMNT_VRF”, “SCADA_VRF”, “DTT_VRF” and so on.

Note: Engineering Access re-uses the “SCADA_VRF” defined on IR1101, to access the IEDs from the Control Centre, either directly (or) using substation RTAC as proxy. SCADA system and the Engineering Access PC would share similar communication path.

2.4 SCADA communication between Control Center and Reclosers/IEDs:

The SCADA, located in the Control Center would perform the required monitoring and control operations on the Substation RTAC, Midpoint recloser controllers, and Point of Interconnect recloser controller. Communication infrastructure could also facilitate the Unsolicited messages from the recloser controllers back to the SCADA system. A Bidirectional communication path is supported between the Control Center and the Substation-RTAC/Recloser controllers.

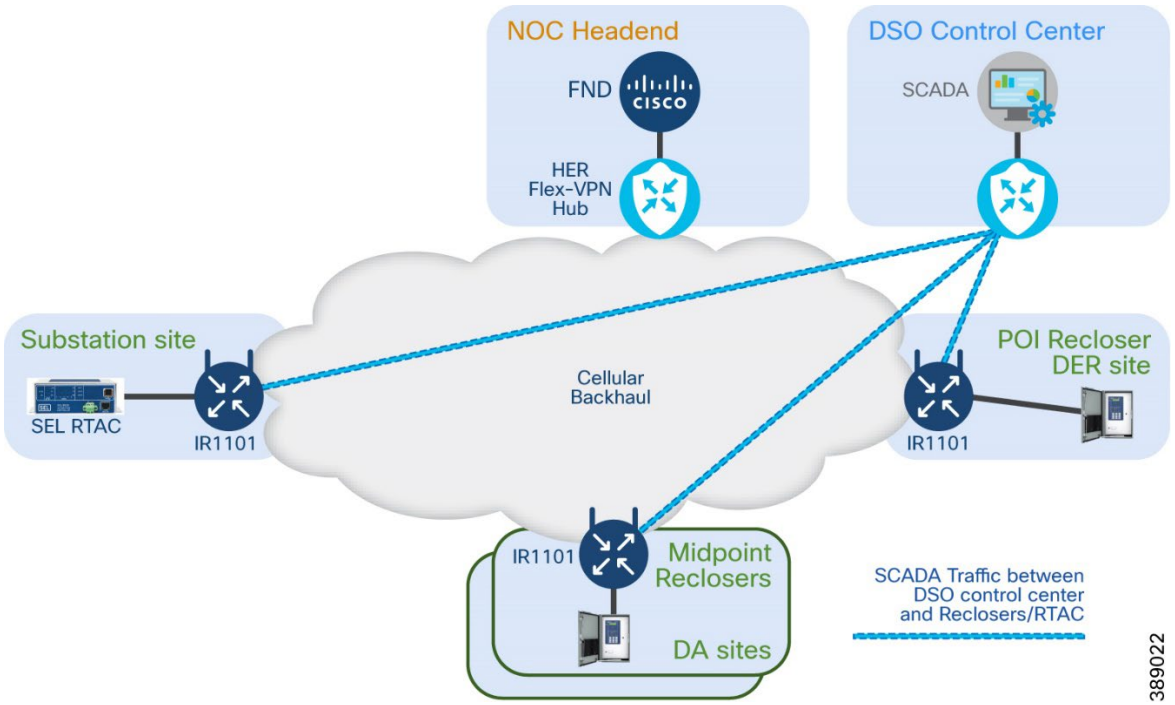
Figure 6. SCADA system



In above figure, the SCADA system communicates with RTAC, midpoint recloser controllers, POI reclose controller using Cisco IR1101 as gateway.

The following Tunnel architecture could be used to enable secure bidirectional communication between Control centre SCADA and the Recloser controllers/RTAC.

Figure 7. Tunnel Architecture for SECURE bidirectional communication between SCADA and RTAC/Reclosers



In the above figure, secure Flex-VPN communication is established between Spoke-IR1101s (located in substation, DA sites, DER site) and the Hub (located in the DSO Control Centre). For Example, it could be Tunnel11 on spoke-IR1101s and Virtual-Template11 on the DSO-Control-Centre1-Hub. This is a secure peer to peer layer3 communication path established between the Substation/DA/DER site and the DSO Control Centre site using Flex-VPN tunnel over the Cellular backhaul.

Note: In case of dual control centre scenario and for resiliency, Second tunnel (for example, Tunnel12) could be established between the spoke-IR1101 and the DSO Control Centre2 Hub.

On Cisco spoke-IR1101s, the Tunnel11 and Tunnel12 (in case of dual control centre scenario) are part of "SCADA_VRF".

2.4.1 IP connectivity of SEL Recloser/RTAC via Cisco IR1101:

IP connectivity for the SEL recloser/RTAC could be enabled with "Network Address Translation (NAT)" or without. For detailed information about the pros and cons of NAT usage, please refer to "Network Address Translation" section of Distribution Automation-Secondary Substation Design Guide. This section is applicable only for L3 services like SCADA, engineering access, not for Layer2 service like Direct Transfer Trip (or) for management of Cisco IR1101 using FND.

This document considers the "Network Address Translation" way of accessing the reclosers/RTACs. SEL device could be configured with same private IP across all the DA/DER sites, substation site. This provides configuration simplicity to the field technician. The SEL devices would be represented to the other sites/control centre using the Loopback IP of IR1101, belonging to SCADA_VRF.

- Loopback address of the Cisco IR1101 is used as the Service Access IP.
- Service Access IP + port combination could be used to access the particular service.

For example:
telnet (port 23) of SEL 651RA could be accessed using Service Access IP + port 30023 (or any custom port)
http (port 80) of SEL 651RA could be accessed using Service Access IP + port 30080 (or any custom port)
SCADA (port 20000) of SEL 651RA could be accessed using Service Access IP + port 20000 (or any custom port)

Refer to the NAT Implementation section for further details.

2.5 Engineering Access to SEL Reclosers, RTACs:

Engineering access typically refers to the capability for a utility authorized person (an engineer or technician) to remotely access and/or configure the Reclosers/RTAC. Engineering access could be done in two ways:

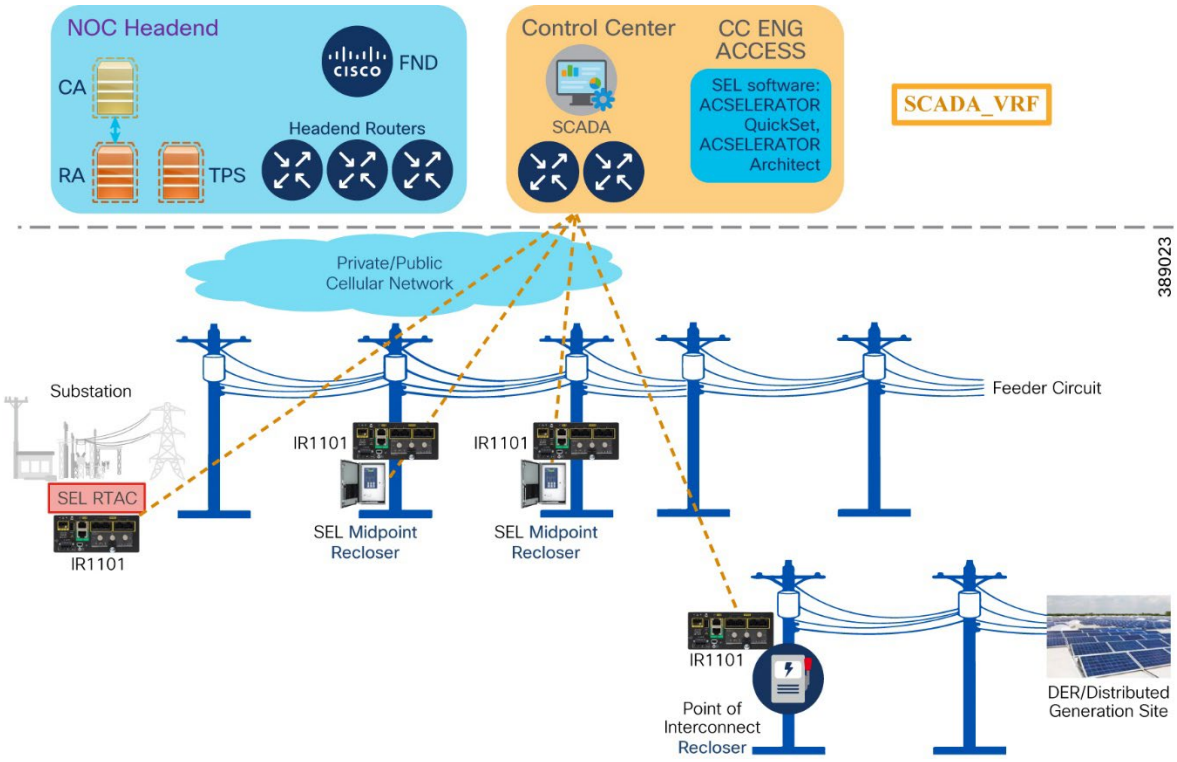
- Direct Engineering Access to SEL Reclosers & RTAC from the Control Center
- Engineering Access to SEL Reclosers from the Control Center using Substation RTAC as an intermediate proxy

A few examples of Engineering access include, accessing the SEL reclosers using http(s) from browser, using telnet from SEL software, ftp, and so on. Some of the SEL software used for this are SEL AcSELerator QuickSet, SEL AcSELerator Architect.

2.5.1 Direct Engineering Access to SEL Reclosers, RTAC from the Control Center:

This provides the capability to access and configure the Substation RTAC, Midpoint reclosers and POI reclosers from a PC located in the Control Centre premise. This communication could re-use the communication path used for SCADA communication.

Figure 8. Direct Engineering Access from Control Center



In above figure, CC_ENG_ACCESS could communicate with RTAC, midpoint reclosers, POI recloser using Cisco IR1101 as gateway. *SCADA communication path could be re-used for Engineering Access to SEL RTAC in substation, Reclosers in (DA sites, DER site).*

The Tunnel architecture described in "Figure 8. Tunnel Architecture for SECURE bidirectional communication between SCADA and RTAC/Reclosers" is re-used for this direct engineering access from the Control Center, to enable secure access to Reclosers/RTAC from "Engineering Access-PC" in control center.

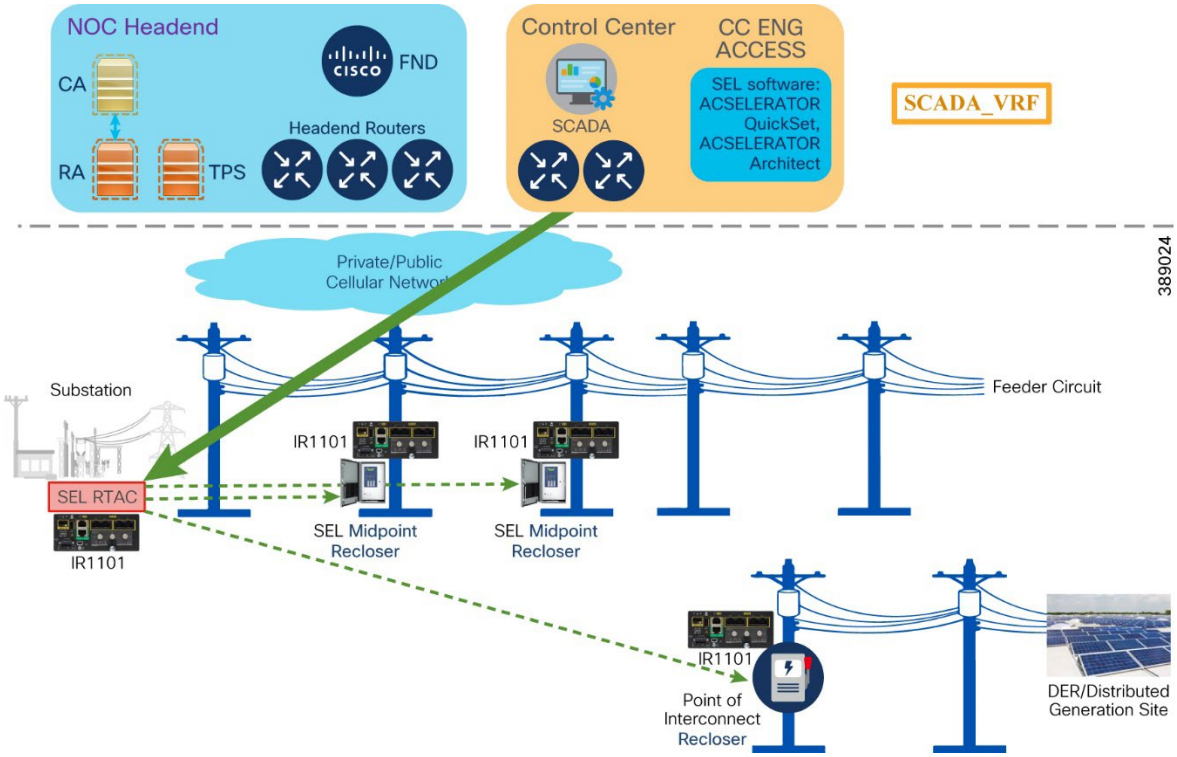
2.5.2 Engineering Access to SEL Reclosers from the Control Center using Substation RTAC as proxy:

SEL reclosers operating GOOSE could possibly limit the telnet access to just one client. In such cases, connections could be established either from control centre (or) from substation, not from both. In such cases, this approach would enable that opportunity to access the SEL reclosers from both substation (directly) and from control center (using substation proxy).

Cisco communication network provides additional way of accessing the field reclosers using substation RTAC as proxy. This is a two-step method:

1. In first step, the substation RTAC is directly accessed from the "Engineering Access PC" located in the Control Center premise. This indeed is direct engineering access to substation RTAC.
2. In second step, the Midpoint reclosers and POI reclosers could then be accessed from the RTAC connection established in the first step. This method of accessing the Midpoint reclosers and POI reclosers using substation RTAC is referred to as "Proxy Engineering Access using Substation RTAC".

Figure 9. Proxy Engineering Access via Substation RTAC



In above figure, CC_ENG_ACCESS from Control Centre could access SEL RTAC in substation using direct engineering access (by re-using the SCADA communication path). On a parallel note, the SEL RTAC from substation could communicate with the midpoint reclosers and POI recloser (as shown by the dotted arrow lines).

This communication between SEL RTAC and midpoint reclosers could be facilitated in two ways:

- Substation RTAC <-> field Recloser communication via Control centre hub routers.
- Peer to peer communication between Substation RTAC and Midpoint reclosers.

The first option requires a simple static route advertisement to facilitate routing reachability between SEL RTAC and POI/midpoint recloser via Control Centre Hub routers.

Note: Communication between SEL RTAC and POI recloser uses the first option.
The communication between SEL RTAC and midpoint reclosers could choose either option.

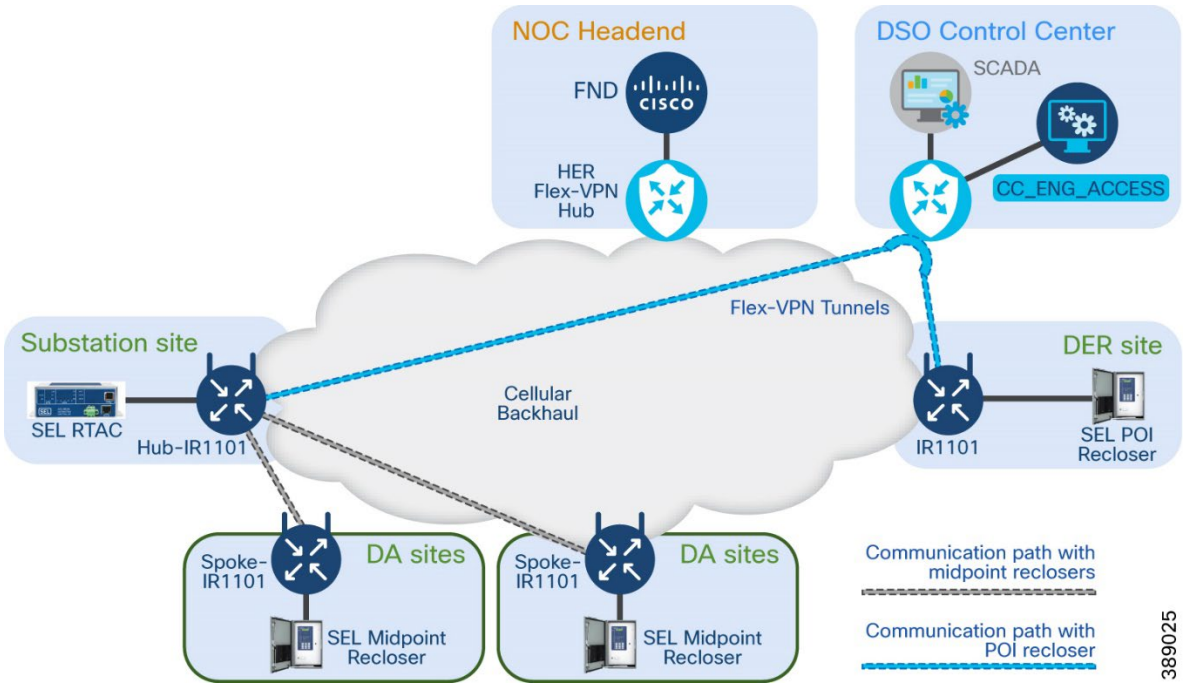
To enable peer to peer communication between substation RTAC and midpoint reclosers,

1. IR1101 associated with substation RTAC must be hosted as Proxy-Hub (say, with Virtual-Template14)
2. IR1101 associated with midpoint reclosers must be configured as Proxy-Spokes (say, with Tunnel14)

This option enables a logically connected interface (Tunnel/Virtual-Access) link between Substation-RTAC/Hub and Midpoint recloser/spokes, thus enabling direct peer to peer communication between the substation/Hub and midpoint recloser/Spokes.

The following Tunnel architecture could be used to enable engineering access to reclosers using substation RTAC as proxy.

Figure 10. Tunnel Architecture for Engineering access using substation RTAC as proxy



The Cisco IR1101 located in substation establishes direct peer to peer Tunnels (grey color as in the figure above) with Spoke-IR1101 at Midpoint recloser sites. This peer-to-peer tunnel helps the RTAC to directly communicate with the midpoint reclosers positioned behind the spoke IR1101s.

In the previous figure,

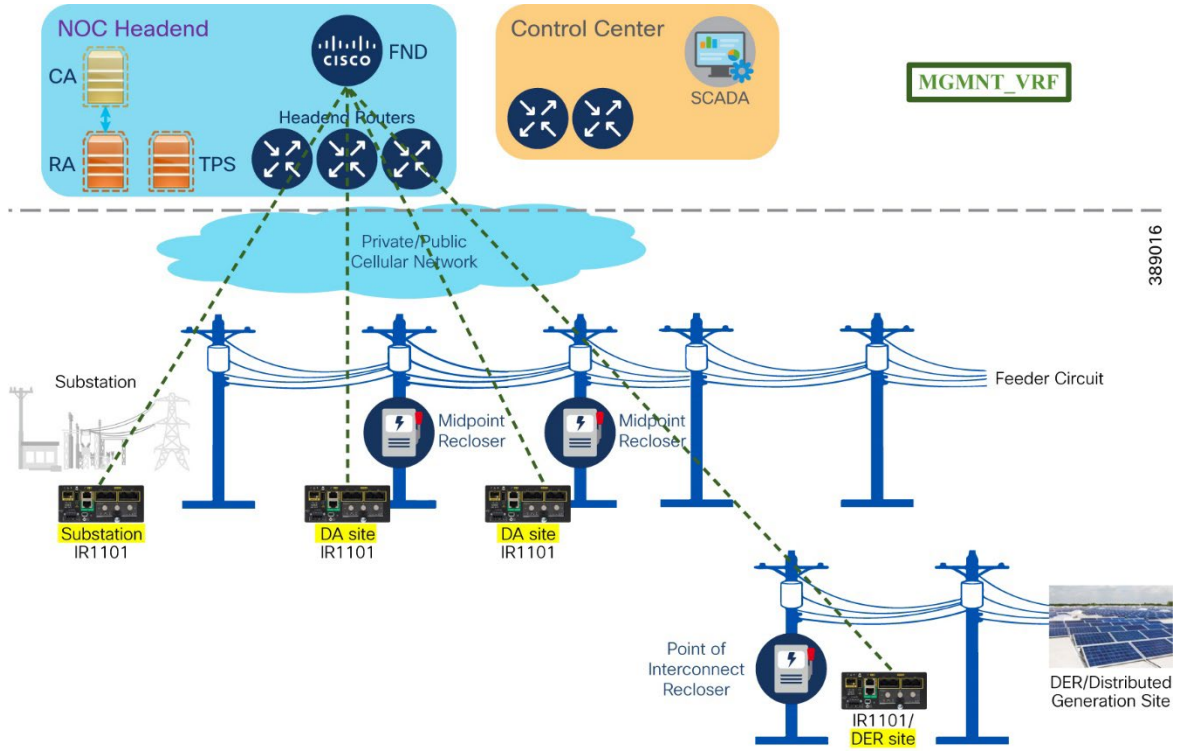
1. Substation RTAC establishes direct peer to peer communication with the midpoint reclosers (using grey path)
2. Substation RTAC establishes communication with the POI recloser via Control centre hub routers by re-using the SCADA communication (blue) path

The ENG_ACCESS_PC (located in the DSO Control Centre) can establish communication with substation RTAC. Using substation RTAC as proxy, engineering access to midpoint/POI reclosers could then be achieved.

2.6 Management of Cisco IR1101s using Field Network Director:

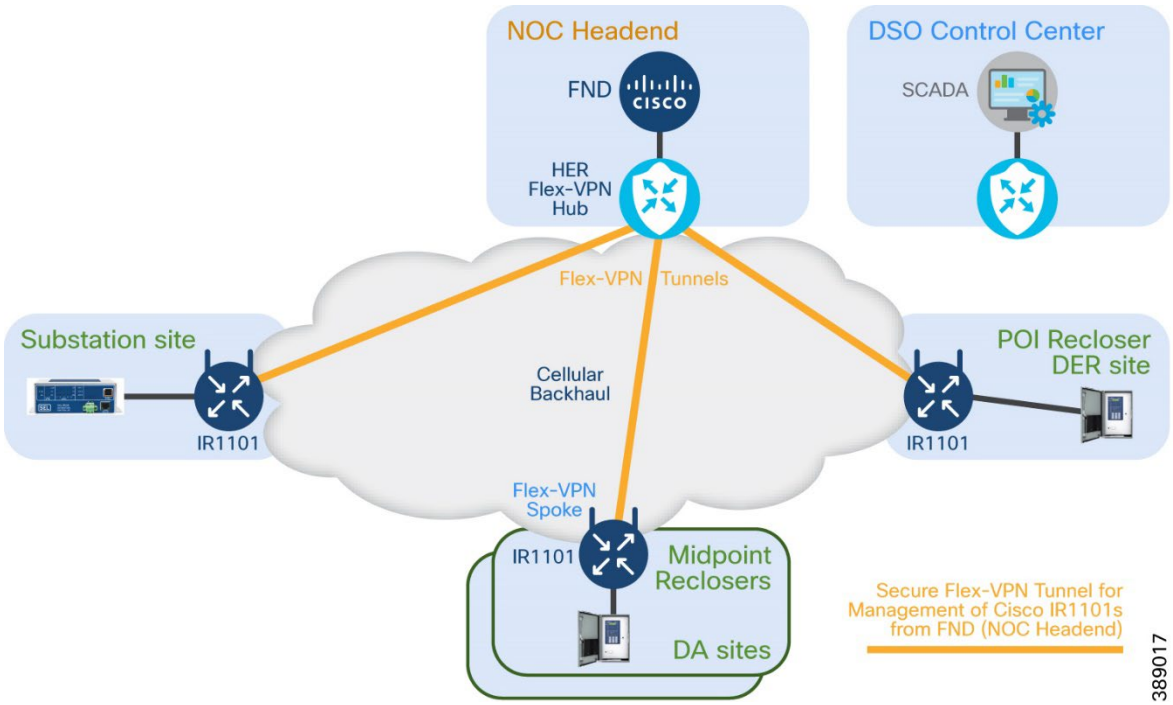
Cisco IR1101s are deployed in various roles such as substation router, DA gateways along the distribution feeder path, DER gateway in DER site, and so on. These IR1101s are managed from a network management system called Field Network Director (FND), located in NOC headend. In below diagram, Headend Routers (cluster) is used as Hub and the Cisco IR1101s positioned in Substation, DA sites and DER site acts as spokes.

Figure 11. FND manages all the IR1101s positioned in the Substation site, DA sites and DER sites.



The following Tunnel architecture would be used to enable secure communication of Cisco IR1101s with FND, hosted inside NOC Headend.

Figure 12. Tunnel Architecture for management of Cisco IR1101s from FND



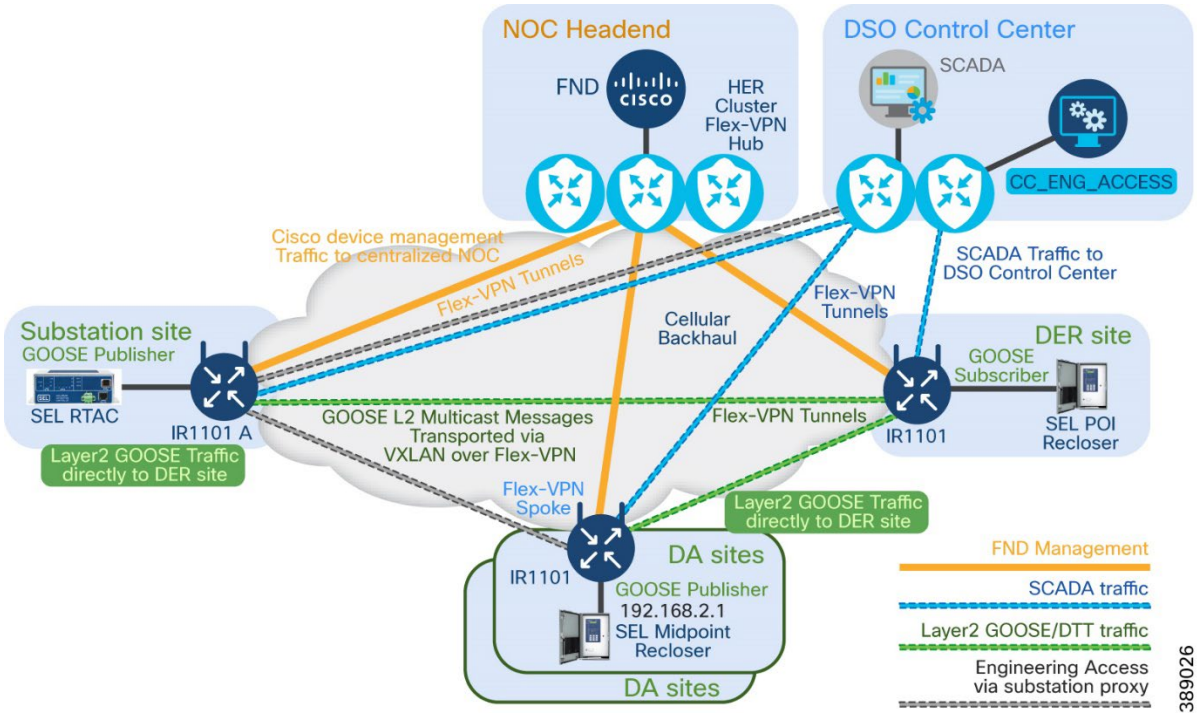
In the above figure, secure Flex-VPN communication is established between Cisco IR1101s (located in substation, DA sites, DER site) and the HER Flex-VPN Hub (located in the NOC headend). For Example, it could be Tunnel10 on IR1101 and Virtual-Template on the HER Flex-VPN hub.

On Cisco spoke-IR1101s, the Tunnel10 is configured to be part of “MGMNT_VRF”.

2.7 Combined Tunnel Architecture:

2.7.1 Combined Tunnel Architecture for DTT, SCADA, NMS & Engineering Access:

Figure 13. Combined Tunnel Architecture



The above figure captures the tunnel architecture that facilitates the service enablement and segregation of various services including management of Cisco IR1101s from FND, Direct Transfer Trip messaging between GOOSE publishing sites to DER site, SCADA communication between RTAC/reclosers and SCADA, along with engineering access to RTAC and all reclosers/IEDs.

The table below is the summary of the Tunnel information used in this architecture, with service isolation:

From	Towards NOC Head End Router Cluster	Towards Control Centre Hub Cluster	Towards DER site, for DTT	Towards Substation RTAC	Towards Midpoint Recloser1	Towards Midpoint Recloser2
Substation RTAC connected IR1101	Tunnel10 (MGMNT_VRF)	Tunnel11, Tunnel12 (SCADA_VRF)	Tunnel15 (DTT_VRF) Tunnel11 (Engineering Access)	N/A	Virtual-Template14 (Engineering Access)	Virtual-Template14 (Engineering Access)
Midpoint Recloser1 connected IR1101	Tunnel10 (MGMNT_VRF)	Tunnel11, Tunnel12 (SCADA_VRF)	Tunnel15 (DTT_VRF)	Tunnel14 (Engineering Access)	N/A	N/A
Midpoint Recloser2 connected IR1101	Tunnel10 (MGMNT_VRF)	Tunnel11, Tunnel12 (SCADA_VRF)	Tunnel15 (DTT_VRF)	Tunnel14 (Engineering Access)	N/A	N/A
POI Recloser (aka DER site) connected IR1101	Tunnel10 (MGMNT_VRF)	Tunnel11, Tunnel12 (SCADA_VRF)	N/A	Virtual-Template15 (DTT_VRF), Tunnel 11 (Engineering Access)	Virtual-Template15 (DTT_VRF)	Virtual-Template15 (DTT_VRF)

Tunnel12 is applicable for dual control center scenarios, for communication with second control center. SCADA_VRF is re-used for Engineering Access at all locations.

Example1: From substation site connected IR1101, Tunnel10 (part of MGMNT_VRF) is used towards NOC HER Cluster.

Example2: From Midpoint Recloser1 connected IR1101,

- Tunnel15 (part of DTT_VRF) is used towards DER site.
- Tunnel11 (part of SCADA_VRF) is used towards Control Centre hub routers.

Example3: From Midpoint Recloser2 connected IR1101,

- Tunnel10 (part of MGMNT_VRF) is used towards NOC HER cluster
- Tunnel14 (part of SCADA_VRF) is used towards Substation RTAC for Engineering Access.
- Tunnel15 (part of DTT_VRF) is used towards DER site.

Example4: From DER site connected IR1101,

- Tunnel10 (part of MGMNT_VRF) is used towards NOC HER cluster
- Tunnel11 (part of SCADA_VRF) is used towards Control Centre hub routers and re-used for Engineering access
- Virtual-Template15 (part of DTT_VRF) is used towards Substation RTAC, Midpoint reclosers 1 & 2.

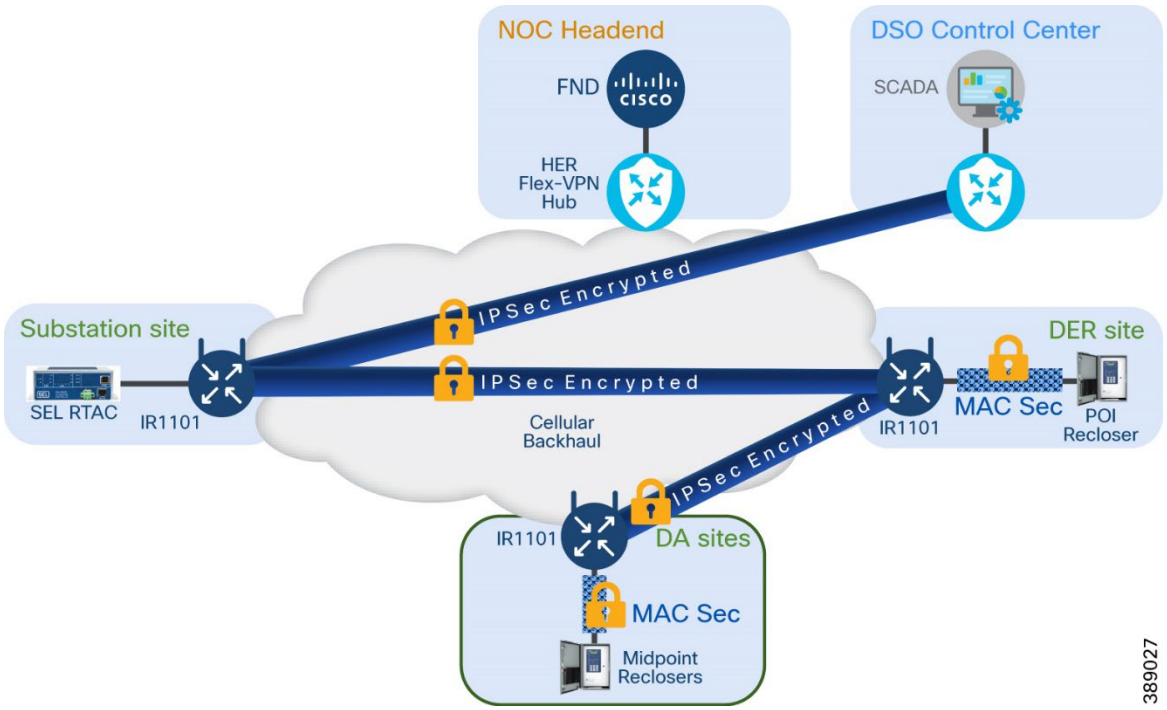
3 Securing the "Last Foot" with Layer2 MACSEC:

The last mile of connectivity between the Reclosers/IEDs and the Cisco IR1101 would usually be cleartext. This leaves room for data manipulation, malicious data injection, attacks, potential credential thefts, etc., The last point of connectivity being cleartext is vulnerable and prone to attacks from malicious actors, who might install man in the middle device that could spoof/eavesdrop/tamper or even inject malicious/manipulated data, leading to undesired consequence in the power grid. A few examples are:

- Sending tampered/manipulated data (aka data spoofing) to the control Centre master. This compromises on the authenticity and integrity of the data received at the control center. This will be a bigger concern for utility customers.
- Cleartext communication is vulnerable to credential thefts. Engineering access would require credentials. If such credentials are exchanged in clear text in the last foot, they would be exposed to the man in the middle actor, with malicious intention.
- Using the stolen credentials, the malicious actor could craft an Open message and cause a power outage, across portions or entire electrical grid.
- Using the stolen credentials, the malicious actor could craft a Close message and energize the electrical grid that was de-energized for maintenance work. **This could risk the lives of field workers, working on the de-energized electrical grid**.

A secure architecture should consider the data security and data integrity end to end, starting from the last mile IED till the Control center or another last mile IED. **Securing the "Last Foot" could be achieved with the help of Layer2 MACSEC between the IED and the Cisco IR1101 gateways. Vendor IEDs must be capable of supporting MACSEC. The SEL 651R recloser is such a device that supports MACSEC and has been validated with the Cisco IR1101 switchports.**

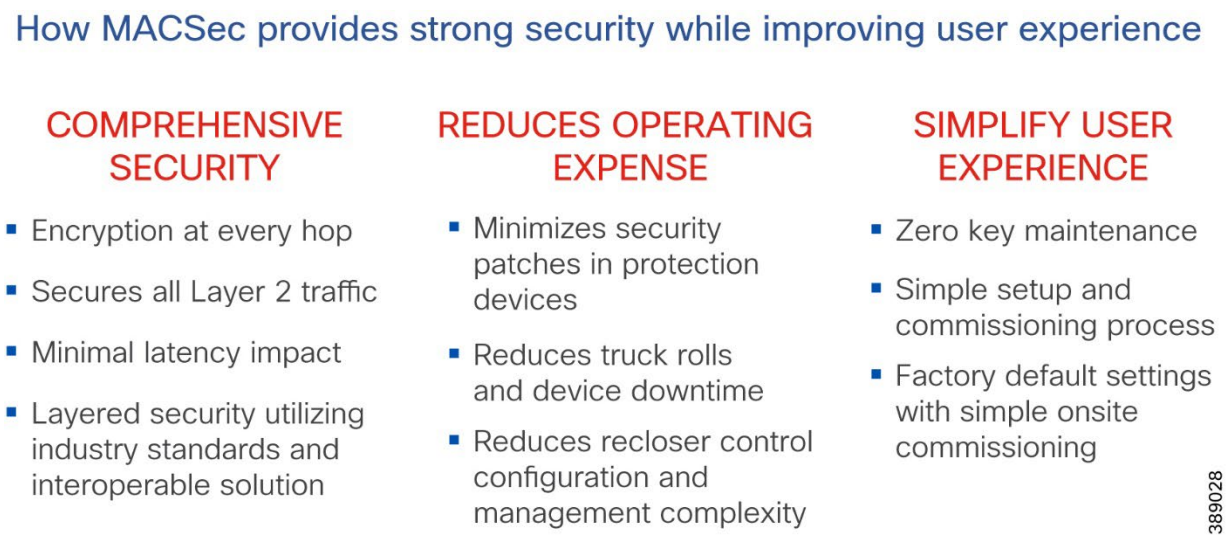
Figure 14. Securing the "Last Foot" connection between Cisco IR1101 and the IEDs with MACSEC



MACSec implementation on IEDs when paired with a Cisco IR1101 manages MACSec for the "last foot" ethernet connection. Cisco IR1101 also acts as the MACSec AES Key server. Cisco IR1101 secures the ethernet based IED connectivity with MACSEC encryption and protects the backhaul IP traffic with FLEX-VPN secure tunnel.

For more details about securing the last point of connection, please refer to "Securing the "Last Foot" in Distribution Automation White Paper".

Figure 15. How MACSEC provides strong security while improving user experience



4 IMPLEMENTATION SECTION

4.1 Direct Transfer Trip (DTT) use case:

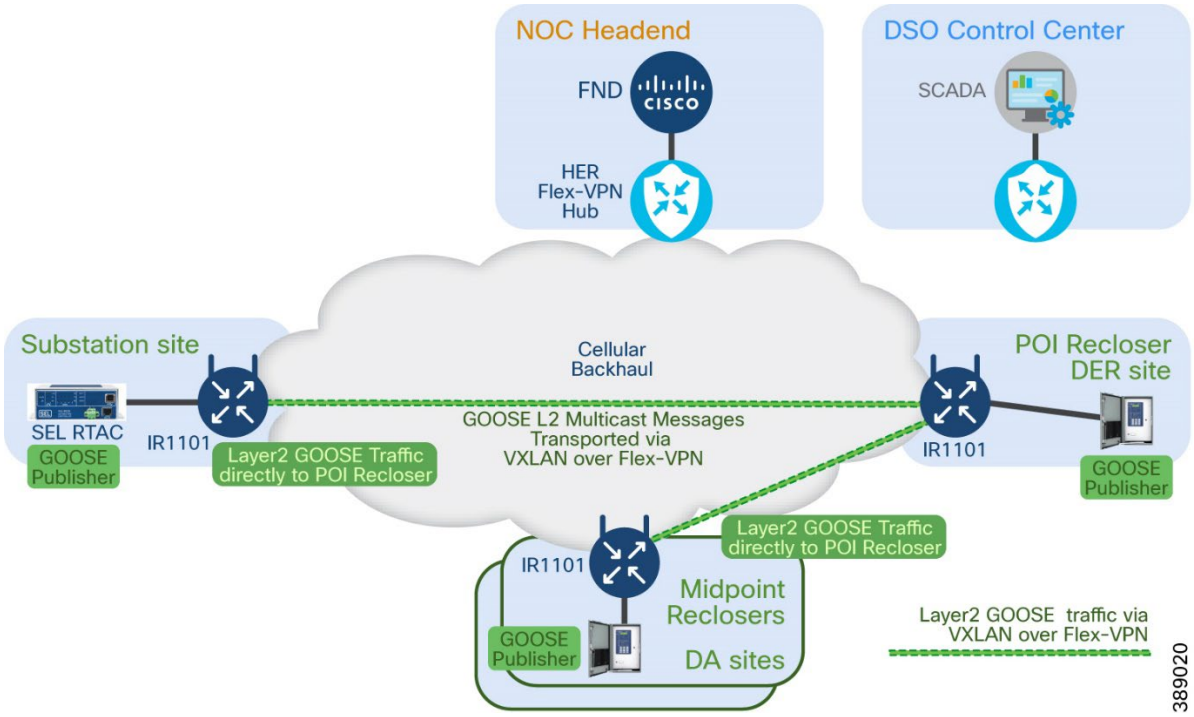
4.1.1 Direct Transfer Trip message to POI recloser using Layer2 GOOSE

SEL 3530 on substation site and SEL 651RA on DA site will publish the DTT L2 GOOSE message to SEL 651RA on DER site which is acting like Subscriber.

Time synchronization is required for the Direct Transfer Trip use case. SEL devices like the SEL RTAC3530 and SEL recloser controller 651RA times are synchronized using the IRIG-B time source.

Network Diagram

Figure 16. Solution Topology



Physical Connectivity between SEL IEDs and Cisco IIOT Gateway IR1101

Reclosers & RTAC	Reclosers & RTAC Interface	Cisco Gateway IR1101	Cisco Gateway IR1101 Interface
Substation RTAC 3530	Ethernet Port 5A	Substation IR1101	Fast Ethernet 0/0/4
POI Recloser 651RA	Ethernet Port 5A	POI IR1101	Fast Ethernet 0/0/4
Midpoint Recloser 651 RA	Ethernet Port 5A	Midpoint IR1101	Fast Ethernet 0/0/4

Note: Although Fast Ethernet 0/0/4 was used for validation, the Customer is free to use any of the four Fast Ethernet ports available on the Cisco IR1101.

4.1.2 Layer2 Extension over Layer3 Cellular Network using VXLAN over Flex VPN

For DTT traffic, all Reclosers and RTAC are provisioned with VLAN 651. The following configuration files have been provided by the SEL team for validation purposes.

- Substation RTAC 3530: Cisco DTT Testing_RTU_3530_R151_VLAN651
- Recloser 651RA: Cisco_DTT_Testing_VLAN651

For DTT traffic all the Reclosers and RTAC are provisioned with VLAN 651. The following configuration files are provided by the SEL team for validation purposes.

- Substation RTAC 3530: Cisco DTT Testing_RTU_3530_R151_VLAN651
- Recloser 651RA: Cisco_DTT_Testing_VLAN651

SEL Applications

- AcSELerator Architect: For pushing the above configuration files
- AcSELerator QuickSet: For verifying DTT trafic

Transport of DTT traffic to the different sites which are located far away, leverage VXLAN over the L3 Network. With VXLAN, the overlay is a layer 2 Ethernet network. The underlay network is a layer 3 IP network.

VXLAN is an extension to the Layer 2 VLAN. It was designed to provide the same VLAN functionality with greater extensibility and flexibility.

Following is the configuration provided for VXLAN.

The interfaces connected to SEL devices are configured with IEEE 802.1q trunk port to allow Layer2 communication using 802.1q VLAN tagged frames and Layer3 communication over Native VLAN.

SEL Applications

- AcSELerator Architect: For pushing the above configuration files
- AcSELerator QuickSet: For verifying DTT trafic

For transport of DTT traffic to the different sites which are located far away, leverage VXLAN over the L3 Network. With VXLAN, the overlay is a layer 2 Ethernet network. The underlay network is a layer 3 IP network.

VXLAN is an extension to the Layer 2 VLAN. It was designed to provide the same VLAN functionality with greater extensibility and flexibility.

Following is the configuration provided for VXLAN.

The interface connected to SEL devices are configured with IEEE 802.1q trunk port to allow Layer2 communication using 802.1q VLAN tagged frames and Layer3 communication over Native VLAN.

4.1.1.4 Substation IR1101 configuration

This section describes the configuration of VXLAN and its related commands.

- The source interface must be a loopback interface that is configured on the IR1101 with a valid /32 IP address. The devices in the transport network and the remote NVE must know this /32 IP address.
- VLAN 651 is created for the DTT traffic to communicate.

VXLAN overlay interface (NVE) that terminates VXLAN tunnel:

- Bridge Domain is said to be a broadcast domain that represents the scope of L2 network. Virtual Network Identifier associate with the bridge domain. VLAN are also members of this bridge domain.
- Protocol Independent Multicast (PIM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- For VXLAN underlay network tunnel 15 is being used to transport DTT traffic

The same configuration is applied across all sites.

```
interface Loopback15
 description used for establishing PIM neighborship between the Cisco IR1101s
 ip address 192.168.1.22 255.255.255.255
 ip pim sparse-mode
 ip nat outside
!
interface Vlan651
description Direct Transfer Trip message exchanged over IEEE 802.1q VLAN 651
 no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
 !
interface nve1
 no ip address
 source-interface Loopback15
 member vni 5555 mcast-group 239.1.1.1
!
bridge-domain 1
 member vni 5555
 member Vlan651 service-instance 1

interface FastEthernet0/0/4
 description connected to Substation-SEL3530
 switchport trunk allowed vlan 1,651
 switchport mode trunk
!
```

```
! 192.168.1.20 is the Loopback15 interface IP address of DER site IR1101
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir

interface Tunnel15
 description Tunnel interface connects to DER site IR1101
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <IPv6 address of POI Recloser IR1101>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
```

4.1.1.5 Midpoint recloser site IR1101 configuration*:*

```
interface Loopback15
 description used for establishing PIM neighborship between the Cisco IR1101s
 ip address 192.168.1.19 255.255.255.255
 ip pim sparse-mode
 ip nat outside
!
interface Vlan651
 description Direct Transfer Trip message exchanged over IEEE 802.1q VLAN 651
 no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
 !
interface nve1
 no ip address
 source-interface Loopback15
 member vni 5555 mcast-group 239.1.1.1
!
bridge-domain 1
 member vni 5555
 member Vlan651 service-instance 1

interface FastEthernet0/0/4
 description connected to MidpointRecloser-SEL651RA
 switchport trunk allowed vlan 1,651
 switchport mode trunk
!
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir

interface Tunnel15
 description to Substation-IR1101
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
```

```
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <IPv6 address of POI Recloser IR1101>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
```

4.1.1.6 POI recloser site IR1101 configuration:

```
interface Loopback15
description used for establishing PIM neighborship between the Cisco IR1101s
 ip address 192.168.1.20 255.255.255.255
 ip pim sparse-mode
 ip nat outside
!
interface Vlan651
description Direct Transfer Trip message exchanged over IEEE 802.1q VLAN 651
 no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
 !
interface nve1
 no ip address
 source-interface Loopback15
 member vni 5555 mcast-group 239.1.1.1
!
bridge-domain 1
 member vni 5555
 member Vlan651 service-instance 1

interface FastEthernet0/0/4
 description connected to POIRecloser-SEL651RA
 switchport trunk allowed vlan 1,651
 switchport mode trunk
!
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir

interface Virtual-Template15 type tunnel
 description used to terminate Tunnel15 from Substation-IR1101 and DA-site IR1101s
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip mtu 1300
 ip pim sparse-mode
 ip tcp adjust-mss 1260
 nat64 enable
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
end
```

4.1.1.7 SEL 651-RA recloser & SEL 3530 RTAC configuration:

Refer to SEL documentation for the SEL 651-RA recloser & SEL 3530 RTAC configuration.

4.1.1.8 DTT Operation & Validation*:*

- "Direct Transfer Trip" is sent by any of the GOOSE publishers and always received by a GOOSE subscriber.
- The SEL 3530 substation RTAC or midpoint recloser site SEL 651RA are GOOSE publishers, also known as a DTT transmitter.
- Point Of Interconnect site SEL 651RA is the GOOSE subscriber, also known as DTT receiver
- "Direct Transfer Trip" being a unidirectional layer2 GOOSE message can be checked for the successful reception only at the receiving side (POI side) SEL 651RA

Time synchronization is must for the Direct Transfer Trip use case. SEL devices like SEL RTAC 3530, SEL recloser are used.

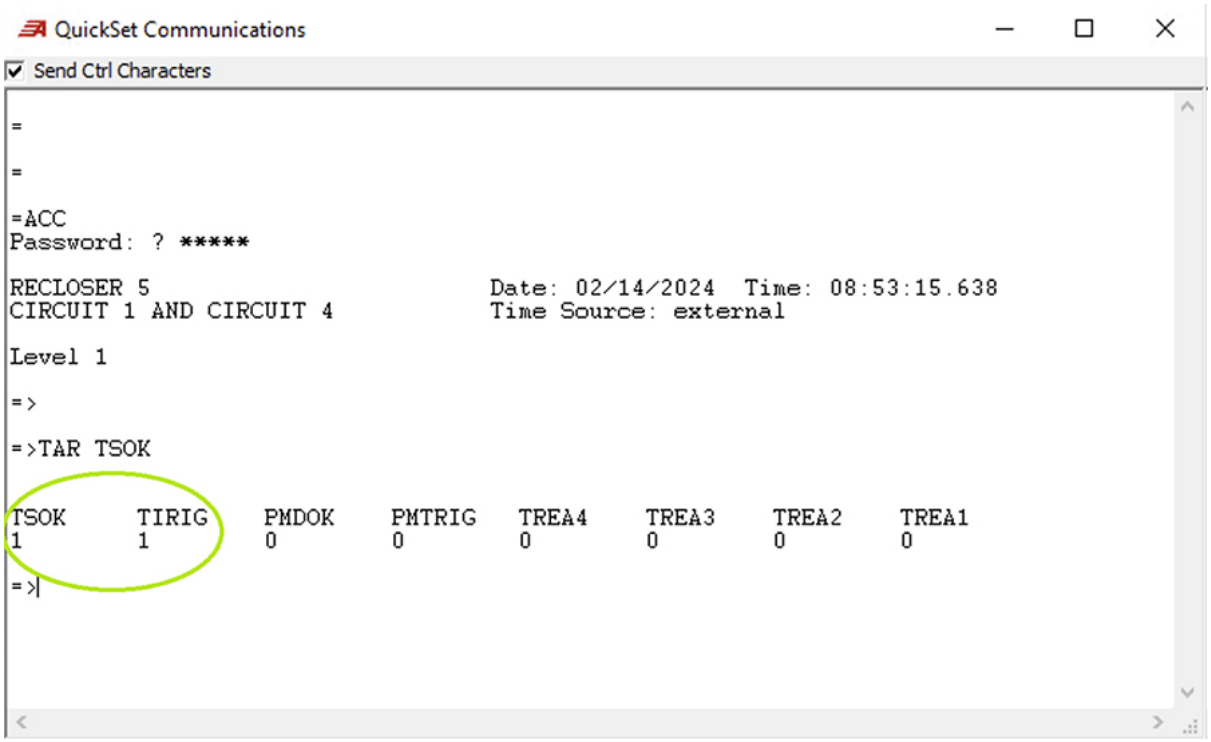
Step-1: Login from the Control Center SEL Accelerator Application using Telnet to the POI Recloser 651RA.

Step-2: Issue the first auth level credential, received from the SEL support team.

Step-3: Issue "TAR TSOK" to verify IRIG-B time synchronization showing in the following screenshot.

Step-4: Here the TSOK and TIRIG values should show as 1.

Figure 17. SEL 651RA IRIG-B Output



Step-5: Issue “GOOSE” command on command prompt.

Step-6: Output will show as in below screenshot.

Step-7: Here TTL value will be same for RTAC 3530 and Reclosers 651RA.

Step-8: Code value will be blank. If it shows “expired” then GOOSE traffic failed.

Figure 18. SEL 651RA GOOSE Output

```
=>id

"FID=SEL-651RA-R106-V0-Z006001-D20230130","0933"
"BFID=SLBT-3CF1-R300-V0-Z100100-D20150729","098A"
"CID=7A5C","026D"
"DEVID=SETTINGS","048A"
"DEVCODE=82","0311"
"PARTNO=0651RA01XAAXAE2A2XXXXXXX","0906"
"SERIALNO=5201670118","0509"
"CONFIG=11242200","03EF"
"SPECIAL=01111","03A2"
"iedName=POI","0448"
"type=SEL_651RA","04E1"
"configVersion=ICD-651RA-R101-V0-Z102005-D20190131","0DAA"

=>GOOSE

GOOSE Transmit Status

 MultiCastAddr    Ptag:Vlan AppID  StNum       SqNum       TTL     Code
-------------------------------------------------------------------------------
No GOOSE publications configured

GOOSE Receive Status

 MultiCastAddr    Ptag:Vlan AppID  StNum       SqNum       TTL     Code
-------------------------------------------------------------------------------
DHN_RTUCFG/LLN0$GO$BESS_DTT
 01-0C-CD-01-00-01 7:651    1       21          81          2000
 Data Set: DHN_RTUCFG/LLN0$RTAC_DTT

MPR1CFG/LLN0$GO$MPR1_BKR_Status
 01-0C-CD-01-00-02 7:651    4098    21          238         2000
 Data Set: MPR1CFG/LLN0$BESS_DTT

MPR2CFG/LLN0$GO$MPR2_BKR_Status
 01-0C-CD-01-00-03 7:651    4099    21          246         2000
 Data Set: MPR2CFG/LLN0$BESS_DTT


=>
```

4.1.3 DTT Service Isolation from SCADA and other services

This section describes the isolation of DTT traffic (L2 GOOSE) from other traffic like SCADA, Engineering Access, and NMS Access traffic.

To segregate DTT traffic (L2 GOOSE), SCADA, Engineering Access, NMS Access traffic several service specific VRF, Tunnels, Virtual-Templates, VLANs and Interfaces created.

Traffic _types	VRF	Loopback	Virtual-Template	Tunnel	VLAN used on IED connecting interface of Cisco IR1101
DTT Traffic	DTT_VRF	Loopback15	Virtual-Template15	Tunnel15	VLAN651
SCADA Traffic	SCADA_VRF	Loopback31		Tunnel11	VLAN1
Eng. Access Traffic	SCADA_VRF	Loopback31	Virtual-Template14	Tunnel14	VLAN1
NMS Traffic	NMS_VRF	Loopback0		Tunnel10	N/A

4.1.2.1 DTT Traffic Segregation on Substation IR1101

Direct Transfer Trip service related communication is isolated from the other services (like SCADA, Engineering Access, NMS communication) with the help of VRF named “DTT_VRF”.

The following configuration shows how “DTT_VRF” is defined and how the interfaces participating in “Direct Transfer Trip” use case are isolated under it.

Interfaces participating in this DTT service are Tunnel15, Vlan651, Loopback15.
Multicast routing must also be enabled for VRF.

```
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan651
 vrf forwarding DTT_VRF

interface Tunnel15
 vrf forwarding DTT_VRF

interface Loopback15
 vrf forwarding DTT_VRF

ip multicast-routing vrf DTT_VRF distributed

ip multicast vrf DTT_VRF auto-enable
```

DTT Traffic Segregation on POI IR1101

```
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan651
 vrf forwarding DTT_VRF

interface Virtual-Template15
 vrf forwarding DTT_VRF

interface Loopback15
 vrf forwarding DTT_VRF


ip multicast-routing vrf DTT_VRF distributed
```

```
ip multicast vrf DTT_VRF auto-enable
```

DTT Traffic Segregation on Midpoint IR1101

```
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan651
 vrf forwarding DTT_VRF

interface Tunnel15
 vrf forwarding DTT_VRF

interface Loopback15
 vrf forwarding DTT_VRF

ip multicast-routing vrf DTT_VRF distributed

ip multicast vrf DTT_VRF auto-enable
```

SCADA/Engineering Access Traffic Segregation on Substation IR1101

SCADA traffic or Transport of Engineering Access traffic is isolated from DTT traffic with the help of VRF named “SCADA_VRF”
Direct Transfer Trip service-related communication is isolated from the other services (like SCADA, Engineering Access, NMS communication) with the help of VRF named “DTT_VRF”.

Below configuration shows how “SCADA_VRF” is defined and how the interfaces participating in “SCADA/Engineering Access” use case are isolated under it.

Interfaces participating in this SCADA/Engineering Access service are Tunnel11, Vlan1, Loopback31.
Multicast routing must also be enabled for VRF.

```
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan1
 vrf forwarding SCADA_VRF

interface Tunnel11
 vrf forwarding SCADA _VRF

interface Virtual-Template14
```

```
 vrf forwarding SCADA _VRF


interface Loopback31
 vrf forwarding SCADA _VRF


ip multicast-routing vrf SCADA_VRF distributed

ip multicast vrf SCADA_VRF auto-enable
```

SCADA/Eng. Traffic Segregation on POI IR1101

```
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan1
 vrf forwarding SCADA_VRF

interface Tunnel11
 vrf forwarding SCADA _VRF


interface Loopback31
 vrf forwarding SCADA _VRF

ip multicast-routing vrf SCADA_VRF distributed

ip multicast vrf SCADA_VRF auto-enable
```

SCADA/Eng. Traffic Segregation on Midpoint IR1101

```
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan600
 vrf forwarding SCADA_VRF

interface Tunnel11
 vrf forwarding SCADA _VRF


interface Loopback31
 vrf forwarding SCADA _VRF

ip multicast-routing vrf SCADA_VRF distributed

ip multicast vrf SCADA_VRF auto-enable
```

SCADA/Eng. Traffic Segregation on Midpoint IR1101

```
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

interface Vlan600
 vrf forwarding SCADA_VRF

interface Tunnel11
 vrf forwarding SCADA _VRF


interface Loopback31
 vrf forwarding SCADA _VRF

ip multicast-routing vrf SCADA_VRF distributed

ip multicast vrf SCADA_VRF auto-enable
```

NMS Traffic Segregation on Substation IR1101

NMS traffic is isolated from DTT, SCADA traffic with the help of VRF named “NMS_VRF” Direct Transfer Trip service-related communication is isolated from the other services (like SCADA, Engineering Access, NMS communication) with the help of VRF named “DTT_VRF”.

Below configuration shows how “NMS_VRF” is defined and how the interfaces participating in “NMS Access” use case are isolated under it.

Interfaces participating in this NMS Access service are Tunnel10, Loopback0.

```
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family


interface Tunnel10        (For NMS Traffic)
 vrf forwarding NMS _VRF

interface Loopback0
 vrf forwarding NMS _VRF
```

4.2 SCADA use case

4.2.1 SCADA communication between Control Centre and Reclosers/IEDs

4.2.1.1 *Control Center Router configuration*

This section captures the configuration snippets of the Control Center Headend router where secure tunnels from substation router, DA router, and DER routers are terminated. These are the south facing gateways for all the control center components.

The GigabitEthernet Interface used for south bound communication for all the secured tunnels from substation router, DA site router and DER site router.

```
interface GigabitEthernet3
description FAR_NW_Southbound
mtu 1600
ip nat outside
negotiation auto
ipv6 address 2001:420:5430:34::28/64
ipv6 enable
ipv6 nd reachable-time 1800000
ipv6 nd cache expire 65536 refresh
ipv6 nd nud retry 3 1000 5
no mop enabled
no mop sysid
```

The virtual-template used for terminating all the secured tunnels from substation router, DA site router and DER site router.

```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1456
ip tcp adjust-mss 1260
nat64 enable
ipv6 unnumbered Loopback0
ipv6 enable
ipv6 mtu 1500
ipv6 tcp adjust-mss 1140
tunnel source GigabitEthernet3
tunnel mode gre ipv6
tunnel path-mtu-discovery
tunnel protection ipsec profile FlexVPN_IPsec_Profile
```

This section describes the configuration required on substation IR1101 for SCADA Outstation to communicate with SCADA Master on Control center and vice versa.

IP address of Loopback31 is used as service access IP by Control Centre to communicate with SCADA Outstation

Tunnel interface (Tunnel11) used for the secured communication purpose with Control Centre

The VLAN used (VLAN1) to separate SCADA/Eng. Traffic from other traffic (DTT & NMS Traffic)

Network Address Translation (NAT) is used with service access IP to provide multiple network/port based specific services like SCADA, Eng. Access (Telnet, FTP, HTTP).

For complete configuration please refer to the Appendix.

```
interface Loopback31
 Description Overlay IP service access IP
 vrf forwarding SCADA_VRF
 ip address 172.31.31.10 255.255.255.255
 ip nat outside
!

interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <IPv6 address of the Control Centre – HER Cluster>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!


interface Vlan1
 description IPv6 traffic to docker container
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address 2001:DB8:ABCD:EF:xx::xx/64
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255

ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf SCADA_VRF
```

4.2.1.2 *Midpoint recloser site IR1101 configuration*

```
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address 172.31.31.12 255.255.255.255
 ip nat outside
!

interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
```

```
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <IPv6 address of the Control Centre – HER Cluster>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!

interface Vlan1
 description IPv6 traffic to docker container
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address 2001:DB8:ABCD:EF:1221::1/64
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255

ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf SCADA_VRF
```

4.2.1.3 *POI recloser site IR1101 configuration*

```
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address 172.31.31.11 255.255.255.255
 ip nat outside
!

interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <IPv6 address of the Control Centre – HER Cluster>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!

interface Vlan600
 description IPv6 traffic to docker container
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address 2001:DB8:ABCD:EF:xx::xx/64
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255

ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf SCADA_VRF
```

4.2.2 SCADA IP connectivity of SEL Recloser/RTAC via Cisco IR1101

This section corresponds to design section “IP connectivity of SEL Recloser/RTAC via Cisco IR1101”. The following section captures the configurations required to enable the IP connectivity to the SEL recloser/RTAC using Cisco IR1101.

As an example, SCADA service is typically used on ports 20000. The following section walks through the configuration required to enable SCADA access.

The following configuration enables bi-directional access to the recloser controller/RTAC device with the help of service Access IP and port number combination. “Service Access IP” is the IP address configured on the Loopback 31 interface of Cisco IR1101.

It is worth noting that, all the devices (RTAC or recloser controllers) can be configured with same IP address of 192.168.0.2. This simplifies the configuration for the field technician. The same local IP of 192.168.0.2 is identified to the outside world using “Service Access IP”.

```
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
```

Assuming Recloser controller and RTAC were configured with IP address of 192.168.0.2 (belong to 192.168.0.0/24 subnet), the devices are identified using access list named “IED_NW”.

```
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
```

Devices matching “IED_NW” access list are represented to the outside world with Loopback 31 interface IP (Service Access IP) under SCADA_VRF.

```
ip nat inside source static tcp 192.168.0.2 23 interface Loopback31 20000 vrf SCADA_VRF
```

The service running on the device is uniquely identified using combination of “Service Access IP” and unique port number.

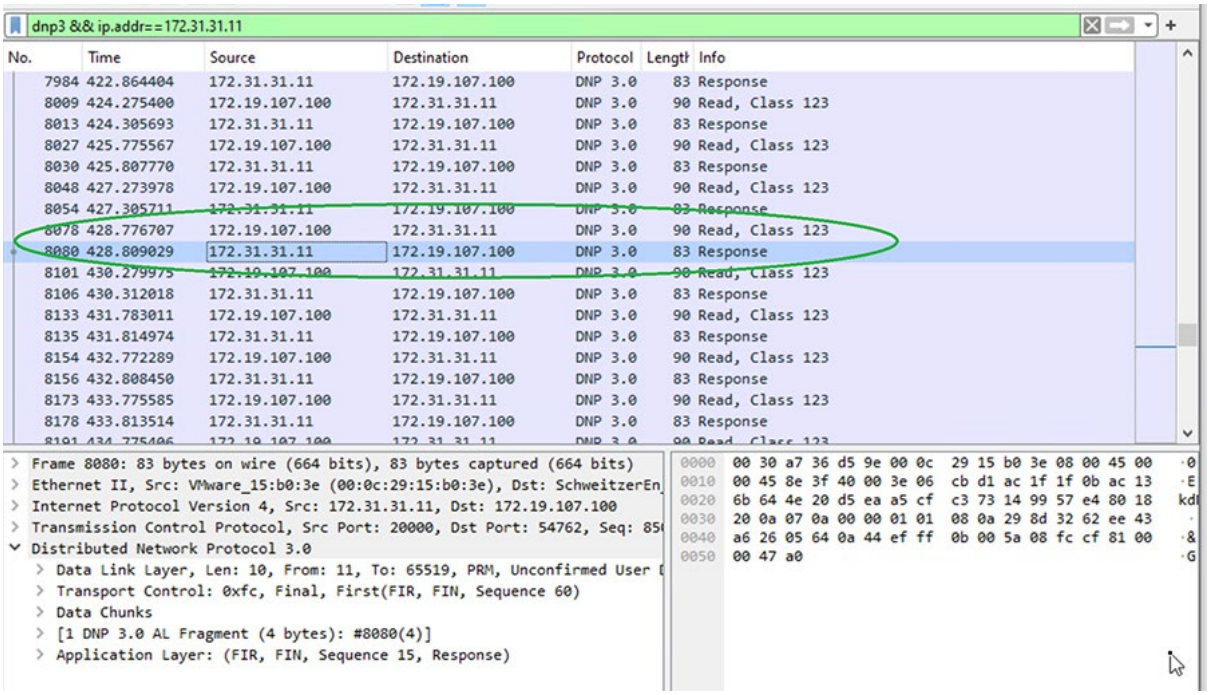
4.2.2 SCADA Operation & Validation

This section explains about how SCADA Control Center DEL3505 read/write and receives SCADA messages from substation SEL 3530 RTAC, SEL 651RA on POI and Midpoint reclosers.

1. Web based login to Control Center SEL 3505 with credentials.
2. Go to interface and capture the packet.
3. Open the packet capture, we can see all the SCADA traffic from all the RTAC & Reclosers happening successfully.

The following screenshot shows for POI Recloser 651RA DNP3 SCADA communication successfully. READ operation from Control Center (172.19.107.100) to Recloser Controller 651RA (172.31.31.11) with RESPONSE from Recloser Controller 651RA (172.31.31.11) to Control Center (172.19.107.100) was successful.

Figure 19. SCADA DNP3 IP Packet Capture at the Control Center



4.3 Engineering Access to SEL Reclosers, RTACs

4.3.1 Direct Engineering Access to SEL Reclosers, RTAC from the Control Center

The SEL Reclosers and RTAC 3530 could be accessed remotely from the control center by re-using the communication network enabled for SCADA communication.

4.3.1.1 Substation IR1101 configuration

This section re-uses the SCADA configuration captured under "4.2.1.1 *Substation IR1101 configuration.* No further configuration is required for this direct engineering access use case. If the SEL recloser controller permits only one telnet connection, in such cases connection could be made either from Substation proxy or from Control center.

Please refer to the 4.2.1.1 section as this Engineering Access is same configuration as SCADA communication.

For Engineering Access communication with Midpoint Reclosers, virtual-templates 14 has been used to create tunnels between substation IR1101 and Midpoint IR1101.
This substation IR1101 will act as proxy to access Midpoint recloser controllers.
This configuration is for proxy engineering access. Tunnel11 is used for communicating with Control Center and Virtual-template14 is used for connecting to midpoint recloser site gateways.

Configuration that follows is for the substation IR1101.

```
interface Virtual-Template14 type tunnel
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip mtu 1300
 ip pim sparse-mode
 ip tcp adjust-mss 1260
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
end
```

4.3.1.2 Midpoint recloser site IR1101 configuration

Refer to the 4.2.1.2 section because this Engineering Access comes with same config as SCADA communication.

4.3.1.3 POI recloser site IR1101 configuration

This section corresponds to the design section “IP connectivity of SEL Recloser/RTAC via Cisco IR1101”. The following section captures the configurations required to enable the IP connectivity to the SEL recloser/RTAC using Cisco IR1101. The device could be accessed from anywhere (Control Center premise or Substation premise).

As an example, Engineering Access service is typically accessed on ports 23 (telnet) and port 80 (http). The following section walks through the configuration required to enable access to these two services. Additional services could be enabled on additional port numbers if required.

The following configuration enables bi-directional access to the recloser controller/RTAC device with the help of service Access IP and port number combination. “Service Access IP” is the IP address configured on the Loopback 31 interface of Cisco IR1101.

It is worth noting that, all the devices (RTAC or recloser controllers) can be configured with same IP address of 192.168.0.2. This simplifies the configuration for the field technician. The same local IP of 192.168.0.2 is identified to the outside world using “Service Access IP”.

```
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
```

Assuming the Recloser controller and RTAC were configured with IP address of 192.168.0.2 (belong to 192.168.0.0/24 subnet), the devices are identified using access list named “IED_NW”.

```
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
```

Devices matching “IED_NW” access list are represented to the outside world with Loopback 31 interface IP (Service Access IP) under SCADA_VRF.

```
ip nat inside source static tcp 192.168.0.2 23 interface Loopback31 30023 vrf SCADA_VRF
```

Similarly, http service (port 80) of the device (configured with IP 192.168.0.2) could be accessed with combination of service Access IP (Loopback31) and port number 30080. The communication is isolated under SCADA_VRF.

4.3.2 Engineering Access Operation and Validation

This section explains the steps involved in validating Eng. Access (HTTP Access) operation for all the reclosers.

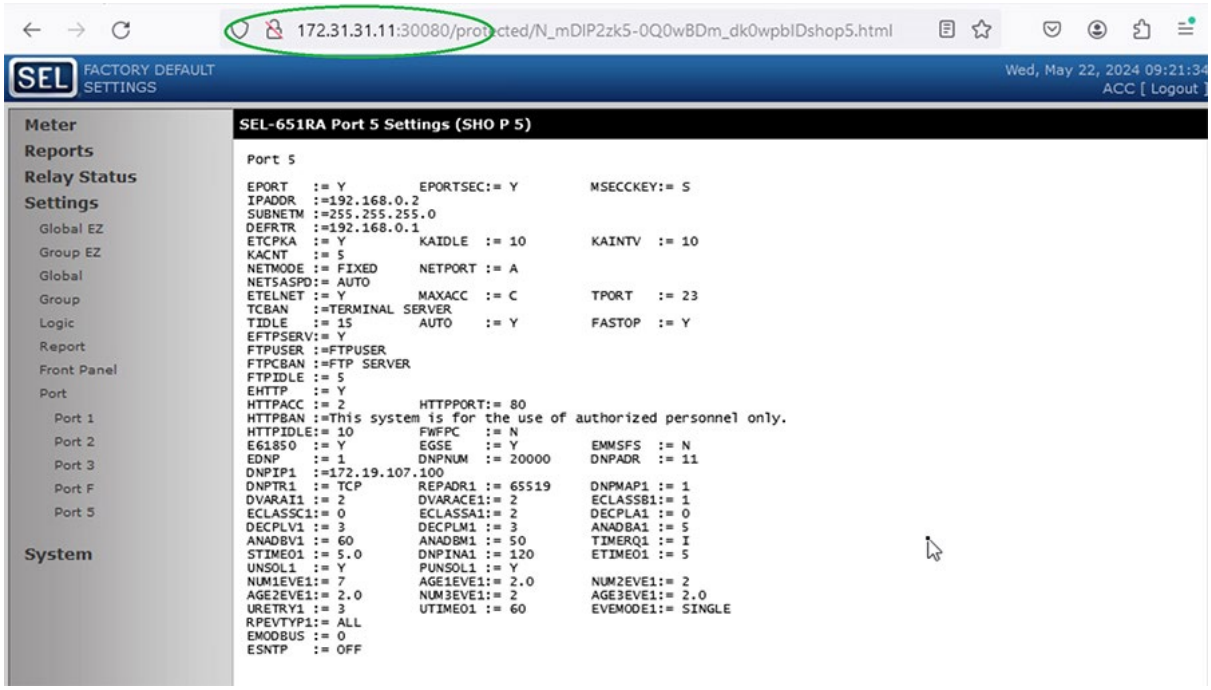
For Web Access from Control Center:

Step-1: Open web browser (Mozilla Firefox/Google Chrom) and provide the URL of the Recloser 651RA(http://172.31.31.11:30080)

Step-2: when the web page of Recloser 651RA displayed, provide the credentials and you can access the device.

The following is the screen shot of POI Recloser 651 RA web access.

Figure 20. SEL 651RA HTTP Access



This section explains the steps involved in validating Eng. Access (Telnet) operation for all the reclosers.

For Telnet Access from Control Center:

Step-1: Open the SEL Accelerator application and provide the IP and port number of the RTAC (telnet 172.31.31.10:30023)

Step-2: Once we connect successfully, we will move to auth Level 1 as “ACC”

Step-3: On Command Prompt: login as “ACC”, then Password: “OTTER”

Step-4: Provide the command “WHO”. This will show all the Reclosers PORT Number

Step-5: Use the PORT Number to login to the POI Reclosers: port 248.

The following two screenshots provide the telnet access of the POI Recloser 651RA.

Figure 21. SEL 651RA Telnet Access

4.4 Combined Tunnel Architecture for DTT, SCADA, NMS & Engineering Access:

4.4.1 Tunnel Architecture

This section describes tunnel architecture for this solution. In this solution all the IR1101 deployed over a IPv6 cellular backhaul network. FlexVPN tunnelling mechanism is used as a secured communication between IR1101 and Control Center. Multiple virtual-templates and tunnels are created for specific service types. Like different types of traffic in a solution like DTT, SCADA, Engineering, and NMS different tunnels are created to provide the services.

All the tunnels are terminated on the Control Center Head-End-Router, which is the gateway for all Control Centre devices.

4.4.2 Substation IR1101 configuration

Refer to 4.2.1.1 and 4.3.1.1 for specific tunnel configurations.

Tunnel 10 is used for NMS traffic from control center to substation IR1101.

```
interface Tunnel10
 description to FNDHE241-C8000V
 vrf forwarding NMS_VRF
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination (IPv6 address of HeadEnd Router)
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
```

4.4.3 Midpoint recloser site IR1101 configuration

Refer to 4.1.1.3 and 4.2.1.2 for specific tunnel configuration.

Tunnel 10 is used for NMS traffic from the control center to Midpoint IR1101.

```
interface Tunnel10
 description to FNDHE241-C8000V
 vrf forwarding NMS_VRF
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination (IPv6 address of HeadEnd Router)
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
```

4.4.4 POI recloser site IR1101 configuration

Refer to 4.1.1.3 and 4.2.1.2 for specific tunnel configuration.

Tunnel 10 is used for NMS traffic from control center to POI IR1101.

```
interface Tunnel10
 description to FNDHE241-C8000V
 vrf forwarding NMS_VRF
 no ip address
```

```
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination (IPv6 address of HeadEnd Router)
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
```

4.5 Securing the "Last Foot" with Layer2 MACSEC

This section provides the configuration for enablement of MACSEC authentication between IR1101 and SEL Devices.

4.5.1 Substation IR1101 configuration

Currently the SEL 3530 RTAC does not support MACSEC. The SEL 3530 RTAC MACSEC authentication is omitted.

4.5.2 Midpoint recloser site IR1101 configuration

The following is the MACSEC configuration for Midpoint Recloser IR1101.

```
key chain MyMACsecKEYchain macsec
 key 9999
  cryptographic-algorithm aes-128-cmac
  key-string 6 ZbBaUbKXiS]iAgcZWYVD\[ha]NI`DY[bRaTHbFZdR^UAgPPAg[[`V]VENBPPO\FbdR\^Q
password encryption aes
!
mka policy MyMACsecPolicy
 sak-rekey interval 300
!
interface FastEthernet0/0/4
 description connected to HUB-Midpoint_Recloser_651RA
 switchport trunk allowed vlan 1,651
 switchport mode trunk
 macsec network-link
 mka policy MyMACsecPolicy
 mka pre-shared-key key-chain MyMACsecKEYchain
```

4.5.3 POI recloser site IR1101 configuration

The following is the MACSEC configuration for POI Recloser IR1101.

```
key chain MyMACsecKEYchain macsec
 key 9999
  cryptographic-algorithm aes-128-cmac
  key-string 6 ZbBaUbKXiS]iAgcZWYVD\[ha]NI`DY[bRaTHbFZdR^UAgPPAg[[`V]VENBPPO\FbdR\^Q
password encryption aes
!
mka policy MyMACsecPolicy
```

```
 sak-rekey interval 300
!
interface FastEthernet0/0/4
 description connected to HUB-POI_Recloser_651RA
 switchport trunk allowed vlan 1,651
 switchport mode trunk
 macsec network-link
 mka policy MyMACsecPolicy
 mka pre-shared-key key-chain MyMACsecKEYchain
!
```

4.5.4 SEL recloser configuration

After the Mid-Point Recloser IR1101 & POI Recloser IR1101 configured is complete, access the 651RA terminal at level 2, and issue the MCS S command.

You will then be prompted to confirm the commissioning process, then asked to enter the key name, and then the key.

After this is complete, the 651RA will listen for the Key Server agreement attempt from the 1101, and the key negotiation/exchange begins. An example of this process follows.

```
=>>mcs s

WARNING: This command should not be issued over the Ethernet link to be
secured, unless the integrity of the cable can be verified. Failure to follow
this practice may result in compromised security.

Continue with MACsec Commissioning process (Y/N)? y

Enter Connectivity Association Key Name (CKN), with or without dashes
? 9999

WARNING: The provided CKN is shorter than 32 octets and will not be padded.
Continue (Y/N)? y

Enter Connectivity Association Key (CAK), with or without dashes
? 92d032aee88c47fbddc7c3f234c6165a

Listening for MACsec Key Agreement (MKA) Key Server Activity..

A Key Server (KS) was found at 7c:21:0e:fc:5d:01

Continue (Y/N)? y

Joining Connectivity Association......

CAK Stored Successfully
SAK Obtained Successfully from KS at 7c:21:0e:fc:5d:01
Secured Port 5

=>>
```

5 Field Network Director Templates

Cisco IR1101s are deployed in various roles such as substation router, DA gateways along the distribution feeder path, DER gateway in DER site, and so on. These IR1101s are managed from a network management system called Field Network Director (FND), located in the NOC headend.

FND is provisioned with different templates for Zero Touch Deployment (ZTD) of IR1101 on multiple sites.

- Bootstrap Template – This template consists of the configuration used to trigger the ZTD of the IR1101
- Tunnel Provisioning Template – This template consists of the configuration used to provision the secured tunnel between the IR1101 and Head End Router
- Device Configuration Template – This template consists of the configuration used to provision the basic router related config and to show the device status on FND

5.1 Appendix A: Bootstrap template – Substation IR1101

```
<#if far.isRunningIos()>

 <#-- New section to support Day 0 operation -->
 <#if isBootstrapping??>
      <#assign sublist=far.eid?split("+")[0..1]>
      <#assign pid=sublist[0]>
      <#assign sn=sublist[1]>
      <#if pid?contains("IR81") || pid?contains("IR11")>
       <#assign http_port=443>
       <#assign isRunningIosXe=true>
      <#else>
        <#assign http_port=8443>
        <#assign isRunningIosXe=false>
      </#if>

      file prompt quiet
      do mkdir flash:Archive

      service timestamps debug datetime msec
      service timestamps log datetime msec
      no service password-encryption

      <#-- Specific commands for IOS and IOS-XE based FAR -->
      <#if isRunningIosXe>
       license smart reservation
       no ip http client source-interface ${far.tunnelSrcInterface1}
      <#else>
```

```
        ntp update-calendar
        ip cef
       </#if>

       hostname FAR${sn}

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
       license boot level network-advantage
       ip domain name ipg.cisco.com
       boot system bootflash:/managed/images/ir1101-universalk9.17.09.05prd18.SPA.bin
       !boot system bootflash:/managed/images/ir1101-universalk9.17.09.03.SPA.bin
       !boot system bootflash:/ir1101-universalk9.17.06.03a.SPA.bin
       !boot system bootflash:/ir1101-universalk9.17.04.01.SPA.bin
       !boot system bootflash:/ir1101-universalk9.17.03.05.SPA.bin
       ipv6 unicast-routing
<#-- END OF SOLUTION TEAM MODIFICATION -->
       aaa new-model

       aaa authentication login default local
       aaa authorization exec default local

       clock timezone IST 5 30

       crypto key generate rsa general-keys label SSH modulus 2048
       ip ssh rsa keypair-name SSH
       ip ssh version 2
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
<#if isRunningIosXe>
         no ip domain lookup
       <#else>
         no ip domain-lookup
       </#if>
ip host ra-vm241.ipg.cisco.com <DMZ_IPv6_ADDRESS_of_REGISTRATION_AUTHORITY>
ip host tps-san.ipg.cisco.com <DMZ_IPv6_ADDRESS_of_TPS>
license boot level network-advantage

<#-- END OF SOLUTION TEAM MODIFICATION -->
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
line console 0
 exec-timeout 0 0
<#-- END OF SOLUTION TEAM MODIFICATION  -->

       ip tcp mss 1260


       crypto pki profile enrollment LDevID
        enrollment url  ${far.scepUrl}
```

```
        enrollment credential  CISCO_IDEVID_SUDI

       crypto pki trustpoint LDevID
        enrollment mode ra
        enrollment profile LDevID
        serial-number none
        fqdn none
        ip-address none
        password ''
        revocation-check none
        fingerprint ${far.caFingerprint}
<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
        auto-enroll 80 regenerate
<#-- END OF SOLUTION TEAM MODIFICATION -->

       username ${far.adminUsername} privilege 15 algorithm-type sha256 secret
${far.adminPassword}

       ntp server 162.159.200.1

       <#if far.tunnelSrcInterface1?contains("Cell") ||
far.tunnelSrcInterface1?contains("cell")>

          <#if pid?contains("IR80")>
           controller Cellular 0
            lte gps mode standalone
            lte gps nmea ip
          </#if>

          <#if pid?contains("CGR")>
           <#assign sublist=far.tunnelSrcInterface1?split(" ")[0..1]>
           <#assign slot=sublist[1]>
           no chat-script lte
           chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
           line ${slot}
            script dialer lte
            modem InOut
            no exec
            transport input all
            transport output all
          </#if>

          dialer-list 1 protocol ip permit

          <#-- Dialer watch feature is configured to force the connection to the LTE network
without waiting for any IP traffic -->
          dialer watch-list 1 ip 5.6.7.8 0.0.0.0
```

```
        dialer watch-list 1 delay route-check initial 60
        dialer watch-list 1 delay connect 1

        interface ${far.tunnelSrcInterface1}
         load-interval 30
         dialer in-band
         dialer idle-timeout 0
         <#if !isRunningIosXe>
          dialer string lte
         </#if>
         dialer-group 1
         dialer watch-group 1
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
          ipv6 enable
          ip address negotiated
<#-- END OF SOLUTION TEAM MODIFICATION -->
         no shutdown

        ip route 0.0.0.0 0.0.0.0 ${far.tunnelSrcInterface1}
        ipv6 route ::/0  ${far.tunnelSrcInterface1}

      </#if>

      cgna profile cg-nms-tunnel
       add-command show hosts | format flash:/managed/odm/cg-nms.odm
       add-command show interfaces | format flash:/managed/odm/cg-nms.odm
       add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
       add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
       add-command show version | format flash:/managed/odm/cg-nms.odm
       interval 10
       url https://tps-san.ipg.cisco.com:9120/cgna/ios/tunnel
       gzip

      cgna gzip
      no ip http server
      ip http secure-trustpoint CISCO_IDEVID_SUDI
      ip http authentication aaa login-authentication default
      ip http secure-server
      ip http secure-client-auth
      ip http secure-port ${http_port}
      ip http timeout-policy idle 600 life 86400 requests 3
      ip http client connection timeout 5
      ip http client connection retry 5

      wsma agent exec
       profile exec
```

```
        wsma agent config
         profile config

        wsma profile listener exec
         transport https path /wsma/exec

        wsma profile listener config
         transport https path /wsma/config

<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
        event manager directory user policy "flash:/managed/scripts"
        event manager policy LDevID-update.tcl type user authorization bypass
<#-- END OF SOLUTION TEAM MODIFICATION -->

        event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
        event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
        event manager environment ZTD_SCEP_Period 30
        event manager environment ZTD_SCEP_Enabled FALSE
        event manager policy no_config_replace.tcl type system authorization bypass
        event manager policy tm_ztd_scep.tcl type system authorization bypass

        event manager applet post_pnp
         event timer watchdog  time 30
         action 10.0 cli command "enable"
         action 11.0 cli command "show pnp profile | inc Active:0"
         action 12.0 regexp "Active:0.*" "$_cli_result" pnpStatus
         action 13.0 if $_regexp_result eq 1
         action 14.0 cli command "config t"
         action 15.0 cli command "no key config-key password-encrypt" pattern ".*"
         action 16.0 cli command "yes"
         action 17.0 cli command "key config-key password-encrypt ${far.adminPassword}"
         action 18.0 cli command "password encryption aes"
         action 19.0 cli command "archive"
         action 20.0 cli command "path flash:/Archive/"
         action 21.0 cli command "maximum 8"
         action 22.0 cli command "ip http client secure-trustpoint LDevID"
         action 23.0 cli command "event manager environment ZTD_SCEP_Enabled TRUE"
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
         action 23.1 cli command "no ip host tps-san.ipg.cisco.com <TPS IP>"
         action 23.2 cli command "no ip host ra-vm241.ipg.cisco.com  <RA IP>"
         action 23.3 cli command  "interface GigabitEthernet0/0/0"
         action 23.4 cli command "description shutdown by post_pnp EEM applet"
         action 23.5 cli command "shutdown"
<#-- END OF SOLUTION TEAM MODIFICATION -->
         action 24.0 cli command "no event manager applet post_pnp"
         action 80.0 cli command "do delete /force flash:express-setup-config"
         action 81.0 cli command "do copy running-config flash:express-setup-config"
```

```
        action 82.0 cli command "no file prompt quiet"
        action 90.0 end
        action 99.0 cli command "end"

       event manager applet save_certificate
        event syslog pattern "%PKI-6-CERTRET|%PKI-6-CERT_INSTALL: An ID"
        action 10.0 cli command "enable"
        action 11.0 cli command "write mem"

  <#else>

   <#if !far.runningConfig.text?contains("kron policy-list reload")>

    <#-- Add IOS configuration commands here -->

    <#-- IOS configuration to schedule a reload in 2h -->
       kron policy-list reload
          cli reload in 2:00
       kron occurrence Reload in 1 oneshot
          policy-list reload
   <#else>
       event manager applet cancel_reload
        event timer countdown time 30
        action 10.0 cli command "enable"
        action 11.0 cli command "reload cancel"
        action 12.0 cli command "conf t"
        action 13.0 cli command "no kron policy-list reload"
        action 14.0 cli command "no event manager applet cancel_reload"
        action 99.0 cli command "end"
   </#if>
  </#if>


<#else>
  ${provisioningFailed("FAR is not running IOS")}
</#if>
```

5.2 Appendix B: Bootstrap template – Midpoint recloser site IR1101

```
<#if far.isRunningIos()>

  <#-- New section to support Day 0 operation -->
  <#if isBootstrapping??>
       <#assign sublist=far.eid?split("+")[0..1]>
       <#assign pid=sublist[0]>
       <#assign sn=sublist[1]>
       <#if pid?contains("IR81") || pid?contains("IR11")>
         <#assign http_port=443>
         <#assign isRunningIosXe=true>
       <#else>
          <#assign http_port=8443>
          <#assign isRunningIosXe=false>
       </#if>

       file prompt quiet
       do mkdir flash:Archive

       service timestamps debug datetime msec
       service timestamps log datetime msec
       no service password-encryption

       <#-- Specific commands for IOS and IOS-XE based FAR -->
       <#if isRunningIosXe>
        license smart reservation
        no ip http client source-interface ${far.tunnelSrcInterface1}
      <#else>
        ntp update-calendar
        ip cef
       </#if>

       hostname FAR${sn}

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
       license boot level network-advantage
       ip domain name ipg.cisco.com
       boot system bootflash:/managed/images/ir1101-universalk9.17.09.05prd18.SPA.bin
       !boot system bootflash:/managed/images/ir1101-universalk9.17.09.03.SPA.bin
       !boot system bootflash:/ir1101-universalk9.17.06.03a.SPA.bin
       !boot system bootflash:/ir1101-universalk9.17.04.01.SPA.bin
       !boot system bootflash:/ir1101-universalk9.17.03.05.SPA.bin
       ipv6 unicast-routing
<#-- END OF SOLUTION TEAM MODIFICATION -->
```

```
        aaa new-model

        aaa authentication login default local
        aaa authorization exec default local

        clock timezone IST 5 30

        crypto key generate rsa general-keys label SSH modulus 2048
        ip ssh rsa keypair-name SSH
        ip ssh version 2
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
<#if isRunningIosXe>
          no ip domain lookup
        <#else>
          no ip domain-lookup
        </#if>
ip host ra-vm241.ipg.cisco.com <RA IPv6 IP>
ip host tps-san.ipg.cisco.com <TPS IPv6 IP
license boot level network-advantage

<#-- END OF SOLUTION TEAM MODIFICATION -->
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
line console 0
 exec-timeout 0 0
<#-- END OF SOLUTION TEAM MODIFICATION  -->

        ip tcp mss 1260


        crypto pki profile enrollment LDevID
         enrollment url  ${far.scepUrl}
         enrollment credential  CISCO_IDEVID_SUDI

        crypto pki trustpoint LDevID
         enrollment mode ra
         enrollment profile LDevID
         serial-number none
         fqdn none
         ip-address none
         password ''
         revocation-check none
         fingerprint ${far.caFingerprint}
<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
         auto-enroll 80 regenerate
<#-- END OF SOLUTION TEAM MODIFICATION -->
```

```
      username ${far.adminUsername} privilege 15 algorithm-type sha256 secret
${far.adminPassword}

      ntp server 162.159.200.1

      <#if far.tunnelSrcInterface1?contains("Cell") ||
far.tunnelSrcInterface1?contains("cell")>

         <#if pid?contains("IR80")>
          controller Cellular 0
           lte gps mode standalone
           lte gps nmea ip
         </#if>

         <#if pid?contains("CGR")>
          <#assign sublist=far.tunnelSrcInterface1?split(" ")[0..1]>
          <#assign slot=sublist[1]>
          no chat-script lte
          chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
          line ${slot}
           script dialer lte
           modem InOut
           no exec
           transport input all
           transport output all
         </#if>

         dialer-list 1 protocol ip permit

         <#-- Dialer watch feature is configured to force the connection to the LTE network
without waiting for any IP traffic -->
         dialer watch-list 1 ip 5.6.7.8 0.0.0.0
         dialer watch-list 1 delay route-check initial 60
         dialer watch-list 1 delay connect 1

         interface ${far.tunnelSrcInterface1}
          load-interval 30
          dialer in-band
          dialer idle-timeout 0
          <#if !isRunningIosXe>
           dialer string lte
          </#if>
          dialer-group 1
          dialer watch-group 1
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
           ipv6 enable
           ip address negotiated
```

```
<#-- END OF SOLUTION TEAM MODIFICATION -->
          no shutdown

        ip route 0.0.0.0 0.0.0.0 ${far.tunnelSrcInterface1}
        ipv6 route ::/0  ${far.tunnelSrcInterface1}

      </#if>

      cgna profile cg-nms-tunnel
       add-command show hosts | format flash:/managed/odm/cg-nms.odm
       add-command show interfaces | format flash:/managed/odm/cg-nms.odm
       add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
       add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
       add-command show version | format flash:/managed/odm/cg-nms.odm
       interval 10
       url https://tps-san.ipg.cisco.com:9120/cgna/ios/tunnel
       gzip

      cgna gzip
      no ip http server
      ip http secure-trustpoint CISCO_IDEVID_SUDI
      ip http authentication aaa login-authentication default
      ip http secure-server
      ip http secure-client-auth
      ip http secure-port ${http_port}
      ip http timeout-policy idle 600 life 86400 requests 3
      ip http client connection timeout 5
      ip http client connection retry 5

      wsma agent exec
       profile exec

      wsma agent config
       profile config

      wsma profile listener exec
       transport https path /wsma/exec

      wsma profile listener config
       transport https path /wsma/config

<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
      event manager directory user policy "flash:/managed/scripts"
      event manager policy LDevID-update.tcl type user authorization bypass
<#-- END OF SOLUTION TEAM MODIFICATION -->

      event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
```

```
        event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
        event manager environment ZTD_SCEP_Period 30
        event manager environment ZTD_SCEP_Enabled FALSE
        event manager policy no_config_replace.tcl type system authorization bypass
        event manager policy tm_ztd_scep.tcl type system authorization bypass

        event manager applet post_pnp
         event timer watchdog  time 30
         action 10.0 cli command "enable"
         action 11.0 cli command "show pnp profile | inc Active:0"
         action 12.0 regexp "Active:0.*" "$_cli_result" pnpStatus
         action 13.0 if $_regexp_result eq 1
         action 14.0 cli command "config t"
         action 15.0 cli command "no key config-key password-encrypt" pattern ".*"
         action 16.0 cli command "yes"
         action 17.0 cli command "key config-key password-encrypt ${far.adminPassword}"
         action 18.0 cli command "password encryption aes"
         action 19.0 cli command "archive"
         action 20.0 cli command "path flash:/Archive/"
         action 21.0 cli command "maximum 8"
         action 22.0 cli command "ip http client secure-trustpoint LDevID"
         action 23.0 cli command "event manager environment ZTD_SCEP_Enabled TRUE"
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
         action 23.1 cli command "no ip host tps-san.ipg.cisco.com <TPS IPv4 IP"
         action 23.2 cli command "no ip host ra-vm241.ipg.cisco.com  <TPS IPv4 IP"
         action 23.3 cli command  "interface GigabitEthernet0/0/0"
         action 23.4 cli command "description shutdown by post_pnp EEM applet"
         action 23.5 cli command "shutdown"
<#-- END OF SOLUTION TEAM MODIFICATION -->
         action 24.0 cli command "no event manager applet post_pnp"
         action 80.0 cli command "do delete /force flash:express-setup-config"
         action 81.0 cli command "do copy running-config flash:express-setup-config"
         action 82.0 cli command "no file prompt quiet"
         action 90.0 end
         action 99.0 cli command "end"

        event manager applet save_certificate
         event syslog pattern "%PKI-6-CERTRET|%PKI-6-CERT_INSTALL: An ID"
         action 10.0 cli command "enable"
         action 11.0 cli command "write mem"

  <#else>

    <#if !far.runningConfig.text?contains("kron policy-list reload")>

     <#-- Add IOS configuration commands here -->
```

```
    <#-- IOS configuration to schedule a reload in 2h -->
        kron policy-list reload
           cli reload in 2:00
        kron occurrence Reload in 1 oneshot
           policy-list reload
    <#else>
        event manager applet cancel_reload
         event timer countdown time 30
         action 10.0 cli command "enable"
         action 11.0 cli command "reload cancel"
         action 12.0 cli command "conf t"
         action 13.0 cli command "no kron policy-list reload"
         action 14.0 cli command "no event manager applet cancel_reload"
         action 99.0 cli command "end"
    </#if>
  </#if>


<#else>
  ${provisioningFailed("FAR is not running IOS")}
</#if>
```

5.3 Appendix C: Bootstrap template – POI recloser site IR1101

```
<#if far.isRunningIos()>

  <#-- New section to support Day 0 operation -->
  <#if isBootstrapping??>
        <#assign sublist=far.eid?split("+")[0..1]>
        <#assign pid=sublist[0]>
        <#assign sn=sublist[1]>
        <#if pid?contains("IR81") || pid?contains("IR11")>
          <#assign http_port=443>
          <#assign isRunningIosXe=true>
        <#else>
           <#assign http_port=8443>
           <#assign isRunningIosXe=false>
        </#if>

        file prompt quiet
        do mkdir flash:Archive

        service timestamps debug datetime msec
        service timestamps log datetime msec
        no service password-encryption
```

```
        <#-- Specific commands for IOS and IOS-XE based FAR -->
        <#if isRunningIosXe>
         license smart reservation
         no ip http client source-interface ${far.tunnelSrcInterface1}
        <#else>
         ntp update-calendar
         ip cef
        </#if>

        hostname FAR${sn}

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
        license boot level network-advantage
        ip domain name ipg.cisco.com
        boot system bootflash:/managed/images/ir1101-universalk9.17.09.05prd18.SPA.bin
        !boot system bootflash:/managed/images/ir1101-universalk9.17.09.03.SPA.bin
        !boot system bootflash:/ir1101-universalk9.17.06.03a.SPA.bin
        !boot system bootflash:/ir1101-universalk9.17.04.01.SPA.bin
        !boot system bootflash:/ir1101-universalk9.17.03.05.SPA.bin
        ipv6 unicast-routing
<#-- END OF SOLUTION TEAM MODIFICATION -->
        aaa new-model

        aaa authentication login default local
        aaa authorization exec default local

        clock timezone IST 5 30

        crypto key generate rsa general-keys label SSH modulus 2048
        ip ssh rsa keypair-name SSH
        ip ssh version 2
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
<#if isRunningIosXe>
          no ip domain lookup
        <#else>
          no ip domain-lookup
        </#if>
ip host ra-vm241.ipg.cisco.com <RA IPv6 IP>
ip host tps-san.ipg.cisco.com <TPS IPv6 IP>
license boot level network-advantage

<#-- END OF SOLUTION TEAM MODIFICATION -->
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
line console 0
 exec-timeout 0 0
<#-- END OF SOLUTION TEAM MODIFICATION  -->
```

```
        ip tcp mss 1260


        crypto pki profile enrollment LDevID
         enrollment url  ${far.scepUrl}
         enrollment credential  CISCO_IDEVID_SUDI

        crypto pki trustpoint LDevID
         enrollment mode ra
         enrollment profile LDevID
         serial-number none
         fqdn none
         ip-address none
         password ''
         revocation-check none
         fingerprint ${far.caFingerprint}
<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
         auto-enroll 80 regenerate
<#-- END OF SOLUTION TEAM MODIFICATION -->

        username ${far.adminUsername} privilege 15 algorithm-type sha256 secret
${far.adminPassword}

        ntp server 162.159.200.1

        <#if far.tunnelSrcInterface1?contains("Cell") ||
far.tunnelSrcInterface1?contains("cell")>

           <#if pid?contains("IR80")>
            controller Cellular 0
             lte gps mode standalone
             lte gps nmea ip
           </#if>

           <#if pid?contains("CGR")>
            <#assign sublist=far.tunnelSrcInterface1?split(" ")[0..1]>
            <#assign slot=sublist[1]>
            no chat-script lte
            chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
            line ${slot}
             script dialer lte
             modem InOut
             no exec
             transport input all
             transport output all
           </#if>
```

```
        dialer-list 1 protocol ip permit

        <#-- Dialer watch feature is configured to force the connection to the LTE network
without waiting for any IP traffic -->
        dialer watch-list 1 ip 5.6.7.8 0.0.0.0
        dialer watch-list 1 delay route-check initial 60
        dialer watch-list 1 delay connect 1

        interface ${far.tunnelSrcInterface1}
         load-interval 30
         dialer in-band
         dialer idle-timeout 0
         <#if !isRunningIosXe>
          dialer string lte
         </#if>
         dialer-group 1
         dialer watch-group 1
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
          ipv6 enable
          ip address negotiated
<#-- END OF SOLUTION TEAM MODIFICATION -->
         no shutdown

        ip route 0.0.0.0 0.0.0.0 ${far.tunnelSrcInterface1}
        ipv6 route ::/0  ${far.tunnelSrcInterface1}

      </#if>

      cgna profile cg-nms-tunnel
       add-command show hosts | format flash:/managed/odm/cg-nms.odm
       add-command show interfaces | format flash:/managed/odm/cg-nms.odm
       add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
       add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
       add-command show version | format flash:/managed/odm/cg-nms.odm
       interval 10
       url https://tps-san.ipg.cisco.com:9120/cgna/ios/tunnel
       gzip

      cgna gzip
      no ip http server
      ip http secure-trustpoint CISCO_IDEVID_SUDI
      ip http authentication aaa login-authentication default
      ip http secure-server
      ip http secure-client-auth
      ip http secure-port ${http_port}
      ip http timeout-policy idle 600 life 86400 requests 3
```

```
ip http client connection timeout 5
ip http client connection retry 5

wsma agent exec
 profile exec

wsma agent config
 profile config

wsma profile listener exec
 transport https path /wsma/exec

wsma profile listener config
 transport https path /wsma/config

<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
event manager directory user policy "flash:/managed/scripts"
event manager policy LDevID-update.tcl type user authorization bypass
<#-- END OF SOLUTION TEAM MODIFICATION -->

event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager environment ZTD_SCEP_Period 30
event manager environment ZTD_SCEP_Enabled FALSE
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm_ztd_scep.tcl type system authorization bypass

event manager applet post_pnp
 event timer watchdog  time 30
 action 10.0 cli command "enable"
 action 11.0 cli command "show pnp profile | inc Active:0"
 action 12.0 regexp "Active:0.*" "$_cli_result" pnpStatus
 action 13.0 if $_regexp_result eq 1
 action 14.0 cli command "config t"
 action 15.0 cli command "no key config-key password-encrypt" pattern ".*"
 action 16.0 cli command "yes"
 action 17.0 cli command "key config-key password-encrypt ${far.adminPassword}"
 action 18.0 cli command "password encryption aes"
 action 19.0 cli command "archive"
 action 20.0 cli command "path flash:/Archive/"
 action 21.0 cli command "maximum 8"
 action 22.0 cli command "ip http client secure-trustpoint LDevID"
 action 23.0 cli command "event manager environment ZTD_SCEP_Enabled TRUE"
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
 action 23.1 cli command "no ip host tps-san.ipg.cisco.com <TPS IPv4 IP>"
 action 23.2 cli command "no ip host ra-vm241.ipg.cisco.com  <RA IPv4 IP"
 action 23.3 cli command  "interface GigabitEthernet0/0/0"
```

```
        action 23.4 cli command "description shutdown by post_pnp EEM applet"
        action 23.5 cli command "shutdown"
<#-- END OF SOLUTION TEAM MODIFICATION -->
        action 24.0 cli command "no event manager applet post_pnp"
        action 80.0 cli command "do delete /force flash:express-setup-config"
        action 81.0 cli command "do copy running-config flash:express-setup-config"
        action 82.0 cli command "no file prompt quiet"
        action 90.0 end
        action 99.0 cli command "end"

       event manager applet save_certificate
        event syslog pattern "%PKI-6-CERTRET|%PKI-6-CERT_INSTALL: An ID"
        action 10.0 cli command "enable"
        action 11.0 cli command "write mem"

  <#else>

    <#if !far.runningConfig.text?contains("kron policy-list reload")>

     <#-- Add IOS configuration commands here -->

     <#-- IOS configuration to schedule a reload in 2h -->
        kron policy-list reload
           cli reload in 2:00
        kron occurrence Reload in 1 oneshot
           policy-list reload
    <#else>
        event manager applet cancel_reload
         event timer countdown time 30
         action 10.0 cli command "enable"
         action 11.0 cli command "reload cancel"
         action 12.0 cli command "conf t"
         action 13.0 cli command "no kron policy-list reload"
         action 14.0 cli command "no event manager applet cancel_reload"
         action 99.0 cli command "end"
    </#if>
  </#if>


<#else>
  ${provisioningFailed("FAR is not running IOS")}
</#if>
```

5.4 Appendix D: Tunnel group template – Substation IR1101

```
<#if far.eid?contains("IR81") || far.eid?contains("IR11")>
  <#assign isRunningIosXe=true>
<#else>
   <#assign isRunningIosXe=false>
</#if>

<#if !(far.ipsecTunnelDestAddr1??)>
 ${provisioningFailed("FAR property ipsecTunnelDestAddr1 is undefined.")}
</#if>
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
!ip host fnd-san.ipg.cisco.com 2001:db8:baba:103::103
ip host fnd-san.ipg.cisco.com 2001:db8:baba:f00d::103
username user  privilege 15 secret User!23
<#-- END OF SOLUTION TEAM MODIFICATION -->

aaa authorization network FlexVPN_Author local

crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = FAN241-ROOT-CA


 ipv6 unicast-routing
 <#if !isRunningIosXe>
   ipv6 cef
 </#if>
<#assign loopbackIpv6Address=far.loopbackV6Address>
<#assign loopbackIpv4Address=far.loopbackV4Address>

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
!
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
```

```
!
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
ip multicast-routing distributed
ip multicast-routing vrf DTT_VRF distributed
ip multicast vrf DTT_VRF auto-enable
!
license smart transport off
!
interface Vlan1
 description IPv6 traffic to docker container for T104 (untagged frames from docker)
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address ${far.ied_vlan_ipv6_prefix1}
!
Vlan 651
name RECLOSER_VLAN
no shut
!
interface Vlan651
description SEL 3505 GOOSE communication on VLAN 651
vrf forwarding DTT_VRF
no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
!

interface FastEthernet0/0/4
 description connected to HUB-SEL3505
switchport trunk allowed vlan 1,651
switchport mode trunk
!
bridge-domain 1
member vni 5555
member Vlan651 service-instance 1
!
!
interface Loopback0
   vrf forwarding NMS_VRF
```

```
  no ip address
  ip nat outside
  ipv6 address ${loopbackIpv6Address}/128
  no shutdown
 crypto ikev2 nat keepalive 30
!
interface Loopback15
vrf forwarding DTT_VRF
ip address ${loopbackIpv4Address} 255.255.255.255
ip pim sparse-mode
ip nat outside
!
!
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address ${far.recloser_access_ip} 255.255.255.255
 ip nat outside
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface Loopback31
!
<#-- END OF SOLUTION TEAM MODIFICATION -->

crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface

crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal

crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy

crypto ikev2 fragmentation mtu 1000
crypto ikev2 redirect client
```

```
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile

<#-- ORIGINAL AND COMMENTED OUT

interface Tunnel10
 description to ${her.eid}
 tunnel source ${far.tunnelSrcInterface1}
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
 !
  tunnel mode gre ipv6
  tunnel path-mtu-discovery
 !
crypto ikev2 client flexvpn VPN_LB
  peer 1 ${far.ipsecTunnelDestAddr1}
  client connect Tunnel10

ORIGINAL AND COMMENTED OUT -->

<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
ip http client source-interface Loopback0
!
interface Tunnel10
 description to ${her.eid}
   vrf forwarding NMS_VRF
   no ip address
   ipv6 unnumbered Loopback0
   ipv6 mtu 1280
   ipv6 tcp adjust-mss 1140
   tunnel mode gre ipv6
   tunnel path-mtu-discovery
   tunnel source ${far.tunnelSrcInterface1}
   tunnel destination ${far.ipsecTunnelDestAddr1}
   tunnel protection ipsec profile FlexVPN_IPsec_Profile
   no shutdown
!
interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
```

```
 no ip address
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head Ended IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel12
 description to BGL-CC2-HER-C8000V
 vrf forwarding SCADA_VRF
 no ip address
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel15
 description to HUB-IR1101
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <DER IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
!crypto ikev2 client flexvpn GOOSE_IR1101_HUB
!  peer 2  <DER IPv6 IP>
!  client connect Tunnel15
!
!
interface Virtual-Template14 type tunnel
 vrf forwarding SCADA_VRF
 ip nat outside
```

```
 ip unnumbered Loopback31
 ip mtu 1300
 ip pim sparse-mode
 ip tcp adjust-mss 1260
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 virtual-template 14
!
ip route vrf SCADA_VRF ${far.poi_recloser_access_ip} 255.255.255.255 Tunnel11
!
interface nve1
no ip address
source-interface Loopback15
member vni 5555 mcast-group 239.1.1.1
!
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir
ip pim vrf DTT_VRF rp-address 192.168.1.20 bidir
!
ip ssh bulk-mode 131072
!
snmp ifmib ifindex persist
!
!
ipv6 route 2001:DB8:CCCC:CCCC::/96 Tunnel10
!
ip route vrf SCADA_VRF 172.19.107.0 255.255.255.0 Tunnel11
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
!
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 443 interface Loopback31 30443 vrf SCADA_VRF
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 30023 interface Loopback31 30023 vrf
SCADA_VRF
!ip nat inside source static tcp 192.168.0.2 80 interface Loopback31 30080 vrf SCADA_VRF
!
```

5.5 Appendix E: Tunnel group template – Midpoint recloser site IR1101

```
<#if far.eid?contains("IR81") || far.eid?contains("IR11")>
  <#assign isRunningIosXe=true>
<#else>
   <#assign isRunningIosXe=false>
</#if>

<#if !(far.ipsecTunnelDestAddr1??)>
 ${provisioningFailed("FAR property ipsecTunnelDestAddr1 is undefined.")}
</#if>
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
!ip host fnd-san.ipg.cisco.com 2001:db8:baba:103::103
ip host fnd-san.ipg.cisco.com 2001:db8:baba:f00d::103
username user  privilege 15 secret User!23
<#-- END OF SOLUTION TEAM MODIFICATION -->

aaa authorization network FlexVPN_Author local

crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = FAN241-ROOT-CA


 ipv6 unicast-routing
 <#if !isRunningIosXe>
   ipv6 cef
 </#if>
<#assign loopbackIpv6Address=far.loopbackV6Address>
<#assign loopbackIpv4Address=far.loopbackV4Address>

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
!
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
```

```
 address-family ipv6
 exit-address-family
!
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
ip multicast-routing distributed
ip multicast-routing vrf DTT_VRF distributed
ip multicast vrf DTT_VRF auto-enable
!
license smart transport off
!
interface Vlan1
 description IPv6 traffic to docker container for T104 (untagged frames from docker)
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address ${far.ied_vlan_ipv6_prefix1}
!
Vlan 651
name RECLOSER_VLAN
no shut
!
interface Vlan651
description SEL 3505 GOOSE communication on VLAN 651
vrf forwarding DTT_VRF
no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
!
interface FastEthernet0/0/4
 description connected to HUB-SEL3505
switchport trunk allowed vlan 1,651
switchport mode trunk
!
bridge-domain 1
member vni 5555
member Vlan651 service-instance 1
!
interface Loopback0
   vrf forwarding NMS_VRF
```

```
  no ip address
  ip nat outside
  ipv6 address ${loopbackIpv6Address}/128
  no shutdown
 crypto ikev2 nat keepalive 30
!
interface Loopback15
vrf forwarding DTT_VRF
ip address ${loopbackIpv4Address} 255.255.255.255
ip pim sparse-mode
ip nat outside
!
!
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address ${far.recloser_access_ip} 255.255.255.255
 ip nat outside
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface Loopback31
!
<#-- END OF SOLUTION TEAM MODIFICATION -->

crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface

crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal

crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy

crypto ikev2 fragmentation mtu 1000
crypto ikev2 redirect client
```

```
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile

<#-- ORIGINAL AND COMMENTED OUT

interface Tunnel10
 description to ${her.eid}
 tunnel source ${far.tunnelSrcInterface1}
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
 !
  tunnel mode gre ipv6
  tunnel path-mtu-discovery
 !
crypto ikev2 client flexvpn VPN_LB
  peer 1 ${far.ipsecTunnelDestAddr1}
  client connect Tunnel10

ORIGINAL AND COMMENTED OUT -->

<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
ip http client source-interface Loopback0
!
interface Tunnel10
 description to ${her.eid}
   vrf forwarding NMS_VRF
   no ip address
   ipv6 unnumbered Loopback0
   ipv6 mtu 1280
   ipv6 tcp adjust-mss 1140
   tunnel mode gre ipv6
   tunnel path-mtu-discovery
   tunnel source ${far.tunnelSrcInterface1}
   tunnel destination ${far.ipsecTunnelDestAddr1}
   tunnel protection ipsec profile FlexVPN_IPsec_Profile
   no shutdown
!
interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
```

```
 no ip address
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination 2001:420:5430:34::28
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel12
 description to BGL-CC2-HER-C8000V
 vrf forwarding SCADA_VRF
 no ip address
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination (IPv6 address of HeadEnd Router)
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel15
 description to HUB-IR1101
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <DER IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
!crypto ikev2 client flexvpn GOOSE_IR1101_HUB
!  peer 2 <DER IPv6 IP>
!  client connect Tunnel15
!
interface Tunnel14
 description to SUB-HUB-IR1101
 vrf forwarding SCADA_VRF
 ip nat outside
```

```
 ip unnumbered Loopback31
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Substation IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface nve1
no ip address
source-interface Loopback15
member vni 5555 mcast-group 239.1.1.1
!
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir
ip pim vrf DTT_VRF rp-address 192.168.1.20 bidir
!
ip ssh bulk-mode 131072
!
snmp ifmib ifindex persist
!
!
ipv6 route 2001:DB8:CCCC:CCCC::/96 Tunnel10
!
ip route vrf SCADA_VRF 172.19.107.0 255.255.255.0 Tunnel11
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
!
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 80 interface Loopback31 30080 vrf SCADA_VRF
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 23 interface Loopback31 30023 vrf SCADA_VRF
!ip nat inside source static tcp 192.168.0.2 443 interface Loopback31 30443 vrf SCADA_VRF
!
```

5.6 Appendix F: Tunnel group template – POI recloser site IR1101

```
<#if far.eid?contains("IR81") || far.eid?contains("IR11")>
  <#assign isRunningIosXe=true>
<#else>
   <#assign isRunningIosXe=false>
</#if>

<#if !(far.ipsecTunnelDestAddr1??)>
 ${provisioningFailed("FAR property ipsecTunnelDestAddr1 is undefined.")}
</#if>
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
!ip host fnd-san.ipg.cisco.com 2001:db8:baba:103::103
ip host fnd-san.ipg.cisco.com 2001:db8:baba:f00d::103
username user  privilege 15 secret User!23
<#-- END OF SOLUTION TEAM MODIFICATION -->

aaa authorization network FlexVPN_Author local

crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = FAN241-ROOT-CA


 ipv6 unicast-routing
 <#if !isRunningIosXe>
   ipv6 cef
 </#if>
<#assign loopbackIpv6Address=far.loopbackV6Address>
<#assign loopbackIpv4Address=far.loopbackV4Address>

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION -->
!
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
```

```
 address-family ipv6
 exit-address-family
!
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
ip multicast-routing distributed
ip multicast-routing vrf DTT_VRF distributed
ip multicast vrf DTT_VRF auto-enable
!
license smart transport off
!
interface Vlan1
 description IPv6 traffic to docker container for T104 (untagged frames from docker)
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address ${far.ied_vlan_ipv6_prefix1}
!
Vlan 651
name RECLOSER_VLAN
no shut
!
interface Vlan651
description SEL 3505 GOOSE communication on VLAN 651
vrf forwarding DTT_VRF
no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
!
key chain MyMACsecKEYchain macsec
 key 9999
 cryptographic-algorithm aes-128-cmac
 key-string 92d032aee88c47fbddc7c3f234c6165a
!
mka policy MyMACsecPolicy
 macsec-cipher-suite gcm-aes-128
 sak-rekey interval 300
!
interface FastEthernet0/0/4
 description connected to HUB-SEL3505
```

```
switchport trunk allowed vlan 1,651
switchport mode trunk
macsec network-link
mka policy MyMACsecPolicy
mka pre-shared-key key-chain MyMACsecKEYchain
!
bridge-domain 1
member vni 5555
member Vlan651 service-instance 1
!
!
!
!
interface Loopback0
  vrf forwarding NMS_VRF
  no ip address
  ip nat outside
  ipv6 address ${loopbackIpv6Address}/128
  no shutdown
 crypto ikev2 nat keepalive 30
!
interface Loopback15
vrf forwarding DTT_VRF
ip address ${loopbackIpv4Address} 255.255.255.255
ip pim sparse-mode
ip nat outside
!
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address ${far.recloser_access_ip} 255.255.255.255
 ip nat outside
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface Loopback31
!
<#-- END OF SOLUTION TEAM MODIFICATION -->

crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface

crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
```

```
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy

crypto ikev2 fragmentation mtu 1000
crypto ikev2 redirect client

crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile

<#-- ORIGINAL AND COMMENTED OUT

interface Tunnel10
 description to ${her.eid}
 tunnel source ${far.tunnelSrcInterface1}
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
 !
  tunnel mode gre ipv6
  tunnel path-mtu-discovery
 !
crypto ikev2 client flexvpn VPN_LB
  peer 1 ${far.ipsecTunnelDestAddr1}
  client connect Tunnel10

ORIGINAL AND COMMENTED OUT -->

<#-- BEGIN OF SOLUTION TEAM MODIFICATION -->
ip http client source-interface Loopback0
!
interface Tunnel10
 description to ${her.eid}
   vrf forwarding NMS_VRF
   no ip address
```

```
  ipv6 unnumbered Loopback0
  ipv6 mtu 1280
  ipv6 tcp adjust-mss 1140
  tunnel mode gre ipv6
  tunnel path-mtu-discovery
  tunnel source ${far.tunnelSrcInterface1}
  tunnel destination ${far.ipsecTunnelDestAddr1}
  tunnel protection ipsec profile FlexVPN_IPsec_Profile
  no shutdown
!
interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 no ip address
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel12
 description to BGL-CC2-HER-C8000V
 vrf forwarding SCADA_VRF
 no ip address
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <IPv6 address of HeadEnd Router>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Virtual-Template2 type tunnel
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip mtu 1300
 ip pim sparse-mode
 ip tcp adjust-mss 1260
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 mtu 1280
```

```
 ipv6 tcp adjust-mss 1140
 nat64 enable
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
virtual-template 2
!
!
interface nve1
no ip address
source-interface Loopback15
member vni 5555 mcast-group 239.1.1.1
!
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir
ip pim vrf DTT_VRF rp-address 192.168.1.20 bidir
!
ip ssh bulk-mode 131072
!
snmp ifmib ifindex persist
!
ip route vrf SCADA_VRF ${far.substation_recloser_access_ip} 255.255.255.255 Tunnel11
!
ipv6 route 2001:DB8:CCCC:CCCC::/96 Tunnel10
ip route vrf SCADA_VRF 172.19.107.0 255.255.255.0 Tunnel11
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
!
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 80 interface Loopback31 30080 vrf SCADA_VRF
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 23 interface Loopback31 30023 vrf SCADA_VRF
!ip nat inside source static tcp 192.168.0.2 443 interface Loopback31 30443 vrf SCADA_VRF

!
```

5.7 Appendix G: Config group template – Substation IR1101

```
<#--
  If a Loopback0 interface is present on the device (normally configured
  during tunnel provisioning) then use that as the source interface for
  the HTTP client, SNMP traps and RADIUS protocol. The source for the HTTP client is not
  changed during tunnel provisioning because usually the addresses assigned
  to the loopback interface are only accessible through the tunnels.
  Waiting insures the tunnel is configured correctly and comes up.
-->
<#if far.interfaces("Loopback0")?size != 0>
  ip http client source-interface Loopback0
  snmp-server trap-source Loopback0
</#if>

<#-- Enable periodic inventory notification to report metrics. -->
  cgna profile cg-nms-periodic
    interval 60
  exit

<#-- Enable periodic configuration (heartbeat) notification. -->
cgna heart-beat interval 20

<#-- Interfaces configuration -->
interface ${far.tunnelSrcInterface1}
 no ip redirects
 no ip unreachables
 no ip proxy-arp

!
!
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
<#-- END OF SOLUTION TEAM MODIFICATION  -->

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
line console 0
 exec-timeout 0 0
<#-- END OF SOLUTION TEAM MODIFICATION  -->

line vty 0 14
 exec-timeout 5
 transport input ssh
 transport output none

service nagle
no service pad
service tcp-keepalives-in
```

```
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
no ip source-route
no ipv6 source-route
no ip gratuitous-arps
no ip bootp server
no cdp run
no ip finger
no boot network
ip tcp synwait-time 5
ip tcp path-mtu-discovery

<#-- Enable BBU discharge if one is present -->
<#if far.hasActiveBattery()>
 <#if far.eid?contains("CGR12")>
  do battery charge-discharge enable
 <#elseif far.eid?contains("IR81")>
  do request platform hardware battery charge-discharge enable
 </#if>
</#if>
```

5.8 Appendix H: Config group template – Midpoint recloser site IR1101

```
<#--
 If a Loopback0 interface is present on the device (normally configured
 during tunnel provisioning) then use that as the source interface for
 the HTTP client, SNMP traps and RADIUS protocol. The source for the HTTP client is not
 changed during tunnel provisioning because usually the addresses assigned
 to the loopback interface are only accessible through the tunnels.
 Waiting insures the tunnel is configured correctly and comes up.
-->
<#if far.interfaces("Loopback0")?size != 0>
 ip http client source-interface Loopback0
 snmp-server trap-source Loopback0
</#if>

<#-- Enable periodic inventory notification to report metrics. -->
 cgna profile cg-nms-periodic
  interval 60
 exit
```

```
<#-- Enable periodic configuration (heartbeat) notification. -->
cgna heart-beat interval 20

<#-- Interfaces configuration -->
interface ${far.tunnelSrcInterface1}
 no ip redirects
 no ip unreachables
 no ip proxy-arp

!
!
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
<#-- END OF SOLUTION TEAM MODIFICATION  -->

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
line console 0
 exec-timeout 0 0
<#-- END OF SOLUTION TEAM MODIFICATION  -->

line vty 0 14
 exec-timeout 5
 transport input ssh
 transport output none

service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
no ip source-route
no ipv6 source-route
no ip gratuitous-arps
no ip bootp server
no cdp run
no ip finger
no boot network
ip tcp synwait-time 5
ip tcp path-mtu-discovery

<#-- Enable BBU discharge if one is present -->
<#if far.hasActiveBattery()>
  <#if far.eid?contains("CGR12")>
    do battery charge-discharge enable
  <#elseif far.eid?contains("IR81")>
```

```
   do request platform hardware battery charge-discharge enable
  </#if>
</#if>
```

5.9 Appendix I: Config group template – POI recloser site IR1101

```
<#--
  If a Loopback0 interface is present on the device (normally configured
  during tunnel provisioning) then use that as the source interface for
  the HTTP client, SNMP traps and RADIUS protocol. The source for the HTTP client is not
  changed during tunnel provisioning because usually the addresses assigned
  to the loopback interface are only accessible through the tunnels.
  Waiting insures the tunnel is configured correctly and comes up.
-->
<#if far.interfaces("Loopback0")?size != 0>
  ip http client source-interface Loopback0
  snmp-server trap-source Loopback0
</#if>

<#-- Enable periodic inventory notification to report metrics. -->
  cgna profile cg-nms-periodic
    interval 60
  exit

<#-- Enable periodic configuration (heartbeat) notification. -->
cgna heart-beat interval 20

<#-- Interfaces configuration -->
interface ${far.tunnelSrcInterface1}
 no ip redirects
 no ip unreachables
 no ip proxy-arp

!
!
<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
<#-- END OF SOLUTION TEAM MODIFICATION  -->

<#-- BEGINNING OF SOLUTION TEAM MODIFICATION  -->
line console 0
 exec-timeout 0 0
<#-- END OF SOLUTION TEAM MODIFICATION  -->

line vty 0 14
 exec-timeout 5
```

```
 transport input ssh
 transport output none

service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
no ip source-route
no ipv6 source-route
no ip gratuitous-arps
no ip bootp server
no cdp run
no ip finger
no boot network
ip tcp synwait-time 5
ip tcp path-mtu-discovery

<#-- Enable BBU discharge if one is present -->
<#if far.hasActiveBattery()>
  <#if far.eid?contains("CGR12")>
    do battery charge-discharge enable
  <#elseif far.eid?contains("IR81")>
    do request platform hardware battery charge-discharge enable
  </#if>
</#if>
```

6 Running configuration – working condition

6.1 Substation IR1101 configuration

```
Building configuration...

Current configuration : 13015 bytes
!
! Last configuration change at 15:30:04 IST Thu Jul 4 2024 by cg-nms-administrator
! NVRAM config last updated at 04:49:07 IST Thu Jul 4 2024
!
version 17.15
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
platform qfp utilization monitor load 80
platform hardware throughput level 250M
!
hostname FARFCW2709Y19D
!
boot-start-marker
boot system bootflash:ir1101-
universalk9.BLD_V1715_THROTTLE_LATEST_20240503_033217_V17_15_0_33.SSA.bin
boot-end-marker
!
!
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
```

```
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 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
no ip gratuitous-arps
!
ip multicast-routing distributed
ip multicast-routing vrf DTT_VRF distributed
ip multicast vrf DTT_VRF auto-enable
ip host fnd-san.ipg.cisco.com 2001:DB8:BABA:F00D::103
ip host ra-vm241.ipg.cisco.com <RA IPv6 IP>
ip host tps-san.ipg.cisco.com <TPS IPv6 IP>
no ip domain lookup
!
!
!
!
!
!
!
!
!
login block-for 60 attempts 3 within 30
login delay 3
login on-success log
!
!
!
!
!
!
no ipv6 source-route
ipv6 unicast-routing
!
```

```
!
subscriber templating
!
!
!
!
!
!
!
!
!
!
!
!
!
password encryption aes
!
!
crypto pki trustpoint LDevID
 enrollment retry count 4
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password 7 074866
 fingerprint FBE6AFCFAF57C192955678F7B73BD06A233F20D2
 subject-name serialNumber=PID:IR1101-K9 SN:FCW2709Y19D,CN=FARFCW2709Y19D
 revocation-check none
 auto-enroll 90 regenerate
 hash sha256
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint fnd
 enrollment url bootflash://PnP-cert_07_08_38_UTC_Fri_Jun_28_2024
 revocation-check none
 hash sha256
!
crypto pki profile enrollment LDevID
 enrollment url  http://ra-vm241.ipg.cisco.com:8080
!
!
```

```
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = fan241-root-ca
!
crypto pki certificate chain LDevID
 certificate 2E403ED73C3BA7731FC54C1B97D87008D6293F58
 certificate ca 4DFB348D48F27F3A19333A8363CD8FA98A31743E
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
crypto pki certificate chain fnd
 certificate ca 4DFB348D48F27F3A19333A8363CD8FA98A31743E
!
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
no license feature hseck9
license udi pid IR1101-K9 sn FCW2709Y19D
license boot level network-advantage
license smart reservation
license smart transport off
archive
 path bootflash:/Archive/
 maximum 8
memory free low-watermark processor 43451
!
spanning-tree extend system-id
!
!
!
username cg-nms-administrator privilege 15 secret 8
$8$mfdgXlEBP1auFE$l4.hDw9C40JjgF.qLD6UHN/IzPcgKc2jP55z9xZbiBw
username user privilege 15 secret 9
$9$kXPE/oxzjxeqN.$WH6rcxn5LgB1ufb81Q.GoIQyn5H9wTWQo6JcwzODtgc
!
redundancy
bridge-domain 1
 member vni 5555
 member Vlan651 service-instance 1
!
!
```

```
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface Loopback31
 route set interface
!
crypto ikev2 redirect client
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 14
!
crypto ikev2 nat keepalive 30
crypto ikev2 fragmentation mtu 1000
!
controller Cellular 0/1/0
!
!
vlan internal allocation policy ascending
no cdp run
!
!
!
!
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
```

```
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 vrf forwarding NMS_VRF
 no ip address
 ip nat outside
 ipv6 address 2001:DB8:BABA:FACE::1027/128
!
interface Loopback15
 vrf forwarding DTT_VRF
 ip address 192.168.1.22 255.255.255.255
 ip pim sparse-mode
 ip nat outside
!
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address 172.31.31.10 255.255.255.255
 ip nat outside
!
interface Tunnel10
 description to FNDHE241-C8000V
 vrf forwarding NMS_VRF
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
```

```
interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel12
 description to BGL-CC2-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel15
 description to HUB-IR1101
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <DER IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface GigabitEthernet0/0/0
 description shutdown by post_pnp EEM applet
 ip address dhcp
 shutdown
!
interface FastEthernet0/0/1
!
```

```
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
 description connected to HUB-SEL3505
 switchport trunk allowed vlan 1,651
 switchport mode trunk
!
interface Cellular0/1/0
 mtu 1358
 ip address negotiated
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip tcp adjust-mss 1318
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
interface Cellular0/1/1
 no ip address
 shutdown
!
interface Virtual-Template14 type tunnel
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip mtu 1300
 ip pim sparse-mode
 ip nat outside
 ip tcp adjust-mss 1260
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Vlan1
 description IPv6 traffic to docker container for T104 (untagged frames from docker)
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address 2001:DB8:ABCD:EF:1227::1/64
!
```

```
interface Vlan651
 description SEL 3505 GOOSE communication on VLAN 651
 vrf forwarding DTT_VRF
 no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
 !
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
interface nve1
 no ip address
 source-interface Loopback15
 member vni 5555 mcast-group 239.1.1.1
!
ip forward-protocol nd
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir
ip pim vrf DTT_VRF rp-address 192.168.1.20 bidir
ip tcp mss 1260
ip tcp synwait-time 5
ip tcp path-mtu-discovery
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-client-auth
ip http secure-trustpoint LDevID
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface Loopback0
ip http client secure-trustpoint LDevID
!
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 30023 interface Loopback31 30023 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 443 interface Loopback31 30443 vrf SCADA_VRF
ip route 0.0.0.0 0.0.0.0 10.10.100.100
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route vrf SCADA_VRF 172.19.107.0 255.255.255.0 Tunnel11
ip route vrf SCADA_VRF 172.31.31.11 255.255.255.255 Tunnel11
ip ssh bulk-mode 131072
```

```
ip ssh rsa keypair-name SSH
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
ipv6 route 2001:DB8:CCCC:CCCC::/96 Tunnel10
ipv6 route ::/0 Cellular0/1/0
snmp-server group cgnms v3 priv
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps fru-ctrl
snmp-server enable traps aaa_server
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps c3g
snmp-server host 2001:DB8:BABA:F00D::103 version 3 priv cg-nms-administrator
snmp ifmib ifindex persist
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
 speed 115200
line 0/0/0
line 0/2/0
line vty 0 4
 exec-timeout 5 0
 length 0
 transport input ssh
 transport output none
line vty 5 14
 exec-timeout 5 0
```

```
 transport input ssh
 transport output none
!
ntp server 162.159.200.1
!
wsma agent exec
 profile exec
!
wsma agent config
 profile config
!
!
!
!
wsma profile listener exec
 transport https path /wsma/exec
!
wsma profile listener config
 transport https path /wsma/config
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager environment ZTD_SCEP_Period 30
event manager directory user policy "flash:/managed/scripts"
event manager policy LDevID-update.tcl type user authorization bypass
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm_ztd_scep.tcl type system authorization bypass
event manager applet save_certificate
 event syslog pattern "%PKI-6-CERTRET|%PKI-6-CERT_INSTALL: An ID"
 action 10.0 cli command "enable"
 action 11.0 cli command "write mem"
!
!
!
cgna gzip
!
cgna heart-beat interval 20
cgna heart-beat active
!
cgna profile cg-nms-tunnel
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://tps-san.ipg.cisco.com:9120/cgna/ios/tunnel
 gzip
```

```
!
cgna profile cg-nms-register
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://fnd-san.ipg.cisco.com:9121/cgna/ios/registration
 gzip
!
cgna profile cg-nms-periodic
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 add-command show platform resources | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/1/0 all | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/1/0 radio details | format flash:/managed/odm/cg-
nms.odm
 interval 60
 url https://fnd-san.ipg.cisco.com:9121/cgna/ios/metrics
 gzip
 active
!
!
cgna exec-profile CGNA-default-exec-profile
 add-command cgna exec profile cg-nms-register
 interval 1
 exec-count 1
!
!
!
end
```

6.2 Midpoint recloser site IR1101 configuration

```
Building configuration...

Current configuration : 13109 bytes
!
! Last configuration change at 15:30:24 IST Thu Jul 4 2024 by cg-nms-administrator
! NVRAM config last updated at 15:30:54 IST Thu Jul 4 2024 by cg-nms-administrator
!
version 17.15
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
platform qfp utilization monitor load 80
platform hardware throughput level 250M
!
hostname FARFCW23380HMK
!
boot-start-marker
boot system bootflash:ir1101-
universalk9.BLD_V1715_THROTTLE_LATEST_20240503_033217_V17_15_0_33.SSA.bin
boot-end-marker
!
!
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition SCADA_VRF
 !
 address-family ipv4
 exit-address-family
```

```
 !
 address-family ipv6
 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
no ip gratuitous-arps
!
ip multicast-routing distributed
ip multicast-routing vrf DTT_VRF distributed
ip multicast vrf DTT_VRF auto-enable
ip host fnd-san.ipg.cisco.com 2001:DB8:BABA:F00D::103
ip host ra-vm241.ipg.cisco.com <RA IPv6 IP>
ip host tps-san.ipg.cisco.com <TPS IPv6 IP>
no ip domain lookup
!
!
!
!
!
!
!
!
!
login block-for 60 attempts 3 within 30
login delay 3
login on-success log
!
!
!
!
!
no ipv6 source-route
ipv6 unicast-routing
!
!
subscriber templating
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
password encryption aes
!
!
crypto pki trustpoint LDevID
 enrollment retry count 4
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password 7 024143
 fingerprint FBE6AFCFAF57C192955678F7B73BD06A233F20D2
 subject-name serialNumber=PID:IR1101-K9 SN:FCW23380HMK,CN=FARFCW23380HMK
 revocation-check none
 auto-enroll 90 regenerate
 hash sha256
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint fnd
 enrollment url bootflash://PnP-cert_07_08_41_UTC_Fri_Jun_28_2024
 revocation-check none
 hash sha256
!
crypto pki profile enrollment LDevID
 enrollment url  http://ra-vm241.ipg.cisco.com:8080
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = fan241-root-ca
!
```

```
crypto pki certificate chain LDevID
 certificate 177B2D94C320BEE7894DC5D02C0D9CA41CBFD535
 certificate ca 4DFB348D48F27F3A19333A8363CD8FA98A31743E
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
crypto pki certificate chain fnd
 certificate ca 4DFB348D48F27F3A19333A8363CD8FA98A31743E
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
no license feature hseck9
license udi pid IR1101-K9 sn FCW23380HMK
license boot level network-advantage
license smart reservation
license smart transport off
archive
 path bootflash:/Archive/
 maximum 8
memory free low-watermark processor 43451
!
spanning-tree extend system-id
!
!
!
username cg-nms-administrator privilege 15 secret 8
$8$2BzRPlwlkQ.h6U$sDVVi8rUVWXggyaY5a4eRWQ1I9Fs4Yqd3wbkW.5zhJQ
username user privilege 15 secret 9
$9$T.5Q4FidldQdHk$eGNoUcCrhmpIZCCSTmjYJiFuA9pMuRbHIvcXzNyOtK.
!
redundancy
bridge-domain 1
 member vni 5555
 member Vlan651 service-instance 1
!
!
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface Loopback31
```

```
 route set interface
!
crypto ikev2 redirect client
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 nat keepalive 30
crypto ikev2 fragmentation mtu 1000
!
controller Cellular 0/1/0
 profile id 15 apn airtelgprs.com authentication none pdn-type ipv4v6
!
!
vlan internal allocation policy ascending
no cdp run
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
```

```
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 vrf forwarding NMS_VRF
 no ip address
 ip nat outside
 ipv6 address 2001:DB8:BABA:FACE::1021/128
!
interface Loopback15
 vrf forwarding DTT_VRF
 ip address 192.168.1.19 255.255.255.255
 ip pim sparse-mode
 ip nat outside
!
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address 172.31.31.12 255.255.255.255
 ip nat outside
!
interface Tunnel10
 description to FNDHE241-C8000V
 vrf forwarding NMS_VRF
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
```

```
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel12
 description to BGL-CC2-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel14
 description to SUB-HUB-IR1101
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip pim sparse-mode
 ip nat outside
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Substation IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel15
 description to HUB-IR1101
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip pim sparse-mode
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
```

```
 tunnel destination <DER IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface GigabitEthernet0/0/0
 description shutdown by post_pnp EEM applet
 ip address dhcp
 shutdown
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
 description connected to HUB-SEL3505
 switchport trunk allowed vlan 1,651
 switchport mode trunk
!
interface Cellular0/1/0
 mtu 1358
 ip address negotiated
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip tcp adjust-mss 1460
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
interface Cellular0/1/1
 no ip address
 shutdown
!
interface Vlan1
 description IPv6 traffic to docker container for T104 (untagged frames from docker)
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address 2001:DB8:ABCD:EF:1221::1/64
!
interface Vlan651
```

```
 description SEL 3505 GOOSE communication on VLAN 651
 vrf forwarding DTT_VRF
 no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
 !
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
interface nve1
 no ip address
 source-interface Loopback15
 member vni 5555 mcast-group 239.1.1.1
!
ip forward-protocol nd
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir
ip pim vrf DTT_VRF rp-address 192.168.1.20 bidir
ip tcp mss 1260
ip tcp synwait-time 5
ip tcp path-mtu-discovery
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-client-auth
ip http secure-trustpoint LDevID
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface Loopback0
ip http client secure-trustpoint LDevID
!
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 23 interface Loopback31 30023 vrf SCADA_VRF
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 80 interface Loopback31 30080 vrf SCADA_VRF
ip route 0.0.0.0 0.0.0.0 10.10.100.100
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route vrf SCADA_VRF 172.19.107.0 255.255.255.0 Tunnel11
ip ssh bulk-mode 131072
ip ssh rsa keypair-name SSH
!
ip access-list standard IED_NW
```

```
 10 permit 192.168.0.0 0.0.0.255
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
ipv6 route 2001:DB8:CCCC:CCCC::/96 Tunnel10
ipv6 route ::/0 Cellular0/1/0
snmp-server group cgnms v3 priv
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps fru-ctrl
snmp-server enable traps aaa_server
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps c3g
snmp-server host 2001:DB8:BABA:F00D::103 version 3 priv cg-nms-administrator
snmp ifmib ifindex persist
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line 0/0/0
line 0/2/0
line vty 0 4
 exec-timeout 5 0
 length 0
 transport input ssh
 transport output none
line vty 5 14
 exec-timeout 5 0
 transport input ssh
 transport output none
!
ntp server 162.159.200.1
```

```
!
wsma agent exec
 profile exec
!
wsma agent config
 profile config
!
!
!
!
wsma profile listener exec
 transport https path /wsma/exec
!
wsma profile listener config
 transport https path /wsma/config
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager environment ZTD_SCEP_Period 30
event manager directory user policy "flash:/managed/scripts"
event manager policy LDevID-update.tcl type user authorization bypass
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm_ztd_scep.tcl type system authorization bypass
event manager applet save_certificate
 event syslog pattern "%PKI-6-CERTRET|%PKI-6-CERT_INSTALL: An ID"
 action 10.0 cli command "enable"
 action 11.0 cli command "write mem"
!
!
!
cgna gzip
!
cgna heart-beat interval 20
cgna heart-beat active
!
cgna profile cg-nms-tunnel
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://tps-san.ipg.cisco.com:9120/cgna/ios/tunnel
 gzip
!
cgna profile cg-nms-register
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
```

```
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://fnd-san.ipg.cisco.com:9121/cgna/ios/registration
 gzip
!
cgna profile cg-nms-periodic
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 add-command show platform resources | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/1/0 all | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/1/0 radio details | format flash:/managed/odm/cg-
nms.odm
 interval 60
 url https://fnd-san.ipg.cisco.com:9121/cgna/ios/metrics
 gzip
 active
!
!
cgna exec-profile CGNA-default-exec-profile
 add-command cgna exec profile cg-nms-register
 interval 1
 exec-count 1
!
!
!
end
```

6.3 POI recloser site IR1101 configuration

```
Building configuration...

Current configuration : 13106 bytes
!
! Last configuration change at 16:13:09 IST Thu Jul 4 2024 by cg-nms-administrator
! NVRAM config last updated at 15:30:59 IST Thu Jul 4 2024 by cg-nms-administrator
!
version 17.15
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
platform qfp utilization monitor load 80
platform hardware throughput level 250M
!
hostname FARFCW2543ZN63
!
boot-start-marker
boot system bootflash:ir1101-
universalk9.BLD_V1715_THROTTLE_LATEST_20240503_033217_V17_15_0_33.SSA.bin
boot-end-marker
!
!
vrf definition DTT_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition NMS_VRF
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition SCADA_VRF
 !
 address-family ipv4
```

```
 exit-address-family
 !
 address-family ipv6
 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
no ip gratuitous-arps
!
ip multicast-routing distributed
ip multicast-routing vrf DTT_VRF distributed
ip multicast vrf DTT_VRF auto-enable
ip host fnd-san.ipg.cisco.com 2001:DB8:BABA:F00D::103
ip host ra-vm241.ipg.cisco.com <RA IPv6 IP>
ip host tps-san.ipg.cisco.com <TPS IPv6 IP>
no ip domain lookup
!
!
!
!
!
!
!
!
!
login block-for 60 attempts 3 within 30
login delay 3
login on-success log
!
!
!
!
!
no ipv6 source-route
ipv6 unicast-routing
!
!
subscriber templating
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
key chain MyMACsecKEYchain macsec
 key 9999
  cryptographic-algorithm aes-128-cmac
  key-string 6
`TMcLZeB^X[EfcdQEFG`]FTVRebLPJIXSS]RUMKNgb]PFPSU^EYMXE`^QaGQJL\QEIRIX
password encryption aes
!
!
crypto pki trustpoint LDevID
 enrollment retry count 4
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password 7 114E5E
 fingerprint FBE6AFCFAF57C192955678F7B73BD06A233F20D2
 subject-name serialNumber=PID:IR1101-K9 SN:FCW2543ZN63,CN=FARFCW2543ZN63
 revocation-check none
 auto-enroll 90 regenerate
 hash sha256
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint fnd
 enrollment url bootflash://PnP-cert_07_08_53_UTC_Fri_Jun_28_2024
 revocation-check none
 hash sha256
!
crypto pki profile enrollment LDevID
```

```
 enrollment url  http://ra-vm241.ipg.cisco.com:8080
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = fan241-root-ca
!
crypto pki certificate chain LDevID
 certificate 58C16A3617795EE996A33B5A01B37397393C8EF7
 certificate ca 4DFB348D48F27F3A19333A8363CD8FA98A31743E
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
crypto pki certificate chain fnd
 certificate ca 4DFB348D48F27F3A19333A8363CD8FA98A31743E
!
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
no license feature hseck9
license udi pid IR1101-K9 sn FCW2543ZN63
license boot level network-advantage
license smart reservation
license smart transport off
archive
 path bootflash:/Archive/
 maximum 8
memory free low-watermark processor 43451
!
spanning-tree extend system-id
!
mka policy MyMACsecPolicy
 sak-rekey interval 300
!
!
!
!
username cg-nms-administrator privilege 15 secret 8
$8$Nzw8sA/UTua9JU$RMsfDmUEZ9HqaYxSgnbi0am2RuHRyd/u0rNekDT3bAQ
username user privilege 15 secret 9
$9$GHdWCZa3XR63RE$Zx9kay.r1EXuKh6L6C4KA0ROuvtaKu.tuE7tQag7h/I
```

```
!
redundancy
bridge-domain 1
 member vni 5555
 member Vlan651 service-instance 1
!
!
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface Loopback31
 route set interface
!
crypto ikev2 redirect client
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 2
!
crypto ikev2 nat keepalive 30
crypto ikev2 fragmentation mtu 1000
!
controller Cellular 0/1/0
 profile id 15 apn airtelgprs.com authentication none pdn-type ipv4v6
!
!
vlan internal allocation policy ascending
no cdp run
!
!
!
!
```

```
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 vrf forwarding NMS_VRF
 no ip address
 ip nat outside
 ipv6 address 2001:DB8:BABA:FACE::1025/128
!
interface Loopback15
 vrf forwarding DTT_VRF
 ip address 192.168.1.20 255.255.255.255
 ip pim sparse-mode
 ip nat outside
!
interface Loopback31
 vrf forwarding SCADA_VRF
 ip address 172.31.31.11 255.255.255.255
 ip nat outside
!
interface Tunnel10
 description to FNDHE241-C8000V
 vrf forwarding NMS_VRF
 no ip address
 ipv6 unnumbered Loopback0
```

```
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel11
 description to BGL-CC1-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel12
 description to BGL-CC2-HER-C8000V
 vrf forwarding SCADA_VRF
 ip unnumbered Loopback31
 ip nat outside
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel destination <Head End IPv6 IP>
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface GigabitEthernet0/0/0
 description shutdown by post_pnp EEM applet
 ip address dhcp
 shutdown
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
 description connected to HUB-SEL3505
```

```
 switchport trunk allowed vlan 1,651
 switchport mode trunk
 macsec network-link
 mka policy MyMACsecPolicy
 mka pre-shared-key key-chain MyMACsecKEYchain
!
interface Cellular0/1/0
 mtu 1358
 ip address negotiated
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip tcp adjust-mss 1318
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
interface Cellular0/1/1
 no ip address
 shutdown
!
interface Virtual-Template2 type tunnel
 vrf forwarding DTT_VRF
 ip unnumbered Loopback15
 ip mtu 1300
 ip pim sparse-mode
 ip tcp adjust-mss 1260
 nat64 enable
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1140
 tunnel source Cellular0/1/0
 tunnel mode gre ipv6
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Vlan1
 description IPv6 traffic to docker container for T104 (untagged frames from docker)
 vrf forwarding SCADA_VRF
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ipv6 address 2001:DB8:ABCD:EF:1225::1/64
```

```
!
interface Vlan651
 description SEL 3505 GOOSE communication on VLAN 651
 vrf forwarding DTT_VRF
 no ip address
 service instance 1 ethernet
  encapsulation dot1q 651
 !
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
interface nve1
 no ip address
 source-interface Loopback15
 member vni 5555 mcast-group 239.1.1.1
!
ip forward-protocol nd
ip pim bidir-enable
ip pim rp-address 192.168.1.20 bidir
ip pim vrf DTT_VRF rp-address 192.168.1.20 bidir
ip tcp mss 1260
ip tcp synwait-time 5
ip tcp path-mtu-discovery
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-client-auth
ip http secure-trustpoint LDevID
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface Loopback0
ip http client secure-trustpoint LDevID
!
ip nat inside source list IED_NW interface Loopback31 vrf SCADA_VRF overload
ip nat inside source static tcp 192.168.0.2 23 interface Loopback31 30023 vrf SCADA_VRF
ip nat inside source static tcp 192.168.0.2 20000 interface Loopback31 20000 vrf
SCADA_VRF
ip nat inside source static tcp 192.168.0.2 80 interface Loopback31 30080 vrf SCADA_VRF
ip route 0.0.0.0 0.0.0.0 10.10.100.100
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route vrf SCADA_VRF 172.19.107.0 255.255.255.0 Tunnel11
ip route vrf SCADA_VRF 172.31.31.10 255.255.255.255 Tunnel11
ip ssh bulk-mode 131072
```

```
ip ssh rsa keypair-name SSH
!
ip access-list standard IED_NW
 10 permit 192.168.0.0 0.0.0.255
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
ipv6 route 2001:DB8:CCCC:CCCC::/96 Tunnel10
ipv6 route ::/0 Cellular0/1/0
snmp-server group cgnms v3 priv
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps fru-ctrl
snmp-server enable traps aaa_server
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps c3g
snmp-server host 2001:DB8:BABA:F00D::103 version 3 priv cg-nms-administrator
snmp ifmib ifindex persist
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line 0/0/0
line 0/2/0
line vty 0 4
 exec-timeout 5 0
 length 0
 transport input ssh
 transport output none
line vty 5 14
 exec-timeout 5 0
 transport input ssh
```

```
 transport output none
!
ntp server 162.159.200.1
!
wsma agent exec
 profile exec
!
wsma agent config
 profile config
!
!
!
!
wsma profile listener exec
 transport https path /wsma/exec
!
wsma profile listener config
 transport https path /wsma/config
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager environment ZTD_SCEP_Period 30
event manager directory user policy "flash:/managed/scripts"
event manager applet save_certificate
 event syslog pattern "%PKI-6-CERTRET|%PKI-6-CERT_INSTALL: An ID"
 action 10.0 cli command "enable"
 action 11.0 cli command "write mem"
event manager policy LDevID-update.tcl type user authorization bypass
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm_ztd_scep.tcl type system authorization bypass
!
!
!
cgna gzip
!
cgna heart-beat interval 20
cgna heart-beat active
!
cgna profile cg-nms-tunnel
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://tps-san.ipg.cisco.com:9120/cgna/ios/tunnel
 gzip
!
```

```
cgna profile cg-nms-register
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://fnd-san.ipg.cisco.com:9121/cgna/ios/registration
 gzip
!
cgna profile cg-nms-periodic
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 add-command show platform resources | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/1/0 all | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/1/0 radio details | format flash:/managed/odm/cg-
nms.odm
 interval 60
 url https://fnd-san.ipg.cisco.com:9121/cgna/ios/metrics
 gzip
 active
!
!
cgna exec-profile CGNA-default-exec-profile
 add-command cgna exec profile cg-nms-register
 interval 1
 exec-count 1
!
!
!
end
```