

Distribution Automation – Feeder Automation Implementation Guide

This *Cisco Distribution Automation–Feeder Automation Implementation Guide* provides a comprehensive explanation of the Cisco Smart Grid Field Area Network solution implementation for Distribution Automation use cases such as Fault Location, Isolation, and Service Restoration (FLISR) and Volt/VAR. This implementation document includes information about the solution architecture, possible deployment models, and guidelines for deployment. It also recommends best practices and potential issues when deploying the reference architecture.

Navigator

The document covers the following:

Introduction, page 2	Describes the solution overview and implementation flow.
Solution Network Topology and Addressing, page 5	Discusses the Cisco DA Feeder Automation solution network topology, along with IP addressing used at every layer of the topology.
IoT Gateway Onboarding and Management, page 19	Discusses the steps to bootstrap the Cellular DA gateways and Cisco Field Area Routers, using a couple of PnP discovery methods, followed by Zero Touch Deployment. Captures the Implementation steps to setup the PnP Infrastructure required for bootstrapping.
Zero Touch Enrollment of Cisco Resilient Mesh Endpoints, page 63	Describes the steps to stage the Cisco WPAN Industrial Router (IR510), as well as Zero Touch Secure onboarding into CR mesh.
Application Traffic Communication Enablement, page 81	Explains the ICT implementation like routing, raw socket, and protocol translation, which are key for application traffic flow. Captures the steps to enable the SCADA communication on both Cellular DA gateways as well as CR mesh DA gateways.
End-to-End Application Use Case Scenarios, page 127	Explains the implementation details of the FLISR (Fault Location Isolation and Service Restoration), Volt/VAR use cases.
Volt/VAR, page 127	Explains the implementation details of the Volt/VAR use cases.
Distribution Automation Use Case Scenario - FLISR, page 144	Explains the implementation details of the FLISR (Fault Location Isolation and Service Restoration) use cases.
FLISR USE CASE SIMULATION using SEL AcSELerator application, page 152	Explains the simulation details of the FLISR (Fault Location Isolation and Service Restoration) use cases, using SEL application AcSELerator.
Edge Compute, page 191	Explains the implementation details to enable Edge compute capability on Cisco IR510 devices, as well as life cycle management of Edge compute applications on the IR510 IOx platform.
IP Services, page 216	Explains the implementation details of various IP services like Network Address Translation and Quality of Service.
Appendix A: PnP Profiles, page 226	Includes configs for the PnP profiles.

Introduction

Appendix B: FND Zero Touch Deployment Profiles, page 235	Includes configs for the FNZ Zero Touch Deployment profiles.
Appendix C: Device Configuration Profiles, page 244	Includes configs for the Device Configuration profiles.
Appendix D: SCADA ICT Enablement Profiles, page 246	Includes configs for the SCADA ICT Enablement profiles.
Appendix E: HER and CGR Configurations, page 250	Includes the HER and CGR configurations.

Audience

The audience for this guide comprises, but is not limited to, system architects, network/compute/systems engineers, field consultants, Cisco Advanced Services specialists, and customers. Readers should be familiar with networking protocols, Network Address Translation (NAT), Supervisory Control and Data Acquisition (SCADA) protocols, and be exposed to Field Area Networks.

New Capabilities in DA2.0 Feeder Automation

- Implementation details of the FLISR (Fault Location Isolation and Service Restoration) use cases.
- Simulation details of the FLISR (Fault Location Isolation and Service Restoration) use cases, using SEL application AcSELerator.

Introduction

The Cisco Field Area Network solution is a multi-service, secured, and scalable architecture, which addresses multiple utility use cases like Distribution Automation (DA), Advance Metering Infrastructure (AMI), Distributed Energy Resource (DER), and Demand Response (DR). This document details the implementation of FAN Distribution Automation, FLISR, and Volt/VAR use cases targeting deployment in the America region.

The implementation in this guide focuses on Distributed Network Protocol 3 (DNP3) and DNP3/IP SCADA protocols. For implementing Distribution Automation use cases using T101 or T104 SCADA protocols, please refer to the *Distribution Automation - Feeder Automation Implementation Guide* at the following URL:

https://salesconnect.cisco.com/open.html?c=06d2f8be-8c59-4d3d-9659-0d780c3da744

The Cisco FAN solution is a centralized two-tier architecture, as shown in Figure 1. Distribution Automation applications like Distribution Management System and Outage Management System reside in the Distribution System Operator (DSO) control center.

Cisco's Distribution Automation Gateways interface with Distribution Automation control devices like Capacitor Bank Controllers (CBCs) and recloser controllers that reside on the distribution feeder (in some cases, inside distribution substations like the Load Tap Controller). This interfacing could be either the Ethernet or Serial type.

Cisco's Distribution Automation Gateways could transport their traffic over a Cellular backhaul or Ethernet backhaul, or via the Neighbor Area Network (NAN) formed by Cisco Resilient Mesh Gateways. Cisco Gateways, which have one leg in the NAN tier and the other in the WAN tier, aggregate the distribution traffic from the NAN tier and route traffic to various DA applications via the WAN tier (which could be a Cellular or Fiber backhaul connection). To choose the correct DA Gateway, please refer to the *Distribution Automation – Feeder Automation Design Guide* at the following URL:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/DG/DA -FA-DG.pdf

Introduction

This implementation guide covers both Cisco Cellular Gateway and Cisco Resilient Mesh Gateway deployments.



Figure 1 Feeder Automation

Cisco Resilient (CR) Mesh implementation will be the correct choice for areas where Cellular coverage is not available or less prevalent. Cisco CR mesh has three types of devices:

- CR Mesh Co-ordination or Field Area Aggregation Router (FAR)
- CR Mesh Gateways or Field Devices (FD)
- CR Mesh Range Extenders

Cisco CGR 1240 with WPAN RF Module router plays the role of CR Mesh aggregator. CGR 1240 aggregates DA traffic and routes traffic to applications in the DSO control center. Distribution Automation controllers are connected to CR Mesh Gateways like IR510 via Ethernet or Serial (RS232) interfaces. When RF mesh coverage needs to be extended, Cisco IR530 could be deployed as range extenders. The CR Mesh is formed using FAR, FD, and range extenders and can be implemented in multiple PHY modes. This implementation guide is focused on DA use cases and requires relatively larger bandwidth when compared to the AMI use case; therefore, OFDM modulation with 800 Kbps profile has been chosen. This implementation covers Fixed OFDM 800 Kbps modulation. Adaptive Rate modulation, although supported, is not covered in this guide.

Cisco Cellular DA Gateways like IR1101, IR807, IR809, and CGR 1120 can be chosen for deployments where:

- DA Application demands more bandwidth and has time sensitive requirements.
- Distribution Feeder has better Cellular signal coverage (for example, urban areas).

The flow of this implementation guide is depicted in Figure 2.

Introduction





Note: For Headend Block Implementation, please refer to the *Cisco FAN - Headend Deep Dive Implementation and FAN Use Cases* at the following URL:

https://salesconnect.cisco.com/open.html?c=da249429-ec79-49fc-9471-0ec859e83872

Solution Network Topology and Addressing

This chapter, which focuses on the network topology used for solution validation and implementation of the Cisco DA Feeder Automation solution and the addressing (both IPv4 and IPv6) used in this implementation, includes the following major topics:

- Topology Diagram, page 5
- IPv4 and IPv6 Addressing, page 6

Topology Diagram

This section describes the high-level solution validation topology that has been used in this Feeder Automation Implementation Guide. Figure 3 depicts the high-level solution validation topology.



Figure 3 Cisco DA Feeder Automation Solution Validation Topology

The multiple layers of topology include:

- The Headend or Control Center Block, which hosts the DSO Control Center, includes:
 - DA application servers (for example, SCADA application server):
 - They could also host other application servers.
 - Network Operations Center (NOC), which hosts the following headend components:
 - Certificate Authority (RSA encryption), Dynamic Host Configuration Protocol (DHCP), Field Network Director (FND), FND Database, Authentication Authorization and Accounting (AAA), Active Directory (AD), Certificate Authority (ECC encryption), Fog Director (FD), Registration Authority (RA), Tunnel Provisioning Server (TPS), and Cluster of Headend Routers.

- These components are essential for the ZTD of the Cisco IOS Routers, which could be DA Gateways (IR1101, IR807, IR800) that are positioned along the Distribution Feeder or CGR1000 series of routers positioned as FARs.
- Headend block, which includes:
 - Private network, where the protected part of the headend is located, along with SCADA and other application servers.
 - DMZ network, where the exposed part of the headend is located; it includes TPS, RA, and HER Cluster.
- The WAN Block commonly refers to the public Internet over Ethernet/cellular backhaul. It could also be a private IP network.
- The Distribution Block, which comprises the following three major sub-blocks:
 - Cisco Cellular DA Gateways, which refer to Cisco IOS Routers like IR1100, IR807, and IR809.
 - Cisco Field Area Routers, which refer to Cisco IOS Routers like CGR1240 and CGR1120. These routers are used for aggregating the Cisco Resilient Mesh Endpoints (also referred as CR Mesh DA Gateways). The NAN Block is a subset of the Distribution Block, comprising CR Mesh devices, including Cisco FAR and CR Mesh endpoints.
 - Cisco Resilient (CR) Mesh DA Gateways with Edge Compute, which refer to the Cisco IR510 WPAN Industrial Router.
- The Utility Controller Devices Block, in which the Utility controller devices (real/simulated) are connected to the Cisco DA Gateways (Cellular DA Gateway or Mesh DA Gateway) over an Ethernet/Serial interface. The following components are simulated using the Triangle Micro Works (Distributed Test Manager or DTM) tool:
 - SCADA Master located in DSO Control Center
 - IEDs located in the Utility Controller Devices Block layer
- The NAN Block, which is comprised of three Personal Area Networks (PANs):
 - CR Mesh–PAN1
 - CR Mesh-PAN2
 - CR Mesh-PAN3

PAN3 has been validated over LTE backhaul. PAN1 and PAN2 have been validated over Ethernet backhaul. Cisco IOx Edge Compute functionality has been validated over PAN2. Fog Director (FD) located in the DSO control center has been used for the lifecycle management of Edge compute applications on the IOx platform of CR Mesh DA Gateway.

For implementation involving dual control scenarios, please refer to the *Distribution Automation – Feeder Automation Implementation Guide*.

IPv4 and IPv6 Addressing

This section, which provides detail about the addressing used at every layer of the Figure 1 Cisco DA Feeder Automation solution validation topology, includes the following sections:

- Addressing in the DSO Control Center Block, page 7
- Addressing in the WAN Block, page 10
- Addressing in the Distribution Block, page 10
- Addressing in the Utility Controller Devices Block, page 14

Addressing in the DSO Control Center Block

Figure 4 captures the granular details of the DSO Control Center.





The DSO Control Center is comprised of two types of network: the Private Network and the DMZ Network

- The Private Network hosts an UCS server (with all the required head end components like FND, Certificate Authority, DHCP server, and so on), SCADA Master as well as Fog Director. Private Network leverages the Cisco NTP for time synchronization, as well as Cisco DNS servers for name resolution.
- The DMZ Network hosts a cluster of Headend Routers (ASR 1000), TPS, and Registration Authority. These components connect to the DMZ Network on one side and the Private Network on the other side.

For more details about implementing the headend in the DSO Control Center, please refer to the *Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases Guide*.

Addressing in the Private Network

Table 1 captures the addressing details of the components located in the private network of DSO Control Center.

 Table 1
 DSO Control Center: Addressing in the Private Network

Component	Address Type	Address used in Private Network	VLAN used
RSA CA/AD/AAA	IPv4	172.16.102.2	102
FND	IPv4	172.16.103.243	103
	IPv6	2001:db8:16:103::243	103

Component	Address Type	Address used in Private Network	VLAN used
FND DB	IPv4	172.16.104.243	104
DHCP Server	IPv4	172.16.105.2	105
	IPv6	2001:db8:16:105::2	105
SCADA	IPv4	172.16.107.11	107
	IPv6	2001:db8:16:107::11	107
Fog Director	IPv4	172.16.103.150	103
ECC CA/AD/AAA	IPv4	172.16.106.175	106
RA	IPv4	172.16.241.2	241
TPS	IPv4	172.16.242.2	242
	IPv6	2001:db8:16:242::2	242
HER1	IPv4	172.16.101.251 172.16.102.251 172.16.103.251 172.16.104.251 172.16.105.251 172.16.106.251 172.16.107.251 172.16.241.251 172.16.242.251	101-107,241-242
	IPv6	2001:DB8:16:103::251 2001:DB8:16:105::251 2001:DB8:16:242::251	103, 105, 242
HER2	IPv4	172.16.101.252 172.16.102.252 172.16.103.252 172.16.104.252 172.16.105.252 172.16.106.252 172.16.107.252 172.16.241.252 172.16.242.252	101-107,241-242
	IPv6	2001:DB8:16:103::252 2001:DB8:16:105::252 2001:DB8:16:242::252	103,105,242
HER3	IPv4	172.16.101.253 172.16.102.253 172.16.103.253 172.16.104.253 172.16.105.253 172.16.106.253 172.16.107.253 172.16.241.253 172.16.242.253	101-107,241-242
	IPv6	2001:DB8:16:103::253 2001:DB8:16:105::253 2001:DB8:16:242::253	103,105,242

Table 1	DSO Control Center: A	Addressing in the	Private Network	(continued)
---------	-----------------------	-------------------	-----------------	-------------

		Address used in Private	
Component	Address Type	Network	VLAN used
HER Cluster (Virtual IP)	IPv4	172.16.101.1 172.16.102.1 172.16.103.1 172.16.104.1 172.16.105.1 172.16.106.1 172.16.107.1 172.16.241.1 172.16.242.1	101-107,241-242
	IPv6	2001:DB8:16:103::1 2001:DB8:16:105::1 2001:DB8:16:242::1	103,105,242
NTP	IPv4	ntp.esl.cisco.com (Cisco's NTP server)	N/A
DNS	IPv4	Cisco's DNS server	N/A
CPNR Server	IPv4	Cisco DHCP Server 172.18.105.2	105
	IPv6	2001:db8:18:105::2	

Table 1 DSO Control Center: Addressing in the Private Network (continued)

Addressing in the DMZ Network

The previous topology in Figure 4 shows that components that are located in the DMZ Network (reachable over WAN) include the following:

- Registration Authority (RA)
- Tunnel Provisioning Server (TPS)
- HER Cluster of ASR 1000 series of routers

Table 2 captures the addressing details of the components located in the DMZ network of DSO Control Center.

 Table 2
 DSO Control Center: Addressing in the DMZ Network

Component Name	Address Turse (IDuA/IDuC)	ID Address
Component Name	Address Type (IPV4/IPV6)	IP Address
Registration Authority	IPv4	10.10.100.241
	IPv6	2001:db8:10:241::5921
Tunnel Provisioning Server	IPv4	10.10.100.242
	IPv6	2001:db8:10:242::2
FAN-PHE-HER1	IPv4	10.10.100.101
	IPv6	2001:DB8:1010:903::2
FAN-PHE-HER2	IPv4	10.10.100.151
	IPv6	2001:DB8:1010:903::5
FAN-PHE-HER3	IPv4	10.10.100.152
	IPv6	2001:DB8:1010:903::6

Note: The Virtual IP for FAN-PHE-HER1, FAN-PHE-HER2, and FAN-PHE-HER3 is 10.10.100.100.

Addressing in the WAN Block

The Public IP WAN has been validated in this implementation guide. Addressing in the WAN block is typically service provider managed. As long as the Cisco FARs or Cisco Cellular IoT Gateways in the Distribution Block receive a dynamically-assigned IP address from the service provider and are able to reach the components in the DMZ network, the requirement would be met.

Addressing in the Distribution Block

Addressing in the Distribution blocks is discussed granularly in the following sections:

- Addressing used in Cisco Cellular DA Gateways, page 10
- Addressing used in Cisco Field Area Routers, page 11
- Addressing used in Cisco Resilient Mesh DA Gateways, page 12

Addressing used in Cisco Cellular DA Gateways

Figure 5 captures the various interfaces on the Cisco Cellular DA Gateways that are involved in the solution.



Figure 5 Addressing used in Cisco Cellular DA Gateways 256396

 Table 3 captures the addressing used in Cisco Cellular DA Gateways.

Table 3 Interface and its Addressing on Cisco Cellular DA Gateways

Interface Name	IP Address	Purpose
Ethernet Interface	192.168.0.1/24 2001:db8:192:168:0::1/64	Connects to IP-capable Ethernet-based Utility Controller device.
WAN Interface	Assigned by service provider dynamically.	Provides underlay routing reachability to the HER Cluster.
Loopback Interface	192.168.150.X/24 2001:db8:baba:face:W:X:Y:Z/128	Provisioned by the FND. Helps identify the DA Gateway uniquely in the solution. This would be in the same subnet as the HER loopback interface.
Tunnel Interface	Uses unnumbered loopback IPv4 and IPv6	Tunnel source is WAN interface IP Tunnel destination is the HER IP.
Async Interface	No IP	Connects to serial-based Utility Controller device.

Note: Some Cisco FAR devices available are CGR1120, CGR1240, IR1101 and IR807.

Addressing used in Cisco Field Area Routers

Figure 6 captures the various interfaces on the Cisco FARs that are involved in the solution.



Table 4 captures the various interfaces used in the Cisco FAR and its associated addressing.

Table 4 Interface and its Addressing on Cisco Cellular DA Gateways

Interface Name	IP Address	Purpose
WAN Interface	Assigned by service provider dynamically.	Provides underlay routing reachability to the HER Cluster.
Loopback Interface	192.168.150.X/24 2001:db8:baba:face:W:X:Y:Z/128	Provisioned by FND. Helps identify the Field Area Router uniquely in the solution. This would be in the same subnet as the HER loopback interface.
Tunnel Interface	Uses unnumbered loopback IPv4 and IPv6	Tunnel source is WAN interface IP Tunnel destination is the HER IP.
WPAN Interface	IP used in PAN1: 2001:db8:ABCD:1::1/64 IP used in PAN2: 2001:db8:ABCD:2::1/64 IP used in PAN3: 2001:db8:ABCD:3::1/64	Cisco Resilient Mesh Endpoints (IR510, IR530) would receive the address from the same subnet. This WPAN IP would serve as the default gateway for the CR Mesh endpoints.

Addressing used in Cisco Resilient Mesh DA Gateways

Figure 7 captures the various interfaces on the Cisco Resilient Mesh DA Gateways that are used in this solution.



Figure 7 Addressing used in Cisco Resilient Mesh DA Gateways

IR510 receives the IPv6 address for the LoWPAN interface from CGR. The IPv6 address of IR510 LoWPAN interface and the CGR WPAN interface are on the same IPv6 subnet. The CGR would serve as the default gateway for IR510.

Table 5 captures the various interfaces used in the CR Mesh DA Gateway and its associated addressing.

 Table 5
 Interface and its Addressing on Cisco Cellular DA Gateways

Interface Name	IP Address	Purpose
LoWPAN	2001:db8:ABCD:3:W:X:Y:Z1	Assigned by DHCP server (IPv6) dynamically.
Interface		Once the CR Mesh DA gateway registers with FND, FND uses this address to establish connectivity with IR510. This address is allocated with permanent lease by the DHCP server.
Loopback	10.153.10.xx	MAP-T BMR IPv4 addresses:
Interface	2001:db8:267:15xx:0:0a99:0axx:0	 10.153.10.xx is used by the IPv4 network outside the MAP-T domain to reach IR510.
		 MAP-T BMR IPv6 address has 1:1 relation with MAP-T BMR IPv4 address.
		 MAP-T BMR IPv6 address should be provided as part of csv file while importing the IR510.csv at FND.
Ethernet Interface	192.168.0.1	Default IP configured on the Ethernet interface of the IR510. Configurable from FND, which serves two purposes:
		 Connecting Ethernet-based Utility Controller device (can be configured with 192.168.0.3 for consistency).
		 Connecting to guest OS for Edge compute functionality.
Guest OS interface	192.168.0.2	Resides internal to the IR510, bridged to the Ethernet interface of the IR510 internally.
Async Interface	No IP	To connect to the serial-based Utility Controller device.

Addressing in the Utility Controller Devices Block

The Ethernet-based Utility Controller devices is to be configured with 192.168.0.3. It can be connected to the Ethernet ports of the Cisco Cellular DA Gateway or the CR Mesh DA Gateway. In this implementation, controller devices were simulated using Triangle Micro Works (Distributed Test Manager) tool. This simulated controller device is configured with 192.168.0.3 during this validation.

Solution Network Topology and Addressing for FLISR validation

This chapter, which focuses on the network topology used for solution validation and implementation of the Cisco DA 2.0 FLISR solution and the addressing (both IPv4 and IPv6) used in this implementation, includes the following major topics:

- Topology Diagram for FLISR, page 5
- IPv4 and IPv6 Addressing, page6

SEL FLISR solution is validated over Cisco Resilient Mesh on two different topologies. One is linear CR mesh with depth of 10 hops, which is typical rural deployment scenario and the second topology is aggregate CR mesh with depth of four rank nodes and four nodes connected at each rank level, Aggregate mesh is typically used in urban deployment scenario. For more details of these two types of deployment scenario, refer to Distribution Automation 2.0 – Feeder Automation Design Guide document.

Topology Diagram for FLISR

This Linear and Aggregated Mesh topology constructed using RF coax cables, power splitters and attenuators, enabling signal variations to construct a 10-hop linear and 23 nodes aggregated mesh network. In mesh network nodes that can hear each other, in that the RSSI (Reverse Signal Strength Indication) is within the acceptable range for a specific modulation (OFDM) fixed modulation and data rate established between parent, child, and neighbor nodes.

The RF connectivity between the DA gateways designed for IEEE 802.15.4 Option 2 (OFDM fixed modulation PHY mode149 on Cisco Resilient Mesh) which corresponds to a physical layer data rate of 800kbps. The OFDM 800kbps maximum Receive Signal Strength Indicator (RSSI) is -101db. To avoid node flapping and instability in the network a new node joining the mesh network for the first time must have minimum RSSI of -91db with respect to its neighbor. So, for a best practice design rule that the link between DA devices is designed the average link RSSI range between -70db to -90db.

The mesh radio parameter configured using IEEE 802.15.4g and Routing Protocol for Low Power and Lossy Networks (RPL) timers. Mesh is also configured to operate in Storing Mode to support peer to peer communication.

This section describes the solution validation topology that has been used in this DA 2.0 FLISR Implementation Guide.

Linear Mesh lab topology for FLISR

In linear topology each node has two neighbors, one parent from upper rank close to CGR and one child from lower rank. The RSSI also designed for same RSSI range as showing in the topology. On lower ranks, as the hop counts increase, the latency values also increase due to each node adds its own processing delays. So the end to end, i.e. each hop to control center path delay will be longer.

Figure 8 depicts the DA 2.0 Linear Mesh Lab Topology.





In the linear topology, fixed and variable attenuators are added to achieve an RSSI range of -70 to -90dB. RF Splitters are added at appropriate RF links, as shown in above lab topology figure, for creating a linear CR mesh.

Each SEL-3505 RTAC is connected to each IR510 device via Ethernet connection. SEL-3530 RTAC, which act as a SCADA Master and DAC Controller is located in Control Center.

Refer to Addressing in the DSO Control Center Block, page 7 section for the Control Center details.

Aggregated Mesh lab topology for FLISR

In aggregate topology the distance between DA Grid device is shorter and nodes can aggregate traffic from multiple children. The ratio of child to parent is higher and the parent available bandwidth is shared among the children. To simulate this network the 2nd, 3rd, and 4th rank nodes were designed to establish physical layer 1 connection with first node of parent rank. The aggregation topology can be designed in multiple way to select their parent, limitations are applied due to lab environment and worst conditions. Refer to the topology for this implementation.

Note: This implementation is purely based on the topology provided in this section.

Figure 9 depicts the DA 2.0 Aggregated Mesh Lab Topology.



Figure 9 Aggregate Mesh lab topology diagram

In the aggregate topology, fixed and variable attenuators are added to achieve an RSSI range of -70 to -90dB. RF Splitters are added at appropriate RF links, as shown in above lab topology figure, for creating a linear CR mesh.

Each SEL-3505 RTAC is connected to each IR510 device via ethernet connection. SEL-3530 RTAC, which act as a SCADA Master and DAC Controller is located in Control Center.

Refer to DSO Control Center Block section for the Control Center details.

IPv4 and IPv6 Addressing

For general and complete IPv4 and IPv6 addressing please refer to the "Solution Network Topology and Addressing" section in this document. The specific FLISR configurations are shown below.

Table 6 Additional compon	ents for Field Block for FLISR	
Component	Address Type	Address Used in Private network
SEL DAC Controller	IPv4	172.18.107.61

CGR 1240 Configuration

```
interface Wpan4/1
no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
ieee154 dwell window 12400 max-dwell 400
ieee154 panid 1
ieee154 ssid mesh-ha-s
```

```
ieee154 beacon-ver-incr-time 15
outage-server 2001:DB8:18:103::200
rpl dag-lifetime 60
rpl dio-dbl 2
rpl dio-min 16
rpl version-incr-time 10
rpl storing-mode
authentication host-mode multi-auth
authentication port-control auto
ipv6 address 2001:DB8:ABCD:1::1/64
ipv6 dhcp server dhcpd6-pool rapid-commit
no ipv6 pim
dot1x pae authenticator
end
```

Please refer to Zero Touch Enrollment of Cisco Resilient Mesh Endpoints for IR510 device.

IoT Gateway Onboarding and Management

This chapter includes the following major topics:

- Tunnel Provisioning Server/Field Network Director Categories, page 19
- Bootstrapping the IoT Gateway, page 20
- Deployment of the Cisco IoT Gateway, page 48

FND is used as the NMS in this solution. In this implementation guide, the terminology "IoT Gateway" is used to refer to both Cisco Cellular DA Gateways and Cisco FARs.

IoT Gateway Onboarding has been made very simple by following the steps below:

- 1. Unpack the box containing the new IoT Gateway.
- 2. Use plug-and-play (PnP) infrastructure to bootstrap.
- 3. After bootstrapping, power off the IoT Gateway and deploy at the desired location.
- 4. Power on the IoT Gateway for Zero Touch Deployment (ZTD).
- **5.** The device is fully operational.

As part of IoT Gateway onboarding with ZTD, the IoT Gateways are registered with the FND. From that point on, the FND located in the Control Center is used to remotely monitor/manage/troubleshoot the IoT Gateways, which are spread across the entire Distribution Automation network. This process has three phases:

- **1.** Bootstrap the IoT Gateway.
- **2.** Deploy the IoT Gateway.
- 3. Remote Monitor/Manage/Troubleshoot the IoT Gateway.

The two different approaches to bootstrapping and deployment of the IoT Gateway are:

- Approach 1-IoT Gateway bootstrapped in staging location, deployed in a different location
- Approach 2–IoT Gateway bootstrapped in deployment location

Both approaches are now supported by Cisco IoT Gateways and this guide.

With Approach 1, bootstrapping of the IoT Gateways is done at the dedicated staging location. Once the devices are bootstrapped successfully, they are powered off and transported to the final deployment locations, where the devices are deployed and powered on.

With Approach 2, bootstrapping of the IOT Gateways is done at the deployment location. Once the devices are bootstrapped successfully, the ZTD process begins and no manual intervention is required.

Tunnel Provisioning Server/Field Network Director Categories

Bootstrapping TPS/FND

The TPS/FND located in the staging/bootstrapping environment that helps with PnP bootstrapping of the IoT Gateways are referred to as the bootstrapping TPS and bootstrapping FND.

Network Operating Center

The TPS/FND located in the NOC/Control Center environment that helps with ZTD of IoT Gateways is referred to as the NOC or Control Center TPS/FND. This TPS/FND located in the DSO Control Center helps with management of the IoT Gateways.

Note: The bootstrapping TPS/FND could be the same as or different from the NOC TPS/FND depending on the chosen approach.

Since Approach 1 is chosen for implementation in this guide, two different pairs of TPS/FND have been implemented:

- Bootstrapping TPS/FND
- NOC TPS/FND

For general implementation of TPS/FND, please refer to the detailed steps covered in the following sections of the *Cisco* FAN-Headend Deep Dive Implementation and FAN Use Cases Guide:

- Implementing Tunnel Provisioning Server
- Implementing Field Network Director

The Cisco loT Field Network Director Installation Guide could also be referred to for implementation of TPS/FND.

Note: This guide focuses on the implementation details for enhancing the TPS/FND servers to also serve the functionality of Bootstrapping TPS and Bootstrapping FND.

Certificate Considerations for PnP and ZTD

Common Name and Subject Alternate Name requirements must be considered while creating certificates for the Bootstrapping TPS/FND and NOC TPS/FND. Table 7 captures the sample certificate parameter requirements of the certificate that are to be installed on the TPS/FND server.

Component Name	Common Name Requirement	Subject Alternate Name Requirement (FQDN) - Mandatory	Subject Alternate Name Requirement (IP) - Optional
PnP TPS	tps-san.ipg.cisco.com	tps-san.ipg.cisco.com	IP address of the TPS
PnP FND	fnd-san.ipg.cisco.com	fnd-san.ipg.cisco.com	Not Required
ZTD TPS	tps.ipg.cisco.com	Not Required	Not Required
ZTD FND	fnd.ipg.cisco.com	Not Required	Not Required

Table 7 Certificate Considerations for PnP and ZTD

PnP TPS and FND need to have their subject alternative name (and optionally their corresponding IP addresses) set to FQDN. Also, the Common Name must match the hostname FQDN used in the URL during a https communication from the IoT Gateways. ZTD, TPS, and FND must have Common Name entries match the hostname FQDN used in the URL during https communication from the IoT Gateways.

Note: If https communication is attempted on https://tps-san.ipg.cisco.com:9120, then the Common Name of the certificate installed on the target server must match the FQDN (tps-san.ipg.cisco.com) accessed in the URL.

Note: If https communication is attempted on https://10.10.242.242:9120, and if the Common Name of the certificate installed on the target server only has FQDN (and not IP), the SSL connection may not establish.

Bootstrapping the IoT Gateway

Bootstrapping can also be referred to with the following terminology:

- Day 0 provisioning
- ZTD staging
- PnP staging
- Application of manufacturing configuration onto IoT Gateway
- Generation of Express Configuration

On the bootstrapping FND, import the bootstrapping csv file and then assign the IoT Gateways to the correct bootstrapping group. Bootstrapping will occur automatically when the IoT gateway is powered on.

Note: To bootstrap the IoT Gateway, in the case of Approach 1, just connect the IoT Gateway to the Ethernet PnP Staging switch, and then power it on. In the case of Approach 2, just insert the LTE SIM cards (or connect the Ethernet link) with internet access on the IoT Gateway and power it on.

Bootstrapping is achieved with the help of the Cisco Network PnP solution. This section focuses on building the infrastructure required for bootstrapping to happen. The "Cisco Network PnP - Available Methods" section of the Design Guide discusses multiple methods for PnP server discovery. Three PnP server discovery methods, which have been implemented as part of this guide, are:

- PnP server discovery through Cisco PnP Connect–validated with Approach 2
- PnP server discovery through DHCP server-validated with Approach 1
- PnP server discovery through manual PnP profile-validated with Approach 1

Preparing the Bootstrapping Infrastructure

The bootstrapping infrastructure, which involves multiple actors, is captured in Table 8.

 Table 8
 Actors in the Bootstrapping Infrastructure

Actor	Name	Description				
PnP Agent	IoT Gateway	Responsible for initiating the bootstrapping request. This agent comes by default with the latest release of Cisco IOS. No implementation is required. The PnP agent on IoT Gateway must be supporting the following PnP services:				
		1. Certificate Install service				
		2. File Transfer service				
		3. CLI - Exec service				
		4. CLI - Configuration service				
PnP Server Information Provider	DHCP server or DNS server or Cloud Redirection Server	The IoT Gateway must somehow learn the details of the PnP server (also called a Bootstrapping server). This could be learnt dynamically or manually.				
		The dynamic approaches, in which any of the following actors provides the PnP server detail, include:				
		– DHCP server				
		 DNS server 				
		 Cisco PnP Cloud Redirection Service 				
		The manual approach, in which the PnP server detail is configured manually in the profile, is:				
		 Custom PnP server profile configuration 				
PnP Proxy	Tunnel Provisioning	Responsible for mediating the bootstrapping request between the IoT Gateway and the FND.				
	Server	Optional but highly recommended. This component has been implemented in this guide, since it is highly recommended.				
		Acts as PnP server for the IoT Gateway and proxies the incoming request from IoT Gateway to the PnP server.				
PnP Server	Field Network Director	Responsible for processing the bootstrapping request.				
		PnP server receives the communication from the PnP Proxy.				
		PnP server is responsible for provisioning the Day 0 configuration on the IoT gateway. The required Day 0 configuration could be created as Template 26 under the Bootstrapping Template section of the FND.				

This section is discussed in the following phases:

- Prerequisites, page 23
- Certificate Creation and Installation, page 23
- Installation of Bootstrapping TPS, page 25
- Installation of Bootstrapping FND, page 26

- Configuration of Bootstrapping TPS, page 27
- Configuration of Bootstrapping FND, page 29

Prerequisites

- The TPS and FND server must be up and running.
- This section focuses only on the incremental portions to make the regular TPS/FND a bootstrapping TPS/FND.
- Routing reachability over IPv4 and/or IPv6 networks from IoT Gateways to TPS.
- Routing reachability between TPS and FND.

Certificate Creation and Installation

This section captures the parameters that need to be considered while creating the certificate for the TPS (PnP Proxy) and FND (PnP server).

Note: For detailed instructions about certificate creation, please refer to the section "Creation of Certificate Templates and Certificates" of the *Cisco FAN-Headend Deep Dive Guide*.

Certificate Creation for Bootstrapping TPS

The certificate for the TPS must be created with both the Subject Name and the Subject Alternative Name fields populated.



		C	ertificate P	roperties	s		x
🛕 Subject	General	Extensions	Private Key	Certificatio	n Authority	Signature	·
The subject can enter in can be used	The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.						
Subject of c	ertificate		i dan the cont	if esta			
Subject nam	compute ne:	r that is rece	iving the cen	Incate			
<u>Type</u> :					CN=tps-sa O=Cisco S	an.ipg.cisco Systems Inc	.com
Organizati	on	~	Add	>		,,	
Value:			< Rem	ove			
Alternative	name:						
Туре:		_			DNS tps-san.ip	a.cisco.con	
DNS		~			172.16.242	.2	
Val <u>u</u> e:			Add	>			
			< Rem	ove			
	OK Cancel <u>A</u> pply						

The Subject Name is the Common Name that must be set to the FQDN of the PnP Proxy. The Subject Alternative Name must be set to the FQDN of the PnP Proxy, along with the optional IP address. The Subject Alternative Name is required for PnP to work. The enrolled certificate is exported as PnP-TPS.pfx and is protected with a password.

Certificate Creation for Bootstrapping FND

The FND certificate must be created with both the Subject Name and Subject Alternative Name fields populated.



		C	ertificate P	ropertie	s		x	
🛕 Subject	General	Extensions	Private Key	Certificati	on Authority	Signature	·	
The subject can enter in can be used	The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.							
Subject of c	ertificate							
The user or o	compute	r that is rece	iving the cert	ificate				
Type:	ie:				CN=fnd-s	an.ipg.cisco	o.com	
Organizatio	on	~	Add	>	O=Cisco S	Systems Inc		
Value:			< Per	0.1/9				
			< Kem	ove				
Alternative r	name:							
Т <u>у</u> ре:		_			DNS fnd-san.ip	g.cisco.cor	n	
DNS		~			172.16.103	.243		
Val <u>u</u> e:			Add	>				
			< Rem	ove				
			s nem					
OK Cancel <u>Apply</u>								

The Subject Name is the Common Name that must be set to the FQDN of the PnP Server. The Subject Alternative Name must be set to the FQDN of the PnP Server, along with the optional IP address. The Subject Alternative Name is required for PnP to work. The enrolled certificate is exported as PnP-FND.pfx and is protected with a password.

Installation of Bootstrapping TPS

The bootstrapping procedure in this implementation considers the use of TPS as PnP Proxy.

Note: As TPS is used in this implementation, TPS would represent itself as the PnP server for the IoT Gateways. Therefore, TPS is referred to as the PnP Proxy. For installation of TPS, please refer to the detailed steps covered under the section "Implementing Tunnel Provisioning Server" of the *Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases Guide*.

TPS Certificate Installation on the Bootstrapping TPS

For installation of the certificate on the Bootstrapping TPS, please refer to the detailed steps covered under the section "Certificate Enrollment Phase for TPS Proxy Server" of the *Cisco FAN - Headend Deep Dive Implementation and FAN Use Cases Guide*.

Note: Please use PnP-TPS.pfx while enrolling the certificate on the TPS.

The following are the brief steps:

To view the content of the "Pnp-TPS.pfx" certificate:

keytool -list -v -keystore PnP-TPS.pfx -storetype pkcs12

<- Enter the password configured during certificate export. Note down the alias name (for example: le-custom_rsa_template- 5090cdbf-2ff8-4ec2-9a97-7b77a3d77912)

To import the certificate:

```
keytool -importkeystore -v -srckeystore PnP-TPS.pfx -destkeystore cgms_
keystore -srcstoretype pkcs12 -deststoretype jks -destalias cgms
```

```
-destkeypass 'Password_Protecting_Keystore_in_TPS'-srcalias le-
custom rsa template-5090cdbf-2ff8-4ec2-9a97-7b77a3d77912
```

Cisco SUDI Certificate Installation on the Bootstrapping TPS

Cisco SUDI CA can be installed into the cgms_keystore of TPS using the following command:

```
keytool -importcert -trustcacerts \
-file cisco-sudi-ca.pem \
-keystore cgms_keystore \
-alias sudi
```

The Cisco SUDI CA file "cisco-sudi-ca.pem" can be fetched from the FND, from the following location "/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem"

Installation of Bootstrapping FND

For installation of FND, please refer to the detailed steps covered under the section "Implementing Field Network Director" of the Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases Guide.

FND Certificate Installation on the Bootstrapping FND

For installation of the certificate on the Bootstrapping FND, please refer to the detailed steps covered under the section "Certificate Enrollment onto FND's Keystore" of the *Cisco FAN Headend Deep Dive Implementation and FAN Use Cases Guide*.

Note: Please use PnP-FND.pfx while enrolling the certificate on the FND.

Cisco SUDI Certificate Installation on the Bootstrapping FND

Cisco SUDI CA can be installed into the cgms_keystore of FND using the following command:

```
keytool -importcert -trustcacerts \
-file /opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem \
-keystore cgms keystore -alias sudi
```

Configuration of Bootstrapping TPS

This section covers the configuration steps and the final verification steps on the TPS.

TPS Proxy Properties Configuration TPS

Proxy Properties file needs to be configured with the following details:

- inbound-bsproxy-destination: Address to which the bootstrapping requests be forwarded.
- enable-bootstrap-service: Is bootstrapping service enabled/disabled?
- bootstrap-proxy-listen-port: Port on which the PnP Proxy must be listening for processing bootstrapping requests (default port is 9125).

```
[root@tps-san ~]# cat /opt/cgms-tpsproxy/conf/tpsproxy.properties ##
Configuration created as part of regular TPS installation. inbound-proxy
destination=https://fnd-san.ipg.cisco.com:9120 outbound-proxy-allowed-addresses=fnd
san.ipg.cisco.com cgms-keystore-password-hidden=7jlXPniVpMvat+TrDWqhlw==
### Configuration required for Bootstrapping.
```

```
inbound-bsproxy-destination=http://fnd-san.ipg.cisco.com:9125 enable-bootstrap
service=true
bootstrap-proxy-listen-port=9125
[root@tps-san ~]#
```

Name resolution entries have to be present for FND FQDN in the /etc/hosts file.

Mandatory Verification Checks on TPS Proxy

The verification checks include the following:

- FND FQDN entry in /etc/hosts.
- TPS must have three certificates installed into the cgms_keystore:
 - Certificate signed by Utility PKI for TPS (with private key)
 - Public Certificate of the Utility PKI CA server
 - Public Certificate of the Cisco SUDI CA
- Hostname consistency with the certificate.
- There shouldn't be any unreachable name servers in /etc/resolv.conf.
- NTP daemon should be running. Time should be synchronized.
- Necessary firewall ports must have been opened up, if the firewall/iptables/ip6tables are enabled:
 - TCP Port 9125 to process http communication
 - TCP port 9120 to process https communication FND FQDN entry in /etc/hosts:

```
[root@tps-san ~]# cat /etc/hosts
127.0.0.1localhost localhost.localdomain localhost4 localhost4.localdomain4 tps
san.ipg.cisco.com
```

::1localhost localhost.localdomain localhost6 localhost6.localdomain6 tpssan.ipg.cisco.com

172.16.103.243 fnd-san.ipg.cisco.com 2001:db8:16:103::128 fnd-san.ipg.cisco.com

[root@tps-san ~]#

TPS must have three certificates installed into the cgms_keystore:

- The certificate entry 'root' represents the Utility PKI CA certificate.
- The certificate entry 'sudi' represents the Cisco SUDI CA certificate.
- The certificate entry 'cgms' represents the private certificate of the TPS server signed by the (custom) Utility PKI CA server.

```
keytool -list -keystore /opt/cgms-tpsproxy/conf/cgms_keystore:
Enter keystore password:
```

```
root, Jun 4, 2017, trustedCertEntry, Certificate fingerprint (SHA1):
CF:A2:61:30:29:B1:1E:46:14:30:A2:DC:5F:62:41:47:CC:EE:64:69
sudi, Jul 11, 2018, trustedCertEntry, Certificate fingerprint (SHA1):
F6:96:9B:BD:48:E5:F6:12:5B:93:4D:01:E7:1F:E9:C2:7C:6F:54:7E
cgms, Oct 5, 2018, PrivateKeyEntry, Certificate fingerprint (SHA1):
B7:2A:74:61:53:74:73:65:2D:61:98:EC:69:09:93:4A:E2:D0:E5:6F
[root@tps-san ~]#
```

Hostname should match certificate Common Name/SAN:

```
[root@tps-san ~]# hostname
tps-san.ipg.cisco.com [root@tps-san ~]#
[root@tps-san ~]# cat /etc/sysconfig/network NETWORKING=yes
HOSTNAME=tps-san.ipg.cisco.com GATEWAY=172.16.242.1
NTPSERVERARGS=iburst [root@tps-san ~]#
[root@tps-san ~]# keytool -list -keystore /opt/cgms- tpsproxy/conf/cgms_keystore -alias
cgms -v | grep "CN=" Enter keystore password: [press Enter]
< .. removed for clarity ..>
Owner: CN=tps-san.ipg.cisco.com, O=Cisco Systems Inc Issuer: CN=IPG-RSA-ROOT-CA,
DC=ipg, DC=cisco, DC=com
< .. removed for clarity ..>
[root@tps-san ~]#
```

Note: No unreachable name servers should exist. Either the name servers should be present and reachable or they should be empty. Any unreachable name server address entry must be taken care or removed under the network interface configuration.

```
[root@tps-san ~]# cat /etc/resolv.conf #
Generated by NetworkManager search ipg.cisco.com
# No nameservers found; try putting DNS servers into your # ifcfg files in
/etc/sysconfig/network-scripts like so: #
# DNS1=xxx.xxx.xxx # DNS2=xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
[root@tps-san ~]#
```

NTP daemon should be running. Time should be synchronized:

```
[root@tps-san ~]# ntpstat
synchronised to NTP server (172.16.242.1) at stratum 6 time correct to within 27 ms
polling server every 1024 s
[root@tps-san ~]#
```

Note: The TPS server should be time synchronized. Otherwise, the https communication from the IoT Gateway might not reach the TPS Proxy Application.

Configuration of Bootstrapping FND

This section covers the configuration steps and the final verification steps on the FND.

CGMS Properties Configuration

The CGMS Properties file needs to be configured with the following details:

- proxy-bootstrap-ip-Address of the PnP Proxy from which the bootstrapping requests are processed
- enable-bootstrap-service-Enable/Disable the bootstrapping service
- bootstrap-fnd-alias—The trust point alias to be used during bootstrapping of the IoT Gateway
- **ca-fingerprint**-fingerprint of the 'root' trustpoint

[root@fnd-san conf]# cat /opt/cgms/server/cgms/conf/cgms.properties

```
## Configuration created as part of regular FND installation.
cgms-keystore-password-hidden=7jlXPniVpMvat+TrDWqhlw==
cgdm-tpsproxy-addr=tps-san.ipg.cisco.com
cgdm-tpsproxy-subject=CN="tps-san.ipg.cisco.com", O="Cisco Systems Inc"
#
## Configuration required for Bootstrapping.
enable-bootstrap-service=true
proxy-bootstrap-ip=tps-san.ipg.cisco.com bootstrap-fnd-alias=root
ca-fingerprint=CFA2613029B11E461430A2DC5F624147CCEE6469
#
[root@fnd-san conf]#
```

Name resolution entries have to be present for TPS FQDN in the /etc/hosts file.

Mandatory Verification Checks on FND

Verification checks include the following:

- TPS FQDN entry in the /etc/hosts file.
- FND must have three certificates installed into the cgms_keystore:
 - Certificate signed by Utility PKI for FND (with private key)
 - Public Certificate of the Utility PKI CA server
 - Public Certificate of the Cisco SUDI CA
- Hostname must be consistent with the certificate.
- No unreachable name servers in /etc/resolv.conf should exist.
- NTP daemon should be running. Time should be synchronized.
- Necessary firewall ports must have been opened up if the firewall/iptables/ip6tables are enabled:
 - TCP Port 9125 to process http communication
 - TCP port 9120 to process https communication

TPS/FND FQDN entry in the /etc/hosts file:

```
[root@tps-san ~]# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 fnd
san.ipg.cisco.com
#
172.16.104.244 fnddb.ipg.cisco.com
172.16.242.2 tps-san.ipg.cisco.com
2001:db8:16:242::128 tps-san.ipg.cisco.com
[root@tps-san ~]#
```

FND must have three certificates installed into the cgms_keystore:

- The certificate entry 'root' represents the Utility PKI CA certificate.
- The certificate entry 'sudi' represents the Cisco SUDI CA certificate.
- The certificate entry 'cgms' represents the private certificate of the FND server signed by the (custom) Utility PKI CA server.

keytool -list -keystore /opt/cgms/server/cgms/conf/cgms_keystore Enter keystore password:

Hostname should match the certificate Common Name/SAN:

```
[root@fnd-san conf]# hostname fnd-san.ipg.cisco.com
[root@fnd-san conf]#
[root@fnd-san conf]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=fnd-san.ipg.cisco.com
NTPSERVERARGS=iburst
[root@fnd-san conf]#
[root@fnd-san conf]#
[root@fnd-san conf]# keytool -list -keystore
/opt/cgms/server/cgms/conf/cgms_keystore -v -alias cgms | grep CN=
Enter keystore password: [press Enter]
< .. removed for clarity ..>
Owner: CN=fnd-san.ipg.cisco.com, O=Cisco Systems Inc Issuer: CN=IPG-RSA-ROOT-CA, DC=ipg,
DC=cisco, DC=com
< .. removed for clarity ..>
[root@fnd-san conf]#
```

Note: No unreachable name servers should exist. Either the name servers should be present and reachable or they should be empty. Any unreachable name server address entry must be taken care or removed under the network interface configuration:

```
[root@fnd-san conf]# cat /etc/resolv.conf
# Generated by NetworkManager
search ipg.cisco.com
# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so: #
# DNS1=xxx.xxx.xxx
# DNS2=xxx.xxx.xxx
# DNS2=xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
[root@fnd-san conf]#
```

NTP daemon should be running. Time should be synchronized:

```
[root@fnd-san conf]# ntpstat
synchronised to NTP server (172.16.103.1) at stratum 6 time correct to within 45 ms
polling server every 1024 s
[root@fnd-san conf]#
```

Note: The FND server should be time synchronized. Otherwise, the https communication from the IoT Gateway might not reach the FND (cgms) application.

Csv File Import on FND GUI

A sample csv file that can be imported into FND for bootstrapping of IoT Gateway is shown below:

```
deviceType, eid, tunnelSrcInterface1, adminUsername, adminPassword, hostnameF
orBs, domainname, bootimage
cgr1000,CGR1240/K9+JAD2043000Q,Cellular0/1,cq-nms-administrator,<encrypted pwd>,
CGR1000 JAD2043000Q, ipg.cisco.com, flash:/cgr1000-universalk9-mz.SPA.158-3.M
ir800,IR807G-LTE-GA-K9+FCW2231004T,FastEthernet0,cg-nms
administrator,<encrypted_pwd>,IR807_BS1,ipg.cisco.com,flash:/ir800l- universalk9-mz.SPA.1573.M
2.bin
ir1100, IR1101-K9+FCW222700K0, GigabitEthernet0/0/0, cg-nms-
administrator, <encrypted pwd>, IR1100 FCW222700K0, ipq.cisco.com, flash:/ir 1101
universalk9.BLD_V1610_1_THROTTLE_LATEST_20181029_041528.SSA.bin
cgr1000,CGR1120/K9+JAD191601KT,GigabitEthernet2/1,cg-nms-
administrator,<encrypted_pwd>,CGR1K_BS1,ipg.cisco.com,flash:/managed/images/cgr1000
universalk9-mz.SPA.158-3.M ir800, IR829GW-LTE-GA-EK9+FGL195024PP, Vlan1, cg-nms
administrator, <encrypted pwd>, IR829 FGL195024PP, ipq.cisco.com, flash:/ir800-universalk9
mz.SPA.157-3.M3
ir800, IR809G-LTE-GA-K9+JMX1941X00B, GigabitEthernet0, cg-nms-
administrator,<encrypted_pwd>,IR809_ JMX1941X00B,ipg.cisco.com,flash:/ir800-universalk9
mz.SPA.157-3.M3
```

Note: Ensure that there aren't any blank spaces while using this csv file.

Table 9Fields of the IoT Gateway Bootstrapping csv File

Parameter	Name	Parameter Value Explanation
deviceType	ir1100	Helps identify the type of device; for example: ir800 cgr1000 ir1100 cgr1000
eid	IR1101-K9+FCW222700K0	Unique network element identifier for the device.
tunnelSrcInterface1	GigabitEthernet0/0/0	Name of the WAN interface that the FAR would use to reach the Headend.
adminUsername	cg-nms-administrator	Username that FND must use to interact with the IoT Gateway.

Parameter	Name	Parameter Value Explanation
adminPassword	<encrypted_pwd></encrypted_pwd>	Password in encrypted form. An unencrypted form of this password would be used by the FND to interact with the FAR.
hostnameForBs	IR1100_FCW222700K0	Hostname for bootstrapping.
domainname	ipg.cisco.com	Domain name for the bootstrapped router.
bootimage	flash:/ir1101-universalk9.SSA.bin	Boot image name.

Table 9 Fields of the IoT Gateway Bootstrapping csv File

Figure 12 Bootstrapping CSV Import at Bootstrapping FND

Inthe IoT	DASHBOARD DEVICES OPERATIONS CONFIG	 Ap
DEVICES > FIELD DEVICES	deviceCategory:router Q Show Filters Guice V Invitibule +	
C All FAM Davices	Map Inventory E) Cellular-CDMA Cellular-GSM Config DHOP Config Elternet Traffic Firmware T Pris Tenamic AddDevcet Label - Buk Oserston - More Actions - Tenamical Tenamic	Tunnel
BENDPOINT (7)	Add Devices Upload File	×
	CSV/XML C-trake path WASTER_CSV_FILE_FOR_PNP.tx Browse File: Download sample .csv template for Router, Gateway, Endpoint and Extender, IR500	

In bootstrapping FND:

- 1. From Devices > Field Devices, click Router in the left pane.
- 2. Click the **Inventory** tab on the middle pane.
- 3. Click Add Devices.
- 4. Browse the csv file created in the previous step.
- 5. Then click Add to import the IoT Gateway CSV list into the bootstrapping FND.

DHCP Server-Assisted PnP Provisioning

This section is discussed in the following phases:

- Prerequisites, page 32
- Bootstrapping in the IPv4 Network, page 33
- Bootstrapping in the IPv6 Network, page 33
- Logical Call Flow, page 38

Prerequisites

PnP Proxy must be reachable either over the LAN or over the WAN/Internet. As TPS is used in this implementation, TPS acts as the PnP server for the IoT Gateways. The DHCP server advertises TPS details in place of the PnP server details.

Bootstrapping in the IPv4 Network

This section discusses the DHCP server-assisted bootstrapping of the IoT Gateways over the IPv4 network. In Figure 13, IoT Gateways obtain the IP address dynamically from the DHCP server along with details of the PnP server (which, in this case, is actually that of PnP Proxy, as TPS is deployed).

- The PnP server details are received using DHCP option 43.
- The PnP agent (residing on the IoT Gateway) then reaches out to PnP Proxy over IPv4 LAN/WAN network over http on port 9125 and then over https on port 9120.



Figure 13 DHCP Server-Assisted Bootstrapping of IoT Gateways over IPv4 Network

Bootstrapping in the IPv6 Network

This section discusses the DHCP server-assisted bootstrapping of the IoT Gateways over the IPv6 network.

- IoT Gateways obtains the IP address dynamically from the DHCP server along with details of the PnP server (which, in this case, is actually that of PnP Proxy, as TPS is deployed).
- The PnP server details are received using DHCP option 9.
- The PnP agent (residing on the IoT Gateway) then reaches out to PnP Proxy over IPv6 LAN/WAN network over http on port 9125 and then over https on port 9120.

Logical Call Flow

This section discusses the logical call flow sequence with the DHCP server-assisted bootstrapping of the IoT Gateways over the IPv4/IPv6 network. Figure 14 shows the following actors:

- PnP Agent (IoT Gateway)
- DHCP Server

- DNS Server
- PnP Proxy (TPS)
- PnP Server (FND)

Figure 14 DHCP Server-Assisted Bootstrapping of IoT Gateways–Logical Call Flow



- When the IoT Gateway is powered on, the PnP Agent on the IoT Gateway checks for the presence of the startup configuration. If the startup configuration is not found, then the PnP agent performs "no shut" and enables DHCP on all the interfaces.
- 2. The IOS on the IoT Gateway sends out a DHCP request, which reaches the DHCP server (either directly or with the help of DHCP relay agent).
- 3. The DHCP server responds back with the IPv4 address along with option 43, or the IPv6 address along with option 9. The option contains the FQDN of the PnP server to talk to (for example, tps-san.ipg.cisco.com) and the port number (for example, 9125) on which the PnP Proxy/Server is expected to be listening. The PnP server detail advertised as part of the DHCP option is the IP address of the PnP Proxy instead of the actual PnP server (with TPS deployed as part of the solution).
- 4. The IoT Gateway then sends out a name resolution request to DNS server to resolve the FQDN to its corresponding IPv4/IPv6 address.
- 5. The PnP Agent attempts its communication with the PnP Proxy over port 9125 (over http). PnP Proxy, in turn, communicates with the FND on port 9125. Bootstrapping begins at the FND from this point. The prerequisite to processing this bootstrapping request from the IoT Gateway is the addition of IoT Gateway details into the FND with the loading of the csv file.
- 6. The FND installs the trust point on the IoT Gateway.
- The IoT Gateway sends out a Get CA Certificate request to PnP Proxy, which, in turn, proxies the communication to the FND. The FND would respond back with the CA certificate of the FND's trust point, which would then be installed on the IoT Gateway.

The following PnP States would have transitioned at the FND:

- CONFIGURING_HTTP_FOR_SUDI
- CONFIGURED_HTTP_FOR_SUDI
- CREATING_FND_TRUSTPOINT
- AUTHENTICATING_WITH_CA
- AUTHENTICATED_WITH_CA
- 8. From this point onwards, the further communication switches over to https on port 9120. The IoT Gateway would communicate with the TPS IP on port 9120, which, in turn, is sent to the FND IP on port 9120. The rest of the IoT Gateway bootstrapping happens over this secure https communication established on port 9120.

Note: Since the communication is over https, time synchronization and certificate parameters matching must be taken care of:

- For example, if <a href="https://<TPS_FQDN>:9120">https://<TPS_FQDN>:9120 is attempted, then the certificate installed on the TPS must have CN/SAN configured with <TPS_FQDN>.
- Similarly, if the <a href="https://<TPS_IP>:9120">https://<TPS_IP>:9120 is attempted, then the certificate installed on the TPS must also have CN/SAN configured with <TPS_IP>. Otherwise, SSL failure might occur and the https://www.scale.org CN/SAN configured with <TPS_IP>. Otherwise, SSL failure might occur and the https://www.scale.org CN/SAN configured with <TPS_IP>. Otherwise, SSL failure might occur and the https://www.scale.org Gateway might not reach the TPS Proxy Application on port 9120.

FND would transition through the following PnP states while the bootstrapping progresses:

- UPDATING_ODM
- UPDATING_ODM_VERIFY_HASH
- UPDATED_ODM
- COLLECTING_INVENTORY
- COLLECTED_INVENTORY
- VALIDATING_CONFIGURATION
- VALIDATED_CONFIGURATION
- PUSHING_BOOTSTRAP_CONFIG_FILE
- PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH
- PUSHED_BOOTSTRAP_CONFIG_FILE
- CONFIGURING_STARTUP_CONFIG
- CONFIGURED_STARTUP_CONFIG
- APPLYING_CONFIG
- APPLIED_CONFIG
- TERMINATING_BS_PROFILE
- BOOTSTRAP_DONE

9. Bootstrapping would be complete with the "BOOTSTRAP_DONE" PnP State.

Custom PnP Profile for PnP Server

This section is discussed in the following phases:

- Prerequisites, page 36
- Bootstrapping over IPv4 Network, page 36
- Bootstrapping over IPv6 Network, page 37
- Logical Call Flow, page 38

As a gateway of last resort, if dynamic ways of learning the PnP Server are not an option, an option does exist to enable learning about the PnP server with minimal manual configuration.

Manual PnP profile configuration with PnP server details:

```
!
ip host tps-san.ipg.cisco.com 172.16.242.2
!
pnp profile fnd-pnp-profile
transport http host tps-san.ipg.cisco.com port 9125
!
```

Note: Only the PnP Server detail is manually configured. Bootstrapping and Deployment (the rest of ZTD) still happens dynamically.

Prerequisites

- The PnP server must be reachable either over the LAN or over the WAN/Internet.
- As TPS is used in this implementation, TPS acts as a PnP server for the IoT Gateways.

Bootstrapping over IPv4 Network

This section focuses on the bootstrapping of the IoT Gateways over the IPv4 network in the absence of the DHCP server, DNS server, and Cisco Cloud redirector server to provide the PnP server details. IoT Gateways are informed about the PnP server detail directly through the Cisco IOS configuration commands.

In Figure 15, the manual PnP profile configuration on the IoT Gateways lets the IoT Gateways learn about the PnP server that should be reached out to and the desired PnP port number. For example, the custom PnP profile is configured to reach out to the PnP server (tps-san.ipg.cisco.com) over the http on port 9125.


Figure 15 Custom PnP Profile-Assisted Bootstrapping of IoT Gateways over IPv4 Network

Based on the manual PnP profile configuration on the IoT Gateways, communication is initially established with PnP Proxy on http://tps-san.ipg.cisco.com:9125. Later, the communication is established with the PnP Proxy on https://tps-san.ipg.cisco.com:9120.

Note: Only the PnP server discovery is made manual. The rest of the bootstrapping procedure is the same as the DHCP server-assisted PnP provisioning discussed above.

Bootstrapping over IPv6 Network

This section focuses on the bootstrapping of the IoT Gateways over the IPv6 network in the absence of the DHCP server, DNS server, and Cisco Cloud Redirector Server to provide the PnP server details. IoT Gateways are informed about the PnP server detail directly through the Cisco IOS configuration commands in order to enable bootstrapping of the IoT Gateways over the IPv6 network.

In Figure 16, based on the manual PNP profile configuration on the IoT Gateways, initially communication is established with the PnP Proxy on http://tps-san.ipg.cisco.com:9125. Later, the communication is established with PnP Proxy on https://tps-san.ipg.cisco.com:9120.

Name resolution happens to an IPv6 address, and the bootstrapping happens over an IPv6 network.

Note: Only the PnP server discovery is made manual. The rest of the bootstrapping procedure (PnP communication on port 9120 and 9125) is still dynamic.



Figure 16 Custom PnP Profile-Assisted Bootstrapping of IoT Gateways over IPv6 Network

Logical Call Flow

This section discusses the logical call flow sequence with the Custom PnP profile-assisted bootstrapping of the IoT Gateways over the IPv4/IPv6 network.



Figure 17 Custom PnP Profile-Assisted Bootstrapping of IoT Gateways–Logical Call Flow

In Figure 17:

- PnP server detail is learned out of the custom PnP profile, configured manually.
- The IoT Gateway reaches out to the PnP server in the configuration, which is http://tps- san.ipg.cisco.com:9125.
- The communication reaches TPS, and is then sent to FND. Bootstrapping of the IoT Gateway begins at the FND.
- The rest of the procedure is exactly the same as the bootstrapping steps discussed as part of DHCP server-assisted PnP Provisioning.
 - Initial communication happens on http://tps-san.ipg.cisco.com:9125
 - Later communication happens on https://tps-san.ipg.cisco.com:9120

PnP Server Discovery through Cisco PnP Connect and Bootstrapping

- Prerequisites, page 39
- Bootstrapping, page 41
- Logical Call Flow, page 42

Prerequisites

PnP Proxy must be reachable either over the WAN/Internet. As TPS is used in this implementation, TPS acts as the PnP server for the IoT Gateways. The controller profile on "software.cisco.com" should be configured with the correct TPS address. The controller profile advertises TPS details in place of the PnP server details.

To create the controller profile, login to software.cisco.com. Go to **Network Plug and Play > Select controller profile** from the toolbar and add the details.

Figure 18 shows the controller profile added on software.cisco.com.

Figure 18 Controller Profile

Controller Profile		×
Profile Name:	DA_SOLUTIONS_PNP_TPS_DMZ_BLR.	
Description:	TPS (PnP Proxy) hosted in Cisco DMZ Bangalore, for the purpose of Plug and Play provisioning of Ethernet/Cellular DA gateways	
Deployment Type:	onPrem	
Primary IPv4 Address	A.B.C.D	
Primiry Protocol:	http	
Primary Port:	9125	
Controller Type:	PNP SERVER	

When a device is ordered through CCW, the device must be attached with the Smart account. For the PnP discovery to be successful using PnP Connect, a device must be added on the software.cisco.com portal. The device can be added either manually or by uploading a csv file. You can refer to "PnP Server Discovery Through Cisco PnP Connect" in the *Cisco Distribution Automation Feeder Automation Design Guide*. Figure 19 shows adding a device manually.



duala	-					AND COLORED IN	O I
cisco	Identify Devic	0			×		
Decs Belware Central > Plug and Play Core	+ Serial Number	FCW225100DA				al Test DemoAccourt	rt1.nex.con + 16-Cem
	Base PD	IR1101-KD			(.e.)		English [Change]
Plug and Play Connect	Controller Profile	DA_BOLUTIONS	PHP_TPS_DM2.)	LR .			Feature Report Hep.
Jevices Controller Profiles 1. National.	Description	HEITON]					
Add Device(s)	Cancel						
am 1 🗸 👘	2	TTP 3	_	m# 4	_		
Mently Source In	ientify Device(e)	Opines & Soirt	-	Arresta			
Identify Devices Enter device itelatic by choking Meetify Device + Meetify Device	t builten and olick Next to pro	seed to the cent alog.			0 ^{AI}	O 1964 O	Ema 😑 Examp
Row Serial Number Base	PID Cert	Roate Serial Number	SOWAN Type	Controller	0	escription.	Actions
		No D	evices to display.				
							his Records is Display
Carcel Back							(100 C

After manually adding the device in the PnP Connect portal, the request is yet to received from the device and the status for PnP redirection will be pending. This is shown in Figure 20.

Figure 20 PnP Redirect Pending after Manual Device Addition

1	-	CEREMINE.								
lug and Pla	iy Conn	ect								Feedback Support Hery
vices Controller P	notice Net	ora Genticales	Mana	ge External Vi	muli Acc	nunt (
+ Add Devices	+ Add S	oftware Devices	1.8	SI Senschelt	118	Detete Salected	Ena	ble External Management	C	
Serial Number		Base PID		Product Gro	up	Controller		Last Modified	Status	Actions
			10	Any	٠	Any	•	E Select Range 🔹	Pending (Redirection) 🗢	Clear Filters
FCW22250000		@1101-K9		Router		DA_SOLUTIONS_P	NP_T	2019-May-27, 08:43:44	(Paning Redeemant)	Show Log 👻
										Showing 1 Barrier

Finally, when the device is added successfully, it should be populated in the devices list as shown in Figure 20, which lists the devices for when the Redirect was successful.

Bootstrapping

This section discusses the PnP Connect-Assisted bootstrapping of the IoT Gateways over the IPv4 network.

In Figure 21, IoT Gateways obtain the IP address dynamically from the service provider.

The PnP agent (residing on the IoT Gateway) then reaches out to PnP Proxy over IPv4 LAN/WAN network over http on port 9125 and then over https on port 9120.





Logical Call Flow

This section discusses the logical call flow sequence with the DHCP server-assisted bootstrapping of the IoT Gateways over the IPv4/IPv6 network.

The actors shown in Figure 22 are the following:

- PnP Agent (IoT Gateway)
- Service Provider
- PnP Cloud Re-direction Service PnP Connect Portal
- PnP Proxy (TPS)
- PnP Server (FND)



Figure 22 PnP Connect-Assisted Bootstrapping of IoT Gateways -Logical Call Flow

- When the IoT Gateway is powered on, the PnP Agent on the IoT Gateway checks for the presence of the startup configuration. If the startup configuration is not found, then the PnP agent performs "no shut" on all the cellular interfaces.
- 2. The IOS on the IoT Gateway sends out a request to the service provider.
- 3. The service provider responds back with the IPv4 address.
- 4. The IOT gateway proceeds for PnP server discovery and connects to the PnP cloud re-direction service connect portal. After successfully connecting the server devicehelper.cisco.com, the server PnP Connect portal sends the publicly reachable TPS DMZ IP(A.B.C.D) PnP proxy IP and the port number (9125) on which the proxy server is listening. The serial number of the gateway should be added to the Cisco Cloud PnP Connect portal for the re-direction service to be successful.
- 5. Once the PnP discovery is successful, the PnP profile is configured on the device with the publicly reachable TPS DMZ IP. Once the profile is configured, the bootstrapping begins.
- 6. The rest of the procedure is exactly the same as the bootstrapping steps discussed as part of PnP server discovery through DHCP server.

Bootstrapping Configuration Template on Bootstrapping FND

The bootstrapping template is a configuration template residing on the bootstrapping FND. As part of the bootstrapping procedure, when the bootstrapping request is received from the IoT Gateway, this bootstrap configuration template is used to derive the Cisco IOS configuration, which is then pushed onto the IoT Gateway.

Once this Cisco IOS configuration is pushed onto the IoT Gateway and copied onto a running configuration successfully, the bootstrapping is said to be SUCCESSFUL.

This bootstrapping of Cisco IoT Gateways from Cisco IoT FND (PnP Server) is entirely Zero Touch. This implementation section includes the following sections:

Creation of Bootstrap Configuration Template Group, page 44

Router Bootstrap Configuration Groups–Populating Templates, page 47

Creation of Bootstrap Configuration Template Group

This section covers the steps required for configuring the bootstrapping group.

Figure 23 CREATE Bootstrap–CONFIG–Tunnel Provisioning

Alada BT	DASHBOARD	DEVICER - OPERATIONS -		e		•
DASHBOARD			Devis Contiguiston		0/0	3
Endpoint States, Over Time	-012/×	Service Providers With Maxmun	Formwark Updats Deutre File Management	Har T.	_00/×	
		Cellular Helieven Cell Id	Rules	Down Routers +	Down Rosters Over Time	
		are units in preparious on specials	Groups	1		

1. From the CONFIG Menu, select the **Tunnel Provisioning** option.

Figure 24 CREATE Bootstrap–Add Group

Steels IST SELD NETWORK DIRECTOR	DADHDOARD DEVICES OPERADONS COUPD ADMIN	🚍 💁 -
CONFIG > TUNNEL PROVISIONING		
Awigh Devices to Group	default-cort 000	
Tuberel General	Group Hembers Router Tuttel Addition HER Tuttel Addition HER Tuttel Celetion Router Distate Cool guration Reprovisioning Addition	Polities
 ADUITER 	Beefstragging.	1

2. With the Router Group selected in the left pane, click the "+" sign (Add Group icon) located on the top right of the left pane.

Figure 25 CREATE Bootstrap–Add IPv4 Group

Group Name:	IPv4-BOOTSTRAP		
Device Category:	Router	*	

3. Configure the group name IPv4-BOOTSTRAP, and click Add.

Figure 26 CREATE Bootstrap–Add IPv6 Group

Add Group			×
Group Name:	IPv6-BOOTSTRAP		1
Device Category:	Router	w.	
		Add	

4. Similarly, configure another group name IPv6-BOOTSTRAP for bootstrapping over the IPv6 network. Click Add.

Figure 27 CREATE Bootstrap–List of Bootstrap Groups



The two newly created bootstrapping groups are displayed in the left pane:

- IPv4-BOOTSTRAP (Created to handle bootstrapping over the IPv4 network)
- IPv6-BOOTSTRAP (Created to handle bootstrapping over the IPv6 network)

Moving Devices under the Bootstrapping Group

Multiple bootstrapping groups could be configured on the bootstrapping FND. IoT Gateways have to be moved under the correct group in order to have it bootstrapped with the appropriate configuration.

Complete the following steps to move IoT Gateways under the correct bootstrapping group.

Figure 28 CHANGE Tunnel Group–Device Under Default Group

Inde IIT		DABHDOARD	DEVICES . OPERATIONS	CONFIG + ADMIN	a 🔍 -
Contris > Tunnic, Provisionnis Responses to Simul Terrint Groups * Internet Groups Detroin spr1990 (2)	Cinifault-int100 Group Wembers Rootskapung Rootskapung	Abdition — HER Tunnist A Mid a day the type and 1+ day	2015pm HER Turnel Deletor	Rauter Boststrap Configuration	Neprovisioning Ázbens – Policies
Default e 1100 (2)	2 Jame assured star (1988) - Die at	Sefection .			
C Celulo ellis (7) N 1944-BODTSTRAP (8)	😔 Narie	Bat. Catheard	Tunnel Source. OSPY Aves 1 Interface 1	OSPFe3 Area 1 Dest Addr 1	GRE Tunnel Tunnel Souther Open Area 2 Dest Add 1 University 2
Revelacionarian (B)	IN1105309-#CH222710002 IN1105309-#CH222710002 IN1105309-#CH222710002	20 there age 12 days age	Gigatettetiar		

 In Figure 28, two IoT Gateways are under the default group. The devices need to be moved to the newly created IPv4-BOOTSTRAP group. In the middle pane, select the **Router** in the pull-down menu, select the **IoT Gateways** to be moved under the new bootstrapping group, and then click **Change Tunnel Group**.

Figure 29 CHANGE Tunnel Group–Pull-Down Menu

THE PELO METWORK OF						CONFIG . ADMIN		= @-
COBING > HUMMEL #REVISION	ind							
And an Internal States	Change Turmet	Group			×			
Encourt Distance					finish Deletion	Noise Distatoj Cottijataten	$(X,Y) \in \{1,2,3,3,4,\dots,2,N\}$	2004 Yakimi
Y O HOLIDA	Tunnel Group	IPv4-BOOTSTRAP						
	-	default+it100 (default) default+i000 (default)			the state of the state of the state		aaayaanni	
103 (24)(4)(4)(4)(4)(4)		Pv4-BOOTSTRAP IPv6-BOOTSTRAP						
123 D-Rose and a 1/1		Gr. tarria	CHAR.	Castingal	Times Service - Child New 1	Oddered Aven & Water Torrett	GRE Tantil	Terrel Diservices and
In watercontinue in					- unitable -	Distrator (- Data with a	interface 2
Section and			11	20 000 120				
1.2.2.2.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1		· · · · · · · · · · · · · · · · · · ·	12	12.0010.000	Grandeliner			

 Choose the correct bootstrap group IPv4-BOOTSTRAP. To perform bootstrapping over the IPv6 network, choose the IPv6-BOOTSTRAP tunnel group.

Figure 30 CHANGE Tunnel Group–Select IPv4 Group

Tunnel Group	IPv4-BOOTSTRAP	

3. With the appropriate bootstrap group chosen, click **Change Tunnel Group** to move the IoT Gateway from the default group to the desired group.

Figure 31 CHANGE Tunnel Group–Updated IPv4 Group



Device migration to the desired group was successful.

Figure 32 CHANGE Tunnel Group–Devices Moved under IPv4 Group

CITATION AND AND AND AND AND AND AND AND AND AN			DASHBOA	to DEVICES	- OPERAT	1045 × 00/1/				-	••
CONFIG > TURNEL PROVISIONING											
Tunnel Groups	Group Members Rocker	Tantei Adi	mor HEA To	Mill Addition H	ER Tunnel Dete	ton RoderBoi	tit në Configin	rkin Reprisis	innig Adiama	Polities	
* G ROSTAR	Backbagareg										
C Detaut-lor1000 (2)	44	a text	a device type and	1- devices to enab	e actions in the	Conclude Se		Capitying	1.211 (Paje	e Di (te la	
Detauter (* 11.00 rd)	Natio	Sur.	Latinari	Tablest Bauros	05PT Avea 1	DDFFv3 Area 1	PsecTuniei	GRE Tunnel	Tunnet Searce	ODPF Nex 2	OIP
Detaute #800 (7)		-	20.00	THE STORE OF				and case 1	and a local second s		
	191101-K9-F CHI2227 00KB	a	12 dais ago	GigabdEther							

In Figure 30, it can be seen that IoT Gateways were moved under the correct bootstrapping group.

Router Bootstrap Configuration Groups–Populating Templates

This section shows where to populate the bootstrapping template in FND, and the template that needs to be chosen for bootstrapping of the IoT Gateways according to the network in which the IoT Gateway would be deployed (for example, IPv4/IPv6 network, located/not located behind NAT, etc).

Note: Working versions of bootstrapping templates can be found in Appendix A: PnP Profiles, page 226.

Figure 33 captures the Router Bootstrap Configuration section that needs to be populated for the purpose of bootstrapping.

Figure 33 Router Bootstrap Configuration

CISCO FIELD NETWORK DIRECTOR	
CONFIG = TUNNEL PROVISIONING	
Assign Devices to Simus	Pv4-BOOTSTRAP
Turrel George	Group Nembers Routes Tunnel Addition HER Turnel Addition HER Turnel Celetion Number Doubtrap Configuration. Reprovisioning Advise Policies
- • ADATAN	Restit approp
Certaus-carsoon (21)	1 Neviasion #1 - Lasi 124-ed av 2016-10 24 (2027)
	Target Firmware Version.
Ed Contactor (100 City	
D Cetaure exits (7)	
No Prid BOSTSTRUP (2)	<pre></pre>
A shattaroota	<pre>************************************</pre>

Every bootstrap group (referred as Tunnel Group in the left pane) can be populated with a unique Router bootstrap configuration.

Table 10 Bootstrapping Template According to the Deployment Model

Network Type	Profile Name for IoT Gateways (located behind NAT)	Profile Name for IoT Gateways (NOT located behind NAT)
IPv4	IPv4-BOOTSTRAP-NAT	IPv4-BOOTSTRAP
IPv6	IPv6-BOOTSTRAP-NAT	IPv6-BOOTSTRAP

With reference to Table 10, for bootstrapping the IoT Gateways for deployment over the IPv4 network:

- If IoT Gateways are located behind NAT, then the bootstrapping template IPv4- BOOTSTRAP-NAT could be used.
- If IoT Gateways are not located behind NAT, then the bootstrapping template IPv4- BOOTSTRAP could be used.

Similarly, for bootstrapping the IoT Gateways for deployment over IPv6 network:

- If IoT Gateways are located behind NAT, then the bootstrapping template IPv6- BOOTSTRAP-NAT could be used.
- If IoT Gateways are not located behind NAT, then the bootstrapping template IPv6- BOOTSTRAP could be used.

Deployment of the Cisco IoT Gateway

This section includes the following topics:

- Prerequisites for Deployment, page 48
- Deployment over IPv4 Cellular Network with NAT, page 48
- Deployment over IPv4 Network without NAT, page 50
- Deployment over Native IPv6 Ethernet Network, page 51

Prerequisites for Deployment

- Cisco IoT Gateway should have gone through the bootstrapping procedure mentioned in Bootstrapping the IoT Gateway, page 20, with the device being part of the appropriate bootstrapping group.
- Bootstrapping is said to be complete, when the Cisco IOS Routers received the bootstrapping configuration from the Bootstrapping FND.
- The bootstrapping status for the router on the Bootstrapping FND must be in 'Bootstrapped' state.

Deployment Infrastructure Readiness

Cisco IoT Gateway should be assigned an IPv4/IPv6 address dynamically over Ethernet/Cellular. If a static address needs to be used on the Cisco IoT Gateway, then assignment of address to the Cisco IoT Gateway's interface needs to be taken care as part of Bootstrapping.

Tip: If any extra configuration is required to receive IP address dynamically, the delta configuration should be fed back into the bootstrapping profile, that was used to bootstrap the IoT Gateway.

- Cisco Field Area Network–Headend (DSO Control Center1) should be UP and running.
 - If it needs to be set up, the Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases' guide could be referenced to set up the headend in the DSO Control Center or NOC.
- All the required headend components like the CA server (RSA), AAA, AD, Registration Authority, NOC TPS/FND, DHCP server, and HERs are expected to be up and running in the DSO Control Center.
- NOC TPS, RA, and HERs must have static IP addresses configured and should be reachable from the Cisco IoT Gateways that are located along the Distribution network.

Note: If the prerequisites for deployment are addressed, ZTD of the IoT Gateways should happen successfully after the gateway is deployed at the desired location and powered on, with the Ethernet cable connected or the LTE SIM card inserted.

Deployment over IPv4 Cellular Network with NAT

Note: This section has no implementation steps. As the term "ZTD" states, it's a zero touch deployment. As long as bootstrapping happened successfully by having the IoT Gateway part of the correct bootstrapping group, this deployment should happen successfully with no manual steps.

Figure 34 captures the deployment steps for IoT Gateway over LTE Cellular.



Figure 34 Deployment over IPv4 Cellular Network

Note: This scenario has been validated with the headend located in the Cisco DMZ.

The following is the summary sequence of steps that occurs during the deployment:

- 1. The IoT Gateway is powered on. When up, it obtains the IP address over LTE Cellular interface.
- 2. The EEM Script for ZTD kicks in and waits for the time to be synchronized. Then, SCEP enrollment happens over port 80 with RA-DMZ-IP.
- **3.** Once the certificate is received for the IoT Gateway (from the RA/CA), the ZTD script disables itself and activates the CGNA profile for tunnel provisioning (cgna initiator-profile cg-nms-tunnel).

Note: "cgna initiator-profile cg-nms-tunnel" must be used when the IoT Gateway is behind NAT, whereas "cgna profile cg-nms-tunnel" must be used when no NAT exists between IoT Gateway and TPS. This CGNA profile is configured as part of bootstrapping.

- 4. TPS/FND provisions the secure FlexVPN tunnel with the HER Cluster located in the DSO Control Center1.
- 5. As an overlay routing, FND and SCADA routes are advertised (by the HER) to the IoT Gateway through the secure FlexVPN tunnel.
- 6. The IoT Gateway sends out a registration request to FND on port 9121. Once registered successfully, the IOT Gateway is remotely manageable from the FND.
- 7. As part of the device registration with the FND, FND also pushes ICT enablement configurations to the IoT Gateway, which enables the communication between the SCADA Master in the Control Center and the SCADA Outstation located in the Feeder Automation/Distribution Network.
- 8. ZTD of the IoT Gateway is successful.

9. Utility Application Traffic - READY TO GO.

Deployment over IPv4 Network without NAT

Note: This section has no implementation steps. As the term "ZTD" states, it's a zero touch deployment. As long as bootstrapping happened successfully by having the IoT Gateway part of the right bootstrapping group, this deployment should happen successfully with no manual steps.

Figure 33 captures the deployment steps for IoT Gateway without NAT over the IPv4 network.



Figure 35 Deployment over IPv4 Ethernet Network

Note: This scenario has been validated with the headend located in the Engineering Lab.

The following is the summary sequence of steps that happens during the deployment:

- 1. The IoT Gateway is powered on. When up, it obtains the IP address over the Ethernet interface.
- 2. The EEM Script for ZTD kicks in and waits for the time to be synchronized. Then, SCEP enrollment happens with RA IP (172.16.241.2) on port 80.
- 3. Once the certificate is received for the IoT Gateway (from the RA/CA), the ZTD script disables itself, and activates the CGNA profile for tunnel provisioning (cgna profile cg-nms- tunnel).

Note: "cgna profile cg-nms-tunnel" must be used when there is no NAT between IoT Gateway and TPS. This CGNA profile has already been configured as part of IoT Gateway bootstrapping. TPS/FND provisions secure FlexVPN tunnel with the HER Cluster located in the DSO Control Center1.

- 4. As an overlay routing, FND (172.16.103.100 and 2001:db8:16:103::100) and SCADA (172.16.107.11 and 2001:db8:16:107::11) routes are advertised (by HER) to the IoT Gateway through the secure FlexVPN tunnel.
- IoT Gateway sends out a registration request to FND IPv4 address 172.16.103.100 (or) IPv6 address 2001:db8:16:103::100 on port 9121. Once registered successfully, the IOT Gateway is remotely manageable from the FND.
- 6. As part of the device registration with the FND, FND also pushes ICT enablement configurations to the IoT Gateway, which enables the communication between SCADA Master in the Control Center and the SCADA Outstation located in the Feeder Automation/Distribution Network.
- 7. ZTD of the IoT Gateway is successful.
- 8. Utility Application Traffic READY TO GO.

Deployment over Native IPv6 Ethernet Network

Note: This section has no implementation steps. As the term "ZTD" states, it's a zero touch deployment. As long as bootstrapping happened successfully by having the IoT Gateway part of the right bootstrapping group, this deployment should happen successfully with no manual steps.

Figure 36 captures the deployment steps for the IoT Gateway over the Native IPv6 network.



Figure 36 Deployment over Native IPv6 Ethernet Network

Note: This scenario has been validated with the headend located in the Engineering Lab over a native IPv6 network. It could be dual stack as well.

The following is the summary sequence of steps that happens during the deployment:

1. The IoT Gateway is powered on. When up, it obtains the IPv6 address over the Ethernet interface.

- 2. The EEM script for ZTD kicks in and waits for the time to be synchronized. Then, SCEP enrollment happens with RA IPv6 address (2001:db8:10:241::5921) on port 80.
- 3. IPv4 communication could be retained between RA and CA in the Control Center private network.
- 4. Once the certificate is received for the IoT Gateway (from the RA/CA), the ZTD script disables itself, and activates the CGNA profile for tunnel provisioning.

Note: "cgna initiator-profile cg-nms-tunnel" must be used when the IoT Gateway is behind NAT, whereas "cgna profile cg-nms-tunnel" must be used when there is no NAT between IoT Gateway and TPS. This CGNA profile has already been configured as part of the IoT Gateway bootstrapping.

- 5. TPS/FND provisions secure the FlexVPN tunnel with the HER Cluster located in the DSO Control Center, over the Native IPv6 network.
- 6. As an overlay routing, FND (172.16.103.100 and 2001:db8:16:103::100) and SCADA (172.16.107.11 and 2001:db8:16:107::11) routes are advertised (by HER) to the IoT Gateway through the secure FlexVPN tunnel.
- IoT Gateway sends out a registration request to FND IPv4 address 172.16.103.100 (or) IPv6 address 2001:db8:16:103::100 on port 9121. Once registered successfully, IOT Gateway is remotely manageable from the FND.
- 8. As part of the device registration with the FND, FND also pushes ICT enablement configurations to the IoT Gateway, which enables the communication between SCADA Master in the Control Center and the SCADA Outstation located in the Feeder Automation/Distribution Network.
- **9.** ZTD of the IoT Gateway is successful.

10. Utility Application Traffic – READY TO GO.

Tunnel Provisioning Template Profiles

Tunnel Provisioning Template profiles, which are needed for Tunnel establishment, are captured in Appendix B: FND Zero Touch Deployment Profiles, page 235.

Device Configuration Template Profiles

Device Configuration Template profiles, which are needed for ICT SCADA Traffic enablement, are captured in Appendix C: Device Configuration Profiles, page 244.

Bootstrapping and ZTD of the Cisco IoT Gateway at the Deployment Location

This section describes the bootstrapping and Deployment of the Cisco IoT gateway at the deployed location. Unlike the previous section, one TPS and FND is sufficient to complete both bootstrapping and ZTD. Although the previous two sections and this section overlap, minor changes in the implementation of TPS and FND need to be done in order for the deployment to be successful.

This section, which covers the minor changes that have to be implemented in the headend setup, describes these phases:

- Prerequisites, page 53
- Certificate Creation and Installation, page 53
- Installation of TPS, page 55
- Installation of FND, page 55
- Configuration of TPS, page 55
- Configuration of FND, page 58

- Device Bootstrapping, page 61
- Device Deployment, page 61

Prerequisites

Prerequisites include the following:

- TPS and FND server must be up and running.
- This section focuses on portions required for TPS and FND to carry out both bootstrapping and ZTD.
- Routing reachability over IPv4 and/or IPv6 networks from IoT Gateways to TPS.
- Routing reachability between TPS and FND.

Certificate Creation and Installation

This section captures the parameters that need to be considered while creating the certificate for the TPS and FND.

Note: For detailed instructions about certificate creation, please refer to the section "Creation of Certificate Templates and Certificates" of the *Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases Guide* at the following URL:

https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-15726915

Certificate Creation for TPS

The certificate for the TPS must be created with both the Subject Name and the Subject Alternative Name fields populated.



Subject	General	Extensions	Private Key	Certifica	ation Authority	Signature	
The subject can enter in can be used Subject of o The user or	of a certi formation in a certi certificate compute	ficate is the n about the i ficate. r that is rece	user or comp types of subj iving the cert	iuter to v ect name tificate	which the certi e and alternati	ficate is issued ve name values	. You that
Subject nan	ne:						
Туре:					CN=tps.ip	g.cisco.com	
Organization Value:		Add	>	O=Cisco Systems Inc			
		< Rem	ove	ĺ.			
Alternative	name:				L		_
Type:				DN5	222244		
IP address	(v4)	~			IP address	(v4)	
Value:		11-	Aula		A.B.C	.D	
			ADD	<i>.</i>			
			< Rem	ove			

The Subject Name is the Common Name that must be set to the FQDN of the TPS.

The Subject Alternative Name must be set to the FQDN - tps.ipg.cisco.com of the TPS, along with the IP address (A.B.C.D - Public reachable DMZ IP). The Subject Alternative Name is required for PnP to work. The IP address must be reachable from the IoT Gateway. TPS is located in DMZ. The IP address is not optional in this implementation. FQDN is optional, but the IP address is not.

The enrolled certificate is exported as PnP-ZTD-TPS.pfx and is protected with a password.

Certificate Creation for FND

The FND certificate must be created with both the Subject Name and Subject Alternative Name fields populated.



L Subject	General	Extensions	Private Key	Certifica	ation Authority	Signature	
The subject can enter in can be used Subject of o The user or	of a certi formation in a certi certificate compute	ficate is the n about the ificate. r that is rece	user or comp types of subj iving the cert	outer to v ect name tificate	which the certi e and alternati	ficate is issue ve name value	d. You es that
Tupe:	ne:	-			CN=fnd.it	a.cisco.com	
Type: Organization		Add	>	O=Cisco	Systems Inc		
Value:			< Rem	ove			
l Alternative	name:				-		
Туре:				DNS fed ing cit			
IP address	(v4)	¥			IP address	((4)	_
Value:			Add	>:	192.168.10	3.100	
			< Rem	ove			

The Subject Name is the Common Name that must be set to the FQDN of the PnP Server.

The Subject Alternative Name must be set to the FQDN of the FND, along with the optional IP address. The Subject Alternative Name is required for PnP to work. The IP address in Figure 38 will be reachable after tunnel is established between IoT gateway and the headend.

The enrolled certificate is exported as PnP-ZTD-FND.pfx and is protected with a password.

Installation of TPS

The bootstrapping procedure in this implementation guide considers the use of TPS as PnP Proxy. For installation of TPS, please refer to Installation of TPS, page 55.

Installation of FND

For installation of FND, please refer to the detailed steps covered under the section "Implementing Field Network Director" of the Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases Guide.

Configuration of TPS

This section covers the configuration steps and the final verification steps on the TPS.

TPS Proxy Properties Configuration

TPS Proxy Properties file needs to be configured with the following details:

- inbound-bsproxy-destination: Address to which the bootstrapping requests be forwarded.
- enable-bootstrap-service: Is bootstrapping service enabled/disabled?
- bootstrap-proxy-listen-port: Port on which the PnP Proxy must be listening for processing bootstrapping requests (default port is 9125).

```
[root@tps-san ~]# cat /opt/cgms-tpsproxy/conf/tpsproxy.properties
## Configuration created as part of regular TPS installation.
inbound-proxy-destination=https://fnd.ipg.cisco.com:9120
outbound-proxy-allowed-addresses=fnd.ipg.cisco.com
cgms-keystore-password-hidden=7jlXPniVpMvat+TrDWqhlw==
```

```
## Configuration required for Bootstrapping.
inbound-bsproxy-destination=http://fnd.ipg.cisco.com:9125
enable-bootstrap-service=true
bootstrap-proxy-listen-port=9125
[root@tps ~]#
```

Name resolution entries have to be present for FND FQDN in the /etc/hosts file.

Mandatory Verification Checks on TPS Proxy

The verification checks include the following:

- FND FQDN entry in /etc/hosts.
- TPS must have three certificates installed into the cgms_keystore:
 - Certificate signed by Utility PKI for TPS (with private key)
 - Public Certificate of the Utility PKI CA server
 - Public Certificate of the Cisco SUDI CA
- Hostname consistency with the certificate.
- There shouldn't be any unreachable name servers in /etc/resolv.conf.
- NTP daemon should be running. Time should be synchronized.
- Necessary firewall ports must have been opened up, if the firewall/iptables/ip6tables are enabled:
 - TCP Port 9125 to process http communication
 - TCP port 9120 to process https communication
- FND FQDN entry in /etc/hosts:

```
[root@tps ~]# cat /etc/hosts
127.0.0.1localhost localhost.localdomain localhost4
localhost4.localdomain4 tps.ipg.cisco.com
```

::1localhost localhost.localdomain localhost6 localhost6.localdomain6 tps.ipg.cisco.com

192.168.103.100 fnd.ipg.cisco.com

[root@tps ~]#

TPS must have three certificates installed into the cgms_keystore:

The certificate entry 'root' represents the Utility PKI CA certificate.

- The certificate entry 'sudi' represents the Cisco SUDI CA certificate.
- The certificate entry 'cgms' represents the private certificate of the TPS server signed by the (custom) Utility PKI CA server.

Keytool -list -keystore /opt/cgms-tpsproxy/conf/cgms_keystore:

```
Your keystore contains 3 entries
root, Jun 4, 2017, trustedCertEntry,
Certificate fingerprint (SHA1):
CF:A2:61:30:29:B1:1E:46:14:30:A2:DC:5F:62:41:
47:CC:EE:64:69
sudi, Apr 4, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
F6:96:9B:BD:48:E5:F6:12:5B:93:4D:01:E7:1F:E9:
C2:7C:6F:54:7E
cgms, May 9, 2019, PrivateKeyEntry,
Certificate fingerprint (SHA1):
03:7E:11:1E:10:16:DD:C8:81:15:41:84:DB:7E:03:
79:6E:96:1B:5E
```

Hostname should match the certificate Common Name/SAN:

```
[root@tps ~]# hostname
tps.ipg.cisco.com [root@tps ~]#
[root@tps ~]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=tps.ipg.cisco.com
GATEWAY=72.163.222.225
NTPSERVERARGS=iburst
[root@tps ~]#
[root@tps ~]#
[root@tps ~]# keytool -list -keystore /opt/cgms-
tpsproxy/conf/cgms_keystore -alias cgms -v | grep "CN="
Enter keystore password: [press Enter]
< .. removed for clarity ..>
Owner: CN=tps.ipg.cisco.com, O=Cisco Systems Inc
Issuer: CN=IPG-RSA-ROOT-CA, DC=ipg, DC=cisco, DC=com
< .. removed for clarity ..> [root@tps ~]#
```

No unreachable name servers should exist. Either the name servers should be present and reachable or they should be empty. Any unreachable name server address entry must be taken care or removed under the network interface configuration.

```
[root@tps ~]# cat /etc/resolv.conf #
Generated by NetworkManager search ipg.cisco.com
# No nameservers found; try putting DNS servers into your
#ifcfg files in /etc/sysconfig/network-scripts like so:
#
```

```
# DNS1=xxx.xxx.xxx # DNS2=xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
[root@tps ~]#
```

NTP daemon should be running. Time should be synchronized:

```
[root@tps ~]# ntpstat
synchronised to NTP server (171.68.38.65) at stratum 6
time correct to within 27 ms
polling server every 1024 s
[root@tps ~]#
```

Note: The TPS server should be time synchronized. Otherwise, the https communication from the IoT Gateway might not reach the TPS Proxy Application.

Configuration of FND

This section covers the configuration steps and the final verification steps on the FND.

CGMS Properties Configuration

The CGMS Properties file needs to be configured with the following details:

- proxy-bootstrap-ip: Address of the PnP Proxy from which the bootstrapping requests are processed
- enable-bootstrap-service: Enable/Disable the bootstrapping service
- bootstrap-fnd-alias: The trust point alias to be used during bootstrapping of the IoT Gateway
- **ca-fingerprint**: fingerprint of the 'root' trustpoint

[root@fnd conf]# cat /opt/cgms/server/cgms/conf/cgms.properties

Configuration created as part of regular FND installation. cgms-keystore-password-hidden=7jlXPniVpMvat+TrDWqhlw== cgdm-tpsproxy-addr=tps.ipg.cisco.com cgdm-tpsproxy-subject=CN="tps.ipg.cisco.com", O="Cisco Systems Inc"

Configuration required for Bootstrapping.

enable-bootstrap-service=true proxy-bootstrap-ip=<Cisco DMZ IP> bootstrap-fnd-alias=root ca-fingerprint=CFA2613029B11E461430A2DC5F624147CCEE6469

[root@fnd conf]#

Name resolution entries have to be present for TPS FQDN in the /etc/hosts file.

In our lab setup, the proxy-bootstrap-ip is a DMZ IP. In cases where FQDN is globally resolvable, then FQDN can be used instead of IP.

Mandatory Verification Checks on FND

Verification checks include the following:

- TPS FQDN entry in the /etc/hosts file.
- FND must have three certificates installed into the cgms_keystore:
 - Certificate signed by Utility PKI for FND (with private key)
 - Public Certificate of the Utility PKI CA server

- Public Certificate of the Cisco SUDI CA
- Hostname must be consistent with the certificate.
- No unreachable name servers in /etc/resolv.conf should exist.
- NTP daemon should be running. Time should be synchronized.
- Necessary firewall ports must have been opened up if the firewall/iptables/ip6tables are enabled:
 - TCP Port 9125 to process http communication
 - TCP port 9120 to process https communication

TPS/FND FQDN entry in the /etc/hosts file:

```
[root@fnd ~]# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4
localhost4.localdomain4 fnd.ipg.cisco.com
::1 localhost localhost.localdomain localhost6
localhost6.localdomain6 fnd.ipg.cisco.com
192.168.104.100fnddb .ipg.cisco.com
```

192.168.103.242 tps.ipg.cisco.com

FND must have three certificates installed into the cgms_keystore:

- The certificate entry 'root' represents the Utility PKI CA certificate.
- The certificate entry 'sudi' represents the Cisco SUDI CA certificate.
- The certificate entry 'cgms' represents the private certificate of the FND server signed by the (custom) Utility PKI CA server.

```
keytool -list -keystore /opt/cgms/server/cgms/conf/cgms_keystore Enter keystore password:
*The integrity of the information stored in your keystore *
*has NOT been verified! In order to verify its integrity, *
*you must provide your keystore password.*
Keystore type: JKS Keystore provider: SUN
Your keystore contains 4 entries
root, Apr 5, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):
CF:A2:61:30:29:B1:1E:46:14:30:A2:DC:5F:62:41:47:CC:EE:64:69
sudi, Jul 11, 2018, trustedCertEntry, Certificate fingerprint (SHA1):
F6:96:9B:BD:48:E5:F6:12:5B:93:4D:01:E7:1F:E9:C2:7C:6F:54:7E
cgms, Oct 5, 2018, PrivateKeyEntry,
Certificate fingerprint (SHA1):
F4:99:72:8E:BA:24:25:8A:1D:23:9B:B6:B1:99:EA:FD:12:9E:A7:34
You have mail in /var/spool/mail/root [root@fnd conf]#
```

Hostname should match the certificate Common Name/SAN:

[root@fnd conf]# hostname
fnd-san.ipg.cisco.com
[root@fnd conf]#

[root@fnd conf]# cat /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=fnd.ipg.cisco.com
NTPSERVERARGS=iburst
root@fnd conf]# keytool -list -keystore
/opt/cgms/server/cgms/conf/cgms_keystore -v -alias cgms | grep CN=
Enter keystore password: [press Enter]
< .. removed for clarity ..>
Owner: CN=fnd.ipg.cisco.com, 0=Cisco Systems Inc Issuer:
CN=IPG-RSA-ROOT-CA, DC=ipg, DC=cisco, DC=com
< .. removed for clarity ..>
[root@fnd conf]#
```

No unreachable name servers should exist. Either the name servers should be present and reachable or they should be empty. Any unreachable name server address entry must be taken care or removed under the network interface configuration:

```
[root@fnd conf]# cat /etc/resolv.conf #
Generated by NetworkManager
search ipg.cisco.com
# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so: #
# DNS1=xxx.xxx.xxx
# DNS1=xxx.xxx.xxx
# DNS2=xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com [root@fnd conf]#
```

NTP daemon should be running. Time should be synchronized:

```
[root@fnd conf]# ntpstat
synchronised to NTP server (192.168.103.75) at stratum
6 time correct to within 45 ms
polling server every 1024 s
[root@fnd conf]#
```

Note: The FND server should be time synchronized. Otherwise, the https communication from the IoT Gateway might not reach the FND (cgms) application.

Csv File Import on FND GUI

A sample csv file that can be imported into FND for bootstrapping of IoT Gateway is shown below:

deviceType,eid,dhcpV4LoopbackLink,dhcpV6LoopbackLink,tunnelSrcInterface1,ipsecTunnelDest Addr1,tunnelSrcInterface2,ipsecTunnelDestAddr2,adminUsername,adminPassword,certIssuerCom monName,tunnelHerEid,hostnameForBs,domainname,bootimage

```
ir1100,IR1101K9+FCW225100DA,192.168.150.1,2001:db8:BABA:FACE::1,Cellular0/1/0,<W.X.Y.Z>
cg-nms-
```

administrator,156qay3OnltOPVTmrDhwVZ426ZyewiRG1gmshsem/I0MP+dPGrDNO1Al7FuvyMZrkcLTd3+L9Q Syc5SZo1BeS/GZ9T337cf+HVhF36G00RerMcg7N5Vh77RH18Fg/SctLRta0gBD4PdcdJeQI0R5UVQpoU3dlPtefC Z4LAOh4gitQJ72avXzygsofG17CPk4ZDdc9cQ9jrpV2fzpzS/Wyv2ryzIkKVMUYDCr9fLBITPtWUwCuX/bylZHaH vBnsq5ZwTC3uaSTzd2LDXvk+iRtynjLXJRcWdaRqnIGVCDp0C8l3du3fxHInJ69jjob924tIH3YjZ101D6gt4VxK dtCA==,IPG-RSA-ROOT-

CA, HER1.ipg.cisco.com, IR1100_FCW225100DA, ipg.cisco.com, flash:/ir1101universalk9.16.11.01.SPA.bin

Parameter	Name	Parameter Value Explanation
deviceType	ir1100	Helps identify the type of device; for example: ir800 cgr1000 ir1100
eid	IR1101-K9+FCW225100DA	Unique network element identifier for the device
dhcpV4LoopbackLink	192.168.150.1	Tunnel IP address on HER
dhcpV6LoopbackLink	2001:db8:BABA:FACE::1	Tunnel IPv6 address on HER
tunnelSrcInterface1	Cellular0/1/0	Name of the WAN interface that the FAR would use to reach the Headend.
ipsecTunnelDestAddr1	W.X.Y.Z	HER ip address on which tunnel terminates. User has to use their own HER IP.
tunnelSrcInterface2	Interface on HER	This field can be used when active-active connections to the Headend is required
ipsecTunnelDestAddr2	Public IP address	This field can be populated when the above field is used.
adminUsername	cg-nms-administrator	Username that FND must use to interact with the IoT Gateway
adminPassword	<encrypted_pwd></encrypted_pwd>	Password in encrypted form. An unencrypted form of this password would be used by the FND to interact with the FAR.
certIssuerCommonName	IPG-RSA-ROOT-CA	Common Name of the CA server should be populated in this field
tunnelHerEid	HER1.ipg.cisco.com	HER id should be populated in this field. This is the HER id with which the gateway
hostnameForBs	IR1100_FCW225100DA	Hostname for bootstrapping
domainname	ipg.cisco.com	Domain name for the bootstrapped router
bootimage	flash:/ir1101-universalk9.SSA. bin	Boot image name

Table 11 Fields of the IoT Gateway Bootstrapping csv File

Device Bootstrapping

After the above sections have been implemented, the headend is now ready for both provisioning and deployment.

The device bootstrapping is an important process as it eliminates the manual intervention to create and copy the express config to the device.

Device bootstrapping using Cisco PnP Connect has been clearly elucidated in PnP Server Discovery through Cisco PnP Connect and Bootstrapping, page 39.

Device Deployment

After the device has been successfully bootstrapped using Cisco PnP Connect, the device is now ready to undergo ZTD. No manual interface is required for the ZTD to begin.

Deployment over IPv4 Cellular Network with NAT, page 48, elucidates the ZTD process that would begin as soon as bootstrapping using Cisco PnP Connect is complete.

IoT Gateway Validation Matrix

Table 12 captures the Bootstrapping and ZTD validation matrix across the various platform types, supported as IoT Gateways.

 Table 12
 IoT Gateway Validation Matrix

Platforms	IP Protocol Type (IPv4/IPv6)	Network Type (Ethernet/Cellular)	Bootstrapping over Ethernet using IP Protocol Type	ZTD over Network Type and IP Protocol Type
IR1101	IPv6	Ethernet	Validated	Validated
	IPv4	Ethernet	Validated	Validated
		Cellular		Validated
IR807	IPv4	Ethernet	Validated	Validated
		Cellular		Validated
IR809	IPv4	Ethernet	Validated	Validated
IR829	IPv4	Ethernet	Validated	Validated
CGR1120	IPv4	Ethernet	Validated	Validated
		Cellular	Validated	Validated
CGR1240	IPv4	Ethernet	Validated	Validated
		Cellular	Validated	Validated

From Table 12, Platform IR1101 has been validated for:

- Bootstrapping over IPv6 Ethernet
- ZTD over IPv6 Ethernet

Similarly, Platform IR1101 has been validated for:

- Bootstrapping over IPv4 Ethernet
- ZTD over IPv4 Ethernet/Cellular

Similarly, Platform IR807 has been validated for:

- Bootstrapping over IPv4 Ethernet
- ZTD over IPv4 Ethernet/Cellular

Similarly, platforms CGR1120 and CGR1240 have been validated for:

- Bootstrapping over IPv4 Ethernet
- ZTD over IPv4 Ethernet/Cellular

All other platform types have been validated for:

- Bootstrapping over IPv4 Ethernet
- ZTD over IPv4 Ethernet network

With this, the Cellular DA Gateways or Cisco Field Area Routers could be on boarded and registered with FND, enabling further remote management and monitoring from FND.

The next section discusses in detail the implementation steps required to onboard the Cisco Resilient Mesh Endpoints like the Cisco IR510 WPAN Industrial Router, to serve the functionality of the DA Gateway.

Zero Touch Enrollment of Cisco Resilient Mesh Endpoints

This chapter includes the following major topics:

- Staging, page 63
- Secure Onboarding of Mesh Nodes into CR Mesh, page 67
- MAP-T Infrastructure in DA Feeder Automation, page 70
- Configuration Options from FND, page 73
- Routing Advertisements from FAR to HER, page 80

Staging

This section describes the implementation steps needed to bring up the CR Mesh using IR510 DA Gateways (also referred to as FDs). The IR510 connects to the CGR (also referred to as the FAR) via the Connected Grid Module (CGM) WPAN-OFDM-FCC module that needs to be installed within the FAR.

Note: For information on setting up the WPAN module, please refer to the *Connected Grid Module (CGM)* WPAN-OFDM-FCC Module - Cisco IOS at following URL:

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/modules/cgm_wpan_ofdm/cgm_wpan_ofdm.html# pgfld-157681

Table 13 lists the basic components along with their software versions needed to bring up the CR Mesh topology depicted in Figure 1.

Component	Product / Model	Software Image	Software Version
CGR	Cisco CGR1240/K9 and CGR1120/K9	cgr1000-universalk9-bundle.SPA.158-3.M.bin	15.8(3)M
CGM	CGM-WPAN-OFDM-FCC	cg-mesh-bridge-6.0weekly-6020-ir510-fedac85.bin	6.0.20
FD	IR510	cg-mesh-dagw-6.0weekly-6020-ir510-fedac85.bin	6.0.20
Configuration Writer Utility	cfgwriter	cfgwriter-6.0.20	6.0.20
HostOne Tool	fwubl	fwubl_win732bit_1.0.5	1.0.5

Table 13 CR Mesh Components

Certificate Creation

The prerequisites for deploying a CR Mesh include obtaining all the necessary ECC certificates from the CA server and configuring the AAA RADIUS server to authenticate the IR510 using a certificate-based authentication method. The FAR facilitates dot1x authentication between the IR510 and AAA server, thereby acting as the dot1x authenticator. The ECC certificate mentioned earlier is part of the configuration binary file (.bin) used to program the IR510 node. The ECC certificates and procedures for generating the config file for IR510 are described in further sections.

Note: While the FD need ECC CA certificates for zero touch enrollment, FAR use RSA type certificate for ZDT.

The following certificates need to be obtained from the ECC CA to program an IR510:

The X.509 certificate of the IR510 node in PKCS#12 format (.pfx) contains its private key and is used to program the node.

- The DER-encoded X.509 certificate (.cer) of the IR510 node without the private key is used to enroll the node with the Active Directory.
- The DER-encoded X.509 certificate (.cer) of the ECC CA server is also used for programming the IR510 node.
- The CSMP certificate downloaded from the IoT FND in binary format (.cer) to validate node CSMP registration with IoT FND.

For details on setting up and configuring the ECC CA and AAA server and on obtaining all of the above certificates, please refer to Secure Onboarding of Mesh Nodes into CR Mesh, page 67.

The following section describes the process for generating a configuration binary file (.bin) used to program the IR510 node.

Bin File Creation

The configuration file for the IR510 nodes is prepared in binary format using the Configuration Writer utility (cfgwriter).

Note: To obtain the cfgwriter utility discussed below, please check with your Account team or Sales representative.

cfgwriter is a java-based utility that takes as input an XML file with the node configuration information and produces a binary (.bin) memory file. This utility may be executed on any host platform with Java Run Time Environment installed. In this deployment, a Windows 10 machine with Java pre-installed was used to host the cfgwriter utility. The node configuration information, among other items, includes the SSID of the WPAN it must join and the security certificates. The schema of the XML configuration file and the corresponding documentation are packaged with the cfgwriter utility as a ZIP file.

Figure 39 cfgwriter Utility



The following XML file is used in this deployment to program the IR510 node:

```
<Csmp Cfg>
   <RegIntervalMax>3600</RegIntervalMax>
   <RegIntervalMin>300</RegIntervalMin>
   <ReqSignedPost>true</ReqSignedPost>
   <ReqValidCheckPost>true</ReqValidCheckPost>
   <ReqTimeSyncPost>false</ReqTimeSyncPost>
   <ReqSecLocalPost>false</ReqSecLocalPost>
   <ReqSignedResp>true</ReqSignedResp>
   <ReqValidCheckResp>true</ReqValidCheckResp>
   <ReqTimeSyncResp>false</ReqTimeSyncResp>
   <ReqSecLocalResp>false</ReqSecLocalResp>
  </Csmp Cfg>
 <NetworkScale Cfg>
   <NetworkScale>small</NetworkScale>
 </NetworkScale Cfg>
</DevCfgSchema>
_____
```

Note: In the above schema, phy mode 149 refers to OFDM modulation with a data rate of 800kb/s.

The cfgwriter utility converts the input XML file into a binary format (.bin) output. Successful execution of the cfgwriter utility with the XML file and necessary certificates as input will return a '0' numeric code to Standard Output (stdout).

From the command prompt on a Windows PC, navigate to the folder where the cfgwriter utility and all the necessary certificates described in Table 14 are placed.

The following is the command syntax used to generate the config (.bin) file needed to program the IR510 node:

java -jar cfgwriter-6.0.20.jar -x <IR510.pfx> -p <password> -ca <CAcert.cer> -w <config.xml> --nmscert <csmpcert.cer> <outputfile.bin>

The command line parameters used in the above command are explained in Table 14:

Table 14 cfgwriter Utility Command Syntax Parameter Options

Parameter	Description
-x <ir510.pfxfile></ir510.pfxfile>	IR510 Cert & Private Key file in PKCS12(.pfx) format to be created and exported from the ECC CA server.
-p <password></password>	Password provided while exporting the IR510 (.pfx) certificate from the ECC CA Server
-ca <cacert.cerfile></cacert.cerfile>	Trusted ECC CA public Cert (DER encoded) to be installed on the IR510.
-w <config.xmlfile></config.xmlfile>	XML config file of the IR510 used to generate the corresponding binary .bin file
nmscert <csmpcert.cerfile></csmpcert.cerfile>	The .pem file certificate downloaded from IoT FND GUI in binary format (with extension changed to .cer) for mutual validation of csmp communication messages between IR510 and IoT FND.
<outputfile.bin></outputfile.bin>	Output bin file generated after successful execution of the specified command. A numeric code of "0 (zero)" seen on the standard output means command was successfully executed.
	This is the same config bin file which is used to program the IR510 later.

Figure 40 shows a sample command issued to generate the .bin file needed for IR510 programming.

esktop\tools>java -jar cfgwriter-6.0.19.ja

Zero Touch Enrollment of Cisco Resilient Mesh Endpoints

Figure 40 Bin File Generation

Bin File Programming

The binary configuration file (.bin) prepared in the previous step, along with the correct firmware, is programmed into the IR510 node using another utility known as HostOne tool (fwubl). This tool is also placed on the same Windows machine where the cfgwriter utility was placed.

Note: To obtain the HostOne (fwubl) tool discussed below, please check with your Account team or Sales representative.

From the same Windows machine, connect to the IR510 console port using an USB to serial converter connected through a Cisco RJ45 to DB9 (female) blue serial console cable. From the command prompt on Windows PC, navigate to the folder where the fwubl tool is placed along with the firmware image and config bin files of the IR510.

Note: Do not power on the IR510 unit without any attenuators, antenna, or RF cabling in place. It is highly recommended to keep the RF port on the node always connected; don't leave it to transmit in free air since without the right connector/RF cables, the radio has a high likelihood of becoming damaged.

Once the node is powered on, issue the following command to verify that the node is in bootloader mode first. If it isn't, power cycle the node and check again as it would re-enter into the bootloader mode.

fwubl_win732bit_1.0.5.exe com<port>

The above command output would show the current bootloader version on the node besides few other parameters. Figure 41 shows the sample output of an IR510 unit initially in bootloader mode.

Figure 41 IR510 in Bootloader State

::\Users\\0	esktop\tools>fwubl_win732bit_1.0.5.exe com18
Serial Config: 115200 8	N1
Bootloader Version	: 1.0.6
Internal Flash RDP stat	us : Level 0
lash WRP option bytes	: 0xfff
Security status	: Disabled
lardware ID	: IR510/1.0/2.0
Internal Flash Start	: 0x8000000
Internal Flash Size	: 1024KiB
External Flash Start	: 0x6000000
external Flash Size	: 8192KiB

The next step is to program the firmware version on the IR510 into the memory location specified in the following command:

fwubl_win732bit_1.0.5.exe -w <IR510 firmware.bin> -a 0x8020000 com<port>

Figure 42 shows the sample output of firmware push issued to an IR510 unit.

Figure 42 Firmware Push on IR510

C:\Users_____\Desktop\tools>fwubl_win732bit_1.0.5.exe -w cg-mesh-dagw-6.0weekly-6020-ir510-fedac85.bin -a 0x8020000 com18 Serial Config: 115200 8N1 Note: Memory space 0x08020000 ~ 0x080dffff has been erased! Wrote address 0x080c3d00 (100.00%) Done.

256419

The next step is to program the config .bin file generated for the IR510 into the memory location specified in the following command:

fwubl_win732bit_1.0.5.exe -w <IR510 config.bin> -a 0x80E0000 com<port>

Figure 43 shows the sample output of config bin push issued to an IR510 unit:

Figure 43 Config Bin Push on IR510



The final step is to enable CR Mesh on IR510 by bringing it out of bootloader mode by issuing the following command:

fwubl_win732bit_1.0.5.exe -g 0x8020000 com<port>

Figure 44 shows the sample output to run CG-mesh software on the IR510 unit.

Figure 44 CR Mesh enabled on IR510



Secure Onboarding of Mesh Nodes into CR Mesh

Staging, page 63 provided details on how to set up an IR510 node to securely join the mesh network. This section discusses the components needed to enable secure onboarding of IR510 nodes into the mesh network.

CR Mesh Endpoint - Authentication Call Flow

The FAR router provides security services such as 802.1x port-based authentication, encryption, and routing to provide a secure connection for the mesh endpoint all the way to the control center. IEEE 802.1x using X.509 certificates is the process used to securely authenticate a mesh node before allowing it to join the PAN or to even send packets into the network.

For details regarding authentication call flow using dot1x, please refer to figure "IEEE 802.1x Device Authentication" under the section "Network Security" in the *Design Guide*.

CR Mesh Endpoint Onboarding - Associated Touchpoints in the Headend

Table 15 lists the associated touchpoints that should be set up and configured as a prerequisite step before enabling secure onboarding process of mesh nodes.

Associated Configuration Touchpoints	Purpose	Reference Link for Configuration
ECC CA Server	Issuing ECC type certificates for mesh end points and AAA server	 "ECC Type CA Server Configuration" at the following URL: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Uti lities/FAN/2-0/CU-FAN-2-DIG/CU-FAN-2-DIG5.html#2827 1
AAA Server	Setting up AAA RADIUS server using Microsoft Network Policy Server (NPS)	 Implementing AAA Server with Microsoft Network Policy Server" at the following URL: https://salesconnect.cisco.com/#/content-detail/da249429-ec 79-49fc-9471-0ec859e83872
NPS	Adding CGR as RADIUS client	 Configuring Network Policy Server for Smart Meter Authentication" at the following URL: https://www.cisco.com/c/dam/en/us/products/collateral/cloud -systems-management/connected-grid-network-managem ent-system/grid-multi-services-zanzibar.pdf
Active Directory	Enrolling mesh endpoints IR510 in AD using public certificate	 "Configuring Smart Meters in Active Directory" at the following URL: https://www.cisco.com/c/dam/en/us/products/collateral/cloud -systems-management/connected-grid-network-managem ent-system/grid-multi-services-zanzibar.pdf
IoT FND	Obtaining CSMP certificate from IoT FND to program mesh nodes	 Browse to point 8 referring to the "Certificates for CSMP tab" in "Configuring a Custom CA for SSM" at the following URL: https://www.cisco.com/c/en/us/td/docs/routers/connectedgri d/iot_fnd/install/4_2/iot_fnd_install_4_2.pdf Click the radio button showing the binary option and download the. pem binary certificate (manually change extension to .cer for programming into the IR510).

Table 15 Associated Configurations/Touchpoints at Different Places In the Solution

Associated CGR Configurations for Onboarding of the Cisco WPAN Industrial Router (IR510)

Note: The following configurations are for reference purposes only. They would be dynamically provisioned by the FND as part of Zero Touch Deployment (ZTD) of CGR.

WPAN Configuration on CGR to Enable Secure Mesh

The following is the sample configuration of a CGR1240 for the WPAN interface. Please note that the SSID configured on the WPAN interface below matches what was configured in the IR510 XML schema shown in an earlier section.

```
CGR1240_JAD20410B2Z#sh run int wpan 4/1
Building configuration...
Current configuration: 573 bytes
!
interface Wpan4/1
no ip address
ip broadcast-address 0.0.0.0
```

```
no ip route-cache
 ieee154 beacon-async min-interval 10 max-interval 20 suppression-coefficient 1
 ieee154 dwell window 12400 max-dwell 400
ieee154 panid 1
 ieee154 ssid mesh-ha-s
outage-server 2001:DB8:16:103::243
rpl dag-lifetime 60
rpl dio-dbl 5
rpl dio-min 16
rpl version-incr-time 120
rpl storing-mode
authentication host-mode multi-auth
authentication port-control auto
ipv6 address 2001:DB8:ABCD:1::1/64
 ipv6 dhcp server dhcpd6-pool rapid-commit
no ipv6 pim
dot1x pae authenticator
end
CGR1240 JAD20410B2Z#
```

AAA RADIUS Client Configuration on CGR

The following is the RADIUS client configuration needed on CGR1240 for enabling dot1x authentication of the mesh endpoint with the AAA server:

```
CGR1240_JAD20410B2Z#

!

aaa new-model

!

aaa group server radius ms-aaa

server name aaa_server

!

radius server aaa_server

address ipv4 172.16.106.175 auth-port 1812 acct-port 1813

key <secret key>

!

aaa authentication dot1x default group ms-aaa

!

dot1x system-auth-control
```

Note: The secret key above configured on the CGR must match the secret key configured on NPS when adding CGR as a radius client.

Mesh Key Configuration on CGR

As part of ZTD, the FAR is provisioned with a mesh key pushed from FND that is used to provide link layer encryption for the communication between the IR510 and the FAR.

The following command is used to verify if the key is indeed present on the CGR:

```
CGR1240_JAD20410B2Z#sh mesh-security keys
Mesh Interface: Wpan4/1
Master Key Lifetime: 120 Days 0 Hours 0 Minutes 0 Seconds
Temporal Key Lifetime: 60 Days 0 Hours 0 Minutes 0 Seconds
Mesh Key Lifetime: 30 Days 0 Hours 0 Minutes 0 Seconds
Key ID: 0 *
Key expiry: Fri Feb 8 20:34:24 2019
Time remaining: 4 Days 0 Hours 51 Minutes 30 Seconds
Frame Counter: 200000
CGR1240_JAD20410B2Z#
```

DHCPv6 Server Configuration on CGR for Address Allocation

The CR Mesh nodes need to be assigned an IPv6 address for reachability from the CGR as well as from the control center. For this purpose, a local IPv6 DHCP pool is configured on the CGR as shown below. However, a central DHCP server option, if available is recommended.

```
!
ipv6 dhcp pool dhcpd6-pool
address prefix 2001:DB8:ABCD:1::/64 lifetime infinite infinite
vendor-specific 26484
suboption 1 address 2001:DB8:16:103::243
!
```

From the above mesh prefix, the first address 2001:DB8:ABCD:1::1/64 is assigned to the CGR WPAN interface while the mesh nodes are allocated an IPv6 address from the remaining pool. The sub-option 1 address specifies the IPv6 address of the IoT FND to the mesh nodes.

Note: Please refer to Appendix E: HER and CGR Configurations, page 250 for the complete configuration of CGR tested to bring up the CR Mesh.

MAP-T Infrastructure in DA Feeder Automation

Basic Overview of MAP-T

MAP-T refers to address and port mapping using a translation mechanism and is used to provide connectivity to IPv4 hosts over IPv6 domains by performing double translation (IPv4 to IPv6 and vice versa) on customer edge (CE) devices and border routers.

A MAP-T domain is comprised of one or more MAP CE devices (IR510) and a border relay router (HER), all of which are connected to the same IPv6 network.

For a MAP-T domain to be operational, mapping rules known as basic mapping rules (BMR) and a default mapping rule (DMR) must be configured. While BMR is configured for the MAP IPv6 source address prefix, DMR is used to map IPv4 information to IPv6 addresses for destinations outside a MAP-T domain. Some port parameters like share-ratio and start-port are also configured for the MAP-T BMR whereas EA bits refer to the IPv4 embedded address bits within the MAP-T IPv6 address identifier of the MAP-T CPE.

For more details on MAP-T, please refer to "Mapping of Address and Port Using Translation" at the following URL:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-mapt. pdf

Packet Flow in MAP-T network:

The following is the logical packet flow between a SCADA client and the SCADA Master:

SCADA Client --> IPv4 --> IR510 --> IPv6 --> CGR --> IPv6 --> HER --> IPv4 --> SCADA Master

An actual sample packet flow, including MAP-T parameters like BMR and DMR used in this implementation, is illustrated in Figure 45.





While configuring MAP-T, the DMR prefix, the IPv6 user prefix, and the IPv6 prefix plus the embedded address (EA) bits must be less than or equal to 64 bits.

Note: MAP-T parameters like the BMR IPv6 prefix and associated prefix length unique to each node are configured as part of the .csv file uploaded to IoT FND whereas the DMR IPv6 and the BMR IPv4 prefixes and their associated lengths along with EA bit length are configured via the configuration template in IoT FND which is later applied to the nodes, as shown later in Configuration Options from FND, page 73.

MAP-T Points in the Network

IR510 - MAP-T CE

A MAP-T CE device connects a user's private IPv4 address and the native IPv6 network to the IPv6-only MAP-T domain by first doing a NAT44 translation from the private to public (inside to outside) address within the v4 domain and then subsequently doing a v4 to v6 translation.

MAP-T BMR Prefix Selection for IR510.csv

The BMR prefix is used by the MAP-T CE to configure itself with an IPv4 address, an IPv4 prefix from an IPv6 prefix. As shown in Figure 45, the Rule IPv6 prefix represents the BMR IPv6 prefix used in the MAP-T network. As such, the BMR IPv6 prefix of 2001:DB8:267:1515::/56 corresponds to the MAP-T IPv4 address of 10.153.10.21 of an IR510 node.

HER - MAP-T Border Relay Router

The following configuration is needed on the HER to enable MAP-T border relay functionality:

```
FAN-PHE-HER#
!
nat64 settings fragmentation header disable
nat64 map-t domain 1
default-mapping-rule 2001:DB8:367:BABA::/64
basic-mapping-rule
ipv6-prefix 2001:DB8:267:1500::/56
ipv4-prefix 10.153.10.0/24
port-parameters share-ratio 1 start-port 1
!
```

Additionally, the CLI command *nat64 enable* needs to be enabled as shown below on the HER interfaces participating in the MAP-T translations (such as the interface where the SCADA Master connects and the tunnel interface towards CGR).

The HER interface connecting to the control center side where SCADA Master resides is IPv4 based whereas the virtual-template interface of the HER connecting to the CGR on the WAN side is IPv6 based, as shown logically below:

CGR --> IPv6 --> (VTI) HER (Gig port) --> IPv4 --> SCADA Master

Enabling nat64 on the SCADA Master-facing interface of the HER below:

```
!
interface GigabitEthernet0/0/1.107
description to-SCADA-Master
encapsulation dot1Q 107
ip address 172.16.107.101 255.255.255.0
standby version 2
standby 107 ip 172.16.107.1
standby 107 priority 253
standby 107 preempt
standby 107 name SCADA_MASTER1
nat64 enable
'
```

Enabling nat64 on the FAR-facing Virtual-Template interface of HER below:

```
!
interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  ip nhrp network-id 1
  ip nhrp redirect
  nat64 enable
  ipv6 unnumbered Loopback0
  ipv6 enable
  tunnel protection ipsec profile FlexVPN_IPsec_Profile
```

Note: For the complete running configuration of the HER, please refer to Appendix E: HER and CGR Configurations, page 250.
Configuration Options from FND

Csv File Import at FND

The following template can be used to add mesh endpoints to the FND database.

eid,deviceType,function,enduseripv6prefix,bmripv6prefixlen

The above fields are explained in Table 16:

Table 16	Parameters	of IR500.csv	File
----------	------------	--------------	------

Parameter	Description
eid	A Unique Element identifier to identify the device in log messages as well as in the IoT FND GUI.
deviceType	Used to identify the hardware platform.
function	Used to identify the functionality of IR510 (i.e., DA Gateway).
enduseripv6prefix	The BMR IPv6 prefix unique to each mesh endpoint.
bmripv6prefixlen	The BMR IPv6 prefix length assigned to the mesh endpoint.

The following are the contents of a sample csv file used in this implementation:

```
eid, deviceType, function, enduseripv6prefix, bmripv6prefixlen
2ED02DFFFE6E0F03, ir500, gateway, 2001:db8:267:1515::,56
2ED02DFFFE6E0F0B, ir500, gateway, 2001:db8:267:1516::,56
2ED02DFFFE6E0F05, ir500, gateway, 2001:db8:267:1517::,56
2ED02DFFFE6E0F27, ir500, gateway, 2001:db8:267:1518::,56
2ED02DFFFE6E0F2D, ir500, gateway, 2001:db8:267:1519::,56
2CD02D10006E0F4E, ir500, gateway, 2001:db8:267:151A::,56
```

- 1. To upload the CSV file into IoT FND, navigate to the GUI.
- 2. From Inventory tab > Devices > Field Devices > Add Devices, click Browse to upload the file as shown in Figure 46
- 3. Click Add.

Figure 46	CSV File	Upload	to IoT	FND
-----------	----------	--------	--------	-----

cisco FIELD NETWOR	IK DIRECTOR		DASHROARD DEVICES . OPERATIONS . CONFIG . AD	MIN
DEVICES - FIELD DEVICE	(a):		Add Devices	
Browse Devices	GUICK VIEWET		Upload File	
C ALTAN Devices		E 14	CSVXXML C: Vakepathi/s10-PAN1-S.c.iv Evance	
			Download sample .cw template for Houter, Bateway 203000, Endpoint and Extender, IR500	
841100 (2)			Status	
PUID0 (0)			No job running	
CORF/000.045				
100404				

Once added, the devices will initially be in **Unheard** state. Once mesh nodes start registering with the FND, their device status turns green as shown in Figure 47.



cisco FIELO NETWORK	ORECTOR					REVICES	· IQUERATIO	ONEW: CO		ik v			
EVICES + FIELD DEVICES													
Browse Devices	Ques Vews					Q	Box Films						
CLASSING Desires		14	Incurtory										
di acautta cia		100	And Devices Land	ol + Bulk Operato	n + mys Arten	• *****	Andrew Volume			Dapa	ing 1 - 25	A L Page 1 (P	58 - 2
and the state of the			Name -	Alashii (3	States		Lastings	Category	tipe	Farquar	(renet)	Timese .	*
. The Endledmin Grat			DEDUDOFFFERENT IN			•	7 days ago	ENDPOINT	#4504	GATEWAY	2	8 Ownership 0	2001 db8 at
CATE WAR-HADE (13)			DEDRIDEFFERENCES				50 minutes age	ENDPORT	#1000	GATEWAY	1	8.0eekty/6.0	2001-058-0
States		5 D	-TEDRESALLERE OLIVI			8	48 minutes ago	ENDPONT	(R500	GATEWAY		8 Oweekly16 G	2001-058-06
O Daws (2)		10	20200207972020737			u	NEWS7	ENDPORT	webbe	GATENNY			
Distance (2)	1	12	36.0430444346.0F20				til monutes ago	ENDPOINT	9536	GATEWAY	+	8.0weekty/6.0	2001 db8 w
C 19 (9)		10	#9870-LTE-64- #9+FCWV211004T				2 months age	ROUTER	19800			15.8(2)MEw	
d conce			AND CHYTELITE OA				2 months age	NOUTER	mase			th AcLMEA	-
			#11101-40+FE.W2221000G				2 minto apr	ROUTER	#1100			BLD_V1610_	
			CORPORTATION - 24225410022				8 minutes ago	ROSTER	COR1000		10 C	15-8(3)M	192 184 15
			TEDRODEFFERENCES				2 minutes apo	ENDPONT	IRG28	GATEWAY	15	8.Overkly(6.0.	2001-068-0
			DEDRICH WEIGER				Sil montes age	ENDPOINT	#R500	GATEWAY		E.Overhijt.d.	2001 chill at
			11-20-20-11-11-11-0F-21			8	21 misutes ago	ENDPOINT	8538	GATEWWY	2	8. Deverty (6.3	2001 JDR al
			Remain Ka+FCW22279040			0	A may ago	ROUTER	#R1100			BL0_V1810_	2001 (failt to
		121											- 01

The nodes must register successfully with IoT FND before other settings like MAP-T, NAT44, and other serial configuration profiles be properly pushed/applied to the nodes. However, if those settings are pre-linked via the default profiles, the configuration would be automatically pushed to the nodes upon device registration.

Creation of MAP-T Group

- 1. To configure the MAP-T settings in FND, navigate to Config > Device Configuration.
- 2. Under Config Profiles and click the Add Profile icon (+).
- 3. Create a new MAP-T profile with the correct settings for BMR and DMR rules, as shown in Figure 48.

Figure 48 Creating a MAP-T Profile

cisco FIELD NETW	ORK DIRECTOR			DASHBOARD	DEVICES *	OPERATIONS ~	CONFIG *
CONFIG > DEVICE CO	NEIGURATION						
Assign Devices to Group	Change Device Properties	Migrated-MA	PT-1				
Groups	Config Profiles	Contraction of Contraction	a Rula	_			
Configuration Profiles	+	IPv6 Prefix.	2001 db8 367 BABA				
TE ENDPONT		IPv6 Prefix Length:	64 *				
▼ FMR PROFILE		Basic Mapping	Rula				
Default-FMR-F	Protile	IPv4 Prefix	10.153 10.0				
▼ DSCP PROFILE		IPv4 Prefix Length	24	1			
Defailt-DSCP	Profile	EA Bits Length (bits)	8	1			
▼ MAP-T PROFILE							
Migrated MAP	rit .						

Creation of NAT44 Group on FND

- 1. To configure the NAT44 settings for mesh endpoints in FND, navigate to Config Profiles > Config > Device Configuration.
- 2. Click the Add Profile icon (+).
- 3. Create a new NAT44 profile with the correct Internal IPv4 address, internal, and external ports, as shown in Figure 49.

Figure 49 Creating a NAT44 Profile

cisco FIELD NETWO	ORK DIRECTOR		DASHBOARD	DEVICES	OPERATIONS ~	CONFIG -	ADMIN
ONFIG > DEVICE CON	FIGURATION						
Assign Devices to Group	Change Device Properties	Default-NAT44-Profile					
Graups	Config Profiles	Ethernet Settings IPv4 Address 192 168 0.1					
Configuration Profiles	+	IPv4 Prefix 24 Length					
ENOPOINT							
▼ FMR PROFILE		NAT44 Mappings					
Default-FMR-Pr	rofile			Dark .			
▼ DSCP PROFILE		Internal IPv4 Address Internal Port	External Port#	Increments			
Orfault-DSCP-R	Protèe	192.168.0.3 20000	20000	1			
♥ MAP-T PROFILE							
Nigrated MAPT	4						
Default-MAPT-P	hotte .						
* DHCP CLIEMT PROF	n,E						
Default DHCP.(Churt-Profile						
* NAT44 PROPILE							
Default-NAT44	Profile						
EdgeCompute_	and_Scada_ED	8					

In Figure 49, the IPv4 address and prefix length of the IR510 are specified under Ethernet Settings.

The Internal IPv4 address refers to the internal address of the NAT44-configured device like the SCADA client, which is connected behind IR510. The internal port refers to the internal port number on which the SCADA client would be listening. The external port refers to the external port number of the SCADA client accessed by devices from outside MAP-T domain.

Note: Since 192.168.0.2 is reserved for the Guest OS inside the IOX portion of the IR510 unit, it is recommended to use a different address such as 192.168.0.3 for the SCADA client and, accordingly, multiple NAT44 mappings like the one shown above could be created for different ports.

Creation of Configuration Group on FND

Initially all the IR510s added to the FND are placed in the Default-IR500 group. Depending on the deployment, some of them can be moved to a newly created configuration group in which the corresponding MAP-T, NAT44 profiles can be selectively applied and a config pushed to these nodes.

- 1. To create a configuration group, navigate to the Groups tab > Config > Device Configuration.
- 2. Click the Add Group icon (+).
- 3. Then create a new group of type Endpoint as shown in Figure 50.

Figure 50	Creating an	Endpoint	Configuration	Group
-----------	-------------	----------	---------------	-------

1000 PT						CONFIG.9	
ONFIG + DEVICE CONFIGURATION						6 J - 5	-
ange lævene in henge 🛛 Charge Deven Properties							
Groups Conty Proties							
Conference I	Group	Venters Edit Contigu	ration Template Plash Configuration	Group Propertie	s - Transmission Ba	tings	
A 100000	1						
• House		lat. Mairer	IF Address	East	Mender	Corrup Pulmet	
- ENDECHT	ALC: NO	Add Group		1000	C (Walk)	×	1
CI Delast MIN (10)							
M Lings_Computer (1)		Name	Scada Group				
		Device Category	Endpoint			*	
PL Read Group (6):							
Rest Group (G)	- 4		Aas				-

- 4. Move some of the mesh nodes from the default endpoint group to the newly created group based on the deployment.
- 5. Navigate to the default endpoint group, select the nodes of interest and click Change Configuration Group.
- 6. Then select the newly created config group in the drop-down menu as shown in Figure 51.

Figure 51 Moving IR510 to the New Configuration Group

cisco FIELD NETWORK DIRECTOR						ERATIONS 👻	CONFIGY
CONFIG - DEVICE CONFIGURATION	_	Automatic States					
Groups Control Profile		Tame Membership Group Members Eth C	of guration Template Push Cathguration	Oracio Pres	ernes 1	ransmission Set	1925
CONT240 Shayan (1)		Change Configuration Donage	Over Sevence				
COR, with MITMAN (0)		C. Stat. Name	il ^a Address		Lett Heard	Member Byncud?	Curring Publied?
Default-sgr1000 (2) Osfault-e1100 (2)		nonsere	10.0F-00 2001.d58 abcid 1.825 54	od lece .	2019-02 20.22	No	talse
Defeate-e000.gt)		Change Config C	Sroup		_	×	talor talor
Certaur-rise0(cr0)		O Contra Group	default-ii500(10) [default] Edge_Compute(1)				talse
Edge_Compute (1)			Mesh Group(0) MESH QOS(1) Scada Group(0) Secured Mesh Group(1)			Yes	talse

- 7. Once devices are moved to the newly created configuration group, from the **Edit** configuration template, select the MAP-T and NAT44 profiles created earlier.
- 8. Click Save Changes for these settings to be applied to the devices part of this group, as shown in Figure 52.

cisco FIELD NETWO	RK DIRECTOR				DASH	BOARD	DEVICES -	OPERATIONS ~	CONFIG ~
INFIG > DEVICE CON	FIGURATION								
ssign Devices to Groop	Change Device Properties		Scada Group						
Groups	Config Profiles		Sync Muniberstep						
-	414	0	Group Members Edit	Configuration Template	Push Co	ntiguration	Group Property	es Transmission Se	ettings
CGR1240-Shayan	0):		Current Configuration	evision #2 - Last Saved of	n 2015-02-	64 20:45			
CGR1240 with wi	an (1)				OF	DM-50kbps			
-	199				OF	DM-200kbps			
- CON_BID_WINK	(0)	H			OF	DM-400kbps			
Default-cgr1000 (2	25				OF	DM-1200kbp	6.2		
Default-ir1100 (2)			Note: This settings is ap	plicable for IR510 & IR530 o	devices onl	Ň.			
Default-ire00 (6)			FMR Profile	None					
			DSCP Profile:	None	(#)				
ENDPOINT			Map-T Domain Profile	Migrated-MAPT-1		E			
Default-in500 (9)		=	DHCP Client Profile:	None					
Edge_Compute (1)			NAT44 Profile	Default-NAT44-Profile		8			
B. Marth Camira 100			DHCP Server Profile.	None	9				
-T mean quant (w)			Serial Port Profile (DCE)	None					
MESH_QOS (1)			Serial Port Profile (DTE)	None					
🗮 Scada Group (1)			ACL Profile	None					
Secured Mesh Gro	up (1)							8	
		141						Save	

Figure 52 Editing the Configuration Template

- 9. Finally, push the configuration to the devices in this group by navigating to the **Push Configuration** tab, selecting **Push Endpoint Configuration**.
- 10. Click Start as shown in Figure 53.

India IoT	ORK DIRECTOR			DASHBOARD	DEVICES	OPERATIONS ~	CONFIG
DNFIG > DEVICE CON	FIGURATION						
ssign Devices to Group	Change Device Properties	Seada Grou	p				
Groups	Config Profiles	Sync Membersh	ιφ.				
-		A Group Member	s Edit Configuration Template	Push Configuration	Group Propertie	s Transmission Se	ttings
CGR1240-Shayan	(1)	Push ENDPOR	IT Configuratio * Start	· · · · · ·			
CGR1240_with_w	pain (1)	Pushing Contr	g version.				
CGR_with_WPAN	s (0):	Device Status					
Default-ogr1000 (2	a	#2.14	(and the second				
Default-ir1100 (2)		Panid	Subnet Prefa	Nodes in Group (Kital	in Subort) Cor	ing synced	
		1	2001 db8 abcd 1 0 0 0 0	1 (7)	0/		
C construction (a)							
ENDPOINT							
Default-ir500 (9)		=					
Edge_Compile (1)						
🌺 Mesti Group (0)							
MESH_QOS (1)							
Scats Oren (1)							

Figure 53 Push Configuration Operation

This completes the configuration settings from FND to the mesh node that are needed to operate as a DA gateway.

11. The final step is to verify that all the configuration settings are properly applied to the IR510. Click on the node inside the configuration group and navigate to the **Device Info** tab, as shown in Figure 54.

Figure 54 Verify Configuration Settings on IR510 (1)

cisco FIELD NETWORK DIRECTOR	DASHROARD DEVICES - OPERATIONS - CONFIG - ADMIN -
CONFIG > DEVICE CONFIGURATION	
Assept Denses to Droug Change Dence Property	n Nex INDUITIVIATION
Groups Carrig Plates	Prog. Transmission Referent Martins Reduced Tarle County Mercanistics Tarle Frenzance Mercanistry River Mercanistics Cranic Science Mark County Mercanistics
CORDAD-Shaver (1)	Device Infe Events Config Projectus Mean Routing Tree (De Work Cetter Assets
B G081248, with, start [1]	Inventory to te classe
E COLUMN (WEAR (I)	Name 2010/02/04/06/07/08 Mesh Link Traffic EXD Author/Projections
D Default-car1908 (2)	Domain 1945
C Detail 21100 (2)	Bevice Type Infolm Manufacturer Cross Springers In
Default (400 (8)	Ration op provide standing Ration Registrer
· CHERCHIT	Part Type N1 First Heart 2019-07-24 12:35
Default-effort Bi	Last Property Heard 2019 02 04 12 00 Meah Path Cost and Hope Last Property Heard 2019 02 04 12 00 Last Property Heard 2019 02 04
Nesk Group (1)	Model Number 01016-04288-702280
MERH, GOS (1)	Vendor Hardware KD H/A
Ma Stade Group (1)	Config Drave Scala Grave Fremane Orage data at with the State of the
Second Math Group (1)	Lication provi

12. On scrolling further down, the MAP-T settings applied to the device can be verified, as shown in Figure 55.

Figure 55	Verify	Configuration	Settings	on IR510	(2))
-----------	--------	---------------	----------	----------	-----	---

HILLIN INT	ORK DIRECTOR					IONN	CONFIG ¥	ADMINIM			20
CONFID . DEVICE COR	NERO RATIÓN										
Assign Develop to Doug	Citarge Develo Projectas	Back IED02	ULL LEVEL OF LEVEL								
Ormage	Carrig Photos	Pres Transition	Referen Instead	April Costly Monitoriality April Formation	Nankaraky	Best D	ala Dennina - Erma	a Node Carlilla	alas Create Mor	e Crubel	
		Device Info	ents Carety Properties	Nesh Nusing Tree IDe Wark Only	ALAPS.						
CORTON Should	101	Here P Au	Alexen (Earrant ID	Sales -	1.64	et Hand				
B_ C081040, ett. a	pel (1) (sp	this element 2001	and where 1 \$25 Seld Period	della 2000000 PF Elle se se	4	21	19-42-04				
CGR_web_WPAG	4 (8)	1 1100 2001	100 and 1 Mills 75-0 and	4 8110 300000000000000000		20	19-02-04				
Defailt og 1900 (21					20	04				
Defail-41100 (2)		3 Highs 192	168 150 36	COA1340K3+M020410832	ω.	20	45				
Densitiven (Raw Sockets									
T		Session D	Data Uptra	Paer Address	Fear	trial Part	beta ineface	To Beller	Ra Bytes	Dinnettele Atempto	Benet
Default intoo (t)			Dewn 5477	172 18 107 11		26000	serui0	0		0	0
Bille_Gampule (16	+	Dewn 5477	172.16.107.11	28000	28000	serielt	8		0	0
Rent Group 12)		Map-T informat	1011								
MESH_ GOS (1)		No. T Port Annual	· Intel and the local	and which they I that Address	Ciaran -						
Scale Drog (1)		Map-T PSiO # of 5 To 4 Transiet	R. 13	# of 4 To 6 Transistory 110							

Routing Advertisements from FAR to HER

Note: HER advertises a default route to all the FARs in order to provide connectivity to control center components.

Advertising Summary Route of LoWPAN Prefix

Once the CR Mesh has been formed, the IR510 nodes have reachability only to the FAR. The mesh nodes need a way to communicate all the way to control center components like IoT FND for management purposes. To achieve this, the IPv6 LoWPAN address subnet assigned to the mesh endpoints is advertised to the HER (which has reachability to the control center components) using the IKEv2 prefix injection over the FlexVPN tunnel. Specifically, the mesh prefix is advertised as part of the IPv6 ACL, which is part of the FlexVPN authorization policy as shown below.

Note: The config shown below is for reference purposes only since ZTD takes addresses it.

```
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface
route set access-list FlexVPN_Client_IPv4_LAN
route set access-list ipv6 FlexVPN_Client_IPv6_LAN
route redistribute connected route-map snapshot
!
ipv6 access-list FlexVPN_Client_IPv6_LAN
permit ipv6 2001:DB8:ABCD:1::/64 any ' Mesh IPv6 LoWPAN prefix!
```

Advertising MAP-T BMR IPv6 Prefix using Snapshot Routing

As discussed above, besides advertising the Mesh LoWPAN prefix of the IR510 nodes to the HER, even the MAP-T BMR IPv6 prefix of the nodes needs to be reachable from the control center to communicate with the SCADA clients connected to the IR510. To achieve this, the IKEv2 snapshot routing feature is implemented wherein the BMR IPv6 prefix assigned to the mesh endpoints is included in the route map redistributed inside the FlexVPN authorization policy, as shown below.

Note: The config shown below is for reference purposes only since ZTD takes addresses it. Basically, the BMR IPv6 /128 address of the nodes that appear/disappear from the HER routing table are the ones that match the route-map snapshot shown below.

```
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface
route set access-list FlexVPN_Client_IPv4_LAN
route set access-list ipv6 FlexVPN_Client_IPv6_LAN
route redistribute connected route-map snapshot
!
route-map snapshot permit 10
match ipv6 route-source snapshot
set tag 10
!
ipv6 access-list snapshot
permit ipv6 2001:DB8:267:1500::/56 any ' BMR IPv6 prefix!
!
```

Application Traffic Communication Enablement

This chapter includes the implementation of the following major topics:

- SCADA Control Center Point-to-Point Implementation Scenarios Over Cellular Gateways, page 82
- SCADA Communication with IP Intelligent Devices, page 83
- SCADA Communication Scenarios over CR Mesh Network (IEEE 802.15.4), page 106
- SCADA Communication with Serial-based SCADA using Raw Socket UDP, page 115
- SCADA Communication with Serial-based SCADA using Raw Socket TCP, page 125
- Legacy SCADA (Raw Socket TCP Server), page 126

In order to ensure the proper functioning of substations and related equipment, such as line-mounted switches and CBCs, most utilities use SCADA systems to automate monitoring and control. New sites typically implement a SCADA system to monitor and control substations and related equipment and devices positioned along the feeder. However, older facilities can also benefit by adding a SCADA system or by upgrading an existing SCADA system to take advantage of newer technologies like IP-capable SCADA systems

The Distributed Automation Solution supports the SCADA service models shown in Table 17.

Service	Connectivity	Service Model
Legacy SCADA (DNP3)	Point-to-Point (Master Slave) Single Control Center	Raw Socket Over FlexVPN
Legacy SCADA (DNP3)	P2MP Multi-drop	Raw Socket Over FlexVPN
SCADA Gateway (DNP3) to IP Conversion (DNP3-IP)	Point-to-Point Multi-drop Single Control Center	Protocol Translation over FlexVPN
SCADA Gateway (DNP3) to IP Conversion (DNP3-IP)	Multi-Master	Protocol Translation over FlexVPN
SCADA (DNP3-IP)	Point-to-Point (Master Slave) Single Control Center	FlexVPN - Single Control Center

Table 17 SCADA Service Models

SCADA Control Center Point-to-Point Implementation Scenarios Over Cellular Gateways

In this scenario, the DSO will be hosting SCADA applications (Master) in a Control Center. The SCADA Slave is connected to the DA Gateway via the serial or Ethernet interface. The SCADA Master residing in the DSO Control Center can communicate with the Slave using the DNP3 or DNP3 IP protocol.

Table 18SCADA Protocol Matrix

Transport Type	SCADA Master WAN Layer	SCADA Slave Field Layer
IP	DNP3 IP	DNP3 IP
Raw Socket	DNP3	DNP3
Protocol Translation	DNP3 IP	DNP3

Operations that can be executed when the communication protocol is DNP3, DNP3 IP. or DNP3-DNP3 IP translation are as follows:

- Poll (Master > Slave)
- Control (Master > Slave)
- Unsolicited Reporting (Slave > Master) Notification

The operations have been executed using a SCADA simulator known as the Distributed Test Manager (DTM), which has the capability of simulating both the Master and the Slave devices.

- If the endpoint is connected to the DA Gateway via the Ethernet port, then it is pure IP traffic. The IP address of the endpoint (i.e., IED) can be NAT'd so that the same subnet between the IED and the Ethernet interface of the DA Gateway can be re-used. This approach will ease the deployment.
- If the endpoint is connected using asynchronous serial (RS-232 or RS-485), then the DNP3 could be tunneled to the control center using Raw Socket, and the SCADA Master would consume as DNP3 or DNP3 to be converted to DNP3 IP at the gateway and the SCADA Master would consume as DNP3/IP.

This document focuses on SCADA protocols such as the DNP3, DNP3 IP, and DNP3-DNP3 IP translation protocols widely used in the U.S. Region with a Control Center.





IR1101 and IR807 are implemented as Cellular DA Gateways. ASR 1000s implemented in clustering mode act as a HER, which terminates FlexVPN tunnels from DA Gateways.

19491

The following sections focus upon:

- 1. SCADA Communication with IP intelligent devices
- 2. SCADA Communication with Legacy devices
 - a. Raw Socket TCP
 - **b.** Protocol Translation

SCADA Communication with IP Intelligent Devices

Protocols Validated

The protocol we have validated for this release is DNP3 IP.

Flow Diagram





As shown in Figure 57, the SCADA Master DTM can perform a read and write operation to a remote Slave via the DA Gateway. The Slave can send the Unsolicited Reporting to the SCADA Master via the DA Gateway over the IP network.

As per the topology, the interface connected to SCADA Slave has the following configuration. This configuration is only for reference purpose only since ZTD of Cellular gateways will address it. Please refer to Appendix D: SCADA ICT Enablement Profiles, page 246.

IR807 DA Gateway Configuration

```
interface Loopback0
ip address 192.168.150.21 255.255.0
interface FastEthernet1
  ip address 192.168.0.1 255.255.2
  ip nat inside
  ip virtual-reassembly in
  duplex auto
  speed auto
interface Tunnel0
  ip nat outside
!
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
```

IR1101 DA Gateway Configuration

switchport access vlan 1

```
interface Loopback0
ip address 192.168.150.21 255.255.0
Interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
int fastEthernet 0/0/1 /*It's a layer 2 port, corresponding layer 3 port int interface vlan1*/
```

```
!
interface Tunnel0
ip nat outside
!
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
```

SCADA Master Configuration

As per the topology, the SCADA Master is residing in the Control Center. The following configuration must be required for the SCADA Master to communicate with SCADA Slave.

- 1. Open the SCADA Master Application and add a new DNP3 Master.
- 2. From the Channel tab, configure the SCADA Master, as per Figure 58.
- SCADA Master, in this case, is configured as a TCP Client interacting with the SCADA Slave, which is configured to act as TCP Server.
- 4. Populate the remote address field with the Loopback IP of the Cellular gateway.
- 5. Populate the port with 20000, which is the port used in the Cisco IOS configuration.

Figure 58 SCADA Master Configuration

DNP3 Master C	onfiguration	-		×
Device Channel	Session Advanced Multiple Devices			
Channel Name mo	NP			
Sehavior				
⊖ All ⊛ Mat	iter 🔿 Monitor 🔿 Peer 🔿 Slave 🔿 Unknown			
onnection Type				
Connection Pros	perties			
Mode				
Client () Server			
Local Address	172.16.107.11 - D-Link DUB-1312/1332 US83.0 to Gigabit Ethernet Adapter #2	_	_	
Remote Address	192.168.150.42			
Port	20,000			-
				- 10
		OK	0	ancel

SCADA Slave Configuration

As per the topology, the SCADA Slave resides in the field area. The following configuration must be required for the SCADA Slave to communicate with the SCADA Master.

- 1. Open the SCADA Slave Application and add a new DNP3 Slave.
- 2. From the Channel tab, configure the SCADA Master, as per Figure 59.
- 3. Populate the remote address field with SCADA Master IP.
- 4. Populate the port with 20000, which is the port used in SCADA Master.

Figure 59 SCADA Slave Configuration

	session balantee nuvariceu multiple bevices	
annel Name sl	NP	
avior		
D AL O A	aster 🔘 Monitor 🔘 Peer 🔹 Slave 🔘 Unknown	
nnection Type Serial	TCP/IP STCP/IP and UDP	
Connection Pro Mode	perties	
Client	Server	
Local Address	192.168.0.3 - Realtek PCIe FE Family Controller	*
lemote Address	172.16.107.11	
Port	20,000	:

SCADA Operations

The Master and the Slave can communicate via Poll, Control, and Unsolicited Reporting. Poll and Control operations are initiated from the Master. Unsolicited Reporting is sent to the Master from the Slave. Figure 60 and Figure 61 show the Poll operation from the SCADA Master. Similarly, Control and Unsolicited Reporting can be seen on the Master Analyzer logs.

Poll

The Poll operation is performed by the Master. The Master can execute a general Poll in which all the register values are read and sent to the Master. In Figure 60 and Figure 61, we see a general Poll executed on the Master side. As Figure 60 shows, the Master Analyzer is initially empty.

10.00per + 8 4	Autor ACMINISTRACIO	8 taract + 8 a
Notana • ∰ 100 to the National • ∰ 100 to t	Anager: activity:020-020 1112114.000 1000000000000000000000000000000000000	Write Write Write
	11 (01) (4, 40) 00 (01 01 01 01 01 01 01 01 01 01 00 00) 00 (01 01 01 01 000) 00 (01 01 01 000) 11 (01) (4, 40) 00 (01 01 01 00 00) 00 (01 01 01 00 00) 00 (01 01 00 00) 00 (01 01 00 00) 11 (01) (4, 40) 00 (01 01 00 00) 00 (01 00 00) 00 (01 00 00) 00 (01 00 00) 00 (01 00 00) 11 (01) (4, 40) 00 (01 00 00) 00 (01 0	
Noture Names	All Dirit 400 PT011 P0110 (0000) 00000 00000 0 All Dirit 400 PT011 P0110 (0000) 00000 0 All Dirit 400 PT00000 0000 00 comparing Pail Non-Section 00000 00000 000000000000000000000000	

Figure 60 Master Analyzer Logs before Poll Operation

However, when the General Interrogation command is executed, the values of all the registers are displayed on the Master Analyzer, as shown in Figure 61.

Figure 61 Master Analyzer Logs after Poll Operation



Control

The Control operation basically sends the control command from the SCADA Master to the SCADA Slave in order to control the operation of end devices. The control command can be executed and the results can be seen on the analyzer. The value of Control Relay Output is changed and is notified to the Master. Figure 62 shows control relay output status before sending the control command to the Slave.

Are Noteine	(Ing s plane		-												· C Childrent
043	farme .	T Puint Type T		C Mile	TOM:	T. Tourisry 1	T Heat	T. Device	T (have)	T. basis	T. Sector	0.T	Description .		· DE HENTLE - HENTLER IN-
	200, 111	10 Dealer for Farms	10	10	Ortes	1110210-032630-004	(Constant)	4049.6	019	-2449					
1 ch car	286, 512	(CTravelie McTravel)	10	08	0.04	1110210-024-01464	(Theat	ONE S	-019	-010					a di minut
300	28,414	(2) Tanaire MI Franks	14	104	Orber	11110103-0401-004	(Property)	OVE S	09	09					Taxa 17 10 100
181-	208, 117	(3) Danskin Sit Frankli	18	106	2004	11110103343646	(Planet	1044.3	1014	1010					12 043
	208.125	(1) Toronto Bit Frances	×		Drive	1010008-00444	(Dame)	1049.3	1014	1019					
	2080, 827	Di Tanatia Me Assult	H		(Delta)	1.11.2010 8.20.01 444	The second	1049.9	1044	104					
	the size	(1) Douanta Ber Franzer	÷.		Grow	11112010-824.01444	Distance.	1049.0	1048	1049					
	COL KIN	(O) Designs BX Process	- C.	-De	Grow	101000080436466	(Constraint)	003	-049	00					
	04, 410	(1) Prodest BA Inquite	÷2	De .	0.04	1/11/2010 8 24:30 494	1	1049.0	1010	-010					
	200, 411	C Double #1 heavier	<u>0</u> -	-04	0.04	COLORIDA DALMA ANY	1000	1010.5	1014	00					
	100, 415	D. Double BJ Trapite	102		0.0.0	1/11/2010 8 24.57 494	-	1004.1	-049	-010					
	100, 110	D. Dealine B.I. Papelle	100		Criste.	1.11.2010 824 31 494	1000	1000 1	1010	1010					
	COL FOR	of Dealer Br sauly	1.00		Crime	Line of the local data	-	cont a		-010					
		The local set where the	0	-12	(Delaw	L'INTERNE L'ANT ANT	1	1000		-					
	and and	The foreign and the base of	-	1.0	Crime .	Language of the lot and		0.000.0		-					
	100.010	10 Double Bit house	-	100	Colors.	Little conversion of the lot Adm	122	1000 1	1000	1000					
		the Division data location	- 2	100	and and	And a reason of the last last	1	stant a	dial .	1000					
	PT V STORE	Contract of the local division of the local	-	11		and should be and should be an									
	and all	1200 Broary Childred Status		1.00	Other	1111 STORE & DR. DT. AND	12000	Cher 1	in the second	1000		_		_	
	80.42	FAIL Brown Channel Statute	1	0.00	Ordina	LIBRORY SIDE MARK	27 month	10171	(CRIP	(CHP					
	90 49	192 Brury Duty of Balance	11	08	Online	1010018340444	(Creat	046.1	CNP	010					
	80.64	100 Binary Dutput Hotus	÷ 8.	108	Oillie	11112210 824 21 466	official and	-CNF 3	09	019					
	ao es	10.8 way Duty of Street	di l	08	Online	101001930400448	(Direct)	099.3	1019	09					
	80.48	(VII. Broary Delpot Roles	a	08	Orient	UNUDER REALED AND	(Court	1019.3	1019	1019					
	80.41	(10), Browy Didgert Statum	11	08	Orbie	11122010-010-014-004	(Distant)	10197.0	1019	1019					
	AD HE	[10] Broary Dylpot Status	11	04	Chine .	UNDER ROAD AND	107mm	(0197.5	,cnie	-cmit					
	80.84	[10] Broary Dulpat Sales		08	(pairse)	10102010-0.04,00-046	(Property)	10197,5	scher	iONP					
	80.410	(10) Broary Chilpot Status	6.19	(28	Debur	101031010324.00444	10 mod	ione s	(Crist	(Chill					
	80.011	(11) Broary Dolgost Station	11	0.00	Orim	10112010-02400-400	10mm	097.0	:014	10%					
	wo eta	(11) New YOrkert Salars	6 12	.0#	0-iw	11112010-024.00-000	(Court	0411	dept	s299 ²					
	30 413	(11) Broary Dalaset Status	cit_	1.04	Orline	1/11/2010 8 24-00-440	1000	041	-014	-019					
	10.414	(11) Brury Didaut Status	6.14	04	Orbe	111120-0124-0144	(Const.)	018.8	04	0.04					
	Cash with	1910 Name Taland Statement	6.76	0.00	dedeel	1/1/2010 0 (also b) Also	(Course)	4048.8	1210	1010					

Figure 62	Slave	Register	before	Control	Operation
-----------	-------	----------	--------	---------	-----------

Figure 63 shows how SCADA Master sends the control command.

Figure 63 Master Control Operation

Notest + +	* Ander included the first of the	CALIFORNIA STREAM	(R beach + 8 +
4 (2) DW - Hen Womann	Sular an electric parts		a CB Distant
A Breen	sector sectors and the sec	 Free second applies plan assessed in the second seco	🕴 🖌 🗮 DESETTP-6/VED/4-(nume)
	111 Decision for Inglish (14	07 Data 200014050440 Tas 2000 4000 4000 4000	Contract of the second se
* 202 com	210 Doutre by Ispan 60	07 Date 212774151440 Tes 2746 400 400 ADP	
200.000	10 Distrete the results 00	07 Down 21277 4355 44 To 2140 1290 1290	1 1
10.00	111 Couble del Inputto Int	Of Date 2/2019 4/5 34 AM Ins Direct 4DM 4DM	
	221 Deutlie Bit Inputs III	06 Delev 2/1001435/0.848 Tea 27666 eDV eDV	
	15 Dealer M reputs 10	08 2ndee 21/2014/1516.442 The 22/46 e214 e214	
	[3] Double the Ingluin [17	08 Joins 2/071143514.00 The Thirt eDW EDW	11
	10 Deutre intropais 36	DR Dollar 21/20114/558-640 Tax 27-bit 4258 4259 1259	54
	201 Dendate Sei Papula	07 Doins 20201435144 State State 2000 x200	
	2013 Blocky Torigon Termines 2	DR Date \$1000 + 000 M	(e)
	210 Bring Dalpak Sature: 9	01 1ptm 201012401346 3m 5m 17m 2010 4020 4020	
	1111 Bridge Delper Deliver 2	De al Record for the local forth in the street where where	121
	21th Marry Durput Tensor: 3	On a fairs Constitute Octo Birch Ina Direct adult adult adult adult	
	110 Binary Dutovir Danuami 4	DR CR In the second state to be and the second seco	
	215 Broady Historic Testucer, 5	CP 2 public in the same initiality build points are not reasons in charge of the same true. Street within which a public subject	10
	210 Steep Depot Summer 4	04 I III 100 100 100 100	
	210 Mary Doput Samer, P	Difference and a second s	
	212 Strate Colors Subart, B	07 E Concentration of the State COV 4019	
	2112 Binary Deput Tomane: 9	UP II And Annual 0. If the Divid schol schol schol	
	2112 Briefs Dubor Summer 14	18 I describe table	
	110 March Traipur Tumper, 11	of a second seco	
	110 Smart Dulpot Tratuani 10	07 0 30 has three store schere	
	218 Bivey Output Values: 10	OF a C feedback Role Data Sectors Sectors 100 The Street allow allow allow	11
	(11) Bries Duty of Balance 54	OF 1 Must Administra	
	210 Name Deput Summer 10	DR III IN AND ADD ADD ADD	
	210 Billery Dogod Salares, 16	DR II THE Appendition from the Drug wind wind wind wind	1
	1111 Stray Delpter Summer, 17	or a Maxar ha Find sDV sDV sDV	1
	111 Annual Calabart Statutes 10	Of the Manuel In-Carnet Schulard The Stand with with a	
	2111 Briers Dubor Summer 19	of a provide strategy strategy have also also	
	[11] Blues Dallad Samer 20	DP I he that any any	
	2112 Terrary Dogost Transmen 21	OF 0 ANY IN CASE IN Disk shot shot shot	
States and states in the state of the state	The Party Colored Textures 12	DE COMM ADDITIONAL DOCUMENTS THE DESCRIPTION ADDITION ADDITIONAL ADDITIO	-

Figure 64 show the Control Command and Control Relay Output status changed on the SCADA Master.

and have been as a second	1 100	0.00													Referred .
	The Local Division of	100 - 10 Big 1 fee - 1 group 5.4													· · ·
1.1.6943	Rana	T Raint Type 7	1 . 1	- 104	T Southy	T Timestamp	7 100	T Dains	T thereit	T Series	T int	H T	Sectiption	T 1	· DE INNER ANALYSI INAN
	100,110	(2) David in the tagents	.19	10	- 1014	CONTRACTOR ADDRESS	at these	1048.0	474	429					
1 1 1 1	200,419	(1) Double Bit Agains	-24	-04	(Online	NUMBER BARDON	44 (1719-14)	1044.0	4747	-1044					· D Incom
100.000	CRL #10	(1) Double Bit Inputs		08	0.04	Narrashkat v	al phone	048.2	694	100					desc 11,01 MB
10000	28.411	(1) Disalter Bil Inpain	10.	-04	Office	1/11/1010 634364	at these	047.5	1249	4000					2.494.5
	CON. P12	(1) Double B1 Inputs	. 10	14	Colore	1/11/019 80436-4	M Street	-048-3	0.00	4094					
	CHL #11	[2] Double #4 treats	10	100	Chine	1/17/2019 8:28:36.4	4 279-4	018.5	- 694	1044					
	CBL F34	(2) Double Bill Hyurts	38	- 28	Onited	0.000004828383	44. 27%44	1049.5	- 00	- 649					
	CBL #15	20 Double 80 Hypots	18	04	0.00	0/07/2018 8:34:36.4	at press	1049.5	-04	4094					
	CBL F18	(1) Double for types		100	1000	1/07/2014 818 96 4	a prod	047	100	404					
	CBL 117	(1) Standing Mit Inpudie	10	100	(Deep	UTUDITE BOAMS	et 27mul	1049.2	254	1294					
	200.000	(1) Disable \$11 Uputs	100	24	0.04	A TURNE STATE	an Shared	-046.2	104	1044					
	200, 411	11 Toute by Paul	11	104	2004	STUDIE KUKNER	of provid	(04)3	09	1044	_			_	
	and the second second	111 Tree Lides New		here -				-			_				
	- Second	112 Browy Culpet Sales		100		100000000000000000000000000000000000000	as press	1000		4000					
	and all	100 Broary Colland Ballion		12	-	A DESIGNATION AND A DESIGNATION OF	an anna	049.5		1000					
		118 Broary Output Batton					as press	2047.5	200	1000					
		110 Briefy Culput Ballion		1.0		110000000000000000000000000000000000000	10 17 14	1048.0	104	1000					
	and and	[11] Bridto Colpor Ballon						104.5		1000					
		THE Brown Culture Bullion	- C		-		10 10 10 10 10 10 10 10 10 10 10 10 10 1	1044.5	0.00	1000					
		111 Borry Collad Ballon	1	1.0	-		-	1000		1000					
	1000	[11] Broary Golgod' Ballion				A REAL PROPERTY AND A REAL PROPERTY A REAL PROPERTY AND A REAL PRO	an prove	1000		- 65 -					
	1000	The strang could be a			-	100000000000000000000000000000000000000	a prese	1000							
	and the second second	The Browy Collect Station								1000					
		the base to be a family			-	and the second second second				- 622-					
		The Bridge Company Street			1000	A long to the local data in the		1000	100	- 0.27					
	and id	The Bridge Colleged Roman	21		1000	Long strain and strains	-	inter a	100	1000					
	Shares .	the base of base has		-	-	the late to be to be		10000	100	-					
	Sec.	110 Room Comparison		1.4	- Contra	Longing all and	Ad internet	1000	1000	100					
	C att	THE ROOM COUNTY NAME	1.1	12	Contrast.	townships \$ 19.10		1041	1000	1000					
	and and a second s	110 Room Comer Street		12	in the second	almenting group of	-	1000	100	1000					
	40.010	our Wines Color Town		14	Concession in succession in su	And the second s	at the	1000	1000	100					
	and all	The survey of the state	1.0	1.2	- Come	Longitude di statut	1		1000	100					
	at att	For Brief, Dated Server	1.0	1.0	theme.	Interviewe Bure No.	at these	10000	124	104				2	
	and the second second	and the second se													

Figure 64	Slave Register	after Control	Operation
-----------	----------------	---------------	-----------

Unsolicited Reporting

Unsolicited Reporting is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are notified to the SCADA Master. This notification can be seen on the Master Analyzer. Figure 65 shows the SCADA Master Analyzer before any unsolicited reporting.

Figure	65	Master	Analy	yzer
---------------	----	--------	-------	------



Figure 66 shows that the binary input of the Slave is going to change. Initially the value of binary input is **OFF**.

Workspiele .		100																					Parlament .	
· She brant			-						-			-	_								_		A - I Childrennet	
4. 4.47		Name .	T	Paint Type	Ŧ		T Miles	T	-	Ŧ	Threatury 1	τ.	- Incat	Daries.	τ.	Channel 7 1	T. Desired	Sene .	τ.	Desciption .		1.2	· Di beater and	
100				The Property Name							L'UNITE COLUMN		-											
· 19				(Classic Pando		A	100		linie -		Unclare stands	and -	(Triut	1.963		0.00	400						+ Dones	
Box		140		(1) Brokis Hatuli		1	100		(mine		1010,0074 (0,0414)	and -	[Triad	1.963	_	0.00	494							e
distant.		140		11 Brans Spectra		1	100		100		1010074434361	-	(Print)	047	_	and .	494					1.0	1041	1.1
		144		The set of		۰	198		Dete		transferre autorite	104	(Phase)	(14)	_	CHP	- 04							
				11 Processing		٠	- 14		pairs.		100.0010.004	-	LTMost	10403	_		0.00							
				11 Briers Taketo		÷	-18		2010		1012010-02400-	-	Division.	104.1		104	114							
		147		11 Birwis Yapate		1	1041		Deliver.		1012010328004	-	[Pised	1044.5	_	499	104							
				Dilling's Sports		+	100		Distr.		1112010-014-014-00-0	- 688	(Tited	194.5		0.0	424							
		- 49		11 Knowy Supply		Ť	108		Dates		101,01118,04,001	net .	[Think	(14)	-	0.00	404							
		100		(1) Really Family		16	105		(Dine)		1010/0018-838-364	104	(Trees	100.5		250	4768							
		6.411		(1) Realizinguite		11	-04		failes -		10103010336363	- 100	Division .	1.993	-	010	-054							
		1410		() Brong Youdo		15	04		(nine)		1010/0010-0.24100-0	-	power.	100.2	_	0.0	00							
		e418		Thinky Tracks		0	08		Drive .		1/11/2014 8/24/02 4	=	(Think	040.2	_	298	4244							
		1414		(1) Brony Topolo		14	:08		Drifter		tyto, bore each of a	int -	[PPMmd	0.640		259	-244							
				11 Binny Inputy		11	08		Dalve		hybridgene boarder	and .	[Think	(10)		674	104							
		1415		11 Breny Instell		14	-04		Draw.		tottopere este alla	and -	12Med	1040.5		69.0	494							
		1412		11) Birwy Amate		67	08		Children .		Longere 644 364	ALC: N	[Theat	048.3		0.0	0.0							
		111		TC Brony Insulo		18	08		Driver -		tritugate épaixel.	ARA	[Trine]	1,943	-	ch#	694							
		1.818		TI Bindry Insulo		18	08		Detrai		University of the second	ALLA	DTHeel	0.985	-	254	det							
		1420		TO Breek Insula		10	.08		Original		LITUDITE BURNEY	49.8	DD4ust	1040 2		254	424							
		i igi		Charles Franks		28-	08		(hiter		http://www.ada.ada	404	Division in	043		04	0.0							
		100		12 Broky Tepolo		22	100		Dollars.		Introduce Adaptive	and a	1274 mart	(40)	-	250	100							
		1241		It been insets		23	108		Distance.		tratument database	-	17Hour	1.960	-	che .	404							
		+0+		11 Bridge Youris		34	208		2014		Longers & Jacks	and i	171648	100.5	-	254	424							
		+11		11 Brary Tabata		18.	204		line.		Locate Bakple	mt :	(Tread	(10.5		done .	100							
		1408.		(1) Bridge Pagester		28	100		loin .		VEGETE BANDO	nie :	(Print)	(44)	-	254	494							
		427		(1) Broky Tupolo		pt.	- 14		linte		1010010-02406-0	nie -	(Triue)	043		Ch4	434							
		818		Pickeyes, Ingenter		28	104		(inite)		11112010-02406-0	100	(Trius)	(10)		000	400							
		400 -		(1) Bridge Franks		29	14		Inia		transferre duta al e	ai.e	(Press)	041	-	0.00	434							
		+		PERMIT		10	-0.0		Doint .		transpression pla	ini i	(Distant)	(14)	-	ine .	210							
				[1] Broniy Yupolit		44	.04		line.		COLUMN & AND	int .	1214100	(14)	-	0.00	010							
		111		[1] Biory Yushin		44	100		inite.		1111-011-0.04-04-0	and .	17Maril	045	-	014	250							
		++++		11 Billion Transfer		11			(min)		100.0010.014.00.0	ant i	10 mark	041		ine .	454							
and the second second	F.	-		interest little of int	Contra da	-																. 9	and the second data	
Strength Reports			-																				Automa Progra Spectar	

Figure 67 shows that the binary input of the Slave is changed from OFF to ON.

Figure 67 Change in Slave Register Value

and statements of the statement of the s	1.1.1.1.00	ALC: NO.												
a secondary	Depresent	- took with the last of		-										· · · · · · · · · · · · · · · · · · ·
1 1 4947	Name	T Peers Type	7.4	T West	T limity	T. Treatury	T. Beet	T. Berla		T. Bearse	T. Setter . T.	Description	T	+ 101 101000 HARDED STAR
	10.00	and the second second				Address of the local division of the local d	-	1000		100				
- 114	2.11	10 Printy Insult	- P.	-04	(bibe	111.00103.00.00 AA	27444	1041	104	104				· · ··································
303.000	and .	10 Programme	1	- 24	Drive	1/11/0019-8.34-30 AM	27444	041	0.00	1044				they set up
Are on	8.41	(Chren haute		14	Dire	1010078-80430 44	37964	- 047	-047	-014				3 494.4
	81.64	(1) Breach Installer		- 24	Oder	101001840430444	1000	1000	100	4040				
	8.45	13 Break Transfer	- N	24	Ories	UTUTO BALADIAN	1000	104.1	1000	104				
	8.44	(1) Brown Hands	M.	24	Critree .	1/11/07/08/06/06 AM	1000		404	-079				
	4.47	(1) Knoley Insteads		-04	Orient	COLUMN ADDA AN	C CTreat	-047	-09	-099				
	4. 15	(1) Knale Instate	t.	- 24	0.04	1.11.00118.04.0144	i (frast	GN /	1014	1044				
	A 17	(1) Bruey Inputs		08	Orben	1.31.0018.834.31.44	a board	001	010	-010				
	AL #15	10 Brany Inputs		08	Orive	1/11/2016 kJik30 AM	- press	001	010	010				
	21.011	(1) Briary Insula		-08	Office	STEL COTH & SHE SO AN	27464	-014.5	-018	-018				
	B #12	TO Briany Installa		08	Online	5/81/0018-8J#30-AM	1.12044	091	634	690				
	30 915	(1) Brivery Instally		08	Ortes	5/51/0/18 #J#30 AM	1 If the	041	100	104				
	81.854	(1) Briery Indely	14	08	0.6w	1/01/2010 0.0430 AM	1 STried		-04	-04				
	BL 915	15 Briefs Insula	- P.	0e	Offee	1/01/2018 8 2 6 30 44	17 April 1	CHP 2	09	1014				
	8.418	25 Rives Inputs	19	08	0-6re	VEDORE BUILDEN AM	1,22404	017.1	04	04				
	81 #12	(1) Brwy have		58	Orive	UNDERFORMANCE	1 Direct		104					
	26.915	20 Brves meuto	- 4	04	(D-free	1/01/2019 8:34 NO 4M	1. 12444	001	04	014				
	24,918	(1) Broars Impuls		.04	Othe	17112018-BOEN AM	a street.	(14)	014	017				
	B 422	212 Brows Instalts	- 28	.08	Drive	3/01/2019 424:30:40	CONTRACT I	(24)	010	CHE				
	20 427	102 Briang Hisparts	21	.0#	Orline	3/91/2019 814.81.44	CONUS.	(20)	1074	674				
	39.422	12 Briefs Inputs	12	.04	Other	3/01/0079 81430-44	1 (Dist.)	09.3	494	474				
	(R) 825	10 Browy Inputs		08	Ordere	VALUETS KARD AN	- District	-074.5	- 674	474				
	81 128	(1) Broaty impute	14	24	(Deltras	1/11/2010 9/24:30 85	1. 27mut	210,0	1254	4294				
	81 625	10 brury mesh		24	Orbra	1.111.001114.0430 45	27904		014	494				
	81428	100 Browin Ingenter	10	124	0.0w	1/11/2014 0.2410 44	1.11000	(14)	-094	-0.94				
	81.427	25 Broady Installe	17	104	Orive	10100103243044	107444	041	1044	104				
	P 410	(15 Prove Installe	19	24	Otes	1/11/2014 8,24 32 44	1 Internal	1093	4249	-428/8				
	P-420	25 Bridg Inputs	19	- 24	0-bree	1.11.007(+).4.0) AM	1 (2Dist.)	041	-04	4240				
	Pr + 10	(1) Bridg Tranks		104	Ordine	1.11.1010-0.14.20 44	1 (Triat	4299.5	424	4769				
	3(4))	(10 Broke Instale		-04	(Indexe	1010019-03430-04	Contract.	100.0	with the	(sleet				
	31.432	(Christing Input)	- 10	- 04	Dire.	10100104343644	1 Distant	016.5	14048	-048				
	Dr +11	(Christ) Inputs		0.04	204	1.01.0076-6.0430 AM	10004	041	1000	1000			1.9	
tion from the	Select State	· · Diamong Diff of 28	P data provins										1	Andrew Subgir Balde

Figure 68 show the Unsolicited Reporting on the analyzer. The value of Binary Inputs is changed and the same is notified to the Master.

telepan + B	· · higheriations	Moniphil Prants in	04-04-09										8 tenets
1 12 I'll iter distant	3 age 1 miles were seen as 1												a 🕼 Dia haberak
. Il stat	States of the Owner,	ALC: NAME: OF	-	and an other D	dimension and an other	140000	COLUMN T		ARCTIC N	Max and	A	1000	a 🔤 bibellije Alvelite imane
- 4 mm	TI denny legula	1	0	11000	ATTUCT STOLET AM		the c	271004	100	-	109		Trees.
* 1 K -100	[11] Browy-Install	4.1	128	Oritor	2/1/02119-0-02-06-0M		- the l	1710	+04	100	104		A CO DUCTOR
	111 Browy Instals	4	00	Oritory	2/1/02/19 #325/34 AMA		(Date)	Unit	1016	104	104		1.
* G.m.	[11] Browly Impuls	1	100	01014	Unvionne explose end		Tot	these.	where	+0.947	ALC: NO		
All Index (Specify	and I'll Among Supports	4	04	Online	2/1/2019 4:05 54 844		the later	(Date)	+Cip	+04	1040		
	[11] Benjety Vapurla		104	0.04	27\0219-43536-AM		7.4	17140-0	+010	+04	104		
	211 Briany majore	4	0.0	(194	211/2015 #30 to and		940	(Presd)	+(10	100	104		
	(1) Brian Inpute	# ()	1.0	(1994	2/1/2019 # (5:00 AM		the l	27444	w0rdi	+04	100		
	111 Review Impacts		0.0	(res	2/1/2019 4:03.04 444		1 to 2	(Press)	- 400	1010	-OVP		
	TT Briang Papels		04	(104	2/5/0019 # 00004 AM		9.4	271mod	404	+04	1004		
	FT Briefs Inputs	10.	04	Drive	2/1/2019-#3239-AM		Tim .	(Deep	+010	109	109		
	111 Briang Paperts	10	UH.	Dyllow	211/2019 4/2019 AM		144	10mm	+014	1000	104		
	[11] Briany Hypothy	12.	Der	-Online	2/5/2019-410(38-4M		Trat .	all had	+258	100	+ONP		
	111 Billion's Yoshille	10.	DR-	Crime	2/1/2016 A 2016 AM		The	1744	+04	+04	1010		
	(T) Reary Topute	14	100	Crewin .	271/0019-0-01236-AM		5.4	(Change)	+010	109	101		
	211 hours read	78	04	1144	STUDYS & SUID AM		Due .	(Press)	+140	+04	.404		
	211) Revery Hyputa	18	10	Drew	21/0719-#31038.AM		See .	(Dream)	wine	+04	wine .		
	(11) Binaris-Inpute	11	01	(rea	2/1/2219 #32:58 444		(Figs.	17962	+010	+24	109		
	TT Reary Trains	14	198	Dev	An and a local second		1.4	(Press)	+2%	104	1000		
	10 Brian Insula	18	04	0.94	211/2019 #10/39 AM		the state	201944	+210	104	109		
	211 Binary Nands	10	UH.	Detter	LITCOM 4/0/54 AM		7.4	(mag)	+04	104	109		
	211 Breasy Inputs	21	08	Grieve	211/2019 4/30/38 444		The	17%ed	+04	+000	100		
	[21] Breaky Installe	22	108	Delay	211/2219 #35158 AM		The	27%64	+010	+04	100		
	TT Bruns Neuro	28 -	114	(Drive)	27V0719-01036-AM		214	(presid	+018	109	104		
	(1) Maria Tapata	24	04	Dille	211/2019 4 (0.04 444		Tran .	[Field	+010	+04	104		
	TT Broke Pauls	25	198	0.64	And any a state wat		0.4	17944	+010	109	104		
	(1) Brooks Inpute		104	(Dilles	(///2019 + 01 to AM		Tue .	(Direct)	+(3)	+04	104		
	ETT Reary reputs	22	198	0mu	Unigers elected and		(Trat	(Pres)	+210	100	104		
	Ets Brows injuste	28.	04	(real)	2703PD 4 (0.06 AM		940	27964	+210	104	100		
	[11] Billary Inputs	29	UM.	(tentres	271/02119 4:00:04 AM		Pat-	the	100	1000	NOP		
	The Brown inputs	39.	0e	Online	211/2019 4/2019 844		2 hat	10%ed	eche.	HONP	109		
And Address of the Owner, Name	STATUTE Briefs Transfer	11	Off	Other	process acts to and		244	12746	with P	woke-	HONE .		

Figure 68 Master Analyzer after Change in Register Value

Legacy SCADA (Raw Socket TCP)

Protocols Validated

The protocol we have validated for this release is DNP3.

Flow Diagram





As shown in Figure 69, the DTM Master can read and write the Slave via the DA Gateway using TCP Raw Socket. In addition, the Slave can send the Unsolicited Reporting to the Master via the DA Gateway using TCP Raw Socket. For more details about Raw Socket, refer to the *Distribution Automation – Feeder Automation Design Guide*.

IR807 DA Gateway Raw Socket Configuration

As per the topology, the interface connected to SCADA Slave has the following configuration:

```
interface Async1
no ip address
encapsulation raw-tcp
!
line 1
raw-socket tcp client 172.16.107.11 25000 192.168.150.42 25000
databits 8
stopbits 1
speed 9600
parity none
!
```

IR1101 DA Gateway Raw Socket Configuration

As per the topology, the interface connected to SCADA Slave has the following configuration:

```
interface Async0/2/0
no ip address
encapsulation raw-tcp
!
line 0/2/0
raw-socket tcp client 172.16.107.11 25000 192.168.150.42 25000
databits 8
stopbits 1
speed 9600
parity none
```

SCADA Master Configuration

!

As per the topology, the SCADA Master is residing in the Control Center. The following configuration is required for the SCADA Master to communicate with SCADA Slave. In this implementation, we used the SCADA DTMW simulator instead of a real SCADA device.

- 1. Open the SCADA Master Application and click Add a new DNP3 Master.
- 2. From the Channel tab, configure the SCADA Master as per Figure 70.
- 3. On the SCADA Master, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching for your device configuration.

Figure 70 Master Configuration

🕼 Dill) Matter Configuration — 🖸 🗙	10	- 0	1 X	
Deutes Charvel Settion Advancel Multiple Devices	Der	wat Owned Sexual Advanced	Multiple Devices, [1]	
Deniel Saine #CNP	20			Ŕ
Interview All # Master © Monitor. © Peer © Siner © Linkenbers Connection Type # Senist © 102/P © 301/31 and UCP Connection Properties Total the Contexts 3		Rahametian Rahametian III Senal Readfune ReitCharMail	342 13000 DfCoriemon Seculify perfect 4600 e	
Beat Faire (500)		NumCetalitis	an,a	-
	2	Parity	arts, i Mitra	
		RefMade	Manie Canava	-
		RochttyMade	Distance Discussion.2009.02.04711C3Phoperture	-
		TefragmentSize Teframetice	2048 2702	
		UseConnector/Head Wei(12)Strating	ж п	
	-	r Hy wolfy the party, for the channel, must b	e noves, sold of nonee	
OK Canad	1		OK.	Center

SCADA Slave Configuration

As per the topology, the SCADA Slave is residing in the field area. The following configuration must be required for the SCADA Slave to communicate with the SCADA Master. In this implementation, we used the SCADA DTMW simulator instead of a real SCADA device.

- 1. Open the SCADA Slave Application and click Add a new DNP3 Slave.
- 2. From the Channel tab, configure the SCADA Master as per Figure 71.
- 3. On the SCADA Slave, select the appropriate serial port, baud rate, data bits, stop bits and parity matching for your device configuration.

Figure 71 Slave Configuration

Der Commen Configuration D	URP3 Cambridge Combyonness	Jex.
Dear Churren Senior Dataser Anarret Multipe Decar	Device Owner Sensor Database Advector Multiple Devices	
Channel Kanel KStd	111 A.R.	Q.
Infrarer 2 Al - August - Manter - Pere - Tare - Literature	Advancion 212 Balancimente 1000	
Connections Type * Senat 10 102/07 and SDR	Example Sealthyperies Example 900	
Constitue Puperior Issue Pup COM14 *	FortChelline II NumChelTimodetseterfine A	
Red fatr 1802 =	Number	-
	Perg NDL PercTition DAL	
	PortName NCHI PortName COM14	-
	Spinn Programs of	
	ECONOMIC DE LA CONTRACTORIA	
	Service 241 Service Se	
August (1997) Desce Rolline . OK General	Inigent (MP) Deven Profile	OK Genal

SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Unsolicited Reporting is sent to the Master from the Slave. Figure 72 and Figure 73 show the Poll operation from the SCADA Master. Similarly, Control and Unsolicited Reporting can also be seen on the Master Analyzer logs.

Poll

The Poll operation is performed by the Master, which can execute a general Poll in which all the register values are read and sent to the Master. In Figure 72 and Figure 73, we see a general Poll executed on the Master side. As Figure 72 shows, the Master Analyzer is initially empty.





However, when the General Interrogation command is executed, the values of all the registers are displayed on the Master Analyzer shown in Figure 73.

		And an increase of the	a sourcemente "	# treat + # -
The second	If the face holds, If the face holds, If the face If the face If the face		0 0	 Image: Second se

Figure 73 Master Analyzer Logs after Poll Operation

Control

The Control operation basically sends the control command from the SCADA Master to SCADA Slave for the purpose of controlling the operation of end devices. The control command can be executed and the results can be seen on the analyzer. The value of Control Relay Output is changed, which is notified to the Master. Figure 74 shows control relay output status before sending the control command to the Slave.

Figure 74 Slave Register before Control Operation

Writers + + + +	 If she is 	Col II													Network + 8 H
· Statistics	The surface in		-												· · · · · · · · · · · · · · · · · · ·
1.57	1	T Autor Type T		1.000	T Guilty	T. Desirery 1	1.000	T Series	T Ound	T basis (T tette	τ	Desciption		• 🖬 111/10 (4000) (400)
1 20 00	10.412	10 Dealer St. hands		100	(hite	27,0070 1,0070 844	-	100	100	100					and Different
	10.10	10 Title 81 March	10	24	Colore	D-COLOR DOI: 10.004		1000	1000	1000					and there
2 State	200, 014	OTTOMAR IN Maler.	14	-08	0-6-8	2-CONTRACTOR AND	1744	100	100	104					
and the second second	28, 411	100 Double Rt Insula	14	04	Ordine	21,0010 2.08.16 444	(Distant)	- day	deal	100					2.000
	246, 1510	Of Double Brillion		08	Ordine	2/1/02/10 1 (20 10 404	Distant	date	-data	-database					
	28.411	(D) Coultrie Bri Impurity	10	08	Orthe	27,0279 108-18 MM	(Cloud	0.0	dee	444					
	28, *35	100 Conditio Bill Impulto	18	OF.	Ordine	27/081930816464	27464	1000	-040	-010					
	250.010	(1) Double Bd Inpuls	18	200	0.0-6-6	3-1,0216 5,0816 MM	10 mod	40%	(CAR)	1004				1	
	(in in)	1118 Kines Cuber Setur	- 11	100	1000	0.5 10 10 1 ALC 10 AM	10 million	- 1000	(104	1000	14	14			
	B(2.8); ;	[75] Briery Gulpot Status	- L =	100	0.0*	21,2210,2210,220,02444	different.	40MP	40MP	-idner	1.	1			
	812.04	(HE Rowly Oxford Status	- 1	100	Chine .	2157019 SIDE 16 AM	UTries.	- down	- donat	-brat					
	82.44	(10) Binary Gulput Balance	m, 4	24	Other	2157016 10616 AM	UTried	1048	1010	1010					
	82.85	210 Knory Gulpet Balance	m.1	28	Grine	21/2019 LOD 16-AM	UT Hyped		dage	0.00					
	80.49	(10) Rivery Oxford Ballys	m 0	08	Ordere	21/2019/108:18:464	UT Hould	(chill)	-dhiP	-down					
	80.81	172 Pres Oxford Testue	#i.†	08	Oxine	21/2014 208-16-644	OTHER	scene	date	10%P					
	90.49	175 Brieg Dolpst Selan	- +	08	Ovine	2/1/2019 10819 494	Office	LONP .	1010	4010					
	80.49	102 Rowy Output Taken	n. 1	08	Otie	210/0019 0 08:18:464	Official		-010	100					
	80.810	(11) Rivers Oxford Testure	ei 10	08	Oxine	21/021810816-044	CTNUE	schut	1014	1014P					
	80.411	1712 Rows Dolpot Salue	m 13	108	Oritize	21,0219 10816-644	27944	stree -	1010	1010					
	80.010	1973 Roads Dulper Salar	e: 12	104	Orline	21.0010.0010.4e4	(Triot	4044	-deal	1044					
	40.411	198 Rowy Dulper Setur	- 11 m	104	Orderan	21,02193,00193,000	(Charles	1048	1048	1048					
	80.916	(10) Reway Distant Status	er, 14	108	(Drive)	2-1,1219 1,08:19 444	27 March	1000	40%	1014					
	80.915	(Fit Brary Galgar Street	w. 10	28	Orine	21,0791,0819 44	27904	1014	upper	1014					
	80.46	110 Briefy Datest Server	- ÷	28	Orien	21,271 24221 84	27944	- Juleet	-dente	1044					
	207 #14	110 Brief Statest Statest	m, 10	191	0.0w	2/12/12/12 12:06:06.004	27444	4044	404	-048					
	80.417	110 King Date Setur	- 17	DF	Drive .	27,0710.0816.044	all sense	1044	1044	10MP					
	20.416	1982 Brony Dulpat Salar	10	28	() from	27/2219 1/0219 AM	27mut	Culture -	4040	1000					
	30.419	(10) Browy Colput Ballon	- 17	24	Ordere	21,00100.00014.464	21muk	1010	1014	-1014					
	80.805	(10) Bring Colput Datus	- T	28	Colore .	311/0219 1.0819 444	(Trings)	100	104	100					
	80.921	102 Rowing Collect Dates	- 11	28	(internet)	21,0010.00016.444	11404	1000	1000	1000					
	b) e(2	110 Rowly Sulpat Salar	10.00	2.0	Order .	21/30110108-10-104	. If that	(strat	1.044	100					
	80.433	175 Rivery Guipel Tellow	- 11	08	(Drive	21,2010.006.14.444	1744	1000	dee	dee					
	80.434	(12) Briany Dolped Homes	- 14	00	(below	27,007010818464	1744	1048	1000	100					
mature birms	Section -	Stations 201 of 201 date	-											1	A Design Colors

Figure 75 shows how SCADA Master sends the control command.



	· Notice percention (Notice Parent)	a second s					
1 2 (Thi fare Burtiped	Section web prints the bypacts	Life and an					· D Interest
A Hanne	STATISTICS IN COMPANY AND ADDRESS.	Designed Trees in the	AM DESIGN M RECEIPTION METERS	RAM DRAFT	CHARLES	MESSMILLEN	A M (Calle-Collin years
-	12 Divide be repuir in	OF Deltai	35201131808.000 Tap	(Date 10)	nd, within	+D+	a contract of the second se
• 16	22 Double Sti Hands 20	Of Ontee	2/201713/888.MA But	10 mag	wite %	+04	tars (mail into
10.00	22 Tandra bit Papara Al	01 0444	L'UNITE STREET AND THE	Diand . add	40.0	104	1.000
0.00	10 Double Bit Hybrids	04 Drive	212211131848.448 five .	the et	404	909	1000
	22 Double Millinguis. 28	Of Orive	Londone property and them.	pland add	909	9090	
	(1) Double bit Hands	OF Orland	Anders State And	STwod +07	404	+04	
	Thill Briefs Collabor Televiser #	Of Joine	4/1 1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/	streng out	ni nini	-che	
	[18] Binero Catpid Statutes 1	OF. 0484	252010 (4222.44) 546	Stand all	404 10	+010	
	THE Browy Output Statutes 3	07 0164	All Contra from Contra from Contra Co	atmax out	100	+210	
	1116 Binario Chilgoil Daturasi 3	Of Dates	Name Council Anno Status Bank	(Date of	nd allow	104	2
	Titl Brury Colput Transac 4	OK Ories	Deciptor	(7ma) +0	404	+04	
	210 Break Output Nature 9	07 0444	The service previous may support theory sortial control oper-energy to multiple table protect to the carrier standards find all protect are test enclosed to chance or the carrier	27mat = 00	404	104	8
	[11] Bries Gelpst Dahsen &	DF Drive	lon.	27%od #27	NF +(347	-sthP	
	2102 Brilling Output Statuter 2	OR Online	A second Option	Utimat +0	of add	+01P :	
	(15) Berry Gulp & Trabase, #	05 0.000	Non Microsoft Lafe for January 1	100000 000	NF +054P	9000	
	Thil Brian Calput Datum: 9	07 004	Control Municipal	17 mar. + 47	-04	+210	
	[10] Brown Output Testurer, 10	04 0464	Apat Norther 1 2	STitut eD	NF +014	+04P	
	2111 Brivana Carlport Walkards: 11	07 0.044	Overficie Union	2784 40	which which	with #	
	118 Broay Culput Salues: 11	OF Date	Note (in few 100 20	(Dist.) +0	with the	+Ch4	
	2118 Briary Gelgod Bahase, 33	Of Orlan	St format hts Data being 10 2	27444 40	who have	+214*	
	110 Brown Codput Statutes: 14	01 0004	Jean Automation	2784 40	9434	+04	
	110 Broay Guppel Statute: 15	08 0.644	Line Constant and the second se	27mat +0	404	104	
	212) Benary Ouspud Balanen 19	OF Online	11 Line Approxime Matter	25mat +02	100	#01P	
	[10] Briels Colput Statute: 17	Of Orley	Status	.07mut edit	HC +(747	+04	
	THE Brown Corput Testuate: 18	Of Color	# free O Hanar O for Conser O Exercise	prine of	nfr indep	=(10 ⁺	
	[11] Brown Output Testure: 18	Off Online	Record	thus e0	NP (100	ndté	
	[110] Brivery Conjust Statuant 20	Of Online	R	diant add	40.00	4047	
	2110 Brease Calgori Daturet 21	OF Debut	App OK Dear	streat add	nd allow	+04	
	Thit Broary Christel Datures 22	OF Original	,549444511344 644.	the eff	40.00	909	
	111 Bries Culps Datum 21	OK Onios	1/10111134232 MR Tue	27md . +0	400 90	1000	
	111(Brian Colori Statuar: 24	04 0444	2/12011 \$4212.448 See	27mat +0	w +0#	-07	
story descents	The party Break Colors Statute: 22	04 Debe	2102019 (4022 AMA True	of west add	of sing	1000	-

Figure 76 shows the Control Relay Output status changed on SCADA Master.



mana .	- marriage	and with the Description of	-											· (2) Distinguist
	tion .	T Autor Taxa		T. Han	T make	T. Testers	T. Bast	T. Basia	T. thend	T. Sealer	T. Satar T	· Inscription ·		a statement of a local statement
	10.11	12 Provide \$1 Supply	11	04	(here	2-2010-0-00-00-000	(Treat	499	294	4799	0.000000000000000000000000000000000000			The second second second second
210	100.012	(C. Downe &t Inputs	182	04	Orline	21,00100.00010.000	(Distant)	104	1094	1000				and all strends
And an average of the second s	2745 415	(10 Tenating \$10 (reputer	39	08	Orden	215,0019 5.08 (8 and	(Distant	010	1044	000				And Distances
100	281.414	(10 Truste B1 Inputs	104	08	Oritine	27,0279 206 (8 864	(Cloud	610	der.	cre				
	281 815	(2,7mile \$1 top/s	10	08	O-free	21,1219 1-1418 244	27mat	-018	-010	-010				1.07
	281 816	10. Novine \$4 hours	10	08	Crime .	2/5/1010 5/M-10 AM	127404	010	1094	694				
	286.011	10 Division Bill Imparty	112	04	Ordere	An an and property.	Street	1014	1010	1094				
	281.416	(1) Tenden BE Inpuly	16	08	0.6w	2102010-00610-004	17 April 1	-04	1014	1010				
	281.478	10 Dating \$4 Papels	10	p#	Chiling	215/2018 \$26516-644	170 made	1014	200	1010				
	82.41.1	Collinery Subject Name	-	100	Citize 1	CONTRACTOR DATA AND AND	-	1. 1. 1.	127.7	1000			1.15	
	30.40	110 Briany Output State	1 mar	08	Othe	27.021630618.444	27444	019	:019	- deep				
	305.47	(11) Brwy Gupot Inst.	1 100	08	Ordere	2/5/2014 3:08:16 AM	Crew	674	674	4244				
	307.04	(10) Brwy Dated Sale	- F (ma)	08	Oder	21.0210.00810.444	. OTHER	4254	-014	-014				
	80.45	(10 Rowy Gripsi San	an 1	08	Odre	2/10/17/10/19 444	(Thui	-014	- 294	474				
	20145	(N) Brury Dopol Tax	4.000	.24	Drive	2-1,10-10 1,08-10 444	27%44	1214	1254	1274				
	20.47	(10) Brury Citized State	- T -	28	Orive	21,101010.0810.044	27964	1054	. 014	CHE				
	30.49	(14) Rewy Corput Net	1 m	24	0.0**	21,2719.108.19.444	27964	014	014	- 674				
	20.045	(10) Broary English Team	an(*	24	(interest	2-1,1219 1,28-16 244	27464	- 254	1264	200				
	202 410	110 Briary Corportion	- 10	20	Orbra	21,127111,0818,084	27964	1000	1014	204				
	82411	110 Bracy Colori Stre	11,000	24	0.0w	27,1277110818.844	27464	494	-094	-094				
	80.412	(15) Browy Dataset State	um 11	- 24	Drive	27,0710010414.00	areas.	1010	1044	(admit				
	202.419	255 Briege Dispet Set	- 11	- 24	() deter	UNCONCINENT AND	The state	-010	-019	-010				
	201.014	150 Brieg Dolput Det	en 14	104	0.0**	2,1,2216 0.0816.464	CONTRACT.	-04	.04	4244				
	80.015	(13) Rowy Dolped State	an 11	104	Ordere	1.1.001010.00.10.000	17Mod	424	424	4260				
	20.0 40	110 Brwy Solped Sale	- 0 m	-04	Other	21,0019 34221 444	10 March	-044	-264	-100				
	100 414	[11] Brony Dopul fam	-	-04	Dire	21,0210,0019,044	12 mad	-049	-048	-048				
	80.417	110 Brury Lingui from	11.000	08	(below)	27,00741.0816.444	12494	010	0.00	0.00				
	20.718	(10 Brary Dolpri Tok	- N	-24	Dates	21,001018-08-084	22464	424	294	1294				
	80.410	(10 Reary listed the	um, 19	24	Oview	21,000 10.08 18.084	27464	. 014	- 014					
	80.40	110 Really Gallery State	- 10		0.619	21,2010.000.00.000	11 Mart	014	- 254	634				
	80.410	(10) Browy Calgori State	- 11 1000		0.046	21,001010810.001	1044	104	-04	104				
	20.40	(15) Briefy Holped State	- 11 (10)	24	Ordere	A 1,00 YEAR OLD AND	(Theat	00	-04	-4764				
	80.453	(15) Binary Conjust State	11.000	- 24	0.0+	21,0010 108 10 AM	These of	494	-044	426				
	201404	(15) Birwy Dolput See	10.000	:08	Orive	3-1,0219 10819 AM	17mm	-014	-054	4294				
	NO NO NO NO NO NO NO NO	(10, Sover (10, Sover (10, Sover (10, Sover (10, Sover)	Todavi Toda Todavi Toda Todavi Toda	Tanland Theorem 22 Campool Theorem 27 Compool Theorem 29 Compool Theorem 29 Cold 207 always provide	Todayah Barkawan III — Diff Dangah Barkawan III — Diff Dangah Barkawan Jin — Diff Int of UKT dana pantika	Dopal Datum II DP 0.000 Dopal Datum II DP 0.000 Dopal Datum II DP 0.000 F // UP data path	Op/or Statum D Orbor L_101111011344 Stapho Statum D D Orbor L_11211101144 Stapho Statum D D Orbor L_11211101144 Stapho Statum JH D Orbor L_11211101144 Stapho Statum JH D Orbor L_11211101144 Status JH D Orbor L_11211101144 Status D Orbor L_11211101144 M	Digital Statuse: E DP Data \$1,1217 (1018) IAAA ETHous Digital Statuse: IP DP Data \$1,1217 (1018) IAAA ETHous Digital Statuse: IP DP Data \$1,1217 (1018) IAAA ETHous Digital Statuse: IP DP Data \$1,1217 (1018) IAAA ETHous U UT Assymptotic DP Data \$1,1217 (1018) IAAA ETHous	Digital Statuto (L) DP (Direc) (L) UTT (LR 10.44) (Timus) OPP Digital Statuto (L) DP (Direc) (L) UTT (LR 10.44) (Timus) OPP Digital Statuto (L) DP (Direc) L) UTT (LR 10.44) (Timus) OPP Digital Statuto (L) DP (Direc) L) UTT (LR 10.44) (Timus) OPP Virial Statuto (L) DP (Direc) L) UTT (LR 10.44) (Timus) OPP Virial Statuto (L) DP (Direc) L) UTT (LR 10.44) (Timus) OPP Virial Statuto (L) DP (Direc) L) UTT (LR 10.44) (Timus) OPP	Digital Dations: EL DP Outrow EXCLUTE TELE ANAL CPUIM OUTP OUTP Output OutP OutP	Digital Statute Diff Diff <thdif< th=""> Diff <thdiff< th=""></thdiff<></thdif<>	Digital Statute Diff Office ALTITUTE ANN Office OUT Other OUT Other OUT Other OUT OUT	Digital Bases ID DP Delaw L_LITITUEI BALL Thesis CPU CPU CPU Based Bases ID DP Delaw L_LITITUEI BALL Thesis CPU CPU	Digital Statement EC DF Defense L_LITITUE ELLAN Thread COVE COVE

Unsolicited Reporting

Unsolicited Reporting is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are reported to the SCADA Master. This notification can be seen on the Master Analyzer. Figure 77 shows an empty screen of the SCADA Master Analyzer before any unsolicited reporting.

Figure 77 Master Analyzer

integen +	** Antor JOPSIMSOV Res JOPSIMSON	T trust + 7 +
 2 The two testages 2 Core 2 Core 2 Core 2 Core 2 Core 2 Core 	2. 2. Imper instructure, Mark Johnson, Mark B. Stateling, Mark B. S. Stateling, Mark B.	Image: State
Annual Annual Contract		

Figure 78 shows that the binary input of the Slave is going to change. Initially the value of binary input is OFF.

Figure 78 Slave Registers

In the Wolfson		and the second se												· In contrast
7 7 - 1														
6 J 💭 🖉	and the second s	T Puter Type	1.1	when .	T Quality	T Townsong 1	in the state	T. Dente	T Channel	T beams	T Secto	 Description		- US 2618707
30.00	100.000	12 Decision for complexity		12	Course .	7.4.7.1.1.0.1.0.1.0.10.10.10.1	1000	100	1040	100				un literat
1.49 m		The second second second	- 11-	100		and the second second second	1000		1000					 B. MOREN
3 China	100.000	of the size of the local division of the loc		100	Course .	And the other states of the state	-	- 55	1000					
	10.40	of the size Bit has to		108	Colors .	5-5-Danie Bulleton And	allowed.	100	010	0.0				1.00
	785.410	100 Double By Institute			Centres	to the party is not been always	and a	1000	100	100				
	280,417	(1) Deside Bit Ingely		08	Centres	Schutzens Sales had been	thead	100	100	234				
	285, 414	101 Decisive Bit Installer		-08	Dates	Articipite Long 10 And	Citized.	dee	1010	634				
	100, 410	100 Disable St Insufer		1.00	Colora	Description Science And	(Cond	1040	100	630				
	80.01	193 Briats Thepart He	Realty 5	Ch.	Diline	271 2019 ILACTO AND	Tital	Chill .	iche	0.00				
	80.61	1101 Brown - Tally of the	1.1	11111	-	CONTRACTOR OF A DECK	1000	1000	1000	1.1			177	
	82.41	(14) Briany Dutynal Ba	Autor: 211	08	Drive	- Drugere bleine AW	1079404	1018	strep	0.0				
	80.14	1993 Briano Chalport Bri	Roman A	.08	Drifter	DIVIDENT DOE TO ANY.	privat.	1000	1010	100				
	90-19	(10) Wrises Codput Sta	Room 2	08	Drive	Distributes to be real week	(Charles	1010	104	674				
	80.00	(H) Brieg Dalpot In	Aug. 4	0.0	Dulton	Long and the lot was	127 Aust	014	0.00	4748				
	80.81	(18) drivery the part for	and the	129	Change .	21122010-2.08-10-200	(Close	1010	che .	104				
	82.19	URD Broarts Output Sta	num: 4	-19	Dreim	2/1/2717 100010 AM	The	1014	019	04				
	80.49	(18) Browy Clubpor Inc	1 mar.	108	Contrar 1	2112010-0.08-08-044	107 March	1010	scher .	atter .				
	80.010	(H) dowy Culput In	nue 11	128	Diving	L/1/2010 1 00:00 00 000	271444	che .	0.0	0.00				
	80.011	1918 Breatly Cholgenti Ba	furmi 11	1.4	Doore .	Locates and ready	Cheve	010	date -	624				
	80.412	110 Broay Colput De	Aureni 12	14	Drive	2/1/10110 DIRE TO ANA	2744	104	1044	det				
	80.410	110 Break Dalper In	Aure, 11.	14	Date:	D'AVERTE S DE TR ANA	27444	010	sites -	474				
	80.416	(195 Broad Dalary In	Apres 14	- 04	200m	any store him reads	(Cites)	1014	1010	424				
	80.810	(10) Rivers Tarlport Tor	Append 18	- 29	price .	2-1/12/19 1/18/19 AM	Stand	270	674	434				
	80.00	(10) Rowy Turbul No.	6 mm	- 14	Drive	21/071934227.44	1744	4040	-010	474				
	85.810	(10) Rivery Delpait In	Rame: 18	1.0	Debe.	2/1/22110.1.04(10).444	27414	1010	1010	-04				
	Bill at th	(10 Kney Dalpel Dr	ine 11	-14	inter .	27/3710103.08164444	27444	1014	1010	454				
	81.110	10 knew Sulpar In	nim: 18	- 14	2004	2/1/2010 5:08:08.484	27444	1254	1014	0.0				
	80.000	(14) Brops Todper In	tione 14	104	2004	27/02/04 2:08:02.444	Plant	010	0.0	04				
	80.405	140 Brown Colput Da	Profile (10	114	Drine	17/0111101010-M	27418	04	09	04				
	80.831	(19) Brees Dalard Its	11 ment	14	2004	Location and in And	The	104	104	494				
	80.40	110 Knew Dalpat Na	Acres 22	100	2mire	Logard Selecter	274vd	104	1000	104				
	80.40	170 Rows Today's In	August 21	100	Date	27,0216 248,16 344	2744	104	1010	474				
	80 414	110 Rows Delpar In	Aure 14	1H	1000	DURING FOR 14 AND	27444	0.00	010	00				
	based where	* Destaures 107 of 107 of											0	

Figure 79 shows the binary input of the Slave is changed from **OFF** to **ON**.

Figure	79	Change	in	Slave	Reg	ister	Value

	4 1 () of a state	114	Infant 2.8.1
· In the Workspace	Dags volume hands and also i have to group by the statement		+ 12 Distingt
- 10.00	Name Y Paint Type Y Three Y Description Dit 01 01 04 044 1 Discription Discription Discription Discription Dit 01 01 044 0444 Discription Discription Discription Discription 01 0444 0444 Discription Discription Discription	τ	
1000	PR PD PD OH OH OH PD OH PD OH PD OH PD PD<		i ee
	DB (P) D (Dark H) span D Original 2 (2)(11)(10)(10)(40) D'mel 2 0/0" 2 0/0" DB (P) D (Dark H) span B OP Original 1 (2)(11)(10)(10)(40) D'mel 2 0/0" 2 0/0" DB (P) D (Dark H) span B OP Original 1 (2)(11)(10)(10)(40) D'mel 2 0/0" 2 0/0" DB (P) D (Dark H) span B OP Original D'mel 2 0/0" D'mel D'mel DB (P) D (Dark H) span B OP Original D'mel		
	Dist Dist <thdis< th=""> Dist <thdist< th=""> Di</thdist<></thdis<>		
	NU Pr Philomy Departments DB Data DUITY 1001 1001 1011 1001 DBM dDM dDM DDM NU Pr Philomy Depart Streams 0 Data DUITY 1001 1001 DBM dDM dDM DBM NU Pr Philomy Depart Streams 0 Data DUITY 1001 1001 DBM dDM dDM NU Pr Philomy Depart Streams 0 Data DUITY 1001 1001 DBM dDM DBM		
	B1 04 Utilizery Data Name 8 D0 Doller Utilizery Data 0 D00		
	N1 01 UE lawy block blockst 11 Die Scient L/L011101010101 Dies D/L011101010101 Dies D/L011101010101 Dies Die D/L0111010101010101 Dies D/L0111010101010101 Dies Die Die Die Dies L/L0111010101010101001 Dies Die Die Die Die Die Die Die Die Die L01111010100100000 Die Die <t< td=""><td></td><td></td></t<>		
	B1 FM Difference And Annual (M. 1996) B1 FM HTER Recognition (M. 1996) Difference And Annual (M. 1996) Difference Annual (M. 1996) Difference Annual (M. 1996) Difference Annual (M. 1996) B1 FM HTER Recognition (M. 1996) Difference Annual (M. 1996) Difference Annual (M. 1996) Difference Annual (M. 1996) B1 FM HTER Recognition (M. 1996) Difference Annual (M. 1996) Difference Annual (M. 1996) Difference Annual (M. 1996)		
	ID 714 FEB Dary Soluti Stream 10 DP Delay LUTE ULU AD DPD DOP DOP DOP DOP R1 01 HE Dary Soluti Stream 11 DP DElay LUTE ULU AD 40 DTmo DOP DOP R1 01 HE Dary Soluti Stream 11 DP Dots LUTE ULU AD 40 DTmo DOP DOP R1 01 HE Dary Soluti Stream 11 DP Dots LUTE ULU AD 40 DTmo DOP DOP R1 01 HE Dary Soluti Stream 11 DP Dots LUTE ULU AD 40 DTmo DOP DOP		
	B1 01 Hit Deep Stand Steams II DF Deep LUTE LISE 44 DF DF DF DF B1 01 Hit Deep Stand Steams II DF Deep LUTE LISE 444 DF DF DF DF B1 01 Hit Deep Stand Steams II DF DE DE <td></td> <td></td>		
	B1 42 Hitkey Data Name 11 DB Delay EVENT HIT B1 B4 Delay DP DP B1 43 Hitkey Data Name 11 DB Data EVENT HIT B1 B4 Dmail DP DP B1 44 Hitkey Data Name 11 DB Data EVENT HIT B1 B4 Dmail DP DP B1 44 Hitkey Data Name 21 DB Delay EVENT HIT B1 B4 Dmail DP DP	-	
Surger Second	Salest Han + Deploying (20 of 30" data junct		Service Industrialized

Figure 80 show the Unsolicited Reporting on the analyzer. The value of Binary Inputs is changed and the same is notified to the Master.

Figure 80 Master Analyzer after Change in Register Value



SCADA Gateway

Protocols Validated

The protocols we have validated for this release are DNP3 and DNP3 IP.

Flow Diagram



Figure 81 DNP3-to-DNP3 IP Protocol Translation Control Flow

As shown in Figure 81, the DTM Master can read and write the Slave via the DA Gateway using protocol translation. The Slave can send the Unsolicited Reporting to the Master via the DA Gateway using protocol translation.

IR807 DA SCADA Gateway Configuration

As per the topology, the interface connected to SCADA Slave has the following configuration:

```
interface Async1
no ip address
encapsulation scada
!
line 4
databits 8
stopbits 1
speed 9600
parity none
!
scada-gw protocol dnp3-serial
channel dnp3 ch1
 link-addr source 4
 bind-to-interface Async1
session dnp3_session1
  attach-to-channel dnp3_ch1
scada-gw protocol dnp3-ip
channel dnp3ip_ch1
  tcp-connection local-port 21000 remote-ip any
 session dnp3ip_session1
  attach-to-channel dnp3ip_ch1
  link-addr source 4
  map-to-session dnp3 session1
scada-gw enable
```

IR1101 DA SCADA Gateway Configuration

As per the topology, the interface connected to SCADA Slave has the following configuration:

```
interface Async0/2/0
no ip address
encapsulation scada
1
line 0/2/0
databits 8
stopbits 1
speed 9600
parity none
I.
scada-gw protocol dnp3-serial
channel dnp3 ch1
 link-addr source 4
 bind-to-interface Async0/2/0
session dnp3 session1
 attach-to-channel dnp3_ch1
scada-gw protocol dnp3-ip
channel dnp3ip ch1
 tcp-connection local-port 21000 remote-ip any
session dnp3ip_session1
 attach-to-channel dnp3ip ch1
 link-addr source 4
  map-to-session dnp3 session1
scada-gw enable
```

SCADA Master Configuration

As per the topology, the SCADA Master is residing in the Control Center. The following configuration is required in order for the SCADA Master to communicate with SCADA Slave:

- 1. Open the SCADA Master Application and click Add a new DNP3 Master.
- 2. From the Channel tab, configure the SCADA Master as per Figure 82.
- 3. SCADA Master (in this case configured as TCP Client), interacts with the SCADA Slave, which is configured to act as a TCP Server.
- 4. Populate the remote address field with the Loopback IP of Cellular Gateway.
- 5. Populate the port with 21000, which is the port used in Cisco IOS Configuration.

Figure 82 Master Configuration

DNP3 Master Co	onfiguration					-		×
Device Channel S	Session Advanced	Multiple Devices						
Channel Name mD	NP							
Behavior								
⊖ All ® Mas	ter O Monitor	O Peer O Slave	O Unknown					
Connection Type								
O Serial ®(10)	P/IP O TCP/IP and	I UDP						
Mode	0.003							
Client) Server							
Local Address	172.16.107.11 - D-L	ink DU8-1312/1332	US83.0 to Giga	bit Ethernet Adapt	ter#2		_	
Remote Address	192.168.150.42							
Port	21,000							-
						OK	0	incel

SCADA Slave Configuration

As per the topology, the SCADA Slave is residing in the field area. The following configuration must be required for the SCADA Slave to communicate with SCADA Master. In this implementation, we used SCADA DTMW simulator instead of a real SCADA device.

- 1. Open the SCADA Slave Application and click Add a new DNP3 Slave.
- 2. From the Channel tab, configure the SCADA Master, as per Figure 83.
- 3. On the SCADA Slave, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration.

Figure 83 Slave Configuration

Del Coleman Della ener	_ 0 X	(NP1D-Annal Configuration		18x
Desce Chevel Senson Database Advanced Multipe Deven		Dever Channel Second	Delature Albertal Multiple Devices	
Channel Name (2007		10 A2		D
angele .		Munetar	298	*
1 Al C Matter II Martin C Feet . Dave II Literate		ReframeTanienut	10000	
Connection Type		A Block	DiCommon Selathroperies	
 Selial (0) TONP (0) TONP and VDP 		Basiliate	9603	
Conscilut Propriet		FeetChaWet	8	
Sena Puri COM14	*	NorChaforedate	eredia: 4	
Baul Rate 1900	(14)	NumCatable	870.8	1.87
		Number	(am) (
		Party	NOV	
		PortDTRMvde	INALS	
		PuriMode	ACME	
		Portfoare	CSM14	
		Pertf23Made	Children and Child	1.0
		System Frequency	40	
		= 10	OTCommon/DNPLOWP11CPProperties	
		Wignercline	2048	
		Munctur.	21/	
		Sector Specify the properties for CMPS of	ent a serie convertion	
Myset (2015) Dense Profile	OK Canal	Import (Part) (many Profile		DE Careel

SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Unsolicited Reporting is sent to the Master from the Slave. Figure 84 and Figure 85 show the Poll operation from the SCADA Master. Control and Unsolicited Reporting can also be seen on the Master Analyzer logs.

Poll

The Poll operation is performed by the Master, which can execute a general Poll in which all the register values are read and sent to the Master. In Figure 84 and Figure 85, we see a general Poll executed on the Master side.

As Figure 84 shows, the Master Analyzer is initially empty.





However, when the General Interrogation command is executed, the values of all the registers are displayed on the Master Analyzer, as shown in Figure 85.

Figure 85 Master Analyzer Logs after Poll Operation

Application Traffic Communication Enablement

Image: Control for the interminant of t		Analyse - Initial - Children Child		· tereste	
	ACTOR AND	1.1 1.0 <th>Image: District State Image: District State Image: District State Image: District State<th>Image: Second Secon</th><th>VED16 (manual rs. 15 and 20</th></th>	Image: District State Image: District State Image: District State Image: District State <th>Image: Second Secon</th> <th>VED16 (manual rs. 15 and 20</th>	Image: Second Secon	VED16 (manual rs. 15 and 20

Control

The Control operation basically sends the control command from the SCADA Master to SCADA Slave for the purpose of controlling the operation of end devices. The control command can be executed, and the results can be seen on the analyzer. The value of Control Relay Output is changed and the same is notified to the Master. Figure 86 shows the control relay output status before sending the control command to the Slave.

and all the second s		and the second s															 A Televille
· B pret Ministers	Degree to	the set that I have a proof	-														· IB Distanti
1.1.00	-	T Balat Type	1.4	T No.	T. Solly	T. Tenestery	٣	these.	7.9	inter .	T. Owned	T. beating	Τ.	Sector .	τ.	Bearing the second	 * · · · · · · · · · · · · · · · · · · ·
and the second	281.410	[1] Sinute \$3 Paints	10	100	Chine .	Litzbre num in ee		1Phone		10	0.0	1019					
· 11	281,411	10 Disable Bit Specie	11	104	Ditte .	L/1,2014 1100 10 44	6	(These	0	-	(Chill)	OW					· D Delaw
200	181.412	10 Station be synche	10	100	- Drive	Artune to see to Ar	4	12746-0	-0	10	04	010					Name OF STREET
deller.	190.012	101 Distantion for singular	11	10	2014	LYND YF DIR LO AN	w	[Tried	10	10	1014	104					1.00
	281.010	(1) Smith St. Synde	10	10	Chie	LINCOME DURING AN	M	(Third)	10	10	1014	1014					
	28,411	10 Deadline All Importe	- 11	100	0444	LOUGHLE DOM: N AN	4	1794-0		10	1014	1010					
	28, 101	(1) Deaths \$1 inputs		100	0.00	And the second s	4	(Division)	0	10	0.0	010					
	28,417	(1) Smalle Relayory	100	100	0.04	Arturnet book to At	6 - C	27144	0	10	1010	de					
	28,414	(1) Description and Ampunda	10	104	0464	Lotuble basis as	w	1274 cold		10	1014	1010					
	28,101	(3) Souther Bd Impoly	38	100	1244	property and the second	H	Division.	10	10	1044	1010					
	80.40	111) Briefy Durpol Stat	tone it	- 10	0.00	Disconte si adoit es	н	Different.	- 40	ALC: NO	1040	1040					
	B1811	1942 Brown Distant No.		- 10		Louis reasons	11	The second									4 J
	80.45	118 Biney Dulpet Sel	1.000	10+	2014	DATE STORE A	W	[Pitest	-0	10	1048	1018					
	82.41	1115 Binary Chalped Sta	first \$.	100	Online	Litrarie Sole of A	6	(Crew)	-	100	100	439					
	80.99	110 Kiney Chipat Sta	1. 1. mar	108	Online	Art Jon's Lot of A	6	(Trine)	10	10	404	4240					
	80.45	1713 Knory Curput Sal	tions 1	108	(Drive	1/1/2010 0.08-18 AA		(Trease)		60	1010	404					
	80.44	100 Kiney Guiput Set	6 mar 6	ile -	Online	1/1/10/10 14 14 14 14	4	Different.	-0	10	100	0.0					
	80.47	(HL Brang Corport Tee	t 7	104	Online	DOUGDING SUDA OF AN	15	[779-baad	-	10	-CHP	010					
	80.46	(10) Brien Culput Set	tione it	-0#	Online	21122216 108-18-44	6	District	ø	10	0.0	010					
	80.49	(14) Breely Challent Sile	1. mil	- 104	Online	LINCOME STREET AN	10	[Thead	0	10	0.0	1019					
	80.410	(11) Broary Durpolt Star	tenii. 12	100	Onlow	211/3010 5.08-10 AV	M	[25-lend	10	40-	1010	1010					
	#0-#11	1915 Briary Ourgoal Stat	ture: 11	-08	Online .	21122210-0.08-10-34		[29 back	0	10	040	048					
	80.412	1995 Binary Gutput Stat	Autor 12	100	Only	17120778 S-0818 A	4	E7thed	- 0	10	0.9	6340					
	82.410	170 Bonary Dutjina Sta	kam-10	10	Oniver	JYLDDTP SOL IS AN	4	Dired.	-	10	100	610					
	82 F16	(70) Brieg Oxford Sea	kemi 18	08	Online	DIVISION CORTE AN	e .	D7Hout	10	10	1000	1010					
	80.419	1111 Briefy Culput Sul	11 mea	08	0.000	DIVIDITIVA NOR TRAA	w.	Offense.	10	10	1000	1240					
	80.8%	371 Browy Output Sal	ture: 16	UR	2004	L'USER SHERA	н.	00408	- 67	10	1014	674					
	80.417	1993 Brown Chatjest Stat	ham: 17	100	0.04	UTURN MARK A	w	CTNet.	10	MP	1010	010					
	80.418	(10) Blony Output Hat	ten 18	18	0me	Arrysone Loss in as		Distant.	-	100	100	100					
	80.418	110) Briary Chargest Stat	ten: 18	108	(Dese	411/10/10 10:00 10:00	6	(Think)	0	10	010	010					
	82.000	110 Array Output Set	11 1994	100	2014	LINCOME AND A MARKED AN	M	(Titud		10	0.0	010					
	80.401	1110 Broary Curgest San	14, 1994	100	0444	LONDONE SHE IF AN	u .	(711.4	0	10	010	dee					
	80.462	111) Briany Durjeut San	10,000	100	-2464	Lytypere see in Ar	w	(Print)	10	10	018	1049					
	80.000	(19) Bring Dutput Sa	10,000	108	-0464	31110010 014 18 AA	4	(Treed	0	10	010	010					•
And Andrews	family have 1	Distances (10) of (20) in	da pieres														 I have be achieved

Figure 86 Slave Register before Control Operation

Figure 87 shows how the SCADA Master sends the control command.

103

Figure 87 Master Control Operation

		and stated in the										
. Can the sector	particular and an unit of the little	and the second se					_				- Contractor	
* [] =000	Print of the Party	and the second second	Million of	A Design of the local diversion of the local	in Decision of the	يستثنه		100	-	ACC PROPERTY AND INCOME.	• • • • • • • • • • • • • • • • • • •	li prem
· 102-000	23,25spe for reputs	00	1004	3,71,02710 0.00,32 840		be .	(friend	+04	+04	-day	4 😜 (hr/12)**	ie (
10+00	119 Newsy Datest Transmit	104	Criter.	2/12/14 610/12 464		1.4	(Distant)	100	100	+09	1.44	
	1910 Broary Dorteut Instance: 1	De-	Crake	2/10/10 01215 244		See .	(Press)	100	1000	+(h4)		
	210 Review Designal Mathematics 1	De .	(rme	Arr.2014.01215-004		Tran .	(Print)	-cas	+040	0.090		
	111 Rivers Dutant Statute: 4	0.0	(one			then in	itteet .	+048	+04	100		
	210 Mary Dubul Subury 3	104	Critica -	(B) constraints (Section of Section		- E	OTHER.	+04	+Chill	w(hsh		
	270 Revery Dulant Televen: 4	-Ore	0.04	Name Connor heigt forgot this is			(Trees	100	+date#	w2NF		
	(15) New Yorked Statuse, 7	08	Other	Description The second design size augment to	mark purposed construct paint advanta for involtante status		(Chest	+010	+076	+010	10	
	275 Brian Culture Damase: 3	OW .	Crime	position the same message but a	al points are two required to therapy at the serve		10-inut	+04	+019	+010		
	110 House Output Datum: #	.04	Debe	500		- 1	(Theat	104	+018	+09		
	219 Revery Duraut Statuter 18	-04	Orderer.	these limits	A Design of the local data and	-	Other.	100	+018	+(34)	20	
	210 Brons Column Dataset 11	08	0.04	Canad Advancement		_	(Theat	+010	+04	a(34)		
	[15] Revery Duraul Humani 12	0.0	Color.	Road Number: T :		18	17464		+04			
	2113 Hours (Sulput Statum, 1)	04	(ning	Complete Augusta		1.0	Triest	worke	+04	01707		
	110 Intern Desput Statutes: 14	104	Coles-	Data Do Terra VIII		14	(Theat	100	+010	acted		
	170 Binary Dutavi Staturari 13	08	Orither				(mean)	+040	+04	10M		
	218 Breary Dodged Statucer, 18	- 24	Orient	Probability 1	Deep Ballyer Sending 100-	- 8	the.	-edate	+1767	+194		
	210 Brone Dulant Hulum: 17	08	Online	Secret Automotion		- 1	(Creak)	+048	+04	+04		
	210 Newsy During Testione: 10	0.0	2444	The barrier black			(These	100	+018	+04		
	210 Novy Duty of Summer 18	104	0.04	al sur opposed into		-	1244	-	+010	4199		
	213 Rows Dulped Tomani, 23	104	(rine -	Seener			(These	1000	+04	+(74)		
	210 Rivery Dotext Statuter 21	0.0	United.	here	Arcenter C. Presser		(Trins)	-scat	+049	4000		
	110 Imars Dulgot Tomari, 32	04	(energia	1000 1000	1.0.11110		These .	worke	+04	404		
	110 Imary Donaut Business 21	200	0.04			_	(Trank	with P	+076	adap		
	1773 Warry Dorput Statures: 24	0#	0.944			and a	United .	+014	104	109		
	[210] Binary Dutyout Stationer, 21	0e	Grane	Another and the same		thus:	(Division)	000	+1742	100		
	110 Brown Culput Bullant 24	-per	Ortice	2/1/2018 0 1215 488		but -	(Change)	+040	+04	+010		
	110 Search Dulphi Stationer, 27	1.04	2-lite	51001641010.000		24	diam'r.	100	+010	+010		
	215 Imary Dutical Induse: 38	104	(cone)	2/12/11/01/01/01/01		Bue	17 March	-	+04	with the second		
111-11 11	111 Revery Dutput Passare	08	(Intere	Andrew and the AM		the .	(Trees	acted.	+010	0090	1.1	

Figure 88 shows the Control Relay Output status changed on the SCADA Master.

Figure 88 Slave Register after Control Operation

· · · · · · · · · · · · · · · · · · ·	The subscripts for	a selling i have a second	Ind stores											 · I of a fail framester
S S	Anna A	Anise Trees		in testam	T. Salar	T. Deseiner		T. Sain	T. Owner	T. Income	T		Barristen .	-
·	and the second second		1000		1.1.1.1.1				1 1 1 1 1 1	1.000	100		10000	 · · · · · · · · · · · · · · · · · · ·
· 10 000	100,000	OC Disates Bit Inputy		- C	-	17-12-10 10 10 10 AND	Distant.	1049	100	100				in these
		10 Danie II Supply	100	- Circler	1000	2122210 2122 20 444	(Prove	-						A Discouting
1 LAP		COLUMN STREET	1.0	100		And the second second second	Contract of	0.00						1.00
and the second s	Con sta	of the state of the state			1000	And there was in the	Contract of	100	100	100				1.00
	10.00	of Design St. Lands	12-	1210	-	ALC: NOTE & AND ADD	(Trees	100	424	494				
	100.000	In Design St Insult	12-	1.0		And inclusion in the state	(Colors	100	474	100				
	100,000	or light in here	10	12 -	Date:	And other the state of the	Other	100	100	404				1. Contract (1997)
	test wire	Of Disable Bit Issues:	1.0	1.0	Date	And address in case of a data	Division	1040	454	414				11
	2002.000	10 Daultin Bit Papelly		- 10	Date:	processing them by start	Distant.	1040	454	100				
	10040	110 Broay Dutyou Dates		04	Color I	Discourse is about one	Distant	1040	100	610				
	00.00	THE REAL PROPERTY.		11		Lines and the second second	1.1	1.1	100 PM	-		14		 14 C
	80.40	110 Brieg Dalast Bala	an 1 .	1.04	(Delow)	LAUGHTER DE LE LE LAN	17Had	-018	400	434	_			6 A
	80.81	112 None fidad Into	- 1	-14	dolore -	DIVISION NOT NOT AN	(free)	100	420	614				
	10.00	(1) Bries Dutylet Hans		104	doning .	LOUGHTE NAME OF ANY	OTHER	010	010	cite				
	80.45	(15) Browy Dubpat Steam	- 1 -	08	Driver .	LYS/SPIRE KARA IN AM	(D)-load	010	0.0	00				
	80.86	(1) Rosey Dulpal Pater	- 1	100	Otive	Employme Excluder Adar	[PHud	210	650	458				
	80.41	(10) Novey Dubpar Steam	- 1 -	08	Drive .	Synchrone Automatical	(Phine)	4768	010	400				
	80.46	(10) Broary Dubyot Data	- 1	08	Other	Division from the second	[DHud	0.0	49.0	-216				
	80.49	[10] Browy Dated Terro	- +	04	Drive	2/1/22/10 1/16 10 444	Distant	0.0	124	014				
	80.410	[10] Breen Output Status	- 11	08	Colve	1/1/2010 1/18 10 444	10Mad	1010	610	1010				
	80.417	102 Brwy Output Italia	an: 11	01	Drive .	311/2019 5.0818 AM	[294ed	1010	100	100				
	80.412	112 Brury Output Status	- 17	.08	Chilw.	Distriction is not in Add	Direct	049	-04	-04				
	80.413	10 Bridy Output Status	en 11	.08	Door .	21122010 LIVE 10 AM	[27+land	610	634	654				
	80.916	112 Every Dutyout Toma	- 14	.08	Draine	2112010 EBR 18 AMP	[27Hand	1000	424	474				
	30.413	113 Briefy Output 2000	- 11	-04	-Driver	21120193.0E18 AM	011404	10MP	654	694				
	80 am	112 Broats Dulped Status	- 10	08	Deleter	211/2010/10/10 10:444	DD4ust	1214	104	694				
	ALC: AVE	[10] Brony Dutyor States	m: 11	100	Detter	TATING THE R WE	CD4set	104	04	- 254				
	80.016	[1] Borry Dated Talls	- 11	108	Dette	21122010-0.0410-000	1711est	404	454	454				
	80.010	112 Briary Dutput Ballia	a. 18	.08	Dete	L'UTITIT CHE 18 AM	1716.0	1040	0.0	00				
	81.412	[10] Briwy Dutyou India	- 2	.04	2014	LAVES AND AND AND	1774-04	1040	0.0	00				
	80.401	110 Brury Oxford Tally	m 27	104	(Date of the local date of the	SPT/2014 STREED AND	27944	1040	414	010				
	10.00	[17] Rowy Dulged Sales	- 11	100	(inter-	211200000448	(Press)	404	474	494				
	80.801	175 Rows Dutyot Sala	- 24	.08	2008	STUDIE DUB TE AM	(THue)	1010	424	-010				-1

Unsolicited Reporting

Unsolicited Reporting is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register changes are notified to the SCADA Master. This notification can be seen on the Master Analyzer. Figure 89 shows an empty screen of the SCADA Master Analyzer before any unsolicited reporting.

Figure 89 Master Analyzer

Artiget + #	A house sold and and	an addredenter	8 texts = 8
· COL COL - See Manager	an entre and and	the below and the second statements of the statement second statement.	n generali (a.) a (@ Daharan
	21100-14,000 vere admp	front inquest is gover busile monthring	The second secon
· 10.00	11/44/12,000/ 1044 ADD 11/46/12,000/ 11/46/12,000/	Appliating Research Shakke Unschlidted Research P and P and P and P and P and P	See 16 day
	11.00.11.000. AND ADD -	100.100-103.42121000 - 010 frammate 20 hptss	Design of the second se
· Contraction	11,46,11,000,	Applicative America Response PAALE FREID THEORY HERE & of 6.5.2 (10.11) THEORY HERE &	I de la constante de la consta
1 M 1	22/00/22.005 1111 4000	Frittens despress to report! Boatla Disclipited	State Mark
	11/06/11.00): 1000 a000	Wills (WS) Weeneye: Mastle Sumilysreed	- Designer
	22144-22.481	To Dejean distingue Detail, vertation 3. qualified bolkiall delater	C Pressor
	22140-22.001	To believe distance betal, veriation 5, mediation bability, meaner	Seraine
	881 440 23. 00 to	To Depart Million Botal, Secondarias & monistics Subbudil Science	of State
	LUMBER OF STREET, NAME ADDR.	Insert Inquiet 10 groups Mighla Westligted	
	11.46.11.401. 11.40.11.401. 11.40.11.401.	Apploation Reader, Budder Thislipsteid Rearrys Finite Thisis (Barde Barde Barde T of a 2 and 2 and 1 and 1 and 1 a	
	121-00-11,0001 ### w000 -	101.108.000.42.01070 - 010 Linnesth 28 hptss	3 term
	11140-11,0000> almi 11140-11,0000 11100-11,0000	Appliancia Massar, Anaponen PARIS Freil (Massar, Massar) A File D (M)	2 Street
	22140.23.000.1112.4002	Privat Suppose he engent: Budia Sterissian	
	\$1,46,22,403;	Paild (MDY Massage: Rodbin Stationited	
	22240122.0611	to object distance behave repetition is goalitier technolit evident	
	33144.35.001	To this of the and the and the second of the second second	
	22144032.0011	to payore disting betal, veriation & guarries butting animal	
	storest mail over all	Innet segment in general Robbin Marklatikan	
	11.44.12.40.1 11.44.12.400 11.44.12.400	Application Header, Analia Franticited Heaneges Finity provid (Heaving Wead) Adam 4 of 1.6 to 5 of the two in the fid	
	31.44.12.000 ### w200 -	192.]48.125.42.21050 - 959 Kranameth 28 byfew	
	11144:12.000	Application Measure, Despenses Place Place (Measure Measure Measure Measure) and 6.0 km cm	
Annual Annual	·	Roomand desponse to regions() Roadia (too)liited	

Figure 90 shows the binary input of the Slave that is going to change. Initially the value of binary input is OFF.

Figure 90 Slave Registers

														a contraction
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Finite	T Paint Type	1.	T these	T Builty	T Treatury	T. Head	T Series	T. thank	T Sentire 1	T Setter T	Description	1.1	· SE INCOMENTATION
3 4 414	28,10	CONTRACTOR DE L'ANNE			()-true	21,001010.0818.044	(Property)	1000	-054	1004				a long
1.14.9	28,411	Clinica Mitaulo		19	0.0+e	37,0010.000.00.000	[[Dist	- 04	104	104				· · ·
10100	28.75	10 Invalid Bit Inpuls		24	0.0-е	3-1,0078 10818 AM	(These	04	-014	1044				
A	28,10	(Cloude Bringel)		- 24	Other	27,0710,0818,004	(These	-04	-014	124				100
	28,414	(Cloain bringets	1.18	-28	Ordere	21,2210,200,00.00	Title	-010	-054	-010				
	28, 115	(Closelin Brillion)	- 11	- 04	(bite	21,0010108-08.444	. 17 Mart	1.004	1.094	1004				
	281.816	10 Distantia del Argonte	- 14	- 104	Odre .	21,2210,000,08,444	10 mat	-048	-048	-014				
	281, 812	20 Doutto del Inputo	11	-04	Odw	21,2210,000,00444	10 kind	104	1000	1000				
	28,10	(2) Double Britsmann	. M.	- 24	Odre	21,0010.0010.001	27464	104	104	274				
	28,809	(Closed Street,	. 34	24	line .	21,0010308-00344	27464	-016	4244	1284				
	20.40	141 Broady Fistered Tes	Autor B	- 04	(Indexe	3-520H4 5-422H Mel	37 No.4	1000	1000	1000	1.0			
	10.000	110 Avera States & Bo				a Contra de Sectión des			1000	1000	1. Sec. 1. Sec			
	80.42	110 Brwy Tolynt Be	from 2		Oder	STATET TANK AN	and.	1404	0.0	0.0				
	20.41	[10] Berny Todayi Sa	- 1 m	24	Orite	27,0010 53819 364	27464	100	100	-079				
	20.44	(18) Knory Colpet No.	1. A 1995	- 24	Chiling	21,000,000,000	Street.	-010	424	424				
	B1 49	(15) Brony Dated Str.	num 1	- 24	064	21,0010.00618.888	1044	1000	1074	1014				
	80.46	(10) Reary Colput To	Arrest St.	100	Grine	2100103021544	0044	010	-040	210				
	80.47	(10) Brwy Dolpal Ter	6 m 7	08	Orline	21,02103.0618.864	(Dave)	010	010	010				
	80.48	(10) Brwy Dalast To	n	-08	Drive	27,0219 5 0818 844	27464	-016	-010	0.0				
	80.49	(10) Shary Dalard Sa	h.in 1	28	Online	24/0016 SARIE and	27464	-024	-010	-294				
	80.010	(10) Smarty Clubbert Sta	Autor: 10	OF.	O-low	2.5.2519 S.M.18 AM	10 March	1010	1014	1014				
	80.415	(10) Broaty Distant The	from 11	-04	O-free	21.7019 LOB 14 AM	STreet	1018	-014	-010				
	80 #12	[51] Brwy Dalpat the	from 17	Of .	Ofer	215/2018 LOE 18 AM	17 March	04	1010	04				
	80 #10	THE Brury Duty of the	Anno 12	08	Griew	71/2018 FOR JAN	17 Mpril	014	04	04				
	80.414	110 Mary Dulput Te	Aven 14	04	Orice	210,0279 308:09 AM	. Unwood	04	CHP	674				
	80.412	110 Brany Output the	nyani 15	08	Orive	2/1/0514 3 08:14 AM	(Press)	- 674	674	574				
	80.418	110 Brwy Output Na	fami: 15	08	0-the	2/1/2010 1/06/18 AM	2044	014	494	439				
	80 417	(15) Reary Gripor Se	Autor 11	08	Outra	2/12/19/12/19 14	(Third	010	4244	474				
	80.418	140 Ready Disput Ter	ner: 18	- 24	0.0w	21,0219 (2019) 444	27mul	494	- 674	474				
	80.410	210 Brury Galjor Ite	nos: 15	28	Oriva	21,12111128-18.001	27464	1014	204	010				
	82.405	110 Bracy Color Str	Renti 22	24	Drive	21,2211 1,18 18 18	27964	494	- 2010	010				
	80.401	(11) New Yorker Str.	Parm (11	14.	0.0w	2/2010/2010 144	27464	014	1010	-094				
	80.412	196 Brieg Dated the	ten 11	24	Odre .	27,0710.0003.000	and a	1010	1010	1.010				
	201403	110 Newsy Darpet the	free 11	24	Odre 1	21/2219 01010 AM	- 27 March	-019	-020	1424				
Freinigen Brennen	Select time.	 Implaying Def of Def a 	and partic										1	Instance Subgly Prints





and the second se	111111111	0.000							_			_		_						National V X A
· Jan · Jan	The party of the	The process leads of the Lines of process lines of the Control of												A US STALAMOUNT						
	New 7	F Anice Type T	4.1	Solue'	17.44	aby 1 T	Tenters	T.C. Not	·	Sector 1	TOM	- C	T. Inteles	17.	Sector.	- T	Description		7 7 4 8	· CON DESIGNATION ADDRESS OF ADDRESS
	10.412	Difference del mando		100	0.0		And show the second second	-		100	-		00							
	181, 911	(Climited &I frank)	10.	10	0.0		deligence from the same	2744		date .	01		1014							 B minute
	120.00	10 Dayler \$1 Paints	10	100	04		Arrighter State of Ada	and the second		100	04		1004							Marco de Prises
	200, 112	III Double #1 Facult	10	100	04	10	3.11.11.11.11.11.11.11.11.11.11.11.11.11	2744		date	100		104							104
	10.114	(Closelin #1 ran/s	34	10	04	-	2-12010 1000-0 Me	2744		dee	0.0		104							
	281, 410	IC Toolin #1 Family	10	10	-Cre		Anima page 4	2744		delle	124		1010							
	100, 110	(15 Daylor & Lynch)		1.00	- 04		property house in sec	2744		-210	- 674		-010							
	286, 417	(Climits \$1 byot)	н.	100	- 04		2 hourse house he was	2754		1000	100		-04							
	281, +14	(2) Despite \$10 Paints	14	.10	04		21,000 1000 1000	2764		1214	104		104							
	200, 101	(Clinics Million)	38	100			21,21113.0016.00	2744		1014	104		104							
	80.40	110 Broay Dated Dates	68.1	.04	-04		Drivere \$49.21 Me	27404		1040	104		104			_		_		
	81.11	110 Brang Brager Ration		0.12			100000101000000000000000000000000000000	4 (27)web												
	an ar	[11] Brian Dalph Salues	e4	100		*	Score man e	4 274-4		450	100		100							
	80.41	117 Kiney Culjud Station	et	100	04		Stational systems and	27ma		104P	1014		- 104							
	80.94	(10) Biranji Output Statione	- 4	106	- 04		2-1,001 tills i it App	27944		1040			494							
	85.95	(10) Bries Oxford Statuse	- 1	08		-	Turning and president way	0794		049	00		-000							
	80.46	(10, Rowy Output Steams	÷ ((fer	- 04	-	2/1/2014 5:42/31 Aug	0744		def	- 24		- 244							
	80.91	(15) Briery Colysia Datural	et	08	. 04	-	Sriver to be the set	07444		440	04		-290							
	80.46	110 Brany Column Stationer	÷ *	-08	04		2/1/2010 1/18/16 84	2764		4284	000		-010							
	812 910	[10] Brieny Dulgart Statutes	69		C/V		2-12019 SIMPLE AND	27444		ione-	010		1000							
	80.410	[15] Bowy Usigal Station	e. 19		04		Survision and units	2764		100	100		1010							
	80.911	[1] Bowy Galgad Statuse	s. 17	108	- 04		Victoria Intelli we	2744		store.	104		104							
	80.412	110 Brvey Output Ballum	- 19	108	04		21,2214 106 IB M	2744		ove	100		100							
	80.413	110 Brany Output Statione	6.13	.08	04		Turdena yrakina we	274.4		10NP	104		100							
	80.8%	210 Brees Output Statuse	. 14	108			Survision and the second	0744		1010	104		104							
	40.7%	[10] Kivery Golgov Hallow	. 18				7,2,0818 20818 18	- 2044		ices.	04		00							
	80 P.S.	[1] Brwy Dulpat Salues	- 18	100	04		COLUMN STREET, MAN			1000	100		- 100							
	80.817	/10 Brwy Dolpsi Datum	e 17		- 04		And all the second second second	2744		1014	-		0.0							
		110 Propy Fulfald Ballow		100	- 19		2-12111 2100 10 AM	279.04		0.00	-		-							
	10.00	110 Boury Columnian	12	100	- 2		A CONTRACTOR OF A	1100		-	100		-							
	80 Apr	THE BOARD CORPUT MAKANE		10-			A VALUE AND A DESCRIPTION OF A DESCRIPTI	1000		-	1000		100							
	ALL ADV.	110 Brief Colper Station	9	- Com-			Colored Sold in Add			1070	1000		100							
	40.422	Lot Block Control (1997)	5 H		- 04		Colorest Line 18, sea	1000		1010	100		-							
	and the second second	Lot pass opposing general	- 77	100			Concernance and the	1000		1040	-								-	

Figure 92 show the Unsolicited Reporting on the analyzer. The value of Binary Inputs is changed and the same is notified to the Master.

Figure 92 Master Analyzer after Change in Register Value



SCADA Communication Scenarios over CR Mesh Network (IEEE 802.15.4)

In this scenario, the DSO will be hosting SCADA applications (Master) in a Control Center. The SCADA Slave is connected to the mesh node via the serial or Ethernet interface. The SCADA Master residing in the DSO Control Center can communicate with the Slave using the DNP3 or DNP3 IP protocol.

Operations that can be executed when the communication protocol is DNP3 or DNP3 IP are as follows:

Poll (Master > Slave)

- Control (Master > Slave)
- Unsolicited Reporting (Slave > Master) Notification

The operations have been executed using a SCADA simulator known as the DTM and Test Harness tool, which has the capability of simulating both the Master and the Slave devices.

- If the endpoint is connected to the mesh node via the Ethernet port, then it is pure IP traffic. The IP address of the endpoint (i.e., IED) can be NAT'd so that the same subnet between the IED and the Ethernet interface of the DA Gateway can be re-used. This approach will ease the deployment.
- If the endpoint is connected using asynchronous serial (RS-232 or RS-485), then tunneling of serial traffic using Raw Sockets (DNP3) must happen at the mesh node only.

This document focuses on SCADA protocols such as DNP3 and DNP3 IP protocols widely used in the Americas Region with a Control Center.



Figure 93 Feeder Automation CR Mesh Lab Topology

The IR510 is implemented as a mesh node, The CGR1240 is implemented as a FAR, and the ASR 1000s implemented in clustering mode act as a HER, which terminates FlexVPN tunnels from the FAR and the HER.

80000

IP-Enabled SCADA

Protocols Validated

The protocol we have validated for this release is DNP3 IP.

Flow Diagram

Figure 94 DNP3 IP Control Flow

1			
	Brad		
4	Read Response		
	Write		
	Notification		
	Unsolicit Report		

As shown in Figure 94, the SCADA Master can perform a read and write operation to a remote Slave via the DA Gateway. The Slave can send the Unsolicited Reporting to the SCADA Master via the DA Gateway over the IP network.

IR510 Mesh Node Configuration

This section describes the NAT44 configuration of the IR510 device. Basically IPv4 address assignment of the SCADA Slave and the gateway IPv4 address and the port SCADA Slave listens.



NPIG > DEVICE CONTIDURATION				
man francisco in Street Street or Street or Street or Street of Street or Street of				
Groups Conty Profiles SPu4 Address 19	68.0.1			
Contansise Profes + IPv4 Prefs 24 Length				
- Dibroke				
PUR PROFES KAT 64 Mappings	12 ertten			
tace provide the provide the provide of the provideo of the provide of the provideo	the Internal Porty Emeral Porty Put			
+ sup resource	And And A			
CHOP CLIENT PRICELE	20000 20000 1			
 PP(17100/04/E 				
C Celsus-MATA Prores				
🍇 Edge Compute_ant_Scale_ED				
Test .				
Page Calabo Your Provide				
 THEOR SERVICE PROPERTY. 				
 SENA, PRONLE 				
 ACLINICILE 				

Note: Enable the front panel Ethernet Port on the Configuration template.

For information on NMS management and MAP-T, please refer to Zero Touch Enrollment of Cisco Resilient Mesh Endpoints, page 63.
SCADA Master Configuration

As per the topology, the SCADA Master is residing in the Control Center. The following configuration must be required for the SCADA Master to communicate with the SCADA Slave.

- 1. Open the SCADA Master Application and click Add a new DNP3 Master.
- 2. From the Channel tab, configure the SCADA Master as per Figure 96.

The SCADA Master, in this case, is configured as TCP Client, interacting with SCADA Slave, which is configured to act as the TCP Server.

- 3. Populate the Remote Address field with the Loopback IP of the Cellular Gateway.
- 4. Populate the port with 20000, which is the port used in Cisco IOS Configuration.

For information on MAP-T, please refer to Zero Touch Enrollment of Cisco Resilient Mesh Endpoints, page 63.

Figure 96 SCADA Master Configuration

Modify DNP	3 Master	1			
Channel Na	me (nDNP m Type				
TCP/IP P	arameters	MAP-1	Addres	s Of Node	
Port Local IP	28000	÷	-]	
			Advan	ced Settings	
Cancel				Modify	1

SCADA Slave Configuration

As per the topology, the SCADA Slave is residing in the field area. The following configuration is required for the SCADA Slave to communicate with SCADA Master.

- 1. Open the SCADA Slave Application and click Add a new DNP3 Slave.
- 2. From the Channel tab, configure the SCADA Master as per Figure 97.
- 3. Populate the Remote Address field with the SCADA Master IP.
- 4. Populate the port with 20000, which is the port used in the SCADA Master.

Modify DNP3 Slave	
Channel Session Next Step	
Channel Name sDNP	
C Serial TCP/IP	
TCP/IP Parameters IPv6 Host 172.16.107.11 Port 20000 Local IP 192.168.0.3	
Advanced Setting	5
Cancel Modify	

Figure 97 SCADA Slave Configuration

SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Unsolicited Reporting is sent to the Master from the Slave. Figure 98 and Figure 99 show the Poll operation from the SCADA Master. Control, and Unsolicited Reporting can also be seen on the Master Analyzer logs.

Poll

The Poll operation is performed by the Master. The Master can execute a general Poll in which all the register values are read and sent to the Master. In Figure 98 and Figure 99, we see a general Poll executed on the Master side.

As per Figure 98 shows, the Master Analyzer is initially empty.

10.00per + 8 1	And States	X terms + 4 a
temper → (2) TH: New Hindow → (1) ANY →	Point Andrew - Hithermolitheratory Data in Angenetic in general in general integritzy field Jun to Baarts Handyitzy Field Jun to Field	Image: State of the state
Statute Second	11.11.11.11.11.11 very wided . Journet in queues Application Confirmation	

Figure 98 Master Analyzer Logs before Poll Operation

However, when the General Interrogation command is executed, the values of all the registers are displayed on the Master Analyzer, as shown in Figure 99.

Figure 99 Master Analyzer Logs after Poll Operation



Control

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

The Initial Control Relay Output status would be noted on the SCADA Slave.

Figure 100 shows the control relay output status before sending the control command to the Slave.

-	++ or	(CMIC)												 A Reduction of A
- Carlos and a second	Stage rolling to		-	-										· · · · · · · · · · · · · · · · · · ·
* 1 thes	Cases	T Paint Spec	14	T mine	T being T	Reading 1		T Desire	7 Owned	T. Benden	T ben	• •	Description	 • DE CENTR MARKEN PAR
. Bell sine	100, 413	10 Daniel Bit Stands	1.0	- 28	Orite	LOUISING BOX III AM	(minut	494.5	0.00	410				and a strength of the state of
	210.00	(1) Dauthie Bit march	14	- 18	- Chilling	LINUS RUN AND AND	27mm	1000.0	010	100				
100-	200,005	[1] Davide Strength		04	Deter	COLUMN KOARD PAR	These .	404.5	424	420				
A CONTRACTOR OF	208,838	(1) Travitie Bit manufi	14	108	(Drite	CONTRACTOR NAMES AND POST	Street	4049.0	1000	100				1
	2081, 8127	(1) Tourish BY Inplant.	37	04	Steine	Tybrighten miller mil som	Sheet	1000.0	1244	date				
	1085, HOF	(1) Associate Reviews	1.00	04	Drine	1/bidderrade.biast	Other	4014.4	-014	104				
	108, 409	(1) Double Bit Inputs	-24	- 04	Orden	NUMBER OF T	1744	4049.3	210	104				
	18, 410	(3) Dealers Bri Ingels	. 10	- 08	Ordine	LOLDIN BOARD AM	1744	1049.5	0.0	100				
	238, 877	[32 Daulite Bil Ingeds	- 10	08	Order	1/31/3279 838-33 444	2744	10107.0	210	129.07				
	2184, 412	(1) Double Bit Inputs	1.83	18	Ordere	1/01/0214 8/38/38 AM	27444	1249.9	-chir	1010				
	28, 433	(7) Donine Bri Impuls.	11	- 18	(Deline	NYTY, DON'S BOARD AN	27444	(049.9	-CAP	019				
	2181, 834	(2) Double Bill Inpuls-	M	08	Criste	NINDER BURNER	27mod	(059.3	-CNP	1299				
	28, 416	(5) Disable Bit Inputs		-18	Orbia	1/35/2019 6.34(8) AM	(Const.	-048.9	-049	494				
	208, 416	(5 Deutlie 84 Inywite	- 14	- 18	Dete	VESTIMATION AND AN	2744	0473	614	04				
	208, 457	(5) Distable \$4 Impute	(F)	- 28	Children .	100-2018 EDKIE AM	2000	1010.5	0.0	0.00				
	58.458	(D. Seculte &t Inputs	10	- 28	Stille	VELOCITE BUT ALL AND	27764	4299.5	674	674				
	218, 415	(C) Troutee Bri Injuste	- 10	1.108	Station	STRUMPIES AND AND	- STitut	4044,5	-234	100				
	6146	155 Binary Torine, Mate	- 1			Contraction and and		1000	1000	1040				
	283.41	152 Binary Chelout Bala	1 (I		Chine	PARTICLE ROW IN WA	2000	-04.5	010	0.00				
	280.40	(All Brony Output Bats	-	28	Crime	VOCUDER BOX REAM	Started.	049.5	610	0.00				
	90.41	(10) Broary Culput Bals	an 1	08	Chille	COLODIA ROKID AM	277404	1010.0	0.0	100				
	980 44	(13) Browy Output Bala	-	08	Chillie	COLODIN ROKELAW	277464	1049.2	00	04				
	80.49	(H) Rowy Gutput Balo	-1.	100	Chilling	COLORIN BOALST AND	27Mart	1049.2	- 254	104				
	80.46	NE Branj Gospot Balo	-		Other	COLORIS & DATE AND	(Print)	1048.5	610	104				
	280 41	(All Browy Dulper Suite	-		(Delice	COLORIS ROAM AN	1.000	1007.5	0.0	0.00				
	80.49	10 Browy Dutpot Halls	- 10	08	Dates	UTUDETS ADADE AM	Course of	1007.3	0.0	0.0				
	10.04	Fill Broary Dulpot Rate	12			COLUMN RULE IN AN	-	1000	-	1000				
	10.00	Fill Broary Christel Balls			10000	LITTLEFT BLUE DI DAL	1000	200.5	210	259				
	10.011	(Fill Breary Cutjout State	-		Contrast -	LUCCOPER REALD AND	10000		0.00	0.94				
	and and a second	(10 New) Dated Sele	-	-		LITTLETT CALL AN	1000			2.94				
	1000	(10) Reary Childred Balls	- 1			Transferre Bracking and	1000		1000	100				
	and some	The Browy Codest Balls	-		1211	111110111000000000	-		100	100				
	Pro 975	17-15 Bridge Tacket States	- 11 Mar			THE REPORT OF A DRIVE WAR.		1000.7	12.00	10.000				 and the second se

Figure 100 Slave Register before Control Operation

As Figure 101 shows, a control operation is then performed to modify the value of the control relay output register on the SCADA Slave. This operation is performed from the SCADA Master on the SCADA Slave.

Robert + A	* Andere individually have a	-0# x0# mit/	8 met + 8 *
. Ca the here the base of	The local and the place place it		a California
 II and 	they have the first the	and in our distance from the second	· · · · · · · · · · · · · · · · · · ·
	CELORDIN DI Papada - 07	2F Disc 21071403140 Tel 2164 400 400 400	and the second
+ 1 Ch - 000	CEDingle In April 10	DP Data L'UTHADIGAT The Disk with adult adult	
200	CONTRACTOR OF A PARTY AND	DR Date LTLDTHADDAM he The she all all all all	U iour
10.00	10 Danies Briegale 24	DF Des L'UDVADANS	
	DE Danke Britagniy 10	DR Date LIUSTIANSAA The Disk of the other	
	CE Double Reinputs 18	400 900 900 900 10 10 10 10 10 10 10 10 10 10 10 10 1	
	CE Puster del Inpuls 11	DP Date 2/2019/12/201401 The 21% sOld sOld	
	CEDING TO NAME OF	DF Date \$1,00143(5).485 The She She she she	5
	CE Studie & Spain 10	or the publication be the star and and	
	CTE Story Dubyd Mason: 8	pt Date \$10004.000.00 be the city of othe	(*)
	210 Brong Oxford Statuse: 1	DF Date (Dimension Date) Tes (Dies + DM + DM + DM	
	(19 Inney Dolgot Nature: 2	De de l'annotant tant - 2 × The shee where where where	0
	TTD Invest Duting Televise, 2	De di Name Consul Mais Tarpet Nove Paul Plus de Date addat addat	
	(10) Kiney Colput Rature: 4	DP 0 The service deals may support tensor subject control panelizes to multiple calas. Their DTrial wDM wDM wDM wDM	
	CPE Imay Output Tomate: 3	De g annu it the same message, but all points are suit regimes to therege at this same that g that the point schapt schapt schapt schapt	
	Trits Among Chaland Stationer &	24 0 tue 25es s0M s0M s0M	
	110 Inter Oxford Statutes 7	28 E the little of balls in balls in the little of the little of the	
	210 Intern Delated Stationer, 8	24 d Lancestones he like the star and add	1
	CE Invest Output National 1	09 9 Authors 8 9 9 10 2010 -009 -009	
	(10 Avery Dolgst Tature) 10	28 B Levering Matter at the Deal and all all all	
	210 Broky Dulphi Nature: 17	20 C Anna Carlos	
	1710 Bries Dubor Nature: 13	24 6 The Third HOM HOM	
	(10) Many Corput Natione 11	De g heatest hit Day fater Sedang 100 R heat 2014ar addar addar	1
	CPE Imag Output Statute: 14	De g Book Advenues the Diver address addre	
	(10) Benery Oxford Statuser, 15	DR 6 THE LARGE BAR AND THE STAR ADDR ADDR	
	110 Intel Output Dataset, 14	04 0	
	THE Brany Dutiest Datums, 17	or a basis	
	TE Imay Deput Values: 10	28 2 Anna	
	CE Ines Oded Nature 19	20 0 10 100 100 100 100 100 100 100	
	100 Imary Octput Statuses 30	24 I The International Action (1997)	
Concernant and Concernant	The International Statutes 21	04 G	
Derivate Association	THE REAL Dright Hallone 22	DF CHAR LY-DFFERENCE THE DFFE HOW HOW HOW	(*)

Figure 101 Master Control Operation

After the control operation is issued from the SCADA Master, the control relay output register of the SCADA Slave is noted. As Figure 102 shows, successful modification of the register value on the SCADA Slave signifies the successful Control operation.

Carl Street Street Street	Deputition		1000													· Distance
A DI AMORT	Name -	T Palet Tank T	4.1	Wite .	T Gully		Dealery 7		T. Detre	T. Canad	T. Issue	T. bet	· · · ·	Desciption		· · · · · · · · · · · · · · · · · · ·
	18, 10	101 Donald in But Supports	.18	100	Ories		100010-024-03-004	1719-04	-046.0	494	-045					a state of the sta
+ 212 Hours	28, 101	10 Dealers Bit Specific	39	19	00w	1/	152071-02620-000	2776-2	444.5	-4748	494					· · · ·
100	28.410	(1) Douglin \$4 Superior		100	(blue	- 1/	11,0719 8,04,71 894	2044	4947.2	1000	450					Max 21 (198
EPS Con	28, 111	10 Disate St Input:	PL	- 26	0.04	1	truiters alle in see	(the	4947.2	104	454					2 1003
	28, 413	(DCInum Release)	-10	108	Shine	. V	TUDYS & Jack Mar	(Time)	1054.0	104	174					
	D8.40	(1) Desittle Bit Imports	11	-08	Orine	1	31,2018-3,3631-464	Direct	-658,5	400	100					
	28, 194	(2) Double Rt Impuls	34	08	Orline	10	14/2018 #34.3d.4mi	2014-0	444.5	dear	010					
	28, 411	(D) Douglaine Bill Inspector	-10	08	0.04	1	11/2019 8:3430 4HH	177444	049.0		00					
	28, 431	(3) Double Bit Impoly	14	- 28	Critre	1/	11,1019 83430 AM	1014-0	1000	dhP	010					
	286, #17	221 Dicable Bill Impolis	37	128	Online	1/	102219-034-19-466	2716-0	1000.0	dNP	dNP					
	186, 418	10 Disable Bill Ingels		126	Ordene	1	102210-02430-004	2710.0	4000.0		-010					
	18, 410	(2) Strukts Bit Hypothy	180	108	Oning		11.12119-8-24.10 AM	17110-0	14949	1284	-CNP	100			_	A
	877.89	111 Knurs Culput Hilling			100		COLORANGE AND	100	1100.0	455	4.64					
	10.11	1923 Bruny Chilput Balance		108	Online	10	11,0019 824,30 444	201940-0	499.5	00	04					
	80.41	1712 Brians Output Datum	GR	108	Other	10	NUTRIN BOARD AND	25Hout	424.2	-054	100					
	80.41	175 Briefs Oxford Statute	· *	108	Orine	1	NUMBER & DAUG AND	Talenter .	4249.5	104	454					
	80.14	(PERrary Oxfort Seise		100	Ories	- 0	10,0075-0,0408-444	259 kod	4947.5	104	454					
	85.48	110 Brany Dalané Statum	et	100	Colore 1		11,0719 \$24,00 404	20144	454.5	-1747	-174					
	80.46	(10) Rowy Colper Dense	÷ 8	- 18	Colora -	- 10	11,0019 \$24,00 \$89	20%4	104.0	- 454	-494					
	80.01	(H) Brany Sulpsi Same	1	28	Othe	1	10219-024.01 444	2754.4	1000.0		454					
	80.40	(11) Briaty Dalgost Detuin	÷ #	100	Otes	1	100010-024-02-000	211164	404.5		414					
	80.49	193 Rivey Solard Dation	÷2	18	Oring	1/	100010-00010-000	2006.0	4999.2	-(74)	1014					
	80.410	1993, Browy Dalgost Patient	÷#	- 108	illine .	1/	10001032435444	2014	-(747,3-	-(74)	-(50					
	80.811	175 Rivers Oxford Datum	6.12	24	0.004	17	11.0019 8,14,14,144	1004	1045	104	404					
	80.410	(11) Rowy Colput Balance	6.11	108	0.04	10	11,1019 8,14,14,464	1004	494.5	1010	-194					
	80.010	110 Briefy Gulput Pation	6 H	108	1004	1	ACCESS & 2-4, N. AND	2779-0	494.5	1010	-010					
	80.016	100 Rowty Statust Statust	14	108	0.04		ALLETTE & Lock M. And	2794	494.5		-040					
	80.010	10 Brian Delpar Despe	÷ H	108	044	V	11,0019-824,01484	1710-0	104.5	100	100					
	80.910	(10 Brian) Colper Dation	÷.	108	1044	10	1.0010.024.02444	122011	-047	100	-04					
	80.917	(10 Bree's Delpai Testion	6.0	104	044	10	11,0010-0,00,03-484	12249	104.5	-04	104					
	80.000	(10 Brats Delper Dates	18	104	Other	1	10,0010-0,24,03-000	1000	1047.5	1014	100					
	80.416	(H) Brony Dalpat Darys	÷.0	104	004	1	11.0018-0.004.004444	22244	494.5	- 1044	1014					
	10.100	(H) Rray (high halos	÷#	19	1044	11	10,0019 624 01 866	1044	494.5	-010	4248					
	BU A21.	(Fit Revery Gulput Pations	6.21	128	1000	1/	NUMBER OF STREET	1779-01	1046.8	1014	1004					

Figure 102 Slave Register after Control Operation

Unsolicited Reporting

Unsolicited Reporting is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are reported to the SCADA Master. This notification can be seen on the Master Analyzer. Figure 103 shows an empty screen of the SCADA Master Analyzer before any unsolicited reporting.

Figure 103 Master Analyzer



Figure 104 shows binary input of the Slave that is going to change. Initially the value of binary input is OFF.

Figure 104 Slave Registers

and the second se	1000	1000												 Parameter a mar
B tow Worksont	The part of the			-										· · · · · · · · · · · · · · · · · · ·
043	Name 1	T Paint Type	Τ.	T. Mee	T own	T Threating 1	COMP.	T Davies	T themat	T. Issim	T New 1	F.	Desciption .	 • DE DERCH AND PRAY
1000	0.0	The sea frame		1.1		Low set and set		1000						in the second
· 19	8.41	(I) Barry Pando		100	(Contract of Contract of Contr	1/1/2018 (0.00.00) (0.00)	(Trive)	1047.3	104	404 -				a Dutant
Box	8.40	(1) Brok's Patuli-	3	10	-2004	1010-0010-0-0410-044	[Tried	104.5	424	424				18an 10.00 TB
difference.	81.41	11 Print Taulo	1		Date:	10100144440684	(Press)	4048.8	474	494				 104.5
	22.44	11 brain tracks		100	2414	Introduce & paral and	(Think	0473	0.00	- 04				
	81.91	11 Promy Traindo			2 dates	11112010-014-04-0404	1274out	1049-3	454	0.04				
	8.85	112 Billion Transfer		2081	2010	1012010-02402-004	Distant.	1047.0	104	194				
	8-17	(1) Blowly Inpute		2081	() dow	1/01/0014 \$28:00 484	Direct	1044.0	250	1048				
	81.49	[1] Binny Yupolo		1081	Distra	1/11/2019 8 (4/20 444	[Piled	1048.5	400	424				
	2.75	[1] Brany Ispate		108	Ditte	101,01148,04,00.004	[Thu?	434.3	404	424				
	8-310	(1) Really Family		108	dation -	1010/0018-834363444	(fried)	1000.5	430	4000				
	81.411	(1) Realizing Agende			-Colorer	tritulopre poletal and	(Privat)	4269.2	650	4214				
	86.410	(1) Brony Youdu		- 04	- Driver -	LUNDONE & CAUSE and	(DPHoid	04.3	00	00				
	81410	(1) Revery Franks	0	04	Online	transform & dwood week	[779-band	010.3	250	cm1				
	81414	(1) Brown Topolo	14	- 09	Deliver	tytrubere is a work and	[Think	4049.2	100	214				
	81415	11 Bines Inputy		-08	College	1/11/2018 8/14/20 484	[[Treat	(147.)	00	1040				
	81415	(1) Brony Islands		- 09	Draw.	toto, yore dute all weat	17Mad	1048.0	450	494				
	at +12	11) Billionly Franks		08	Children .	LOCATE & Jack And	Distant	048.5	00	0.0				
	8-810	(1) Brony Insulo		08	Drainer	transpore duals to And	Divised	GNP 3	che	694				
	81918	(11 Binstry Instals	- 18	00	- Dribwi	101/0016834363484	DTHeed.	1016.0	454	410				
	81.420	10 Rivers Inputs			Original	LITTLEDTF & JAINE AND	(Diver.	4047.2	000	04				
	8-421	(Children) Papelo	21		-Online	LOUGHT ADDRESS	(CO-base	614.3	00	100				
	124-14	117 Brany Inpute	- 22	100	Dotter	Introduce & depict and	Division	(14)	000	00				
	91921	111 Board Insula	- 21	- 108	Distance	UNLIDER & ALLER AND	17Hour	040.0	04	404				
	m-101	112 Beners Younts		100	Drive	Longers (Jack) and	171644	4040.0	100	690				
	8-40	111 Brans Palate		100	inter .	Longers & Jacob and	(Theat	date 2	640	100				
	81.418	TO Brans Panits		100	(Internet)	Vendere states aire	(Print)	(047.3	410	434				
	0.427	(1) Brance Transfer	1	- 100	(mage)	1010010-0030-004	(Triut)	614.3	0.00	434				
	0.000	(1) design ingenie		100	Dist.	11112010-02403-044	Divised	1048.0	000	434				
	ai-420 .	(1) Bridge Stands		1.0	(Desire)	LOUGHT & Land and	(Prind	041	4240	424				
	10.410	Fit Bridge Transfer		- 18	(pairs)	Lobit Date & Local And	10mod	(144.)	4740	200				
	41.411	11 Brain Issuelli			2004	transforth index to and	10 total	1000.0	454	010				
	N 111	111 Binary Younds	1.1	- 10	interes .	transport to be led and	17Maria	1204.5	100	254				
	81.410	(1) Bilary Transfer		108	- Distance -	transport data internet	10 mart	404.8	100	104				
	- I Canada and a state of the	and the state of the	11.1											 A COLUMN AND A DESCRIPTION OF A DESCRIPR

Figure 105 shows the binary input of the Slave is changed from **OFF** to **ON**.

Figure 105 Change in Slave Register Value

C fan Moleyner	(the same	-		444	-																		· C 2710 famorie
- 1 AMA	Name :		Paint Type		• 1	the later	Υ.	Deality.		Terrature	τ.		T. DH	. T.I	herest	T been	Υ.	Barber	T	Description	7	1.0	· Di printir insistri iner
	0.0		1		10	0	12	de la co	- 111	Adapted Second And	1	-	1100		-								
· 10.0	8.41	- 1	Chiefy Talak		•	100		244		101-001-010-010-04	1.29	les:	1010	8 6	- 44	1000						1.1	a la monte
Box	845		1 Bindy Synth		1.	-14		244		10100-040400-04	1.00	test .	040	A	240	00							10.0 March 10
And see	0.01		Chief Street			100		100		LTUIT ARE IN	1.07	-	440	P	100	1040						1.1	§ 4943
	8.24		Chevro reports		•	106		244		11112014-82400-84	1.07	hef	100	P	- 40	100							
	8141		C Brees Inputs		۰	100		24im		17110118-0030-00	1 25	5at	date	×	194	100							
	8.45		C Broad Provide		ŧ	108		Select .		LOLIDHERICAN AN	1.00	5et	1240	2	784F	- 694							
	8.41		C Renter Strande		t	0.0		2454		12120249 \$2430 84	1.00	•ef	1240	8	-	-00							
	8.41		State and		ŧ	108		Select .		1.01.0019 8,24.00 84	1.0	hul	1284	A	24.0	0.0							
	B 45		Diary input-			100		ordere .		LOLDER & LAND MA	1.00	***	0.00	2	-	1010							
	8.410		S \$ Ferry Hallety		16	-08		Selve .		UNLIDER ROAD IN	4. 22	het	1040	P		104							
	8.411		C Briary Typelo		M	100		244		URLIDING REACID BA	4 27	5e8	- 200	2 1	DAR.	104							
	8.412	- 7	C Brury reputo		9	-08				UNUSPERSED IN	1 20	-	0.00	2		00							
	8.413		C Brony Inputs		÷	08				COLUMN RUNCIO AN	1 20	444	1044	A	254	104							
	8.414		C Barrers Inspector		14	10#		100		COLUMN & DESIGNA	4 . 05	444	104	2	-	- 104							
			Careful Library		-					1912009323400 44	1.2	×	104		-	- 00							
		- 3	C Brivery Imports		18	100		20.8		101001941410-0	1.27	чя	1014	2		104							
	8.417		Calman admin					200		191001232400-00	1.5	×	1044		-	00							
		- 1	C Broary Instanto			100				1010079-02410-09	1.27	÷	1004		-	100							
		- 1	C Breaty Topolo		10	100				1.91.00094241046		-	1010	· · · · ·	-	100							
	B 115		C Broky Parols			100				1111111-1424.00 04		-	1044	· · · · ·	-	100							
	8. TUT		Construction of the local division of the lo		PT	- Com-		-		COLUMN PLACE AN			100	· · · ·	-								
		-2	C Brown reports		2	10-1-1				101,000 8,04,80 84			1.1	<u></u>	-	100							
			C Brown Capacity		<u>n</u>	1000		-		1.01.0000 8.24 82.46			1014		-	104							
			Construction of		<u> </u>					Contraction of Repairing and		-	-	-	-	-							
		-0	Contraction of the local division of the loc		2-	G		-		Concerning a log of the	1		1.5	5 - 5	-	-							
	and the second				-	1.00		2		the same a part of the	1.1	-	122	0-13	-								
	-	- 1	Colored Transfer		-	-		200		Los man a la se a			1		-	-							
			Contractor of		-	1		-		total company of the last set		-	1.00		-	100							
			and the second			1		2			112	-	122	2 1	-	100							
	an and	- 1	Second Second		- E	-		1		1.01.0000.0.00.00	112	-	1.50	200		-							
	C	-1	and a second		3-	12		2		COLUMN A DAMAGE			100	-	-	-							
	1.1		and the second			12-		1		the second second law			-	-	-	-							
	Contraction of the local division of the loc		A COLUMN TWO IS NOT			110000		-				-										-	

Figure 106 show the Unsolicited Reporting on the analyzer. The value of Binary Inputs is changed and the same is notified to the Master.

- • • •	Antern Lincolnuct	sponthall have a	-ing sche sche											Part of the local diversity of the local dive	*.*
a 12 Chr. fan Hotson	- Traj a present taxon and		4 mar										- 11	2 174 heres	*
. Il start	STREET, SQUARE,	MALANS.	COMPARED IN COMPARING INCOME.	SALE OF	Media and media	a description	ALLOW	ACCOUNT.	distant in	Million	AL	100.00		🖌 📑 0000	+ stratting press
	TE Brang Panets		0	21616	2/L0010 310212 AM		See	(printed)	adata.	+014	-			100	
* 1 Bear	213 Among Pagests		0.0	Online	2/1/2010 4:25 tot.440		Tran	17944	1010	+010	eine .				- 144/01/16
1.0.00	TO BRANCHARD	E	08	Diet	2/12/19 4:15:34.464		line .	(Frend	100	+044	109		381	1	+04
* 10 -CV	(1) Brief Yourie -	1.1	-10	284	2/5/2019 4:35 (9).445		100	(17mm)	+058	100	100		11		
The Desider Desidered	Ci Anger Yandi		0e	Oritine	2122278 425 56 460		The	27464	wolat	+04	+04		111		
	TO Brief THUS	1	0.9	Inter	3/(0110-615306.400		Tot	(Const.	+014	+0%	+010		-		
	(1) bias input		Off	2100	2/1/2014 # 25/56 AM		Tue .	(Crime)	-schip	+047	1004				
	The second second		0.0	Deter	2/1/2019 4 25 No. Ave		9.4	27444	wind	+0%	+094				
	[1] Booty Parents		-CHI	(Date:	07/001842526289		700	(Class	+014	+014	+04				
	TO Anary Vends		0#	Drive.	2/12/0110 4:35:36.484		the state	(Trinal	-0244	+010	alte				
	211 Billion TSANK	10	08	2164	2712010-025/04.466		9.4	(Deep)	+040	+04	with				
	(1) Stars fund	10	CR.	Dee	2702019-42536-464		5 at 1	(Tread	+014	+000	+04				
	FEBrary Panis	tg.	0#	0.84	2/1/2010 4/25/26 AM		744	(Prival)	-000	+0%	-04				
	(1) Birary Yearts	10	0.0	244	2/5/2010 4:25:36.4M		50	27mm	+0.94	+058	+1747				
	(1) An any Paper	16 -	04	Ories	3/\2018.43536.MM		Tra	27464	+040	+04	+04				
	Ci Brialy Yapahi	10	04	Ordere	2/12018 4 25 26 449		7.0	1000	1010	+010	+04				
	TT Brief Territ	16	07	2164	2722019 4 25.56,864		the state	27404	worket	+010					
	TT Brans Inputs	10.	0.0	0104	2/1/2010 4:05/06.460		he	27464	100	+04	+016				
	[1] Biary Inputs	10	CM.	Date	2/12/010-4:25.04.46F		Tue -	(Cited)	adap.	+049	+0.04				
	[1] biasy specie	10	08	2164	2/12/01/04 25 54 444		Sur.	(Theat	odne.	+014	04294				
	CT Rrany Parent	10	-0#	Dee	2/1/2018 4 25 10 AM		The l	(Chief	+010	+076	01342				
	21 Stary Tariti	10	08	U-lee	2102019-42536-464		7ue	(Contract)	+04	+04P	+04				
	718ney renki	10	Ċ#	Online	2/1/2019 #3510 Aut		her	(Crimes)	-104	+010	- elas				
	TT Bears Issue	15	CIR.	Order	2/1/2018 #35.58 AM		The	(27-Mod	+0167	+04	+010				
	T Bairy Merce	14	08	Onine	3/12/11 425 36 AM		The	(Const.)	-124	+04	4010				
	(1) bias involu-		0#	210m	0112010 4 (5 Nr Avi		Due .	attend.	0.00	+047	1404				
	(1) here; renty	10	0.0	2184	2/10019 4 (5 M Her		714	(Const.)		+04	+094				
	[1] Boarly Vessel	12	08	Drifter	27/2010 4 (5.82.400		700	(Cited)	inchel.	+0%	+(34)				
	COMING YORK	10	0#	(Index	2/12/07/19 4 (5):36.484		0.4	(China)	-	+010					
	[[] they have	10	Car.	Drive	27120104/0.00.000		9.0	(Denot	octol	+014	+014				
	Diff Kingy Parent		C#	2164	2/1/2010 4/2010 AND		104	(Theat	w0nit	+010	+04		10		
many strength	TT Aren result	10	0.00	Children	Universe with the weak		344	125464	ACMP.	ACRE	Addate in the		141		

Figure 106 Master Analyzer after Change in Register Value

SCADA Communication with Serial-based SCADA using Raw Socket UDP

Protocols Validated

The protocol we have validated for this release is DNP3.

Flow Diagram

Figure 107 DNP3 Control Flow



As shown in Figure 107, the SCADA Master can poll and control the Slave via the DA Gateway using UDP Raw Socket. The Slave can send the Unsolicited Reporting to the Master via the DA Gateway using UDP Raw Socket.

IR510 Mesh Node Raw Socket UDP Configuration

As per the topology, the SCADA Master resides in the Control Center. Three step configurations on FND:

- 1. Creation of serial profile
- 2. Linking of the serial profile to the configuration template
- 3. Configuration push to the device

The following serial configuration profile requires the mesh node to communicate with the SCADA Master.

- Peer IP Address–SCADA Master IP Address.
- Peer Port–SCADA Master Port Address, where SCADA Master is listening.
- Local Port-This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator.
- Packet Length & Packet Timer–Any integer value.
- Special Character–You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer.

Figure 108 IR510 Mesh Node Raw Socket UDP Configuration

CARE FIELD NETWO	HIR DIRECTOR								04	SHEARD	DEVICED	OPERATIONS -	CONFIG-	
INFIG > DEVICE CON	FIGURATION													
Ausign Devenente Oreal	Dierge Deutie Migartes		Reve Socket	LIPP										
Groups	Config Profiles		-Secial Interface Port attesty:	Bettings B DA Gab	war 0.1013	lode		Porta	Minity is only app ps with not be us	ocatre to gale	ways with ICe fai	ide. When set to 10x i	Mindy the followin	0.001
Cartinistic Profes		+	Media Type:	R8232			Baud rate:	8605		14				
ENDPORIT			Data Orts											
· rus more c			Parts	None		140	Dirp Bit	1		14				
· page more r			Fise Custoi	Note		*								
 And Tablets F 			have earing	(neor man		. (5)								
 March March 201 			Rew Socket See											
 DHOP CUDIT PROF 	1.1		TCP tate Time Outpecci	Connect Time Outlisecsi	Peer P Adda	19.2	Peer Post	Lazal Par	Packet Length(byles)	Packel Timechal	Special C	haracter(0.255)	Connection Trans	
₱ NATER PROFILE				0	172.16.107.1	6	28000	26030	512	500	48		UDP	
F DHOP DERVER PRO	F3.6													
. SERVE PROFILE											8			
B Mgrated-Barrel	(E)													
By Read Second U.S.	9. S													
Debut Secard	Proble													
Enge, Compute	"Sanat_Platte													
Raw Samet TO	P Charl													
Raw Some TO	P Lanat													

SCADA Master Configuration

As per the topology, the SCADA Master resides in the Control Center. The following configuration is required for the SCADA Master to communicate with the SCADA Slave. In this implementation, DNP3-IP acted as a SCADA Master instead of the DNP3 Raw Socket Server. The configuration provided below is specific to DNP3-IP.

- 1. Open the SCADA Master application and click Add a new DNP3 Master.
- 2. From the Channel tab, configure the SCADA Master as per Figure 109.
 - Network Type—To configure a Master or Slave as a UDP only device, Network Type should be set to UDP_ONLY.
 - Type-This can be configured as UDP_TCP.
 - DestUDPPort-Port Address of Raw Socket initiator or client.
 - LocalUDPPort-Port Address of the SCADA Master.
 - WinTCPinAddress-MAP-T Address of the Node.
 - WinTCPipPort-TCP Parameter 'WinTCPipPort' will be the local port number on which datagrams will be received.
 - WinTCPmode-To configure a Master or Slave as a UDP-only device, WinTCPmode should be changed to UDP.

dity DNP3 Master		Mar Mavenced Settings			U .
nnel Session Next Ste	9	1 2 I III			
		 Configuration Settings 			
hannel Name (nDNP		Active	True		
		ChannelResponseTimeout	10000		
Connection Type		ConfirmMode	NEVER		
C Pullet / TCDID		ConfirmTimeout	2000		
Senal of IChine		ConnectDelay	0		
		ForceDisconnected	False		
TCP/IP Parameters		GenderType	MASTER		
N	AAP-T Address Of Node	Id United States			
Host 10.153.10.23		LinkNetries	3		
		Maxuueuesize	0		
Port 28000	÷	Name	HDD ONLY		
ocal IP 172 16 107 1	1 2	Network i ype	ODP_ONET		
Live in 1993		ByB Hartina	250		
		By Commentation	2048		
		ByErameSize	2010		
		ByErameTimered	15000		
		TyErapmentSize	2048		
		TyErameSize	292		
		Tune	LIDP TCP		
		UseConnectorThread	Tore		
		Win232Disabled	False		
		Y TCP/IP Communications Configure	ration Settings		
		1 DestUDPPort	28000		
	Advanced Settings	DisconnectUnNewSyn	False		
Cannal	Madik	I DualEndPointlePort	20000		
- and	mouny	InitUnsolUDPPort	20000		
		LocalUDPPort	28000		
		NetworkRole	MASTER		
		TCPConnectTimeout	1000		
		ValidateUDPAddress	True		
		WinTCPin4dfreas	10 153 10 23 MAP-T	Address Of Nod	je
		WinTCPipPort	28000		
		WinTCPlocallpAddress	172.16.107.11		
		WinTCPmode	UDP		
		WinUDPBroadcastAddress	192, 168, 1, 255		
		> TCP/IP TLS Communications Cor	niguration Settings		
		Name The name of this channel.			

Figure 109 SCADA Master Configuration

SCADA Slave Configuration

As per the topology, the SCADA Slave resides in the field area. The following configuration is required for the SCADA Slave to communicate with the SCADA Master. In this implementation, we used the SCADA DTMW simulator instead of a real SCADA device.

- 1. Open the SCADA Slave application and click Add a new DNP3 Slave.
- 2. From the Channel tab, configure the SCADA Master as per Figure 110.
- 3. On the SCADA Slave, select the appropriate serial port, baud rate, data bits, stop bits and parity matching of your device configuration.

Figure 110 SCADA Slave Configuration

INFI Oversen Company	Diff i Gestation Configuration	IN STREET, STRE	Lex.
Desce (Lenvel Senior Datase Atarvel Milips Devor	Dekis Owner Senses Da	Interest Multiple Design	
Channel Kante KERUP	TR. 64		م.
helippine	Munda	212	
ID AL ID Matter ID Monter ID Peer # Sale ID Mexicon	Refracted instant	11080	
Consertion Type	 B 5-4 	Common SenalProperties	
Innat 10 100/07 00 100/07 and 100/	- Amother	9400	1
Complete Propriet	FirstCha/Watt	1	
Serie Put COM14	NumChallenseletwie	etrac A	1.10
Baul fair 1023	Nethelits	875,8	
	Number	975,5	
	Perty	NOM:	
	RutCTSHole	ENALS	
	FortMade	NONE	
	Portflame	COM14	
	Aunt212Aoute	DISABLE	
	Spittern Freeguernity	42	
	+ 10	CICLIMMON 2NP3 2NP3 CPP Inperton	
	Magnettize	3048	1.1
	Shandar	200	*
	Serial Specify the properties for (DVP) see	a setal convectors	
ingust DVPL Device Ruther DV Careat	Argant DNP3 Device Profile		OK Centel

SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Unsolicited Reporting is sent to the Master from the Slave. Figure 111 and Figure 112 show the Poll operation from the SCADA Master. Control and Unsolicited Reporting can also be seen on the Master Analyzer logs.

Poll

The Poll operation is performed by the Master. The Master can execute a general Poll in which all the register values are read and sent to the Master. In Figure 111 and Figure 112, we see a general Poll executed on the Master side.

As Figure 111 shows, the Master Analyzer is initially empty.

Figure 111 Master Analyzer Logs before Poll Operation

fig Types	sign in man ing	NAME OF COLUMN		
U Inex U Treatment U Treat	P == 101 P == Transmit P == tag = 100 P = 100	Dataset Name - F Sam - F Data - F Cyclin - F Samony Sam - F Sam - F Sam - F Cyclin - F Samony	. Der Begin [™] Pene Treper Andrecking Heufter Some Level II	
Daniel I				
20 ·	Curl			

However, when the General Interrogation command is executed, the values of all the registers are displayed on the Master Analyzer shown in Figure 112.

Figure 112 Master Analyzer Logs after Poll Operation

lines.	0	Desine	Care Dayler	
Tire Sans Taget	P	Name V San V See V Set V Seen	C - Rean Dapte Na Auditority Machine (Instance)25 (42)	
Decision in a	5.e.)	Command Wilstow 202014444 *Tonegot	ty Dete Poll - Class 117P	
20,000		admpiotegrity seasion t		
No.		17131110.3151 (+++ a200 - 845	in 1989 Meenge: Clase Data Full	
		1713(111.315) 28	Opjeit 40(flass Dets), versettum 7, quelifies DelGibli Frintes	
		1713/111-3151 28	Capers 40(Class Data), verietion 1, qualifier Deltikli Pointe)	
		17+31120-3031 74	Doyer Colland Detel, versetoon 4, guellfier teleikit Pointer	
		17151110-8081 TA	Nçarı Grizlana Devej, Verletive 1, geallfler Terrikil Polstel	
		17(3)(11.00)+ a090 Inv	ern request in queves libre bete bill	
		17131110.325) come a230 Aug 17131110.3251 713 17131110.3251 61	lintive Beaded, Read Bequest (1) FIRID (CONS) EBCOR 5 0.0 m 01 m 0- 0 He A 4 0 Ho TA, 64	
		17:31:10.345: almy Tra 17:31:10.349: 17:31:10.349:	napiet Beeder 41 FERTI BER 4 6 2 5 6 2 5 4 2 5 4 20 11 54 Au (4 16 3c 41 06	
		17:51120.5459 (addy 901 17:51:105.5459 (5 addy 100 17:51:105.5459 (50 17:51:105.5459 (50 17:51:105.5459 (60	ANTY FINAN - THOUNITING D'ANT THIA 1780 108/11 PHRINI FINIS DIATAN DATAN MULAN 40 4 4 4 4 4 10 10 10 10 10 1 10 52 50 52 54 50 53 68 50 54 56 50 10 48 81	
		17151110-3451 818 6000 - 10-192.	18.23.3000 - 128 teakamit 27 botas	
		17+31+10.545+ + #DHF 05 17+31+10.545+ 2r	#4 19 19 49 40 00 00 47 12 19 49 61 14 16 20 16 19 19 19 49 49 10 11 11 11 11 11 11 11 11 11 11 11	
		17131111.204/> #290 08		
		1713111112191	ff + 13 10 34 10 47 60	
		17131111.2041) #DEF 43 17131111.2041) #DEF 43	uš 10, 40 10, 01, 01, 02 27 56 40 26 00 00 10 Na	
		17:11:11:2041> mDNP 01	or oo 27 50 88 88 58 58 58 88 88 88 88 88 88 88 88	

Control

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

1. The Initial Control Relay Output status would be noted down on SCADA Slave. Figure 113 shows the control relay output status before sending the control command to the Slave.

Figure 113 Slave Register before Control Operation

Contrast for Herman Adver		12 St C 10 C Tangle Married	ag harring														
the base integer based	Witness																0
6644,21	09.59	21 -															
Bullgard F	1 + 1 H ADV	Children I.															a hatant
· phaseman	Trail a little	lands and they i have to prival for the	a later														- I Ditkings
1.2.00	Name	T Asian Tapar T		This	T Gualty	T Testing 1	-		-	Dated 1	f Senter	۲	Sector	τ.	Description	τ.	· · · · · · · · · · · · · · · · · · ·
a Bag uner	20,418	(D) Drowthy BH Hands	16	19	27484	and the second second second	1779-0		-	410	100						
	200.017	ST Doore in rave	10	181	27494	unumer round and	1110-0		and the	dear	400						• · · · · · · · · · · · · · · · · · · ·
103	20,40	Stationers in react.	18	18	0100	property report and	100.0		-	dee	499						
	310, 411	(12 Induite in April	18	18	2464	And the residence of the second	Dime.		10	-014	104						1 04
	240, 816	US Include the travels	10	18	1000	Distance repaired and	Direct	140	nd .	-014	494						
	2081,451	(CD) and the instance	11	19	10444	DAUGHT HINGT AND	211400	-4	5.P	-254	426						
	216.432	US Dates in space	10.00	1.00	10000	Deline reaction	25100,00	14	5.P	47.0	424						
	244 #11	(12 Danies Britspan)	35	10	(ree	District House and	1716-0		a.	0.00	240						
	2285, 414	(1) Davides der Typiciti	34	18.	(Intern	Department in the other data	(Press)	1	14	1048	454						
	201.411	20 Tunine Bringum.		18	-0488	1000010101100001000	(Prind)	10	24	1244	614						
	201.450	(1) Takine be reputs	10	18	1988	1000010101110027.008	(Presd)	14	5.0	1214	014						41
	20,411	(1) Double Bri reputer.	IP	18	(Drive	2010/07/07 12:00 17:00	it must	1.14	1.0	1210	1216						
	200, 010	(1) Taxate bit repairs		100	(Deep	24030101011100211004	Direct	1.1	2.0	date	(216						
	286.429	DE Danale de tipute		D#1	10444	10000101010001000	1000		÷	-016	104						
	242.46	1750 Benary (Natural Stations)	44	18.	2044	240010-000211764	101418		10	-016	1014						
	101041	110 Dames Trained Reven			1000	And the second sec				1000	410						
	82.42	[75] Brony Oxfeyt Ballon	- F	18	()+848	CONTRACTOR CONTRACT	1794		10	1014	1094						
	82.41	(10 New) Duty of Balance	1	28.	Crew	JALING TOULT AM	27/04	14	14 C	444	der						
	80.99	(10 Bine) (statut Balan	1	28.	21000	Distant Product and	1000	14	14	0.00	der						
	20.41	(10) Broady Chapter Ratione	1	18	1100	340010113627.44	(mark)	-6	-	100	494						
	10.44	(15) Broug Cospet Balton	6. F	18	(Deares	Disperie House and	1000		nd .	-014	474						
	80.41	(10) Browy Despet Statust	6.1	14	2000	2/6/2018 11:06/27 444	271600	- 4	5.0	-254	450						
	10.044	(10) Howy Coppet Statust	4.	18	2444	244010101110001444	1000		5.0	-254	-050						
	10.00	715 Brony Colput Indust	<t< td=""><td>1.4</td><td>1084</td><td>104x10141130x01044</td><td>27404</td><td></td><td>-</td><td>1210</td><td>1014</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	1.4	1084	104x10141130x01044	27404		-	1210	1014						
	20400	(10) Benning Philipsel Stational	< 10	1.0	1044	2010/01/01/01 01:00	1000	- 04	-	deat	458						
	85.411	(10 from Tulant Balant	- H)#	1000	04000101100017.000	(French		1.0	1018	104						
	14.63	(10) Servey (Salas) Balant	<10 ····)#	2184	2400010110001040	(Fried		nd .	1214	104						
	30.410	(10) Newsy Technol Stations	6.10	18.	1100	24001911003144	Direct		84	-014	494						
	80.016	(1) Newsy Christel Stations	1.16	1#.	Comp.	24/01010110041448	1716ud	- 4	10	414	494						
	80.415 ···	(75 Story Delaid States	6.75	18	Dee	206/01101126-01444	271940	14	14	450	4747						
	80.416	(12 Root Dated Salar	e 16	18.	(Same	Service management	271840		2.0	100	494						
	40.417	(15) Strong Chilped Stations	6.12	100	-Onton	ARE DRIVEN TO BE AND	phile.	- 4	2.0	-254	0.00						
	40.418	110 Newsy Colored Status	n 19	18	1000	LINE TO BE TRANSPORT	Drived		2.0	-425.0	1000						2011 C
	Test, and	State Street, Print of Concess		Take .		belowers we do to and	- And Annual	1.1.1	4.4	-rail.	-1405						* B

2. As Figure 114 shows, a control operation is then performed to modify the value of the control relay output register on the SCADA Slave. This operation is performed from the SCADA Master on the SCADA Slave.

74 DN	P3 Commands (mDNP:mDNP) —	×	74 CROB Configuration - 🗆 🗙
Run	Options Target Add Command		
	Integrity Data Poll - Class 0123	-	Name: Control Helay Dubput Block. Target: Use Command Window target selection
1	RBE Data Poll - Event Class 123		Description The remote device may support binary output control operations to multiple data points in the same message, but all points are not required to change at the same
Ø	Read Specific DNP3 Data Type		time.
	Control Relay Output Block		Mode: 150 - Qualifier Code: 16bitindex -
	Control Relay Output Block		-Control Information Point Number: 1
\checkmark	Analog Output Block		Control Code: Ion 😩
\bigcirc	Time Synchronization		Feedback Pol Delay before sending 0 \$
\geq	Clear Restart IIN		Equivalent Tcl command line arguments
%	Enable/Disable Unsolicited Messages		mdnpbincmd session 0 point 1 control Ion
Ę.	File Read		Copy to Clipboard
3	File White		1 Seconds Start Repeat
\Box	File Delete		Once Close

Figure 114 Master Control Operation

 After the control operation is issued from the SCADA Master, the control relay output register of the SCADA Slave is noted down. As Figure 115 shows, successful modification of the register value on the SCADA Slave signifies the successful Control operation.

Figure 115	Slave Registe	r after Control	Operation
------------	---------------	-----------------	-----------

Contract of the later of the later		to the state because the same											
the lost relate that it	module 1945												0 4
B66 16 4.12 * 1	59,1391	Er											
Weitgend = 1	· · · · · · · ·	1000											Notest P. R. H.
· · · · · · · · · · · · · · · · · · ·	-	and the second second											· I The balance
											1	a little	
+ 1 th	and the second	F Past Spe T	· · ·	T Guety	T Towards I along the	Prest.	Y Dense	T Danse	Y Seamer	T Setter		Description	· Call Control Publicity practice
+ 210 cm	201.408	(2) Denite bit Vanto	24 -128	Children	202010-01108-01-000	27mm	010	04	010				Class.
	201,427	20 Downe be vaue	27	Chaine -	2/6/07/01/10/07 AM	10mat	4010	1000	4000				a ge through
and star	28,418	20 Double Bt Nave	14 114	(Deltre)	24,007 (10007 Mil	(Tread	1299	010	4044				The same
ALC: LOUGH	20, 10	22 Desire ht favor	10.00	1100	LAURY FURNITIAN	(Const.	4044	4014	4040				1.8.57
	28,410	(1) Dealths & Appen-	31	1000	100,001011100,01044	(Const.	4044	1010	4044				
	201.011	22 Trades \$1 Spain	101 108	Cisline .	Linuted House Advances	(Const.	(DMP)	-Dim-	-DMP				
	281+12	20 Doniel Bit Sport	1M 100	Codes	24,001411.0031444	(Const.)	-1044	-iDHP	ADMP-				
	78, 46	(2) David III Supplie	114 (104)	(later	Distance in case of the	17 mail	(Date)	down.	(Date)				
	28,494	"(1) Coulor MI Haven	14 100	Contract (Displayed of cauch and	12464	dam	- down	(Date)				
	20,40	In tradie to experi	15	20404	Artistical in solar and	12 mail	00	1010	1000				
	28,49	10 Daniel M Haven	a	2000	24cmmi Hostal Me	diant	00	(Dell	-(747				
	286,417	TEL Danies (M. Sautt	127	10000	SAUST FLORIDAN	(Crosse)	4294	40%	(Dept)				
	2014	(1) Danies Int report:	10 100	Colored	BACTORN FLORIDA MIL	(Const.	4299	1010	4DMP				
	210, 410	101 Davide (H. Naver-	10 10	Orme	DISTORT FUNCTION	(Cost)	4048	1049	40%				
	282.49	1942 Brown Taland Balance	4 24	1044	24,0019 120231 1944	(Const.	4040	1010	4040				
	(1) (m) (And Person Parlament Restored			Second company is not		1454	100	100				
	20147	(10) Drivey Daland Balance	1 108	10444	2/0.0719 11:00.07 AM	(Final)	12MP	1DHP	- uDHP				
	20141	(18) Brees Taland Statum	 (1)	10 million	Distance Homes And	(Course)	(DMP	(Dist	(Dur-				
	20.044	(11) Broad Taland Statement	+	12 March 10	Disality Hole IV AND	(Contract)	(DMP	dist.	(Dist)				
	80.45	(10) Dramy Dataset Statuses	(1 308)	1000	JACTOR COULD AND	(Projet)	404	0.0	4Dill*				
	81.45	174 Brees Tatent Balance	1	(Index	DALEYS IN MUCH AND	(Frend	-019	010	-01/P				
	202.47	(20) Browy Person Remain	1	(index	24,074110,07.84	(Frank	-044	104	4044				
	82.46	(10 hours Dated Street	4	1000	24,014 11 16,07 844	(Property)	1049	1014	10%				
	20.49	(10) Newsy Cadenal Testamore	(8) OF	Cides	DATES FOR AN	(Print)	4044	1040	dant.				
	82410	(14) Browy Datest Balance	10 108	Chilm	24,01101010-07.000	(Theat	-019	-017	1010				
	80.411	(10) Broats Forbard Dataset	11 38	10444	LIGHT FORTAGE	(Project	4044	4014	-0%				
	10.412	(10) Broats Dataset Balance	C12 (107	Chillen	SAUTON CONTRACT	(Dreed)	4044	42405	4048				
	201-912	1988 Brings Chapter Datum	08 09	1000	24,0018 https://aki	(Date)	104/P	1049	4019				
	207-816	1700 Kinaina Chalanat Balances	14	1144	LONGOOM TO DELL'AND	division.	1040	0.0	1010				
	20.415	100 Brany Codput Topone	16	(Critical	2010/01911 (10:07 444	Pine	1048	1048	040				
	262.416	1918 Broady Chalant Balance	16	Ordine	DRUDTH HUMIT AND	Clines	048	0.0	045				
	114 (30)	(10) Brury Dutest Between	17 .04	Ortice	Debaterie in labor And	(Phone	date	dour.	down				
	00.410	110 Brony Colord Balance	18	Order	2/6/07/9 11/18/27 AM	different.	de	00	00				
	an arts	And Association and Processor	14. 14	Sector 1	And Andrea Annual States	adding.	1.444	1000	date.				

Unsolicited Reporting

Unsolicited Reporting is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are reported to the SCADA-Master. This notification can be seen on the Master Analyzer. Figure 116 shows the SCADA Master Analyzer before any unsolicited reporting of binary input is in the OFF state.

Figure	116	Master	Analyzer	
--------	-----	--------	----------	--

Data Window - "De	fault" View										- 0	\times
File Options Vie	w											
🗄 🙀 Test Harriess		Channel	Session	Sector	Type	Number	Value	Rage	Time Updated	Description	Protocol Specific	e
i) V mDNP		mDNP	mDNP	N/A	[1] Brnary Inputs	0	Off	Online	06Feb1912:27:10.051 (reported)			
		mDNP	mONP	N/A	[1] Binary Inputs	1	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mDNP	N/A	[1] Binary Inputs	2	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mONP	N/A	[1] Binary Inputs	3	Off	Online	06Feb19 12:26:00.139 (assumed)			
		mDNP	mDNP	N/A	 Binary Inputs 	4	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mONP	N/A	[1] Binary Inputs	5	Off	Online	06Feb19 12:26:00.139 (assumed)			
		m DNP	mDNP	N/A	[1] Binary Inputs	6	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mONP	N/A	[1] Binary Inputs	7	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mDNP	N/A	 Binary Inputs 	8	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mDNP	N/A	 Binary Inputs 	9	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mDNP	N/A	 Binary Inputs 	10	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mDNP	N/A	 Binary Inputs 	11	Off	Online	06Feb1912:26:00.139 (assumed)			
Tax I am I am an	1	mDNP	mDNP	N/A	 Binary Inputs 	12	Off	Online	06Feb1912:26:00.139 (assumed)			
🛯 🔁 🖾 Modiły		mDNP	mDNP	N/A	 Binary Inputs 	13	Off	Online	06Feb1912:26:00.139 (assumed)			
Configuration Catio	-	mDNP	mDNP	N/A	 Binary Inputs 	14	Off	Online	06Feb1912:25:00.139 (assumed)			
Configuration Settin	6	mDNP	mONP	N/A	 Binary Inputs 	15	Off	Online	06Feb1912:26:00.139 (assumed)			
Description		mDNP	mDNP	N/A	 Binary Inputs 	16	Off	Online	06Feb1912:25:00.139 (assumed)			
PointNumber	0	mDNP	mONP	N/A	 Binary Inputs 	17	Off	Online	06Feb1912:26:00.139 (assumed)			
PointType	1	mDNP	mDNP	N/A	 Binary Inputs 	18	Off	Online	06Feb1912:26:00.139 (assumed)			
PointTypeName	Binary Inputs	mDNP	mONP	N/A	 Binary Inputs 	19	Off	Online	06Feb1912:26:00.139 (assumed)			
Misc		mDNP	mDNP	N/A	 Binary Inputs 	20	Off	Online	06Feb1912:25:00.139 (assumed)			
Flace	1	mDNP	mONP	N/A	 Binary Inputs 	21	Off	Online	06Feb19 12:26:00.139 (assumed)			
ReintTime	005-b 10 12-27-10 061	mDNP	mDNP	N/A	 Binary Inputs 	22	Off	Online	06Feb1912:26:00.139 (assumed)			
Point lime	00P60131227.10.001	mDNP	mONP	N/A	 Binary Inputs 	23	Off	Online	06Feb19 12:26:00.139 (assumed)			
Quality	Unine	mDNP	mDNP	N/A	 Binary Inputs 	24	Off	Online	06Feb1912:26:00.139 (assumed)			
Value	False	mDNP	mONP	N/A	 Binary Inputs 	25	Off	Online	06Feb19 12:26:00.139 (assumed)			
		mDNP	mDNP	N/A	 Binary Inputs 	26	Off	Online	06Feb1912:26:00.139 (assumed)			
		mDNP	mONP	N/A	[1] Binary Inputs	27	Off	Online	06Feb1912:26:00.139 (assumed)			
les cristice		mDNP	mDNP	N/A	[1] Binary Inputs	28	Off	Online	06Feb1912:26:00.139 (assumed)			
textual description of the	in an int	mDNP	mONP	N/A	 Binary Inputs 	29	Off	Online	06Feb1912:26:00.139 (assumed)			
sextual description of a	is point	mDNP	mDNP	N/A	 Binary Inputs 	30	Off	Online	06Feb1912:26:00.139 (assumed)			

1. Figure 117 shows that the binary input of the Slave is going to change. Initially, the value of binary input is OFF.

Figure 117 Slave Registers

		t and t													a defende a
		and has direct on													· IN the head
	1	T burnham		al later	T. Daller	7 1-		T. Sector	7 Ores 1		T. Sector		Description		
		The Real Property lies of the lease of the l			and the second second	No. of Concession, Name			The statement of the	and plant in the local		-			
N.	2.41	THE BOLLEN MALLER		124	Contra .	240,0000 102401 194	Inches	04	1040	016				-	A D DOMESTIC
	10.0	TT Shee Make		- 100	(mine	Discours showing mar	(Thinks	04	000	0.0					
100	20.42	TO Brune Insure	3	08	Coline 1	DAOTH LODALT PM	2744	cie	010	440					Lon
	22.44	TO Briats Insuits	4	08	Ontere	pages topatop	2044	04	0.0	000					
	21.45	111 Brian Mercele		108	Dates	216/0219 12/24/31 PM	STREET	104	610	de					
	31.40	101. Briaria Messala		100	(Driftree	2012/0119 10:24:21-PM	(Clinest	1010	iche	0.0					
	10.47	11 Brief Insult		128	Chilme	200301012220011254	0744	OF	CNP -	09					
	21.42	IT Brury Heads		108	Colorer .	28/01910/228311998	2744	100	614	04					
	21.07	TO BRAN HAVE		tim.	United	2/6/2015 12/26/31 PM	2719-03	1000	1010	674					
	31.410	273 Breary Inputs		108	Chaire .	Second Logest PM	2744	124	100	424					
	22 411	21 Brian Input	-10	07	Outree	DRUDIN UDKIT PM	074m	674	124	614					
	10.412	215 Brians Imputer	10	100	Dates	DRIVER LOAD MAN	504at	1294	674	124					
	10.412	25 Brees Import	10	109	Dates	24000 UDBJUM	1271404	1294	chir .	100					
	20-910	CTL Briefs Inputty	14	108	COMM .	24/0719 102421-294	277 Mart	0.00	1010	404					
	20.410	11 Bruy Input	+	100	Crow	Deligina submittee	(Plant	1294	1010	100					
	20.015	. (20 Briefs Hands	10	107	Done	2010/07/11/2017 (19)	277.944	1049	010	634					
	31.011	20 Bries Innote		108	Dillet	DAGETS GURSTIM	2044	4014	1014	474					
	21.412	10 Bridge March	18	100	Colleg-	24/071112/431244	2044	101	1014	494					
	21410	(1) Bries Make	11	108	Colory .	20,0019102621794	27544	1294	4240	634					
	21.422	21) Brian Hants		100	Conne	24/0119102431-956	10.644	014	634	400					
	34.427	10 Broat Insula	11	100	0.0ve	14/0019 1/pad1 He	2744	1010	4099	499					
	34.400	(1) Bruey report	- 10	100	1000	28/00191/2431198	274,4	100	4010	499					
	31.4(1)	(1) Brianis Hispotte	18	100	Ditte	24/0019103431364	27444	1294	1014	1254					
	31.430	(1) Anny Naver	34	108	Distance	2010010102431744	(These	12547	1014	104					
	10.423	21 Bruth Marrie	18	104 -	Crime	24/0019102431764	279.64	09	CHP	CHP .					
	34.420	TO Brues Marvin	- 14	10	Dotes	(A/27151(3431 PM	224.0	04	1010	099					
	1.422	11 Breas House	10	10	1000	14/0119 132431 PM	27944	104	1014	404					
	0.412	(1) Brokis Marcin		10	1000 m	LACENE LILLESE PM	2044	174	1014	04					
	P-4/0	The second second	24	-14	Trans.	04/079 122431 PM	1044	09	-010	434					
	20.400	11 Brief Teach		108	100mg	29/014 737431 (44	2744	674	010	ch4					
	AL 401	(Chines Needs	34.	100	Date	24/2010 102421-294	27444	104	014	49.0					
	80 M [2]	11 Briery Valette	- 14	.08	Date	28/0119102831294	2744	404	1044	104					
	30.431	101 Broats Materia	1.04	100	Dalara	2012010 102421 064	200 dead	1000	1040	200					

2. Figure 118 shows that the binary input of the Slave is changed from OFF to ON.

	- C	(NATE:											2 Names
1 Annual	in the second second	al ship of the lot spinst											· IB Ind Indent
		Participant Taxan			T Date	7 Terrar 7	-	T Date	T. Count	7 5 7	Law T	Description .	
100		and the second second		1.1	Contraction of the	the second second		10000	and sector sector		of the local division in which the local division in the local div		
0.41		Ultrary Name	18.	24	(Inline)	2012/01010 12/20/27 704	(Const.)	674	624	4294	1		 A C Include
8.42		Things insure /-	1	29	Trees	29,0010 122821-04	all state	4249	1000	424			And Date Street
8.43		Chruty Issue	- 4	08	Ordere	24,0014103431164	22 March	200	dag.	0.0			 2 44
22.94		Chown marks		08	Critere.	24/0819 12/24/11/94	10 mod	400	0.00	010			
21.93		Chrony reports	÷.	28	Delet	2/6/1016102401/964	17mm	-0147	- 624	100			
31.45		Chively Installe		28	Chine	216/001810240211964	12 month	1000	109	1000			
30.47	1.0	Chrwy ments	. F.	-104	Orlew	2/6/2019 12/24/21 /94	. IT is a	-679*	-674	-674			
21-12		Devely inputs .		104.1	Chieve	28-2818 1224 (1994	of the state of th	674	474	474			
10.07		Shree insuls	. 9	OF .	Orlea	5/6/2014 12:34:31 PM	(David	014	(Chr)	674 ⁴			
8.410		they would	10	04	Conteres	Wenterph upped the	The	014	014	-04			
10.411	- 1	Citrary Isolation	- 11	08	Orive	3/4/2014 122431-994	cone.	1000	1010	424			
20 410		C Brives Impoli	14	08	Ordina	2/0/2018 12:2421 994	Office .	1000	1016	510			
20.415		C Brown Haplets	10	08	Orlean	10/011103431064	(Creat		474	4249			
30.816		diver rent	18	.28	124848	28/2010/22431/996	UPrior.	674	- 574	-04			
30.413		C Browy Hypott	15	04	O-fee	10020310123431394	(Dist.)	4294	474	424			
21.415		Children Installe	- 16	-24	Orders	28/2010 121401104	(Date)	1014	494	434			
8.417		Spend and	;#t	24	13-dee	DAMES FOR STREET, PAR	227464	1210	1239	12147			
80.410		Chevro enviro	18	24	1100 m	242211122431744	(Press)	04	04	424			
2. *11		Chroniy Installe	18	104	Orient	24,0010122401-044	27964	-014	434	404			
31.411		Christin Industry	- 10	20	Chine	260010122401791	27%ed	-0747	474	474			
(0 A)		Clanks Ment	11	14	(blive	24/2014 (224)1 PM	27mm	404	404	4249			
21.411	10	C Brung Halurb	11	28.	(later	24/001012/01/PM	22404	0.00	010	010			
31401		Chines Melvill	-11		10.000	24/1014 12/4/1/M	CODE:	424	-04	-0#			
0.410		Chorej Inputo	-14	104	1949	24/1014 (32431-96/	Titles.	424	439	434			
0.43		(Bowy Agent)	15	-04	() data	28,001110,0401104	127 Mark	1000	14240	1010			
20.428		Citizen Inputi	14	0.0	(interest	2952014122421994	27 mod		-010	4049			
20.427		(Presidente	- P	-08	()-bra	24/2014 1224 (1994	22464	174	1094	1000			
89-403		Chevela Indexe		-100	10494	54/10141134011M	127464	1294	424	424			
30.628		Chinese Insurts	34	24	0.0+0	34,0014 (1343) /94	. IT had	-634	-624	-014			
20.000		Chives have	199	24	Other	34,00111340176	1044	-014	-034	-674			
20.401	- 1	Divers Insult	181	19	(346+8	28.0014122631796	These	-014	-074	-674			
21.411		Divest Insult		24	()-0+0	25.01111201794	The	014	-074	-074			
91.431		C Brudy Inquite		-08	Online	24,0014 (2243) (%)	27464	-CNP	1099	1094			 and the second sec

Figure 118 Change in Slave Register Value

3. Figure 119 show the Unsolicited Reporting on the analyzer. The value of Binary Inputs is changed and the same is reported to the Master.

Filmen Filmen Filmen Filmen Filmen	P so the P so the P so the	2 -Saure F -Saure F Special	States States & Same & Loss & Coll Data & Same & Loss & Coll	i V Secola V Secola	Clerite 1" Anne Antice Bachari	ante Complem direg									
Decision for Decision of the	- 		(1011110.1001> x000 1011110.1001> x000	00 2 1014	1 21 30 6	- Decid	ut «) diamet land tala	2							
200-0	w	S bertier	and Total Van			. Therefore	and a second second		240			_		×	
		In Spin	ni inni											and the second sec	
		Di 11 U		22222222222222222222222222222222222222		3mlpr 5.5 5.5 5.5 5.5 5.5 5.5 5.5 5.	Top: Strate Factor Strate Strate <td></td> <td></td> <td>Pag 344 344 344 344 344 344 344 34</td> <td>1 The Expert 1 The Expert 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 - 2 1 second of 1 For</td> <td></td> <td>Principal Sector</td> <td></td> <td></td>			Pag 344 344 344 344 344 344 344 34	1 The Expert 1 The Expert 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 1 2 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 2 3 - 2 1 1 second of 1 For 1 - 2 1 second of 1 For		Principal Sector		
			n B ann Bann taolt Dana (100 m) Dana Dana (100 part)	1221222222222222	222222222222	12.2 52.5 52.5 52.5 52.5 52.5 52.5 52.5	Brown Works	o esta concerta a	00000000000000000		$\begin{array}{c} {\rm High} (k \in \mathbb{C} \times $				
			10111110-1001 - 000 adam 10111110-2001 - 000 adam 10111110-2001 - 0	- 19-254.0		- 199	tratamit (8 kyra 10 ba 60 60 62 0								

SCADA Communication with Serial-based SCADA using Raw Socket TCP

IR510 Mesh Node Raw Socket TCP Client Configuration

As per the topology, the SCADA Master resides in the Control Center. Three step configurations on FND???

- 1. Creating the serial profile.
- 2. Linking the serial profile to the configuration template.
- 3. Pushing the configuration to the device.

The following serial configuration profile requires a mesh node to communicate with the SCADA Master.

- Peer IP Address–SCADA Master IP Address.
- Peer Port–SCADA Master Port Address, where SCADA Master is listening.
- Local Port-This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator.
- Packet Length & Packet Timer–Any integer value.
- Special Character-You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer.

Figure 120 IR510 Mesh Node Raw Socket Configuration

cisco FIELD NETWO	REDIRECTOR							(DRADIBHE	DEVICES	OPERATIONS -	CONFID - ADMIN-
ONITIO > DEVICE CONF	FIGURATION										
Aning Devices to Group	Charge Device Properties	Re= Souket	TCP Clust								
Groups	Config Profiles	- Saval Interface	Settings								
Configuration Profiles		Fort attnity	· DA Gal	www. O IOs No	te.	Port a settor	therty is only app go will not be up	acalle la gale ed	ways with IOx No	de Villen setts lOx s	ifferity, the following port
ENDPOINT		Mettia Type	83252		 Baudirate 	8620		(ii)			
· FUR PROFILE		D ma Bits	8		*						
 A second s		Parity	Note		+ Stop Bit	1		*			
# DECP PROFILE		Flow Control	lions		*						
 MANUT PROFILE 		DOCP Marking	Fpor mail		5						
 DHOP DUBNT PHOP 	1,3)	Rev Doubsil Sea									
 NOH PROFILE. 		TCP Idle Time Outlaiece)	Canned Time Subtress	Peer P Address	Peer Put	Local Peri	Pactel Lengthchites)	Packat Timer(ms)	Special Cr	ure-two(0.215)	Connection Type
 DHOP SERVER PRO 	FN.E.	1000	12	172.16.107.11	28099	280.00	512	500	48		TCP Client
· BERLAL PROPERTY									-		
Ba bigraten derten	4										
By Raw Second 120	P.										
D Detailt denial P	Tuttie										
Elips_Compute	Detai_Piolia										
Nov Securit 10	P-Diam										
Rew Sector TC	Player										
 ACLINIONAL 											

Legacy SCADA (Raw Socket TCP Server)

IR510 Mesh Node Raw Socket UDP Configuration

As per the topology, the SCADA Master is residing in the Control Center. Three step configurations on FND.??

- 1. Creating the serial profile.
- 2. Linking the serial profile to the configuration template.
- 3. Pushing configuration to the device.

The following serial configuration profile requires the mesh node to communicate with the SCADA Master:

- Peer IP Address–SCADA Master IP Address.
- Peer Port–SCADA Master Port Address, where SCADA Master is listening.
- Local Port-This Port signifies the Raw Socket initiator port number. In this case IR510 node is the Raw Socket initiator.
- Packet Length & Packet Timer–Any integer value.
- Special Character-You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer.

ISCO FIELD NETW	ORKORECTOR							112.00	200500000777	n anna anna an taonna amhann an	a contract of the second
NFIG > DEVICE CO	NEISURATION	The survey	TOTA NAME								
and sectors in Gauge	Conge Concer Property	NAME DOLLOT	PLF HEISE								
Groups	Contra Profiles	- Enviel Internation	Settings								
Configuration Profiles		Purt affecty	* DA Gat	eway 010x3	lode		Part a	Minity is only app 24 will not be use	incadria to gale ad	ways with IOs Node. When set to IO	affinity, the following port
INCPONT		Media Type	R5232			Baud rate:	9000				
AND PROPERTY		Data Bitu:	8								
a production sets.		Party	None			Ship Bit	1		*		
 DDCP PROFILE 		Flow Control:	None		1.4						
MARTPROFILE		DOCP Marking	Normal								
DHOP CLIDIT PRO	OF N.E.	Rear Social Sea	alana'.								
• SATA PROFILE		TOP Ide Time Outpace)	Connect Time Dut(secs)	Pair P Adde		PairPat	Linui Port	Pacent Length(butes)	Paceal Tenaronal	Special Character(0-258)	Convector Type
DHOP SERVER PR	OPER-	1000	8.	172.16.107.11		29000	28000	512	500	48	TCP Server
IERNA PROFILE										_	
Norstan-Ger	WF T									B	
In File Second	1D#										
The first and from	During										
and settings that	Here and the second										
Campo	An Sprint, Profile										
Rain (bouriet)	CP Cheit										
Ma How Secret 1	Ciff Server										
ADD INCOME.											

Figure 121 IR510 Mesh Node Raw Socket TCP Server Configuration

End-to-End Application Use Case Scenarios

This chapter includes the following major topics:

- Volt/VAR, page 127
- VAR Control (Power Factor Regulation), page 131
- Voltage Control (Conservation Voltage Reduction), page 140
- Fault Location, Isolation, and Service Restoration (FLISR), page 144

Volt/VAR

The main purpose of Volt/VAR Control (VVC) is to maintain acceptable voltage level at all points along the distribution feeder under all loading conditions. For optimizing the movement of electric energy, it is necessary to minimize the reactive power flows, which is done locally by reactive power compensation equipment such as capacitor banks.

The advanced VVO (Volt/VAR Optimization) application will be using a two-way communication infrastructure and remote control capability for capacitor banks and voltage-regulating transformers to optimize the energy delivery efficiency at distribution level. In fact, the reactive power flow creates a voltage drop on inductive element of wires. Therefore, in order to keep the voltage always within certain limits, the reactive power flow and voltage control must be considered together, as we call it VVC (Volt/VAR Control). For the voltage and reactive power control, load tap changer (LTC) transformers, switched shunt capacitors, and step voltage regulators are used. A minimum requirement for voltage control is the possibility for the operator to maintain the voltage on the feeder at an acceptable range by changing the position of the movable tap changer on a voltage regulator.

Note: Volt/VAR Control = Power Factor Regulation + Conservation Voltage Regulation

Please refer to the Design Guide for more information about the Volt/VAR architecture and infrastructure setup.

For this implementation guide, we have chosen the radical feeder setup for simulating the Volt/VAR use case.

Volt/VAR Devices

All the devices involved in Volt/VAR use case are listed in Table 19.

Table 19 Volt/VAR Devices

Device	Location	Description
End of Line Voltage Monitor	At 1.0 in Feeder line	Monitors the end of the line voltage
CBC 1	At 0.25 in Feeder line	Monitors the voltage and On/Off CapBank
CBC 2	At 0.50 in Feeder line	Monitors the voltage and On/Off CapBank
CBC 3	At 0.75 in Feeder line	Monitors the voltage and On/Off CapBank
Load Tap Controller	At Substation	Raises/lowers load tap
Substation Meter	At Substation	Monitors substation device status/reading

Data Points

All the data points involved in Volt/VAR use case are listed in Table 20:

Table 20 Volt/VAR Devices Data Points

Device	Register Type	Description
End of Line Voltage Monitor	Analog Input	Voltage at End of line
CBC 1	Binary Output Statuses	CBC - Status
	Analog Input	Voltage at CBC
CBC 2	Binary Output Statuses	CBC - Status
	Analog Input	Voltage at CBC
CBC 3	Binary Output Statuses	CBC - Status
	Analog Input	Voltage at CBC
Load Tap Controller	Analog Input	LTC Position
	Binary Output Statuses	Raises LTC
	Binary Output Statuses	Lowers LTC
Substation Meter	Analog Input	Power (kW)
	Analog Input	Q-Power (kVAR)
	Analog Input	Power Factor
	Analog Input	Losses (kW)
	Analog Input	Substation Meters

Volt/VAR Use Case Simulation Components

The Volt/VAR use case is simulated using TMW's DTM application and the entire event sequence of the Volt/VAR use case is simulated using Java script. Table 21 describes the components involved in the Volt/VAR simulation:

Table 21 Volt/VAR Simulation Components

Role	Component / Application	Description	Version
SCADA Control Center	TMW's DTM application	Triangle Microwork's DTM application is used to simulate the SCADA Control Center functionality.	DTM v1.3.1.4
Outstation Devices / IEDs	TMW's DTM application	Triangle Microwork's DTM application is used to simulate the Outstation/IED devices.	DTM v1.3.1.4

SCADA Control Center General Configuration

The following steps detail the common SCADA Control Center Configuration for Volt/VAR Control and FLISR use cases.

1. Choose the DTM Role as DTM Master from the Tools > Configure DTM Services menu.

Figure 122 DTM SCADA Control Server Role



2. Choose the correct network interface adapter in the Adapters tab.



Figure 123 DTM SCADA Control Center Adapter Configuration

The chosen network interface adapter would be used for communication between the DTM Master and the DTM Slave/Client PC.

Outstation General Configuration

Outstation or IEDs are configured in the DTM machine. There are five IEDs and one substation-monitoring device. All six devices are simulated in TMW's DTM application.

1. Start the DTM service in the client machine with the role as Client, and the Master IP pointing to the SCADA Control Center.

Figure 124 DTM Outstation Role

Adaptor	s Service	s Logging				
Configure this co	mputer as the l	DTM Master				
Listen on Port	-4048					Lizzenie -
			service and the service of the servi			
		uttine a verking a	surgester.			
 Automatically Must chosen pit 		utti olim loading a otting a norkipasa				
Workspace Folder		ott viten hading a etting a norkipasa eta Kalega Marowa	aisi DNA DNAasage/We			
Workspace Folder	mputer as a DT	enting a nerkipala Maturia di Norkipala Maturia	nin var e del DTM DTMange/Wa			
Workspace Folder Configure this co DTM Master Hos	mputer as a DT t or IP Address	M Slave 10.64.66.51	DTM Master Po	ort 42,145	:	

Note: When the DTM Master is loaded with the Volt/VAR workspace and the DTM service is started in the Client, then the outstation configuration is also automatically loaded into the client machine.

Outstation or IEDs data points per the following details.??

Name T	Point Type 🛛 🗑	1 1	٣	Value T	Quality 🔻	Device T	Channel 1	Y
LTC Tap Raise	[10] Binary Output Statuses	0		Off	Online	LTC Controller	sDNP	
LTC Tap Lower	[10] Binary Output Statuses	1		Off	Online	LTC Controller	SDNP	
LTC Tap Poistion	[30] Analog Inputs	0		0	Online	LTC Controller	sDNP	
Power (kW)	[30] Analog Inputs	0		1	Online	Substation Meter	SDNP	
Q-Power (kVAR)	[30] Analog Inputs	1		1	Online	Substation Meter	sDNP	
Power Factor	[30] Analog Inputs	2		1	Online	Substation Meter	sDNP	
Losses (kW)	[30] Analog Inputs	3		1	Online	Substation Meter	SDNP	
Substation	[30] Analog Inputs	4		0	Online	Substation Meter	SDNP	
Cap Bank Controller 3 Status	[10] Binary Output Statuses	0		Off	Online	Cap Bank Controller 3	sDNP	
Cap Bank Controller 3	[30] Analog Inputs	0		0	Online	Cap Bank Controller 3	sDNP	
End-of-Line Voltage Monitor	[30] Analog Inputs	0		0	Online	End-of-Line Voltage Monitor	SDNP	
Cap Bank Controller 2 Status	[10] Binary Output Statuses	0		Off	Online	Cap Bank Controller 2	SDNP	
Cap Bank Controller 2	[30] Analog Inputs	0		0	Online	Cap Bank Controller 2	SDNP	
Cap Bank Controller 1 Status	[10] Binary Output Statuses	0		Off	Online	Cap Bank Controller 1	SDNP	
Cap Bank Controller 1	[30] Analog Inputs	0		0	Online	Cap Bank Controller 1	SDNP	

Figure 125 DTM Outstation Data Points

VAR Control (Power Factor Regulation)

VAR Control is achieved with the CBC On/Off operation.

Event Sequence Diagram

Figure 126 Volt/VAR–VAR Control Sequence Diagram 256670

Use Case Steps

- 1. Event class data poll to the following devices from RTU:
 - Substation meter, poll Measured Value (Analog Input) registers.
 - All CBC(s), poll Measured Value (Analog Input), and Binary Output Statuses Point registers.
 - End-of-Line voltage monitor, poll Measured Value (Analog Input) register.
- 2. The Volt/VAR Optimization processor processes the data received from the devices and makes a control command decision based on the power factor calculation.
- 3. The control command sent to RTU via SCADA to capacitor banks to close CBC N by writing in a Control Relay Output Block (CROB) command register in DNP3.
- 4. Event class data poll to the following devices from RTU:
 - Substation meter, poll Measured Value (Analog Input) registers
 - All CBC(s), poll Measured Value (Analog Input) and Binary Output Statuses Point registers
 - End-of-Line voltage monitor, poll Measured Value (Analog Input) register
- 5. The above steps are repeated to the CBC on the feeder line to maintain Power Factor value always close to value 1.

VAR Control Use Case Simulation

1. Import the Volt/VAR workspace, which is available in Appendix E: HER and CGR Configurations, page 250.

Figure 127 DTM Import Workspace



2. Start all the host machines.

Figure 128 DTM VVC Start All Hosts



3. Update the Remote IP address of all the RTU devices.

Figure 129 DTM VVC Channel IP Config

Cap Bank Controller 1	DNP3 Channel Editor
Cap Bank Controller 2 Cap Bank Controller 2 Cap Bank Controller 3 Cap Bank Controller 3 Cap Bank Controller 3 Cap Cap Bank Controller 3 Cap Cap Controller Cap Controller	Channel Name Cap Bank Controller 1 Behavior All Master Monitor Peer Slave Unknown Connection Type Serial TCP/IP TCP/IP and UDP Connection Properties Server/Client Mode IP Address Mode
Simulation Monitor Display.tgf	Client Server IPv4 IPv6 Assign IP Addresses
Substation Meter	Local Address 172.16.107.50 *
Outstations	Remote Address 10.153.10.13
UTC Controller	Port 20,000
Substation Meter	
Cap Bank Controller 1	
Cap Bank Controller 2	
Cap Bank Controller 3	
End-of-Line Voltage Monitor	

4. Make sure all the channels are connected.

Figure 130 DTM VVC Channel Status



Figure 131 DTM VVC Start All Scripts



6. Start the simulation by clicking Auto Play or Next.

Figure 132 DTM VVC Simulation Auto Playscript



20092

7. Initialize the Outstation data points to default values.

Figure 133 DTM VVC Data Points Initialization



The substation meter data are initialized to zero before starting the VVC simulation.

8. Data points from the two CSV files are applied appropriately by the simulation script to simulate the real time Volt/VAR events sequence.

Figure 134 DTM VVC Event Class Polling



- 9. Verify the voltage drops along the feeder line, as shown in Figure 134. Also, verify that substation meter values are not zero values.
- **10.** The Volt/VAR Optimization processor processes the data received from the devices and makes a control command decision based on the power factor calculation.
- 11. The control command is sent to RTU via SCADA to capacitor banks to close the CBC3.

Figure 135 DTM VVC CBC Closing



0,4450

12. Verify the CapBank is ON, as shown in Figure 135.

13. Event class data poll to the following devices from RTU:

- Substation meter, poll Measured Value (Analog Input) registers
- All CBC(s), poll Measured Value (Analog Input) and Binary Output Statuses Point registers
- End-of-Line voltage monitor, poll Measured Value (Analog Input) register



Figure 136 DTM VVC Event Class Polling with CBC3 Closed

With CBC N On, voltage drop level decreased and power factor value increased.

14. All the above steps are repeated to all the CBCs on the feeder line to maintain a Power Factor value always close to 1 at all the points in the feeder line.

256446

Figure 137 DTM VVC All 3 CBC Closed



- 15. Verify that all the CBCx are ON and power factor is increased to 99.1%.
- 16. To stop the simulation, re-click Auto Play.
- 17. To re-start the simulation, click Restart.

Voltage Control (Conservation Voltage Reduction)

Conservation Voltage Reduction (CVR) can be achieved by moving the LTC up or down to maintain the Power Factor close to 1.

Event Sequence Diagram

Figure 138 Volt/VAR–CVR Sequence Diagram



Use Case Steps

- 1. Event class data poll to the following devices from RTU:
 - Substation meter, poll Measured Value (Analog Input) registers
 - All CBC(s), poll Measured Value (Analog Input) and Binary Output Statuses Point registers
 - End-of-Line voltage monitor, poll Measured Value (Analog Input) register
- 2. The Volt/VAR Optimization processor processes the data received from the devices and makes a control command decision based on the power factor calculation.
- 3. Control command sent to RTU via SCADA to the LTC to lower/raise LTC.
- 4. Event class data poll to the following devices from RTU:
 - Substation meter, poll Measured Value (Analog Input) registers
 - All CBC(s), poll Measured Value (Analog Input) and Binary Output Statuses Point registers
 - End-of-Line voltage monitor, poll Measured Value (Analog Input) register
- 5. All the above steps are repeated to maintain Power Factor value always close to value 1.

CVR Use Case Simulation

- 1. Follow Steps 1 to 8, under CVR use case simulation.??
- 2. The Volt/VAR Optimization processor processes the data received from the devices and makes a control command decision based on the power factor calculation.
- 3. Control command sent to RTU via SCADA to the LTC to lower/raise the LTC by writing in a command register. The LTC is lowered to -2, by the script.

Figure 139 DTM CVR LTC Lowering



4. Event class data poll to the following devices from RTU:

- Substation meter, poll Measured Value (Analog Input) registers
- All CBC(s), poll Measured Value (Analog Input) and Binary Output Statuses Point registers
- End-of-Line voltage monitor, poll Measured Value (Analog Input) register





5. Verify that the data from feeder devices (extreme right window) are updated in SCADA control center and that graphs and substation meter values are displayed.

All the above steps are repeated to maintain Power Factor value always close to 1 at all points in the feeder line.

Distribution Automation Use Case Scenario - FLISR

Figure 141 DTM CVR End of Simulation



6. Verify that the outstation device data are updated to SCADA Control Center and the Power Factor values to 1; in the above example, the Power Factor value is 0.992(99.2%).

Distribution Automation Use Case Scenario - FLISR

Fault Location, Isolation, and Service Restoration (FLISR)

Fault Location, Isolation, and Service Restoration (FLISR) is the process for dealing with fault conditions on the electrical grid. When a fault occurs in a section of the grid, first identify fault location and isolate the smallest possible section affected by the fault. Then restore the power to larger possible section of the grid.

The goal of the FLISR to minimize the fault affected area with very short turnaround time by identifying the fault location, isolating the fault section, and restoring the power to the remaining section of the grid within a short turnaround time.

Note: Prerequisite for executing the FLISR use case is stable CR mesh in which two-way communication between Headend to DA gateway IR510 device. Refer section "Solution Network Topology and Addressing for FLISR validation, page 14" in this document.

Schweitzer Engineering Laboratories (SEL) Devices

SEL FLISR products works reliably with the Cisco Resilient Mesh network, in aspects of tripping time, data alignment, service restoration and operation consistency on ISM 902-928MHz and IEEE802.15.4g/e standard using OFDM modulation with a physical data rate up to 1.2 Mbps can support the performance requirements of FLISR application.

This guide captures the configuration and simulation of SEL FLISR application on Cisco Resilient Mesh with physical data rate of 800kbps, over a variety of topologies and places in the network.
All SEL devices and application involved in simulating the FLISR use case are listed in the below table.

Table 22 SEL devices		
Device	Location	Description
SEL RTAC - 3505	IED	Simulates recloser controller
SEL RTAC - 3530	Substation/ Control Center	Distribution Automation Controller (DAC)

Table 23 SEL Software

Device	Version	Platform	Description
SEL AcSELerator	R144	Windows 64bit	Used for FLISR project and use case simulation
SEL projects	R144_20191106	SEL RTAC 3530/3505	FLISR logics and device configuration

Urban topology

Electrical line diagram

The one-line diagram for the urban topology, including four feeders that were interconnected between them with reclosers in Normal Open state (green box) is shown in the figure below.





The legend for the FLISR electrical line diagram is below.

Figure 143 FLISR electrical line diagram legend



Each feeder capacity was designed for 540A and it was sourced from an independent transformer. Substation breakers located at the beginning of each feeder offered protection for the entire distribution line. Different loads were placed on the feeders so that the SEL FLISR controller can select the most optimal feeder as the next power source during an outage and service restoration phase.

Aggregate topology lab setup

Below topology captures the 1 to 1 mapping of SEL recloser devices to Cisco's IR510 devices. The controller device is located in the Primary control center. CR Mesh is aggregated at the Field Area Network aggregator (using CGR1000 series of router) which could be located in the substation. The communication between substation and control center could happen over public/private WAN. The SEL device is positioned behind IR510 and connected using Ethernet.





Table 24 FLISR Urban Topology Components

One-Line Diagram Dev Label	SEL Name	Mesh Node	Mesh Node Hop Depth
Rec1	SEL3505-1	IR510-1	1
Rec6	SEL3505-6	IR510-12	1
Rec9	SEL3505-9	IR510-13	1
Rec2	SEL3505-2	IR510-21	2
Rec7	SEL3505-7	IR510-22	2
Rec10	SEL3505-10	IR510-23	2
Rec4	SEL3505-4	IR510-32	3

Rec8	SEL3505-8	IR510-33	3
Rec3	SEL3505-3	IR510-4	4
Rec5	SEL3505-5	IR510-42	4
DA Controller fro FLISR	SEL3530-2	N/A	N/A

Rural topology

Electrical line diagram

This section explains the linear CR mesh deployment scenario, the below electrical diagram depicts the linear deployment scenarios, which is simulated over 10 SEL reclosers between two substations where the recloser Rec6 was in Normal Open state (NO) while all other reclosers were in Normal Close state (NC).

Figure 145 FLISR Rural electrical line diagram



Linear topology lab setup

The SEL reclosers were still connected via the Ethernet to each Cisco IR510 and all the IR510 devices are connected in linear CR mesh with following configuration.



Figure 146 FLISR linear topology lab diagram

Refer to Linear Mesh lab topology for FLISR section of this document for more details about this lab topology.

FLISR simulation network

FLISR simulation network is used for transporting FLISR events simulation traffic SEL RTAC 3505 and SEL RTAC 3530, which act as a DA Controller.

SEL RTAC 3530 was installed in the Control Center. The FLISR controller (DA FLISR Controller) was configured to communicate with each SEL RTAC3505 and work as a system to perform Service Restoration also known as Circuit Reconfiguration during a grid outage event.

A second SEL RTAC3530 (DA Simulator) was used to simulate different grid conditions and to create different failures over a dedicated network called Simulator Ethernet Network, which is depicted as red line. A laptop running the SEL AcSELerator software is used for SEL device configuration, FLISR topology monitoring and fault simulation.

The red line in below figure represents the Ethernet network, which is used for out-of-band communication for FLISR events simulation. The OT traffic of actual FLISR events are communicated through in-band via Cisco CR mesh to DAC and vice versa. All in-band communication is via Cisco CR mesh and FLISR events simulation uses out-of-band communication via Ethernet.



Figure 147 FLISR simulation network

The SEL RTAC 3505 controllers are used in our lab validation instead of real SEL-651R reclosure electrical device. The SEL 651R device functionality and features are emulated in SEL RTAC-3505 devices to generate typical FLISR events and OT communication traffic in our lab environment, without connecting to actual electrical power grid.

FLISR Event Sequence Diagram

Figure 148 FLISR event sequence diagram



Use Case Steps

- 1. Class 123 Read happens every 60 seconds. For each Class read, there is a Response from IED. There is also Class0123 periodic poll, but with a longer duration than the class 123. This Class 0123 polling may or may not fall within the time duration of actual FLISR event sequence.
- **2.** Unsolicited Response happens whenever any change in value of DNP3 point list in IED. For each Unsolicited Response from IED, there is a Confirmation message from DAC.
- 3. On receiving the Unsolicited Response from IED, the DAC sends a Control Command Select to selective recloser(s) to block for sending the actual control command. For each Select command, there is a Response from IED/Recloser.
- **4.** After successful Select command, the DAC sends the Control Command Operate to selective recloser(s) to Open/Close. For each Operate command, there is a Response from IED/Recloser.

 After successful control command operation, confirmation of IED/Recloser status shall be updated by Unsolicited Response and overall grid status is updated by another Class 0123 Read operation. For each Class Read, there is a Response from IED/Recloser.

FLISR USE CASE SIMULATION using SEL AcSELerator application

This section describes the validation efforts conducted indoor for testing Fault Location, Isolation, Service Restoration (FLISR) using Schweitzer Engineering Laboratories (SEL) equipment. SEL is one of the major utility grid equipment and DA solution vendor in North America.

SEL RTAC 3530/3505 initial configurations Schweitzer Electric Laboratories (SEL) has a comprehensive solution for the DA FLISR application that can be deployed in distributed or centralized architectures. The solution uses a controller device to provide advanced restoration capabilities that can be located in the distribution substation or control center. Combined with Cisco Resilient Mesh communication infrastructure the FLISR application can operate in fully automatic mode.

The SEL reclosers connect to the Cisco Resilient Mesh Industrial Routers (IR510) via ethernet port.

The SEL FLISR was tested in a Centralized configuration where a SEL RTAC 3530 was installed in the Control Center. The FLISR controller (DA FLISR Controller) was configured to communicate with each SEL RTAC3505 and to work as a system to perform Service Restoration also knows as Circuit Reconfiguration during a grid outage event. A second SEL RTAC3530 (DA Simulator) was used to simulate different grid conditions and to create different failures over a dedicated network called Simulator Ethernet Network. A laptop running the SEL AcSELerator software was used for SEL device configuration, FLISR topology monitoring and fault insertion.

Refer to the Design document for more information about the FLISR architecture and infrastructure setup.

Note: For additional information on the SEL RTAC product family, visit: https://selinc.com/products/3530/

When SEL devices are not available FLISR use case shall be simulated using the TMW DTM application, refer to Appendix F: FLISR Simulation using DTM, page 264 for more detail.

SEL RTAC Ethernet Interface Configuration

- 1. Use the included USB cable to connect your computer to the type-B USB port on the front of the RTAC.
- 2. Follow the prompts to install the USB driver. The USB driver provides an Ethernet connection to the RTAC.
- Type the USB default IP address https://172.29.131.1 to access the secure RTAC web interface using any web browser.

Figure 149 SEL RTAC Web page login

📧 Schweitzer Engineering Laborat X	+	
← → ♂ ☆	0 🔥 https://172.29.131.1	
SEL		
	User Login Usemame: admin Password: ••••••• Login	Web Access For Authorized Personnel Only This system is for the use of authorized personnel only. Individuals using this device are subject to having their activities monitored and recorded. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals usage in excess of authority or criminal intent, then the evidence shall be provided to law enforcement officials.

If accessing the web page of the device for the first time, the web page prompts the user to create username and password. After the username and password are created, the same credentials can be used to access the web page on subsequent visits.

4. Click the Interface Under Network tab on the left panel.

Device: SEL-3	530-4-0030A7	1DFCD7		0.00			admin (
Navigation 4							
Dashboard	Network	Settings					
System	List Inte	erface Settings Edit	Global Settings				
ate/Time	Hostnam	ne					
evice Management le Manager	SEL-3530	0-4-0030A71DFCD7					
roject Upload	Socket T	CP Keep Alive Time (se	econds)	Socket TCP Keep Alive I	Interval (seconds)	Socket TCP Keep Ali	ve Probes
cionseo reacores	10			10		5	
USEF Accounts Jser Roles	Interfa	ces					
DAP Settings ADIUS Settings	Status	Interface Name	IP Address	Default Gateway	MAC Address	Enable Ping Enable Database Access Enable Web Access	Options
etwork terface		Eth_01	172.18.107.61/24	172.18.107.1	00:30:a7:1d:fc:d7	True True True	Edit
tatic Routes losts		Eth_02	172.168.100.21/24		00:30:a7:1d:fc:d8	True True True	Edit
ecurity		USB_81	172.29.131.1/24		00:30:a7:1d:fc:db	True True True	Edit
509 Certificates A Certificates SH Keys assword Report							

Figure 150 SEL RTAC Ethernet interface details

There are three ethernet interfaces available in the SEL-RTAC device, one is used for USB console port, which the user using it to configure the device via the web page. On the other two ethernet ports, Eth1 is used to connect to IR510 and Eth2 is connected to the FLISR simulation network.

- 5. Click on Edit button against the Eth1 interface, to edit the network information for that interface.
- 6. Edit the first interface with Control Center IP/ IED IP.

Figure 151 SEL RTAC IPv4 settings for CR Mesh

IPv4 Address Settings			
Enable DHCP			
IP Address: 172 . 18 . 107 . 61 / 24 v			
Default Gateway: 172.18.107.1	Primary Gateway		
		Submit	Cancel

Configure the Control Center IP for the SEL RTAC 3530 device, which acts are a DAC Controller.

For the other SEL RTAC 3530 device which acts as a Simulator, no configuration is required.

For all SEL RTAC 3505 devices, configure this interface with CR Mesh IP network address and gateway as the IR510 interface IP.

7. Edit the second interface with FLISR simulation IP subnets.

Figure 152 SEL RTAC IPv4 settings for FLISR simulation

Enable DHCP			
IP Address:			
Default Gateway:	Primary Gateway		
		Submit	Cancel

Configure the second Ethernet interface Eth2 with the FLISR simulator network interface for all the SEL RTAC devices.

FLISR Project setup

SEL developed a comprehensive FLISR projects for the two topologies, Urban and Rural topologies. SEL provides set of project files for both these topologies, which needs to be pushed to the SEL RTAC devices before executing the FLISR use case simulation. The details and usage of these project files are listed below in the table

Device	Platform	Description
CISCO_DAC_3530_R144_20191107 _Topology_1	SEL-RTAC 3530	Used for DAC/SCADA server for Rural or Linear CR Mesh topology.
CISCO_DAC_3530_R144_20191107 _Topology_2	SEL-RTAC 3530	Used for DAC/SCADA server for Urban or Aggregate CR Mesh topology.
CISCO_Simulator_Adapter_v2_3530 _R144_20191107_Topology_1	SEL-RTAC 3530	Used for simulating the FLISR use case events for Rural or Linear CR Mesh topology.
CISCO_Simulator_Adapter_v2_3530 _R144_20191107_Topology_1	SEL-RTAC 3530	Used for simulating the FLISR use case events for Urban or Aggregate CR Mesh topology.
CISCO_RecN_3505_R144_2019110 6	SEL-RTAC 3505	Used to emulate Recloser and Recloser Controllers. Where, N is number represent Recloser position

Table 25SEL Project files details

These project files shall be provided by the SEL team.

User should push all Recloser files to all the SEL RTAC devices, the Recloser project is same for both the topologies. But the DAC and Simulator file are loaded based on the topologies under testing.

To push the project file to the SEL RTAC devices, follow the steps described in the Simulation Go Online section.

1. AcSELerator Application login.

Figure 153 SEL AcSELerator application login

Connection	RTAC Default Co	nnection	
Server	localhost	Port	5433
Database	RTAC		
User Name	admin		
Password	****		

By default, the username is admin and password shall be shared by SEL team.

2. To import FLISR projects into the application, click on SEL icon and select Import.

Figure 154 FLISR Project Import menu

New	Database: RTAC@localhost
Import Items	
Export Items	
Close Project	
Save	6
Save As	
Import	Import (Ctrl+Alt+I)
Export	Import an AcSELerator RTAC project into the database.
Read	
Send.	
Manage Libraries	
Exit Application	

3. Choose SEL project files from the local machine to import into the application. Multiple files can be selected and imported all at once.



Timport AcSELerator RTAC Project			×
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This PC \rightarrow C	OS (C:) > Ashok > SEL > sel-project-files > 20191108_FilesForCisco >	✓ ひ Search 201911	08_FilesForCisco 🔎
Organize 👻 New folder			📰 🕶 🔲 😢
📙 20191108_FilesForCisco 🖈 ^	Name	✓ Date modified	Туре
📙 sel-applicationProfiling- 🖈	Network Data Flow	2019-11-11 10:45	File folder
segment_6	CISCO DAC 3530 R144 20191107 Topology 1.exp	2019-11-07 17:14	EXP File
segment_9	CISCO_DAC_3530_R144_20191107_Topology_2.exp	2019-11-07 16:37	EXP File
segment 10	CISCO_Rec1_3505_R144_20191106.exp	2019-11-06 16:55	EXP File
segment 11	CISCO_Rec2_3505_R144_20191106.exp	2019-11-06 16:56	EXP File
	CISCO_Rec3_3505_R144_20191106.exp	2019-11-06 16:57	EXP File
OneDrive	CISCO_Rec4_3505_R144_20191106.exp	2019-11-06 16:57	EXP File
This PC	CISCO_Rec5_3505_R144_20191106.exp	2019-11-06 16:58	EXP File
3D Objects	CISCO_Rec6_3505_R144_20191106.exp	2019-11-06 16:58	EXP File
	CISCO_Rec7_3505_R144_20191106.exp	2019-11-06 16:59	EXP File
Desktop	CISCO_Rec8_3505_R144_20191106.exp	2019-11-06 16:59	EXP File
Documents	CISCO_Rec9_3505_R144_20191106.exp	2019-11-06 17:00	EXP File
👆 Downloads	CISCO_Rec10_3505_R144_20191106.exp	2019-11-06 16:56	EXP File
b Music	CISCO_Simulator_Adapter_v2_3530_R144_20191107_Topology_1.exp	2019-11-07 17:15	EXP File
Pictures	CISCO_Simulator_Adapter_v2_3530_R144_20191107_Topology_2.exp	2019-11-07 16:39	EXP File
sel on ASTHIRUG-M-K1YT			
🗧 Videos			
Y	<		>
File name:		✓ AcSELerator R	TAC Exports 🗸 🗸 🗸
		Open	Cancel

4. To import DAC Libraries into application, click on SEL icon and then select Manage Libraries.

Figure 156 FLISR DAC Manage Library menu item

New		Database: RTAC @kcalhist	
marth	-		
Expert the			
Cine Pro	d.		
Save	•		
346(74)			
Import			
Export			
Read			
-			
ManageL	braries	Hanage Libraries Datal, uninstal libraries	
Exit Apple	ation		

Libraries can only be imported one at time. Multiple file import is not supported. User need to wait for the first file import to complete, before importing the second file.

5. Click on Install New.

Figure 157 DAC Library installation

1	Manage Logic Engine Libraries	×
	Installed Libraries	
	Installed Libraries SEL DynamicDisturbanceRecorder 3.5.0.0 SEL Dictionaries 3.5.1.0 SEL Dictionaries 3.5.0.1 SEL CrossTaskData 3.5.0.0 SEL CrossTaskData 3.5.0.3 SEL CrossTaskData 3.5.0.1 SEL CrossTaskData 3.5.0.2 SEL ChannelMonitoring 3.5.1.1 SEL ChannelMonitoring 3.5.0.0 SEL AnalogCond 3.5.1.1 SEL AnalogCond 3.5.1.1 SEL AnalogCond 3.5.1.1 SEL AnalogCond 3.5.1.1 SEL AnalogCond 3.5.1.0 SEL AnalogCond 3.5.1.0 SEL DynamicDisturbanceRecorder 3.5.1.0 SEL DynamicDisturbanceRecorder 3.5.1.0	Uninstall
	SEL DynamicDisturbanceRecorder 3.5.2.1	

Note: Initially, there are not any SEL DAC library selections in the window. The user must click **Install New** to install new DAC libraries into the SEL application and make them available in the Manage Library window.

6. Choose library files to Import.

Organize 👻 New folder		
· · · · · ·		100 v 💷
Name	Date modified	Туре
Cuick access Network Data Flow	2019-11-11 10:45	File folder
OneDrive DA_Adapter_v2.5.4.compiled-library	2019-08-14 07:49	COMPILED-LIBRARY File
This PC DA_Library_v4.5.4.compiled-library	2019-08-14 07:49	COMPILED-LIBRARY File
DA_SIM_UB_3_v1.4.0.compiled-library	2018-11-08 14:31	COMPILED-LIBRARY File
DA_SIM_LIB_3_v1.4.1.compiled-library	2019-03-21 05:52	COMPILED-LIBRARY File
Documents		
Downloads		
Music		
E Pictures		
sel on ASTHIRUG-M-K1YT		
🖥 Videos 🗸 K		
File name: DA Adapter v2.5.4 compiled-library	~	All Library Files (*.library: *.com

Figure 158 DAC Library files

The four library files in the table below must be selected and installed one at a time.

Device	Description
DA_Adapter_v2.5.4.compiled library	Used for FLISR use case simulation.
DA_Library_v4.5.4.compiled library	Used for FLISR use case simulation.
DA_SIM_LIB_3_v1.4.0.compiled library	Used for FLISR use case simulation.
DA_SIM_LIB_3_v1.4.1.compiled library	Used for FLISR use case simulation.

Table 26 SEL DAC Library details

7. Load project file.

Figure 159 Load FLISR project

		SEL AdSELerato	RTAC					- 0	×
OCL									- 😡 v
REAL SECTION	1619						S	EL) 👬	WEITZER NICERING SAAFORIES
New Project		Projects						V 910	Tree
		Drag a column header here to group by that column							
		Name	Description	Lest Editor	Last Arressed	SL Ve	rson 87.4C Type		
BACK		CISCO_DAC_3530_8144_20191107_Tearlings_1		athin	4/18/0020 11:48 AM	81	HA REAC, Dates		
New SEL RTAC R	Read SEL RTAC	CISCO_DAC_3530_R144_20191107_Tepelegy_2		admin	1/21/0020 2:32 PM	81	HI RTAC/Asian		
Project	Settings	CISCO_01P_Menter_20200227		admin	2/28/29/29 8:40 PM	83	RTAC/Autor		
		CISCO_DIP_Outstation_A_20200227		admin	2/28/2020 0:35 PM	83	901-3505		
Applications		CISCO_01POutstation_8_2000028		admin	3/28/2020 0:34 PM	81	901-3505		
Papersona		CISCO_Rec1_3505_R144_30191106		admin	4/18/2020 12:24 PM	RS	44 501-3505		
		CISCO_Rec10_3505_R144_20191106		admin	2/18/2020 3:37 PM	83	44 581-3505		
S (S)		CISCO_Rec2_3505_R1+H_20191106		admin	3/9/2020 2:46 /94	8.	HI SEL-3505		
		CISCO_Rec3_3505_R1+H_20191106		admin	3/8/2020 10:49 AM	83	44 581-3505		_
SEL Company		CISCO_Rect_3505_R144_20191106		admin	2/18/0020 3-19 PM	A.1	44 581-3505		
		CISCO_Ret5_3505_R144_20191106		admin	2/18/2020 3:21 PM	83	981-3505		
		CISCO_Red6_3505_R344_30191306		admin	2/18/2020 3:24 PM	83	981-3505		
		CISCO_Rec7_3505_R344_20191306		admin	2/18/2020 3:27 PM	83	H4 98L-3985		
		CISCO_Reck_3505_R344_30191106		admin	3/18/2020 3:29 PM	83	981-3985		
		CISCO_Rec9_3505_R344_30191106		admin	2/18/2020 3:33 PM	RS	44 981-3585		
		CISCO_Simulator_Adapter_v2_3530_R144_20191107_Topology_1		admin	3/23/3020 11:06 PM	R.1	HA RTAC/Axtor		
		CISCO_Smulator_Adapter_v2_3530_R144_20191107_Topology_1.0		admin	2/18/2020 2:46 PM	R	H4 RTAC/Axion		
		CISCO_Simulator_Adapter_v2_3530_R144_20191307_Topology_2		admin	1/29/2020 12:49-04	83	H4 RTAC/Anton	1	
		Record Lef 18 2023							12
AddLerator RTAC Rea	ady						0	Mire 📒 D	atabase

When the user opens the SEL AcSELerator application after importing the projects and libraries files, the user is presented with list of available projects to load, as shown above.

Select the required project to load on the application workspace.

SEL 3530 DAC configuration

One of the SEL RTACs 3530 is used as a DAC Controller and the other one used as a FLISR simulator, which simulates the SCADA Server, Breaker switches and also FLISR use case events to all SEL-RTAC devices.

The following section describes on how to configure DAC and Recloser for DNP3 communication protocol.

1. Navigate to the DAC project folder structure shown below.

Figure 160 SEL3530 RTAC project folder structure



When the user loads the project, the left panel displays the complete folder structure of the projects loaded. The two major configurations which requires modification with respect to the deployment or test bed configuration are Server (explained in Step2) and IED configurations details (explained in Step3).

2. Click on the SCADA_Eth_DNP under Server menu item on left panel.

Figure 161 SEL3530 RTAC SCADA DNP configuration

SEL RTAC	Settings	Setting	Walat.	Hange	Deampton	Christian
Devices	FOU Pri Settinge	· Communications		and the second second		
L & DA Column DEP	Controles	Server IP Port	20000	23,1024-65534	The IP port that RTAC monitors for moming DNP requests.	
a Contract North		Thansport Protocol	UCF	1CP,UDP	Use TCP or UCP as the ethernet transport protocol.	
ChemetDevices		Date-Time				
- Birt OVP		UTC Officet	-400	-720 to 840 (m	Local Tate offset from Universal Tate	
- Br2_DI#		DST Enabled	Fabre	True,False	Enable Daylight Savings Time	
- 🖬 Rec1_DNP		a ore				
- Rec2_DMP		Server DN# Address	21	0-65319	CRP source address. The local address of this RTAC server session. Addresses 65520.	
- Reg Die		Gent DIP Address	22	0-65534	UNP destination address. The address of the remote client polling this RTAC.	
- Becs DIP		Allow Anonymous DEP IP	False	True,Folse	If set to FALSE, the 'Client IP Address' setting must be set to a valid IP Address.	
- Rec5_DFP		Clent IP Addresses	172.168.100.22	Vald 3Pv4 Addr	IP addresses of up to 30 renote DNP client connections allowed to communicate with t.	
- 🖬 Rec7_010		Allow Unsolicited Hessages	True	True,False	Set to TRUE to allow the DNP Client to enable / deable uncollated messaging through .	
- Rect CNP		Unsolcted Nessaging Retr.	3	2-10	Number of retries that will be attempted after a fulled unsolcited message transmissio.	
- 🖬 Recs_DNP		Map Name	DA_Scheme_DVP	Valid Map Name	The name of the map	

When the user loads the project, the left panel display the complete folder structure of the projects loaded. The two major configurations which requires modification with respect to the deployment or test bed configuration are Server and IED configurations details.

Update the configuration as shown in the table below.

Device	Reference Value	Description
Server IP Port	20000	Port number on which server listen for DNP3 messages. This port needs to be opened on mesh node during NAT configuration. Refer section "Creation of NAT44 Group on FND, page 75"
Transport Protocol	UDP	Protocol used to DNP3 message transmission
Server DNP Address	11	DNP3 source address
Client DNP Address	21	DNP3 destination address
Client IP Address	172.18.x.x	SCADA Control Center IP
Allowed Unsolicited Messages	True	To enable unsolicited message
Unsolicited Messaging Retry	3	Number of retries that will be attempted after a failed unsolicited message transmission

Table 27 SEL RTAC 3530 DNP Server configuration

3. Click Rec1_DNP under EthernetDevices menu item.

Under the Ethernet Devices, DNP3 configuration for Reclosers and Breakers are listed in Figure 27.

Devices	Settings	Setting	Value	Range	Description	Commen
Server	Binary Inputs	Communications				
SCADA Eth DNP	Double Rit Innute	Transport Protocol	UDP	TCP,UDP	Use TCP or UDP as the ethernet transport protocol.	
EthernetDevices	boube bit signs	Client IP Port	20011	23,1024-65534	Local RTAC IP port for this DNP client session.	
Bkr1_DNP	Binary Outputs	Client UDP Broadcast Port	20000	1-65534	Remote UDP port to which this DNP client transmits UDP broadcast messages.	
- Bkr2_DNP	Counters	Server IP Address	10.153.10.21	Valid IPv4 Addr	IP address of the remote DNP server connection.	
- Rec1_DNP	Analog Inputs	Server IP Port	20000	23, 1024-65534	IP port of the remote DNP server connection.	
Rec2_DNP	Analog Outputs	Date-Time				
- Rec4 DNP	Datacata	UTC Offset	-480	-720 to 840 (ml	Local Time offset from Universal Time	
Rec5 DNP	Datasets	DST Enabled	True	True,False	Enable Daylight Savings Time	
- Rec6_DNP	POU Pin Settings	ONP				
- Rec7_DNP	Custom Requests	Client DNP Address	21	0-65519	DNP source address. The local address of this RTAC client session. Addresses 65520	
- Rec8_DNP	Tags	Server DNP Address	11	0-65519	DNP destination address. The address of the remote IED polled by this client session	2
Rec9_DNP	Controller	Integrity Poll Period	300000	0, 100-1000000	Class 1,2,3,0 integrity poll period. Set to 0 to disable.	
Taos	Been Street	Class 1,2,3 Polling Period	60000	0, 100-1000000	Class 1,2,3 Poling Period. Set to 0 to disable.	
Tag Processor		Poll Timeout	7000	100-65535 (milli	Time allowed for attached DNP Server to respond to a poll. If time is exceeded, this D	2
System		Number of Poll Retries	1	0-255	The number of poll retries before the connected DNP Server is considered offine.	

Figure 162 SEL3530 RTAC Recloser configuration

Update the configuration as shown in the table below.

Update all ten Reclosers with the configuration details shown below. The two Breaker switches typically do not require an update.

	3	
Device	Reference Value	Description
Transport Protocol	UDP	Protocol used to DNP3 message transmission
Client IP Port	20011	Port number on which server listen for DNP3 messages
Server IP Address	172.168.x.x	Simulator Eth2 interface IP
Server IP Port	20011	Ip port of remote DNP server connection
Server DNP Address	22	DNP3 source address
Client DNP Address	11	DNP3 destination address
Integrity Poll Period	60000	Class 0123 polling period in millisecond
Class 1,2,3 Polling Period	5000	Class 123 polling period in millisecond
Poll Timeout	7000	Time allowed for attached DNP server to respond to request.
Number of Poll Retries	1	The number of retries before the connected DNP server is considered offline.

Table 28 SEL RTAC 3530 Recloser configuration

SEL 3505 Recloser configuration

There are ten SEL RTAC 3505 in this FLISR test setup. Each of these ten devices emulates Recloser and Recloser controller functionalities.

All ten Recloser project configurations need to be updated for the deployment or testbed setup.

The following section describes on how to configure the Reclosers for DNP3 communication protocol.

1. Recloser Project Folder Structure

Figure 163 SEL3505 Recloser folder structure



When the user loads the project, the left panel display the complete folder structure of the projects loaded. The two major configurations which requires modification with respect to the deployment or test bed configuration are DAC Server (explained in Step 2) and SIM Client configurations (explained in Step 3) details.

2. Click on DAC_Server_DNP under EthernetConnections menu item on left panel.

ces	Settings	Setting	Value	Range	Description	Commer
psor	POU Pin Settings	Communications				
	Cashalar	Server IP Port	20000	23,1024-65534	The IP port that RTAC monitors for incoming DNP requests.	
	Controver	Transport Protocol	UDP	TCP,UDP	Use TCP or UDP as the ethernet transport protocol.	
e_Control		Date-Time				
gs		UTC Offset	0	-720 to 840 (mi	Local Time offset from Universal Time	
		DST Enabled	True	True,False	Enable Daylight Savings Time	
Courtage		DNP				
iller's		Server DNP Address	11	0-65519	DNP source address. The local address of this RTAC server session. Addresses 65520	
		Client DNP Address	21	0-65534	DNP destination address. The address of the remote client polling this RTAC.	
ed		Allow Anonymous DNP IP	False	True,False	If set to FALSE, the 'Client IP Address' setting must be set to a valid IP Address.	
ctions		Client IP Addresses	172.18.107.61	Valid IPv4 Addr	IP addresses of up to 10 remote DNP client connections allowed to communicate with t	2
DNP .		Allow Unsolicited Message	True	True,False	Set to TRUE to allow the DNP Client to enable / disable unsolicited messaging through	4
2		Unsolicited Messaging Ret		2-10	Number of retries that will be attempted after a failed unsolicited message transmissio	
		Map Name	mRec1_DNP	Valid Map Name	The name of the map	

Figure 164 SEL3505 DAC Server configurations

Update the configuration as shown in the table below.

	•	
Device	Reference Value	Description
Server IP Port	20000	Port number on which server listen for DNP3 messages. This port needs to be opened on mesh node during NAT configuration. Refer section "Creation of NAT44 Group on FND, page 75"
Transport Protocol	UDP	Protocol used to DNP3 message transmission
Server DNP Address	11	DNP3 source address
Client DNP Address	21	DNP3 destination address
Client IP Address	172.18.x.x	SCADA Control Center IP
Allowed Unsolicited Messages	True	To enable unsolicited message
Unsolicited Messaging Retry	3	Number of retries that will be attempted after a failed unsolicited message transmission

Table 29 SEL RTAC 3530 DNP Server configuration

3. Click on SIM_Client_DNP under EthernetConnections

Figure 165 SEL3505 Client Configuration

	Settings	Setting	Value	Range	Description	Comment
cessor	Boary Inputs	Communications				
	Dauble Dit Ise in	Transport Protocol	UDP	TCP,UDP	Use TCP or UDP as the ethernet transport protocol.	
troller	Double bit inputs	Client IP Port	20011	23,1024-65534	Local RTAC IP port for this DNP client session.	
me_Control	Binary Outputs	Client UDP Broadcast Po	rt 20000	1-65534	Remote UDP port to which this DNP client transmits UDP broadcast messages.	
mTags	Counters	Server IP Address	172.168.100.22	Valid IPv4 Addr	IP address of the remote DNP server connection.	
t I/O	Analog Inputs	Server IP Port	20011	23,1024-65534	IP port of the remote DNP server connection.	
ints int Routers	Analog Outputs	Date-Time				
(Instans	Datasate	UTC Offset	0	-720 to 840 (mi	Local Time offset from Universal Time	
seGen	COURSE OF	DST Enabled	True	True,False	Enable Daylight Savings Time	
tetained	POU Pin Settings	ONP				
onnections	Custom Requests	Client DNP Address	11	0-65519	DNP source address. The local address of this RTAC client session. Addresses 65520	
ver_DNP	Tags	Server DNP Address	22	0-65519	DNP destination address. The address of the remote IED polled by this client session	
ient_DNP	Controller	Integrity Poll Period	60000	0, 100-1000000	Class 1,2,3,0 integrity poll period. Set to 0 to disable.	
1 DNP		Class 1,2,3 Polling Perio	5000	0, 100-1000000	Class 1,2,3 Poling Period. Set to 0 to disable.	
		Pol Timeout	7000	100-65535 (mili	Time allowed for attached DNP Server to respond to a poll. If time is exceeded, this D.	4
		Number of Pol Retries	1	0-255	The number of poll retries before the connected DNP Server is considered offine.	

Update the configuration as shown in the table below.

	-	
Device	Reference Value	Description
Transport Protocol	UDP	Protocol used to DNP3 message transmission
Client IP Port	20011	Port number on which server listen for DNP3 messages
Server IP Address	172.168.x.x	Simulator Eth2 interface IP
Server IP Port	20011	Ip port of remote DNP server connection
Server DNP Address	22	DNP3 source address
Client DNP Address	11	DNP3 destination address
Integrity Poll Period	60000	Class 0123 polling period in millisecond
Class 1,2,3 Polling Period	5000	Class 123 polling period in millisecond
Poll Timeout	7000	Time allowed for attached DNP server to respond to request.
Number of Poll Retries	1	The number of retries before the connected DNP server is considered offline.

Table 30 SEL RTAC 3530 Recloser configuration

Pushing Configuration Changes to the devices

The SEL FLISR project needs to be pushed into each SEL device for the simulation to work. The following steps describes on how to push the configuration or update the configuration of SEL devices. The steps are common for all types of SEL devices, whether it is SEL RTAC 3530 or 3505.

There are four stage process for pushing the configuration to the devices,

Load the Project → Click Go Online →Enter Credentials→Confirm Go Online

1. Load the FLISR Simulation project file. Select the project to load by double clicking on the project file name.



OEI	SEL AcSELerator RTAC					-		×
SEL								<u>@</u> •
ACSEL ERATOR RTAC						SEL	SCHWEI ENGINE «LABOR/	TZER ERING ATORIES
New Project	Projects					V 0	rid T	ree
	Drag a column header here to group by	that colum	n					
	Name	Descripti	Last E	Las	S Versio	n RTAC Typ	e	
	CISCO_DAC_3530_R144_20191107_To		admin	2/1	R144	RTAC/Axi	n	
New SEL RTAC Read SEL RTAC	CISCO_DAC_3530_R144_20191107_To		admin	12/	R144	RTAC/Axi	on	
Project Settings	CISCO_Rec1_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Rec10_3505_R144_20191106		admin	2/1	R144	SEL-3505		
Applications	CISCO_Rec2_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Rec3_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Rec4_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CI5CO_Rec5_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Rec6_3505_R144_20191106		admin	2/1	R144	SEL-3505		
SEL Compass	CISCO_Rec7_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Rec8_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Rec9_3505_R144_20191106		admin	2/1	R144	SEL-3505		
	CISCO_Simulator_Adapter_v2_3530_R1		admin	4/2	R144	RTAC/Axi	n	
	CISCO_Simulator_Adapter_v2_3530_R1		admin	1/9	R144	RTAC/Axi	n	
	Record 3 of 14 DBBC							
AcSELerator RTAC Ready						Ø Offine	B Data	base

2. Click **Go Online**. Go online with SEL RTAC devices by clicking Go Online. This action will push the configuration or update configuration on SEL RTAC device with the latest configuration in the SEL application workspace.

Figure 167	Push configuration t	o SEL device	by Going Online
------------	-----------------------------	--------------	-----------------

0	CISCO_Rec1_3505_R144_20191106 - SEL AcSELerator RTAC – 🛛 🗙
Home Insert	Vew 🖉 👻
	Go Online Go Offine Tools Comm Monitor Online
Project	Project Proper bes
SEL-3505 - R 144 V	90
SEL_RTAC	Modified By: admin
— 20 Tag Processor — 30 Tags	Modified Time: 02/19/2020 07:51:53
System	Tag Count: 253
- @ System_Time_Co	Project Description(404/20000)
SystemTags Contact I/O Contac	20191031- MG - This RTAC project simulates a recloser. The NoiseGen function generates a random number from 1 to -1 to add noise to the analog values. The Scale variable is multiplied by the noise. The noise is added to the value coming from the simulator. The scale values for voltage =, current, P, and Q can be set from the web interface.
DAC_Server_DNP	
SIM_Client_DNP	
Maps	Information
	S/3/2020 9:23:14 PM: Opening project
AcSELerator RTAC Ready	🖉 Öffline 📕 Database 🚽 Password Off

3. Input SEL RTAC credentials and then click Login. Provide the SEL RTAC credentials to enable the application to access and updated the configuration on the device.

Figure 168 SEL RTAC credentials window

Login	Options	Advanced Status	
Con	nection Name	SEL RTAC Default Connection	
RTAC A	ddress	172.168.100.11	
Use	r Name	admin	
Pa	ssword	*******	
		Login	
		· · · · · · · · · · · · · · · · · · ·	

4. Click Go. Details of connection status to the SEL device and the details of the project being pushed into the SEL display in this window.

Figure 169 Go Online confirmation window



5. Confirm the SEL device is online. Confirm the SEL RTAC device online status, by verifying the logs message has 0 errors and the status is Online with green dot on status bar.

Figure 170 SEL Device Online status

	CISCO_Rec1_3505_R144_20191106 - SEL AcSELerator RTAC	-		×
Sec inte inet	Tex			4-
2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Colores Howther			
Propert	Product Properties	_	_	
RE-2865-8394				2110
Constant and a c	Modified By: Modified Tone: Tag Count: Project Description(404/30000)			
SystemTap SystemTap Contact 1/0 Attess Funds Contact 1/0 Contact	20191233: MO - This RTAC project smulates a redown. The tioxeCan Surction powerates a random mate to the analog values. The Scale values for watage by the noise. The runs is added to the value coving The scale values for values p., current, P., and Q can be set from the web interface the scale values for values p., current, P., and Q can be set from the web interface the scale values for values p	number from 1 from the pinu 	1 ho - 1 ho dator	10
- SN(Clerk,DIP				-
-> oRaci_DHP	2 BC 61131: 640			U
	Comple complete - 8 errors, 8 warrings			5
	3	-		10
O Acizianato RTAC Ready	O Day B	- 2	7800+0	eo#

Simulation Go-Online for FLISR simulation

6. Load the FLISR Simulation project file. The FLISR simulation filename starts with *CISCO_Simulator*. Double click the filename.



SEL		SEL AcSELerator	RTAC				-	o x
-								@+
RTAG	4 21102						SEL	SCHWEITZER ENGINEERING LABORATORIES
New Project		Projects					10	Orid Tree
		Drag a column header here to group by that column						
		Name	Description	Last Editor	Last Accessed	St Versio	n RTAC Type	
1000		CISCO_DAC_3530_R144_20191107_Topology_1		admin	4/18/2020 11:48 AM	R144	RTAC/Axion	
New SEL RTAC	Read SEL REAC	C19C0_D4C_3530_R144_20191107_Topology_2		admin	1/21/2020 2:32 PM	R144	RTAC/Axion	
Project	Settings	CISCO_DNP_Master_20200227		admin	2/28/2020 8:40 PM	R244	RTAC/Axion	_
		CISCO_DMP_Outstation_A_20200227		admin	2/28/2020 8:35 PM	R144	SEL-3505	
Applications		C19C0_DAP_Outstation_8_2020028		admin	2/28/2020 8:34 PM	R144	SEL-3505	
		CISCO_Rec1_3505_R144_20191106		admin	4/18/2020 12:24 PM	R144	SBL-3505	
		CISCO_Rec10_3505_R144_20191106		admin	2/18/2020 3:37 PM	R144	SEL-3505	
		CISCO_Rec2_3505_R144_20191106		admin	3/9/2020 2:46 PM	R144	SEL-3505	
		CISCO_Rec3_3505_R144_20191106		admin	3/6/2020 10:49 AM	R144	SBL-3505	
SEL Compass		CISCO_Ree4_3505_R144_20191106		admin	2/18/2020 3:19 PM	R199	SEL-3505	
		CISCO_Rec5_3505_R144_20191106		admin	2/18/2020 3:21 PM	R144	\$81-3505	
		CISCO_Reo5_3505_R144_20191106		admin	2/18/2020 3:24 PM	R144	SBL-3505	
		CISCO_Rec7_3505_R144_20191106		admin	2/18/2020 3:27 PM	R144	SEL-3505	
		CISCO_Redl_3505_R144_20191106		admin	2/18/2020 3:29 PM	R144	581-3505	
		CISCO_Rec9_3505_R144_20191106		admin	2/18/2020 3:33 PM	R144	\$81-3505	
		CISCO_Simulator_Adapter_y2_3530_R144_20191107_Tepelogy_1		admin	3/22/2020 11:06 PM	R111	RTAC/Axten	
		CISCO_Simulator_Adapter_v2_3530_R144_20191107_Topology_1.0		admin	2/18/2020 2:40 PM	R144	RTAC/Axion	_
		CISCO_Simulator_Adapter_v2_3530_R144_20191107_Topology_2		admin	1/29/2020 12:48 PM	R144	RTAC/Axion	
		Record 35-of 38 District						
AcSELerator RTAC	Ready						Ø offine	Batabase

7. Open Main Visualization. The Main Visualization GUI is a dashboard graphical user interface, providing a means for all FLISR user case events to be initiated, monitored, and visualized.





8. Go Online, by clicking Go Online.

The main visualization provides the electrical line diagram of the topology with the recloser, breakers and source of power. It also shows the details of status of each device, load points.

The GUI provide buttons to simulate a fault, restore, RTN events.

More details of this line diagram can be found in the DA Feeder Automation Design Guide.

Figure 173 Initial Offline state



9. Input SEL RTAC credentials and then click **Login**. Providing the SEL RTAC credentials enables the application to access and update the configuration on the device.

Figure 174 FLISR Simulator credentials window

Connection	[
Name	SIM	<u> </u>
RTAC Address	172.168.100.22	
User Name	admin	
Password	*******	
		Login
	_	

10. Click **Go**. Details of connection status to the SEL device and the details of the project being pushed into the SEL display in this window.

Figure 175 FLISR simulation Going online



11. If you need to make changes to the project, click **Yes**. This window appears only when there is change in the configuration between the device and current configuration being pushed into it.

Figure 176 FLISR send settings to simulator device

CISCO_Simulator_Adapter_v2_3530_R144_2019110	×
Login Options Advanced Status	
Connecting to RTE	
Send Settings 🔯	
Settings have changed. Send settings and overwrite?	
Yes No	
Eg Gom	I

12. Click Enable/Disable DAC to initiate the communications to all RTACs including the DAC and simulator.

By default, when the simulation goes online, the simulated electrical circuits remains unarmed, which means there is no flow of current in the circuit. To start the current flow and arm the circuit, the GUI provides an Enable/Disable DAC button. The status of electrical circuit can be verified by "UNARMED" in legend box and as well the Enable/Disable button color, white when it is Disabled and Green when it is Enabled.





1. Verify the there are no errors are displayed, before proceeding to use case execution.





After enabling the DAC, verify that no "Abnormal" text box appears below the status box in the electrical line diagram. When "Abnormal" text appears, when there is a communication failure between one or more of the SEL RTAC devices. Fix the communication errors before proceeding to FLISR Use case simulation.

FLISR Fault Lockout simulation

Figure 179 FLISR Fault Lockout use case flow diagram



Fault Lockout Simulation, Simulate the fault between any two reclosers. Once the fault is inserted in a segment, the FLISR simulation recognizes the fault and initiates FLISR process in which, the first step is Identifying and Isolating the faulty segment by opening the Reclosers closest to the segment. And, the next step is Restoring the power to the other segments in the circuit from the other available source by closing the Normally Open Recloser6.

Clear Fault Lockout, Clear the fault created in the first step, which means in real deployment scenario the fault is fixed or resolved, but still the power is not restored to this segment.

Return to Normal, Reset the simulation to the normal state. Return to Normal process involves, resetting the circuits to its initial state before the fault occurrence. Typically, the power is restored to the faulty, which is fixed now segment by closing the Reclosers which are opened during Fault Isolation process and opening the Normally Open Recloser6.

For more details on FLISR use case, refer to Distribution Automation Feeder Automation Design Guide.

Fault Lockout simulation steps

1. Click on the yellow colored load icon 10A, between the reclosers Rec2 and Rec3





On clicking the load icon 10A, a table appears at bottom right corner of the GUI window, with the title as *Line Section: Rec2-LineB*. The table has fault type on first column and next three columns A, B & C represents the phases of current.

2. To start simulating Fault lockout, click on the white box on second row, which has the Fault Type as Lockout.



Figure 181 Fault Lockout fault simulation

For the simulation, there is no difference between column A, B or C. So choosing any box on these columns produce the same results. The Fault Type is a more important factor parameter when deciding which FLISR use case needs to be executed in the setup.

3. Wait for the simulation events to be executed by the application. When the Fault simulation is successfully completed the **Fault** button is highlighted in orange color and there are no errors displayed on the simulation window.

Figure 182 Fault lockout FLISR state



Verify the simulation has created a Fault in between reclosers Rec2 and Rec3, then the Fault is identified by the simulation, based on the fault the circuit is reconfigured to isolate the faulty section and power is restored to the other section of the circuit from the available power source.

In this example, the fault is created in between reclosers Rec2 and Rec3, this fault is Identified by the DAC controller and this section is Isolated by opening reclosers Rec2 and Rec3. Finally, the power is restored from Source2 by closing the Normally open recloser Rec6.

For more details on FLISR events, please refer to the FLISR Event Sequence Diagram, page 151 section.

4. Click on the DA SIM Clear Fault button on the top panel.

Figure 183 Clear Fault Lockout



Verify that fault icon, the red x on load line between Rec2 and Rec3 disappears and also the orange color disappears on row two against the Lockout fault type, which is displayed on the Line Section box at the bottom right corner of the GUI window.

 Return to Normal command, to reset the simulator and all SEL RTAC device setting to the Normal state, click on RTN Cmd to DAC.



Figure 184 Fault Lockout Return To Normal

The RTN command to DAC resets the simulator and as well as all SEL RTAC device settings to normal state, which is prior to the FLISR event.

6. Verify the setup has returned to Normal state.

Verify the circuit returned to Normal state by confirming that all Normally closed reclosers are Closed, in this example Rec1 to Rec2 are Closed. And, all Normally opened reclosers are Opened, in this example, the Rec6 is Open.

Also, verify that both Breakers are in Closed state and there are no errors displayed.

The total time taken for successful Fault Isolation and Restoration over CR mesh is well within the recommended industry standard. The time take by the FLISR events can be viewed from the event duration time from FLISR events logs. Refer to the section "Events HTML file".

Figure 185 Fault Lockout back to normal state



FLISR Open Phase simulation

Figure 186 FLISR Open Phase use case flow diagram



Open Phase Fault Simulation, Simulate the fault between any two reclosers. Once the fault is inserted in a segment, the FLISR simulation recognizes the Open Phase in the circuit and initiates FLISR process in which, the first step is Identifying and Isolating the faulty segment by opening the Reclosers closest to the segment. And, the next step is Restoring the power to the other segments in the circuit from the other available source by closing the Normally Open Recloser6.

Clear Open Phase Fault, Clear the open phase fault created in the first step, which means in real deployment scenario the fault is fixed or resolved, but still the power is not restored to this segment.

Return to Normal, Reset the simulation to the normal state. Return to Normal process involves, resetting the circuits to its initial state before the fault occurrence. Typically, the power is restored to the faulty, which is fixed now segment by closing the Reclosers which are opened during Fault Isolation process and opening the Normal Open Recloser6.

Open Phase Fault simulation steps

1. To simulate the Open phase, click on the yellow load icon 10A, between the reclosers Rec8 and Rec9.





On clicking the load icon 10A, a table appears at bottom right corner of the GUI window, with the title as *Line Section: Rec9-LineB*. The table has fault type on first column and next three columns A, B & C represents the phases of current.

2. To start simulating Open Phase fault, click on the white box on the third row, which has the Fault Type as **Open Phase.**





For the simulation, there is no difference between column A, B or C. So choosing any box on these columns produce the same results. Whereas, the Fault Type is more import factor parameter which decide which FLISR use case needs to be executed in the setup.

3. Wait for the simulation events to be executed by the application. When the Fault simulation is successfully completed the **Open Phase** button is highlighted in orange color and there are no errors displayed on the simulation window.



Figure 189 Open Phase FLISR state

Verify the simulation has created an Open Phase fault in between reclosers **Rec8** and **Rec9**, then the Fault is identified by the simulation, based on the fault the circuit is reconfigured to isolate the faulty section and power is restored to the other section of the circuit from the available power source.
In this example, the Open Phase fault is created in between reclosers **Rec8** and **Rec9**, this fault is Identified by the DAC controller and this section is Isolated by opening reclosers Rec8 and Rec9. Finally, the power is restored from Source1 by closing the Normally open recloser **Rec6**.

For more details on FLISR events, please refer to the FLISR Event Sequence Diagram, page 151 section.

4. Click on the DA SIM Clear Open Ph button on the top panel, to clear the Open Phase fault on the circuit



Figure 190 Open Phase clear fault

Verify that fault icon, the red x on load line between Rec8 and Rec9 disappears and also the orange color disappears on row three against the Open Phase fault type, which is displayed on the Line Section box at the bottom right corner of the GUI window.

 Return to Normal command, to reset the simulator and all SEL RTAC device setting to the Normal state, click on RTN Cmd to DAC button.





The RTN command to DAC resets the simulator and as well as all SEL RTAC device settings to normal state, which is prior to the FLISR event.

6. Verify the setup has returned to normal state.





Verify the circuit returned to Normal state by confirming that all Normally closed reclosers are Closed, in this example **Rec9** to **Rec9** are Closed. And, all Normally opened reclosers are Opened, in this example, the **Rec6** is Open.

Also, verify that both Breakers are in Closed state and there are no errors displayed.

The total time taken for successful Fault Isolation and Restoration over CR mesh is well within the recommended industry standard. The time take by the FLISR events can be viewed from the event duration time from FLISR events logs. Refer section "Events HTML file, page 188".

FLISR Loss of Source simulation

Figure 193 FLISR Loss of Source use case flow diagram



Loss of Source Fault Simulation, Simulate the Loss of Source, by simulating the Voltage Loss on one of the sources. Once the loss of voltage is inserted in a circuit, the DAC recognizes the voltage loss in the circuit and initiates FLISR process in which, the first step is to Identify and Isolate the Source by opening the Breakers closest to the Source, which lost the voltage. And, the next step is Restoring the power to other segments in the circuit from the available source by closing the Normally Open Recloser6.

Restore Voltage on Source, Clears the fault created in the first step, which means in real deployment scenario the fault is fixed or resolved, but still the power is not flowing to the circuit from the source.

Return to Normal, Reset the simulation to the normal state. Return to Normal process involves, resetting the circuits to its initial state before the fault occurrence. Typically, the voltage is restored from the faulty source, which is fixed now. Power is restored in the circuits by closing the Breakers, which are closed during Fault Isolation process and opening the Normally Open Recloser6.

Loss of Source Fault simulation steps

1. Simulate Loss of Source on circuit 1 by clicking the source transformer xfmr1 icon.





On clicking the transformer icon *xmfmr1*, a table appears at bottom right corner of the GUI window, with the title Transformer: Xfmr1. The table displays the status of the voltage on the circuit. One type of loss of source is due to fault in the transformer which fails to serve required voltage to the circuit resulting in a loss of source.

2. Click on the Loss Volt button on table Transformer: Xfmr1, to simulate the Loss of Source.





Verify the simulation has created a Loss of Source in transformer **Xfmr1**, by confirming the change of color of Xfrm1 icon from Red to Green. The electrical line also changes color from Red to Green representing there is no Voltage on the circuit.

For more details on FLISR events, refer to the FLISR Event Sequence Diagram, page 151 section.

3. Wait for the simulation events to be executed by the application. When the Loss of Source simulation is successfully completed, the **Restore volt** button appears and no error message is displayed on the simulation window.

Figure 196 Loss of Source FLISR state



Verify the Loss of Source simulation successfully completed by confirming that Source Transformer **Xfmr1** is isolated by opening the **Breaker1** switch. Power is restored to circuit1 from the other source Transformer **Xfmr2**, by closing the Normally open Recloser **Rec6**.

4. Click the **Restore Volt** button in the *Transformer: Xfmr1* table, as shown in previous Figure 55.



Figure 197 Loss of Source Restore voltage state

Verify the voltage is restored in source *Transformer: Xfmr1*, by the icon color change from green to red and **Restore Volt** toggles to **Loss Volt**.

 Return to Normal command, to reset the simulator and all SEL RTAC device setting to the Normal state, click on RTN Cmd to DAC button.



Figure 198 Loss of Source Return To Normal

Verify the circuit returned to Normal state by confirming that all Breakers those are Normally closed are Closed, in this example **Breaker1** is Closed. And, all Normally opened reclosers are Opened, in this example, the **Rec6** is Open.

Also, verify that both the source Transformers are Red, which represents the Voltage flowing to the circuit from these transformers and confirm there are no errors displayed.

The total time taken for successful Fault Isolation and Restoration over CR mesh is well within the recommended industry standard. The time take by the FLISR events can be viewed from the event duration time from FLISR events logs. Refer to the section "Events HTML file, page 188".

FLISR Event Logs

Sequence of Events

1. Open https://172.29.131.1/home.sel

using any web browser and the console cable is connected between the windows PC and the SEL device.

Click on the SOE menu item under the Reports tab on left panel.

Figure 199 FLISR Sequence of events

SEL Device: SEL-3	530-4-0030A71DFCD7				•	admin [Logol				
Navigation										
Dashboard	Sequence of Events Report									
	Actions	Download CSV	Reloa	d Table		Display: Page 1				
System	Category ~	And ~	Category	×						
Date/Time	Time Stamp		1 -		Filter Peret	Theme Ber Brees 100				
Device Management	Time Stamp		10		Filter Reset	Items Per Page: 100				
File Manager	Details - Time Sta	mp Priority Categ	lory	Tag Name	Message	Ack Time Stamp Origin				
Project Upload	[open] 2020-04-18	3 Secur	rity	SystemTags.User_Logged_On	admin logged on device via Web	SEL_RTA				
Licensed Features	[open] 2020-04-18	3 Secur	ity	SystemTags.User_Logged_Off	admin logged off device via ODBC	SEL_RTA				
User	Q2:47:33.9	DA St	tatus	Cir2 Armed	Asserted	SEL_RTA				
Accounts	00.37.17.7	DA St	tatus	Cir1 Armed	Asserted	SEL_RTA				
User Roles	00:57:17.7	DA St	tatus	CISCO DAC Enabled	Asserted	SEL RTA				
RADIUS Settings	00:57:17.5	31 B Field :	Status	Bkr2 DeviceOnline	Asserted	SEL RTA				
	00:53:24.8 2020-04-18	30 Field	Status	Bkr1 DeviceOnline	Asserted	SEL DTA				
Network	2020-04-18	30	500103	SAT DEVREGNATE	Post lea	JEL_KIN				
Interface	[open] 00:50:16.7	18 Secur	rity	SystemTags.User_Logged_Off	admin logged off device via ODBC	SEL_RTA				
Hosts	[open] 2020-04-18 00:48:37.3	30 Field :	Status	Bkr2 DeviceOnline	Deasserted	SEL_RTA				
Syslog	[open] 2020-04-18 00:48:35.8	30 Field :	Status	Bkr1 DeviceOnline	Deasserted	SEL_RTA				
	[open] 2020-04-18 00:47:44.8	30 Field :	Status	Bkr2 Voltage Side B	Live Lvl 2	SEL_RTA				
Security	[open] 2020-04-18	Field :	Status	Bkr2 Voltage Side A	Live Lvl 2	SEL_RTA				
CA Certificates	[open] 2020-04-18	Field :	Status	Bkr1 Voltage Side B	Live Lvl 2	SEL_RTA				
SSH Keys Password Report	[open] 2020-04-18	Field :	Status	Bkr1 Voltage Side A	Live Lvl 2	SEL_RTA				
TRADITION DEPORT	[open] 2020-04-18	DA AL	arm	Bkr2 Abnormal	Deasserted	SEL_RTA				
Reports	[open] 2020-04-18	30 DA AI	arm	Bkr1 Abnormal	Deasserted	SEL_RTA				
Connected IED	[open] 2020-04-18	B DA AL	arm	Bkr2 CommAlarm	Deasserted	SEL_RTA				
SOE	[open] 2020-04-18	B DA AL	arm	Bkr1 CommAlarm	Deasserted	SEL_RTA				
Event Collection	[open] 2020-04-18	3 Secur	rity	SystemTags.User_Logged_On	admin logged on device via ODBC	SEL_RTA				
Diagnostics	[open] 2020-04-18	3 Secur	ity	SystemTags.User_Changed_Settings	Time System modified settings	SEL_RTA				
	[open] 2020-04-18	B DA O	perating	CISCO Source Detection Enabled	Asserted	SEL_RTA				

The above Sequence of Events table captures each and every event that occurred during the FLISR user case event. This table can be downloaded to local system as csv file, if further analysis is required on sequence of events or for debugging purpose.

FLISR Fault Report

Events HTML file

- 1. Open the link https://172.29.131.1/home.sel using any web browser and the console cable is connected between the windows PC and the SEL device.
- 2. Click on the File Manager menu item under the System tab on left pane.

Figure 200 DAC Events file

a management of the second			
Navigation 4			
Dashboard	File Manager		
	Name 🔺	Date Modified	
System Date/Time	DAC Events	Sun Mar 22 12:12:35 2020	
Usage Policy	File Upload		
Device Management File Manager	Browse No file sel	ected.	Upload

All FLISR events and their details are captured and stored in html file format. These html files are consolidated under the folder named **DAC Events**.

To view all DAC event files, click on the DAC Events folder link.

3. Click on the DAC Events link.

Figure 201 DAC Events HTML files

SEL Time: Sat, Ap Device: SEL-3	r 18, 2020 11:56:26 PM 530-4-0030A71DFCD7	00000		ad	lmin [Logout
Navigation 4					
Dashboard	File Manager				
System Date/Time	Name •	Date Modified Wed Feb 19 01:44:54 2020	Size 0	/	DAC Events/
Usage Policy Device Management	.retainedState	Sun Mar 22 12:12:35 2020	256	Rename	Delete
Project Upload Licensed Features	.unsent	Sun Mar 22 12:12:35 2020	1147	Rename	Delete
User	2020-02-19-01-44_DA Event.html	Wed Feb 19 01:44:55 2020	2149	Rename	Delete
User Roles LDAP Settings	2020-02-19-22-44_DA Event.html	Wed Feb 19 22:44:40 2020	2097	Rename	Delete
RADIUS Settings	2020-02-19-22-49_DA Event.html	Wed Feb 19 22:49:53 2020	2151	Rename	Delete
Interface Static Routes	2020-03-09-02-34_DA Event.html	Mon Mar 9 02:34:18 2020	1210	Rename	Delete
Hosts Syslog	2020-03-09-02-37_DA Event.html	Mon Mar 9 02:37:04 2020	2097	Rename	Delete
Security X.509 Certificates	2020-03-09-02-38_DA Event.html	Mon Mar 9 02:38:54 2020	2158	Rename	Delete
CA Certificates SSH Keys	2020-03-09-02-42_DA Event.html	Mon Mar 9 02:42:51 2020	2151	Rename	Delete
Reports	2020-03-18-04-04_DA Event.html	Wed Mar 18 04:04:23 2020	1210	Rename	Delete
Connected IED Alarm Summary	2020-03-18-04-06_DA Event.html	Wed Mar 18 04:06:57 2020	2158	Rename	Delete
SOE Event Collection Live Data	2020-03-18-04-21_DA Event.html	Wed Mar 18 04:21:00 2020	2097	Rename	Delete
Diagnostics	2020-03-19-05-37_DA Event.html	Thu Mar 19 05:37:45 2020	2158	Rename	Delete
	2020-03-19-05-42_DA Event.html	Thu Mar 19 05:42:00 2020	2151	Rename	Delete
	2020-03-20-05-04_DA Event.html	Fri Mar 20 05:04:52 2020	2099	Rename	Delete

Each FLISR events are captured in an individual html file with time stamp appended to its file name.

4. Click to download the FLISR events HTML file to the local machine.

Figure 202 DAC Events details

DAC EVENT ON CIR1, CIR2

Permanent Fault at 2019-12-12-18:30:28

Event Circuit:	Cir1, Cir2	Event Duration:	28.7 Seconds
Restoration Status:	Reconfiguration Complete	Isolation Switches: Restoration Switches:	Rec3, Rec2 Rec6
Best Solution Post-Event Loading			
Initial Load Lost:	80 A		
Load Restored:	60 A		
Faulted Zone Load Lost:	20 A		
Non-Faulted Zone Load Unrestored:	0 A		
Diagnostic Information			
Failure Root Cause:			
Details:			

Report Generated by the SEL Distribution Automation Controller.

The file provides details of the FLISR events, especially time taken for the event and load details.

Edge Compute

The sample IOx Edge Compute application running on Mesh Gateway IR510 devices executes the following functions:

- Sends an Unsolicited report from IED to Control Center through UDP.
- Receives request for an Integrity poll from Control Center and forwards the request to IED controller through serial communication. Also, reads the response for integrity polling and forwards the response to Control Center through UDP.
- Receives a Control Command from the Control Center and forwards the command to IED controller through serial communication. Reads the response for the command and forwards the response to the Control Center through UDP.



Figure 203 Edge Compute Schematic Drawing

For more details on infrastructure and setup, please refer to Solution Network Topology and Addressing, page 5.

Refer to Appendix E: HER and CGR Configurations, page 250 for details on how to get this pre-compiled sample Edge Compute application.

For details on IOx, IOx application development, and all information-related IOx and Edge Compute, refer to the following URL:

https://community.cisco.com/t5/cisco-iox-documents/getting-started-with-cisco-iox/ta-p/3619379

Application Life Cycle Management

Cisco Fog Director

Installing Cisco Fog Director

To install the Cisco Fog Director, refer to the Cisco Fog Director Reference Guide, Release 1.5 at the following URL:

https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/fog-director/reference-guide/1-5 /fog_director_ref_guide.html

Integration Steps on FND

Adding Mesh Gateway into Fog Director

Mesh Gateway is automatically imported into Fog Director (FD) from the FND. To enable this, complete the following configuration:

Create FD User

1. Open FND and create a new user.

Figure 204 Create New User

(i) 🖧 https://172.16.103.243/homeseum					
DIRECTOR	DASHB	OARD DEVICES	· OPERATIONS ·	CONFIGM	ADMIN ~
					Access Management
	- C 🗈 🖉 🛪	Service Providers (With Maximum Down	n Routers for C	
		Cellular Network	Det 10	Router	Ades
	CirkEctToH	© € https://172.16.103.243/home.seam DIRECTORE _ © ∅ ≠ ×	CASHBOARD OEVICES OEVICES OEVICES OEVICES OEVICES OEVICES OEVICES OEVICES OEVICES	Image: Service Providers With Maximum Does Cellular Subserv	© ▲ https://172.16.103.243/home.seam DRECTOR DASHBOARD DEVICES ▼ OPERATIONS ▼ CONFIG ▼ ■ © ② ▲ Service Providers With Maximum Down Routers for C Cellular National Cell 18 Routers

2. Create a FD user.

Figure 205 Create FD User

dude IoT cisco FIELD NETWOR				
ADMIN > ACCESS MANAG	IEMENT > USE	RS		
User Name •	Default	Enabled	Time Zone	Remote User
	reat	true	ute	fatee
0 0 1001	1001	true	uto	Talan

3. Provide FD user details, user name as FD, password, and Time Zone as UTC.

Figure 206 Provide FD User Details



4. Assign FD user role as NorthBound API.

Figure 207 Assign FD Role

Hei Name	FO							
New Password			Dómain Assignment.					
Confirm Password								
tine Zone	UTC		Domain Name: root	(x)				
A CONTRACTOR OF			Role Abaigsment					
Arrent Demonstra			Rote	Permission(s)				
Sovicies Name	Detaut no Domain	ielin.	Administrator	Administrative Operations, is sue Nanagement, Label Management, Password Policy, Rules Management, View Device Config. View Head End, View Work Orders	k:			
ter yete te ar pipter t	daptin		C Endpoint Operator	Endpoint Configuration, Endpoint Firmware Update, Endpoint Group Management, Endpoint Rabod, Label Nanagement, Password Policy View Device Config. View Head-End, View Work Orders				
			Monitor Only	View Device Config. View Head-End, View Work Orders				
			 Northbound API 	NBAPI Audit Trail, NBAPI Device Management, NBAPI Endpoint Operations, NBAPI Event Subaccise, NBAPI Group Management Operations, NBAPI Isaues, NBAPI Grothestration Service, NBAPI Reprovidien, NBAPI Faules, NBAPI Search, Pasarove, NBAPI Reprovidien, NBAPI Faules, NBAPI Search, Pasarove Oplicy, View Device Config. View Head-End, View Work Orders				
			Router Operator	Label Management, LoRa Modern Rebool, Password Policy, Router Configuration, Router File Management, Router Firmware Update, Router Coup Management, Router Reboot, View Device Config. View Head-End, View Work Orders				

5. Save FD user details.

Figure 208 Save Changes

NOMIN > ACCESS	MANADEMENT	> UBER#	
od User.			
/ser fiame	FD		
Vew Password			
Confirm Password			
1016 2016	utc	10	
amaine.			
ange Dreen			
Domain Name	Default Domain	Note(s)	Addisis
foot	2	Northbound AP1	# fint # Deliere
	10		

6. Save FD user.

Figure 209 Save User FD

ritudes and catco mano la					
ADDAME + ACCESS HOS UNKY	MARAGENENT	- USERS			
User Hartie Non Palawitt Contro Palawitt Time Zone Time Zone	PD UTC				
inter Name	Datast Donare	Notices	(Antonio		
uat	8	formound into	NAME OF TAXABLE PARTY.	-	
				User FD details saved as	X coesstuity

Enable Serial Communication on Endpoints

1. Enable serial service in endpoints.

Figure 210 Enable Serial Service from FND

cisco FIELD NETWO	RKIDIRECTOR				DA:	DRAOBHE	DEVICES	OPERATIO	NS V CONFIG V
ONFIG > DEVICE CONF	IGURATION								1
Assign Devices to Group	Charge Device Properties	Edge_Comp	ute_Serial_P	otile					
Groups	Config Profiles	- Sertal Interface	Settings						
Default-MAPT-PO	offie	Port attinity:	O DA Gatew	ay 🕑 10x Node		Port al setting	minity is only app as will not be use	icable to gatew.	ays with IOx Node. Wh
* DHOP CLIENT PROF	LE	Media Type:	R\$232		Baud rate:	9600	S	•	
Default-DHCP-C	lient-Profile	Data Bits:	8						
· NAT44 PROFILE		Parity:	None		Stop Bit	1		-	
Detroit NATA 4	te office :	Flow Control	None						
E CHANNEL CON		DSCP Marking	Medium	1					
EdgeCompute_	and_bcada_RLD	Raw Socket Sea	aiona						
Test		TCP Idle Time	Connect Time	Peer IP Address	Peer Port	Local Port	Packet	Packet	Special Characte
S DNP3 NAT Profi	• 1	oui(secs)	Out(sets)				E anglin (oynex)	ana a	
T DHCP BERVER PROF	ni, E			121.0.0.1	×.		214	500	
Default-OHCP-S	erver-Profile							-	
* SERIAL PROFILE									
🍋 Migrated-Serial-	Ŧ								
Raw Seckel UD									
Detauth Senal-P	rolle								
Edge_Compute	Serial Profile								

2. Select IOx Node and verify that the serial settings are added as in Figure 210.

Integration Steps on Fog Director

1. Open FD, go to Settings > Extensions and click on the Configure link.

Figure 211 Configure FND Extension

uluilu cisco	Fog Director	APPS DEVI	es cartridges	SETTINGS			Φ
Settings	Extensions						Deminut
						Add New	Extension
	FND Integration Extension	v1.8					
	The FND Integration Exten	sion lets Fog Director i	nteract with Cisco IOs	devices managed by the Cisco	SoT Field Network Director product.		
					G	digue	

2. Provide the required details in FND Integration Extension and then click Update Configuration.

falid Metwork Director (FHD) Hostmanne or IP Address		FND Port	
172.16.103.243		443	
ND User ID		FND Password	
FD			
og Director Hottsame in 19 Address		TND Heartheat Interval (Seconds)	
172.16.103.150		10	-
efault Device Profile			
System Default Profile	0		
inata new Profile			

- 3. Provide the FND IP, FNP port, FND User name, FND Password, and FD IP.
- 4. Go to Devices, click on more (...) link and select Profile menu item.

Figure 213 Choose Device Profiles



5. Choose the profile to edit.

Figure 214 Edit Device Profiles

Profiles			
wallable Profiles:	•		
	THE REPORT OF A DOMESTIC	state would be understand	d
ADD VIEW	are evaluable when only	one home sector	
ADD VIEW	EDIT	ade prove sector	
ADD VIEW	EDIT MARK AS DEFAU		

6. From the Communication tab, provide the Proxy address as FND IP and Proxy port as 9094. Click Update to save the settings.

Figure 215 Edit Proxy Details

MONITORING COM	NUTRICATION	SECURITY		
Default timeout for control acti	ons 600 *	-	seconds	
Timeout for file transfers	3600 -	-	seconds	
Proxy address	172,16.	103.243		
Proxy port	9094 -	-		

Application Installation

1. Upload Edge Compute application in FD.

Figure 216 Select Edge Compute Application Package

		Add new app	×
Unpublished Apps	Add New App	You can other upload an application package created application package from a Docker image present in a Choose one: Qupload from my computer Count	via the IDs SDK, or lat Fog Director create an Docker registry (such as the Docker Huld), a from Dircker image
		SUJECT AND PACKAGE	Tyboling. O
			*

2. To publish the application, click Publish.

Figure 217 Publish the Application

Available Apps	Export Apps	
		No Available Apps fourst.
Unpublished Apps	Add New App	
F		
Feeder-Auto Henne 11 D		

3. To install the application, click the **Application** icon.

Figure 218 Select the Edge Compute Application Package to Install



Figure 219 Install the Selected Edge Compute Application Package



- 4. Click Install to initiate the install of the application.
- **5.** Select device(s) to install.

Figure 220 Select the Device

	25			Feed	er-Automation-D	 tracApp
nu care and d	d more devices how be	um labe			institution of	Added in
					See: 24	
0	Notes	manual 1	C Mar	1000	e Nada	
	10.0.012	10.131-0.22				
Ċ.	apup/Heart	10.110.10.14				
É2	201201106020	10.153.15.19	(Assessed and)			
D	3820320493680423	10/10/10/19				
8	algocarrena of the	16,151,01.12	Tenterial Farm Adventor D	nature . Para	an Automation Descarge	
i i	A g o a A	 Barn per page 				A- 214 Marson
4 4	a 2	 provide hold 			Jacob Harrison W	A - D of Yorker
A A	nd Devices	a horayyy	lat.		Sect. Survey, P	A- 2 d Yolan
A A A A A A A A A A A A A A A A A A A		 Basepergrege Stream WHERE 	Tere Teremointy - Person-Automation		Tarit Paranet 7	A- 0 d Year

6. Select all the devices on which the edge compute application needs to be installed.

200mm

Figure 221 Add Selected Device

econfigure App			Feede	r-Automation-D	emoApp
to an add more devices from be	itse table			Secol Institution If A	and the second second
				See. Jarry	
8	2 and as	14	parents.		
20020191946018	10.110.10.12	Freder-Aut Freder-Automation-Greek	Hat Prede A	donation Denisland	0
	Normi per pega				11 filling
Selected Device:				South Process & A	
Selected Devices	PARTIC	No.	i inami-	Test Server	a.tun
Inen mene	17 AMARAN NG 115 30 37	Ner Nedal Auf - Nedal Administration Demokracy		See	
Selected Devices:	17-14-14-14 16-152-16-12	Trans Feeder Auf - Fander Automation Demokrat	00	Second Production of A	*
Selected Devices	17-000-011 (No.152.10.12	1949 Peedal Aut Pyedal Automation Dimong	00	Set Treed Minimum Back	i (al time
Selected Devices	F 444 + 1 1	tragi Pendul Aut – Pandar Automation (Jonnarga	00	Hard Taxad Marindan Back	Andreas Andrea
Selected Devices	17 AMARKA (Period	00	And Sector	in cal tame

7. Configure application parameters.

Figure 222 Customize Application Configuration

Edge Compute

sco Fog Direc	OF APPS DEVICES CARTRIDGES SETTINGS	
initaliation Summary		Feeder-Automation-DemoApp
ected Devices		2 fast up ofer redulates C Back Done, Lette C
Selected Devices		
Customize Configuration		
app.sptime		
heal, hird, pi	448	
hold, hold, part.	0000	
mode/ord.p	72.14.507.58	
sends, but, pot	0000	
torg juilet	im-m/UD0	
send, head tells	600	
serial party	elial/ARTY_NOIS	
said, staplits	mid STOPETS, ONR	
unial Apresian	mikD0HT8T5	
tarial Stream	0	
interface providents	8	
scholules, pet, it, request, bla	ant films yet, studiege	
schebules.pd.id.top	atta	
ichekino, prt, theo, period	8	
schedules, pet, dois, respect, bla	ert, fried get, stand de	
achashalan part class ton.	aba a	

8. Customize the SCADA Control Center IP address, DNP3 UDP port on Control Center, and Outstation/IED device.

Refer to Figure 203 for more details.

9. Configure Network Mode.

Figure 223 Edit Network Details

	cisco Fog Director APPS DEVICES CARTRIDGES	SETTINGS	۵ 🔺
	Installation Summary		Feeder-Automation-DemoApp
	Selected Devices		😨 Start app after installation 🦳 🛛 🖉 Done, Letter
	Selected Devices		
	Customics Configuration		
	Configure Resource Profiles		
	Configure Networking		•
	O Leaser that the Physical Disign interfaces an the de-	reas are operationally up liefs	en mapping the interfaces.
	Unaffected (1) O All Devices (1) Falters: Sensitiv Histories. IP Attribute.	All Tega 🗸	Preferred networks:
	Click on a device (if any) to configure it.		eth0 :
Edit Network Details -			Network ica-bridge0 🗸
			iPrd iPv6
Restname: 21000000000000000000000000000000000000	WINCLE TILL TO THE		Mode: O Static # Dynamic: O Duable
leterface_eth0 :			DHCP Direct Ma Trainin DHCP Character
semit.			
tailed.			

256470

- 10. Select the Network Mode as Bridge mode.
- 11. Configure the Edge Compute application IP.

Installation Summary		Feeder-Automation-DemoAp
lected Devices: 1		Start app after installation 🗧 Back Done. Let
Selected Devices		
Customize Configuration		
Configure Resource Profiles		
Configure Networking		9
C Ensure that the Physical/Bridge interfaces on the devices	are operationally up befor	re mapping the interfaces.
Unallocated (1) O All Devices (1) Filters: Search Heatmania, UP Address,	All Tags 🕹	Preferred networks:
Click on a device (if any) to configure it.		eth0:
		Networic iox-bridge0 🗸
		IPv4 IPv6
		Mode: Static O Dynamic O Disable
		1P Address: 192,168.0.30 / 24
		DNS:
		REASSIGN NETWORKS

256469

Figure 224 Configure Application IP Address

- **12.** Configure the Edge Compute application and its gateway.
- 13. Configure the serial port.

Figure	225	Configure	Serial	Port

Installation Summary						Feeder-Auto	omation-	DemoA	pp
Selected Devices:					8	Start app after installatio	e Back	Done.L	et's (
Selected Devices									
Customize Configuration									
Configure Resource Profiles									
Configure Networking									•
Configure Serial Devices									
Unatiocated (0) • All Devices (1)	Fibers Search II	istrana, IP A	data mai.	All Tag	P ♥ Select ser RTU_DEV	al devices:			
Unatiocated (D) All Devices (T) Click on a device (if any) to configure it: Internal Details	Fibers Stards II	otruma IF A	ddrws.	All Tag	P V Select ser RTU_DEV REASS	at devices: O SO GN STRIAL PORTS		v	
Unatiocated (0) All Devices (1) Click on a device (if any) to configure it. Internet Interne	Fibers Stards II	ceruma di A	da wa	AB Tag	¤ ♥ Select ser RTU_DEV REASS	at devices: O 50 GN SERIAL PORTS		v	
Unatiocated (0) O All Devices (1) Click on a device (if any) to configure it. (id) Serial Details trame: DCHFFEEDF09(10.133.10.1)) F (Feeder-Aut) st Seeial Port:	Fithers: Search 19	inistana, di X		All Tag	P ♥ Select ser RTU_DEV REASS	al devices: 0 50 GN SERIAL PORTS		3	

- 14. Select the serial interface as S0.
- **15.** To install the application, click **Install**.

Figure 226 Application Installation Progress

	Feeder-Automation-DemoApp	Feeder-Automation-DemoApp
F	Feeder-Automation-DemoApp Land required 6.0 bad operate on, for 6.2019 64259 for	
	 Installed Feeder Automation Comologi on & out of 1 Devices 	
(mr	35	- The field in some instant
I i bullen I i Sill Haren nany i 64.548		C terre bini Han have (IMCININGSON Transmission 195
p Links		Ann Transmitting Nation Editories interesting Tab

16. Verify that the installation completed without any error.

Figure 227 Application Installation Complete

	Feeder Automation-DemoApp		Feeder-Automation-DemoApp
F	Feeder Automation Dem Land result 1:10 Land annual ar fee 3, 2019 March 194	oApp	Head Monto App Hormal
otrer 1. Insuite Polle I., instan PC - 302 danse Annosy I. 64.66	Instalation Successful on 1 Devices	Actions Falled on O Devices	Upgrade Required on O Devices
as1yer (DOODE	the line of second states. The second		
ep Links	<u>R</u>		

Stopping the Edge Compute Application

1. Click Monitor App.



Figure 228 Application Monitor to Stop the Application

2. Click Stop.

Figure 229 Stop the Application

and the second			• •
Monitoring View		Feeder	Automation-DemoApp
Approximitely included on 1 Decision,			Setup to Configure Tree
44 Contrast 1 1 1 1 1 1 1 1 1 1 1 1 1	The files	100% Saray Zamas	0%
Ass Consumation			
			March March Company

3. Verify that the application is stopped.

ŝ

increased tube		Feeder-Automation-DemoApp
a sumiduly installed on 1 Develop		Switch to Cardigate Very
13 13 14 15 15 15 15 15 15 15 15 15 15	New Mark	0% brong Obrease • nor • vectors
Consumption		The State
	Maan Minnung Comunigation	Maan Thik Comumphism Maan Nationik Comumphism

Figure 230 Stopped State of the Application

Starting the Edge Compute Application

1. Click Start.

Figure 231 Start the Application

Manitaring Vine		Feed	ker-Automation-DemoApp
or successfully installed on 9 Devices).			Burlish to Configurat Visio
12 12 14 14 14 14 14 14 14 14 14 14	The second secon	0%	100% Juner Itours
ne Cernargine			The Date Marth
Heat Chi Conservation 6 010 8 000	Have Manage Consumption Base	Near Dea Concurption	Has literal Countries

2. Verify that the application is running.

Figure 232 Application Started

service of a sea		Feeder-Automation-DemoApp
p sconstdy installed on 1 Deviador.		Setto to Carillans the
f pureering	The Name State	
Ľ	(100% 0%
12		
1.00 100 100 100 100 100 100	n 2226 bide ales men 2706 eren Jaar Ales - Uning My melon & Mygar Dears	• 244 - 144 (March 1)
Countryllor.		See Sec. Sec.
	March Marriery Concerning Street	Non-Das Lanuaryten Man New Yorkshi Lanuaryten
Marco 197 Conservation		
Marc 170 Conservation	-	
6451 (Second Sec		
6400 8400 8400		5

Uninstalling the Edge Compute Application

1. Select the application to uninstall.

Figure 233 Select the Application to Uninstall



2. Uninstall the application.

Figure 234 Uninstall the Application



3. Select the device on which the application should be uninstalled.

Figure 235	Device	Selection	for	Uninstalling	the	Application
------------	--------	-----------	-----	--------------	-----	-------------

hinstall App				Feeder-Automat	tion-Demo/	App HT App
u can add more devices from	below table			Seanch Hostma	me IP Address	
				Show	т. Айзар	
M Head Name	U Address	tage		installed type		
2ED02DFFFE6E0F18	10.153,10.12	Feeder-Aut Feeder-A	tomation-DemoApp	Feeder Automation DemoAp	10	0.0
1 - 1 - 5	≠ items per page				2-141	h
IS I	→ Rems per page			Search History	1-tal I me, IP Address	
id Selected Devices	★ Rems per påge Ø åddøres	, Taga	- Health -	Sharch Hostna Last Heard	3 - Yald me P Address Adage	
In a b b S Ind Selected Devices	 Items per page IP Address 10.153.10.12 	Taga Feeder-Aut Feeder-Auto	Health	Shareh Histha Latheed 9 minutes	1-1al I me IP Address Address Address	
H I I I I S Sd Selected Devices: Hected Devices: Hunt Name 25D02DFFF5550F18 H I I F P S	 Rems per page # Address 10.153.10.12 Rems per page 	Taga Feeder-Juit Feeder-Juito	Hestin :	Search History Last Head	1-1all me, IP Address Address Back R (1-1all	A P
d 1 1 4 5 dd Selected Devices: Hected Devices: Mult Namy 24D020FFF660F18 d 1 7 9 9 5	 Rems per page # Address 10.133.10.12 Rems per page 	Taga Feeder-Aut Feeder-Auto	nation are:	Sharch History Last Head	1-1all	Alerenti Harrent

4. Application uninstallation progress status.

Figure 236 Application Uninstallation Progress

cisco Fog Director	APR. DIMOR CATROES INTING	ه ا
	Teeder-Automation-DemoApp	Feeder Automation DemoApp
F	Feeder-Automation-DemoApp Unit answer 110 Last united to 5210 tight (7 Apr	
H	Strentabet Inside Automation Constrainty on Birst of I Devices	
	D	() procedent
more Piche ; meer		Peak Nama 1200020199680118
V SDD planes	Dimensi B Complete Ris-Second Bland	
a 1er 2008		
op Units	Description Nede Automates Tena Application Helesant Notes	

5. Application uninstallation complete status.

Feeder - Automation - DemoApp Last ensure if 10 L

Figure 237 Application Uninstallation Complete

6. Application removal.

Figure 238 Application Removal

nstalled Ap	ps		
1	Facility Automotion Da	Status	
-	Ventor 01	Memory	
F	This age is not included an any deviced	00	
	Ramania		

SCADA Traffic via Edge Compute Application

Unsolicited Reporting

1. Verify that the unsolicited reports are sent from the IED to the Control Center periodically.

Figure 239 Unsolicited Report

Bit Manie Colf I Colf Age_Compton 415 Die Die Alleman 40 Die Die Die Alleman 40 <th></th> <th>B -000</th> <th></th> <th></th> <th></th> <th></th> <th>Multiplet</th> <th></th>		B -000					Multiplet	
Def Def Aussign Plant Fyre Y Verter Plant Fyre Y	05.18.Mask CNP3.00F BageCompute v0.5	The Exclusion feasier and		-	-		And drild(21,21d) - Appl(cattor Washer, Response)	sia internet in the second
DP31Mane ed Q3Mane ed Q3Mane ed Q3Mane ed Q3Ma 12,1284 000000000000000000000000000000000000	ChuPE Carla Autoriaja	Paint Sygne	Y + 1	F Value	T Duality		401 07(34(2),2301 P36(1) P36(1) 026(0) 085(0 401 07(34(2),2301 P36(1) P36(1) 00 00 2	7) 540# i 7 49 80 40 80 80 81 81
Marrie (1) Mary Typen 2) (2) <td>Taritt Martin and Columnia of</td> <td>(1) Breary imports</td> <td>8</td> <td>De</td> <td>Onine</td> <td></td> <th>44.0 407(34(13, 258) 60 40 27 55 55 55 55 55 55 55</th> <td>5 55 55 55 55 4x 40 AV</td>	Taritt Martin and Columnia of	(1) Breary imports	8	De	Onine		44.0 407(34(13, 258) 60 40 27 55 55 55 55 55 55 55	5 55 55 55 55 4x 40 AV
Verr (1) Seep 1940 2 01 One 000 <th< td=""><td>and successing and containeds</td><td>(11 Briver) implate</td><td>1</td><td>OFF</td><td>Drive</td><td></td><th>404 (01)54(23,2001 00 23 40 40 40 40 40 40 40 40 40 40 40 40 40</th><td></td></th<>	and successing and containeds	(11 Briver) implate	1	OFF	Drive		404 (01)54(23,2001 00 23 40 40 40 40 40 40 40 40 40 40 40 40 40	
THEI Commandes 1 0	Meter	TTD Intern Training	2	OF	Online		414 (01:34:21,230: 01 01 01 01 14 01 00 0	2 14 00 00 00 00 00 00
Image: Definition of the second of the se	100	(1) Investigants		04	Onine		412 87:34:11.230: 00 00 00 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00 00 00
Impair	L DNPS Commended	11 Keeper James in		100	California		AND 07:15-12.2201 00 00 00 00 00 00 00 00 00 00 00 00 0	2 00 00 00 00 00 00 00 00 00 00 00 00 00
1 1	11 HONP	10 Book of the local		-	Defendence -		#79 87134125.2281 00 00 00 00 00 00 00 00 00 00	8 88 88 88 88 88 88 88 88
Image: Space Image: Space <td< td=""><td>4 +</td><td>11 pears where</td><td></td><td>1.</td><td>Conces.</td><td></td><th>#75 #7134(21,22#) Be of do do do do do do do</th><td>0 00 00 00 00 00 00 00</td></td<>	4 +	11 pears where		1.	Conces.		#75 #7134(21,22#) Be of do do do do do do do	0 00 00 00 00 00 00 00
Image: provide in the construction of the construling and the construction of the construction	· 2 (1) -015	1) bruey reports		0.0	Cound		471 07134121.2301 00 00 00 00 00 00 00 00 00 00 00 00 0	2 00 00 00 00 00 00 00 00 00 00 00 00 00
Image: Display Image	2 · · ·	[1] Binary imputs		04	Drive		*3* #7:34121.22#1 00 00 15 09 00 14 00 0	2 20 20 20 20 20 20 20
Production III Barry Span C Office Provide	200	(1) Brivery implying		04	Online		676 87(34:21,210) De	2 40 40 42 40 40 40 40
Constaine 11	a deciment	(1) Brivary Triputs		C/F	Online		4.74 07134121.2301 00 00 00 00 00 00 00 00 00 00 00 00 0	
Normalization Normalization Normalization Normalization Normalization Change Damp B Contract Contract <t< td=""><td>D. million</td><td>Hiterry Sector</td><td></td><td>10</td><td>Sec.</td><td>2.1</td><th>#78 #7()#(21,2)#1 00 00 00 00 00 00 00 00 00</th><td>2 00 00 00 00 00 00 00</td></t<>	D. million	Hiterry Sector		10	Sec.	2.1	#78 #7()#(21,2)#1 00 00 00 00 00 00 00 00 00	2 00 00 00 00 00 00 00
	Contraction .						47% 07134123.2201 Be be be be be be be be	a de ao es as as as -
Contract	(Provide and a second	Select View - Displa	4149 287 of 28	T-Hala you're	-		Ann 07 (34.122.230) 00 00 00 00 00 00 00 00 00 00 00 00 0	
Intel City Hape Intel Address Intel Addres Intel Address Intel A	and complexantly	Table of Control of Co					41 87(34)21,2001 81 80 80 80 80 80 80 80 80	2 20 20 20 20 20 20 20 20
Definition Part attract state	CINRS CEV Haja	Ed Cutomer				-	++1 #7(14(11,118) Be de de de de de de de de de	0 00 00 00 00 00 00 00
Diff Can Paint Type V + T Veter C Guelly Diff Can Diff Can <thdiff can<="" th=""> <thdiff can<="" th=""> <thdi< td=""><td></td><td>The summary links and</td><td>CONSTRUCTION OF</td><td></td><td></td><td></td><th>Ana 07(34(21,238) 80 00 00 00 00 00 00 00 00 00 00 00 00</th><td>0 00 00 00 00 00 00 00</td></thdi<></thdiff></thdiff>		The summary links and	CONSTRUCTION OF				Ana 07(34(21,238) 80 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00
Constraine Outputy Inf Paint Type V V Vote Constraine Operation Outputy Inf Diff Operation Outputy Inf Diff Operation Outputy Inf Diff Operation Output Inf <thdiff inf<="" operatin="" operation="" output="" th=""> <thdiff operatin<="" td=""><td>I Distigna</td><td></td><td></td><td></td><td></td><td>- 1</td><th>410 07154121,250: 00 00 00 00 00 00 00 00 00 00 00 00 0</th><td>8 85 85 85 85 85 85 85 85</td></thdiff></thdiff>	I Distigna					- 1	410 07154121,250: 00 00 00 00 00 00 00 00 00 00 00 00 0	8 85 85 85 85 85 85 85 85
Littlew III Barry span B DA Onion Constraint Des 00 00 00 00 00 00 00 00 00 00 00 00 00	0	Point Type	T 4 7	Value	T - Quality	- 61	est 87:14(11,21#: 00 of 00 00 00 00 00 00 00 00 00 00 00 00 00	8 40 40 48 40 68 10 50
Unit Difference Difference <td>Pref. Ortunterine Disbally Uk</td> <td>TI Browy Hyputs</td> <td></td> <td>Do .</td> <td>Othe</td> <td>- 11</td> <th>446 07:14:21.230; 00 00 00 00 00 00 00 00 00 00 00 00 0</th> <td>2 88 88 58 50 90 90 90 90</td>	Pref. Ortunterine Disbally Uk	TI Browy Hyputs		Do .	Othe	- 11	446 07:14:21.230; 00 00 00 00 00 00 00 00 00 00 00 00 0	2 88 88 58 50 90 90 90 90
Image: Space This tray bags 1 0.9	11 12119	20 Browny Propuls	1	0.0	Orited		410 07154121.2301 00 00 00 00 00 00 00 00 00 00 00 00 0	1 00 00 00 00 00 00 00 00
CuP C	2 *	111 Broard Joseph	2	04	Crime		*10 07:19(21.210) 00 00 00 00 00 00 00 00 00	0 40 40 80 90 98 90 98
Image: Child State Image:	· BAS LOAD	111 Report Install		20	College		410 87(34(21,228) 00 00 00 00 00 00 00 00 00 00 00	* 30 40 40 40 40 40 40
Image: Second and the second	A - +	Concerns and		1	1000			
Import Cliffing Cliffing <thcliffing< th=""> <thcliffing< th=""> <th< td=""><td>EDM and</td><td>11 Briefy Prints</td><td></td><td>- CH</td><td>Drane</td><td></td><th>*** 07.1*.21.21d1 00 00 00 00 00 00 00 00 00</th><td>8 88 90 88 80 88 88 88</td></th<></thcliffing<></thcliffing<>	EDM and	11 Briefy Prints		- CH	Drane		*** 07.1*.21.21d1 00 00 00 00 00 00 00 00 00	8 88 90 88 80 88 88 88
PLB/may Space 6 Cn Online 671 (H12.126) 080 00 00 00 00 00 00 00 00 00 00 00 00	Carl Con	21, Broary Inputs	3	01	Online		416 87134122.22d) D0 00 00 00 00 00 00 00 00 00	e ao eo eo oo ao ao
State Contract Op/Subject Op/Subject <td>The sector of</td> <td>PC Brwy Inputs</td> <td>4</td> <td>On</td> <td>Online</td> <td></td> <th>eve existing 22134122.2381 88 88 88 88 88 88 88 88 88 88 88 88 8</th> <td>z zo ao zo ao ao ao ao</td>	The sector of	PC Brwy Inputs	4	On	Online		eve existing 22134122.2381 88 88 88 88 88 88 88 88 88 88 88 88 8	z zo ao zo ao ao ao ao
[]] Browy Seguith 6 0.9 Online MI MI<	A M LINE SALES	[1] Breary Hybols	1	04	Online		414 87-14 (1) 11d1 00 00 00 00 00 00 00 00 00 00 00 00 00	1 44 45 45 45 48 48 48
Till Brany legals 9 04 04 07/14/121,22401 34 42 40 40 11 40 00 41 40 40 40 40 40 40 40 40 40 Till Brany legals 9 04 94 104 97/14/121,22401 34 42 40 40 41 40 40 41 40 40 41 40		TO Browny Hispatte		09	Ordinat		100 00 00 00 00 00 00 00 00 00 00 00 00	a do do do do da da da
· · · · · · · · · · · · · · · · · · ·		Difference instantion		04	Oritine		141 87134123.2381 26 42 46 40 18 45 40 46 4	. 80 85 81, 80 80 81, 88
		D and a second s		-	4.1		00 01 00 01 01 00 00 01 00 00 01 00 00 0	
	Residences Subjects	Salest View .* Dopla	ving 281 of 281	data perit			525 07(54(2),210(00 0) 00 00 0) 00 00 01 0	0 00 01 00 00 01 00 00

2. Verify that the changed data on IED is reported to the Master by verifying that the Outstation point list (middle bottom window) matches the Master point list (middle top window).

Integrity Polling

1. Right-click the Integrity Data Poll command.

Figure 240 Execute Integrity Polling



2. Verify that the poll data from the IED to the Control Center is updated.

Figure 241 Integrity Polling Response

	B-me					
DNP1 Data Access/P	Dependent	مويا شما (يون ياد است	a to the second			11: 00 20 20 20 20 20 20 20 20 20 20 20 20
09/73 Macter and Dutstation ja	Hame	T Point Type	7.1.7	Neve	T Goalty	11 00 00 00 00 00 00 00 00 00 00 00 00 00
Mader	8.42	212 Binary Inputs	8	04	Coing	The control of the second seco
-	0.41	111 Binary Hyuts		08	Online	
DNPS-Commandit_(4	0.42	20 Broke Hawkin	2	04	Oning	11 H M M AL
1 - CT - T	16.45	[1] Brony Hands	1.0.1	(De	Onine	
· · · · · · · · · · · · · · · · · · ·	81.84	(1) Binary Inputs	4	08	Online	to seas star fraces request to request: Class Data Poll
241-04	10.45	(1) Briary Insula	5	CH.	Online	So So Object Silleren the of Structure), veriation 1, wellfile Soll(
	8.46	[1] Biney Inputs		On .	Onine	Time - Borebill Alcology 20
* 100 + CNP	8.47	(1) Binary Inputs		OR .	Online	As Object 2(Hinary Deput Diarge), variation 3, qualifier Bel2(8 Mit 3
	0.44	(TERNAR) Inputs		04	Online	6) BiFat19 Dic17(21,118 (Invalid) Minary Input 000000 + dott.
Control Relay Curput Block		THE ROOM STREET		100	Children and	
O Instite Unsaliched Menagen	Select Very	· Displaying Set of Set	date protect			In Object Silcomen time of Octarrence), variation 1, qualifier dedity in time = MPAGIF MIABADE.200
Construction of the local division of the	800					As Object 2001ary Dept Dangel, weisting 1, wallflar BE219 821 5
Construction from the statement of	10000	Contract Contractor	-11010-1			A: Directo Deuteret, 20 (Invalid) Sinery Dout 20000 + Dell Directo Directo Directo Alt (Invalid) Sinery Dout 20000 + Dell
Artistee	Day a course		a to the course			
	Name	T Point Type	TIT	Nalue	T Gualty	No. Time + difebab double.300
Change Data (1	11.42	111 Brown Instalts		04	Ordere	
DNPS CS1 Filep	8.41	111 Binary Inputs	1	CH	Delive	TO STARLY DELOGISE, INS Invalid) Blary Input BODOD + Buti
tradit	2.52	THE Broke basels		10	Crime	Real and the second sec
a poster	0.43	[1] Brany inputs		- D4	Cellie	Binary Input (00000 - Bell)
Dutstative Duplay for	81.44	[1] Broky Inputt	4	C6	Online	fi Binary Input 000001 - 2x45
4214	8.41	(1) Binary Inputs		CM.	Cintine	Binary Teput 000001 + 0401
*	1 m	[1] Breary Inputs		01	Crime	fill Blowy Input 600004 - Belli
E KO NONA		[1] Breey Inputs		04	Dohne	Bikary liput 600000 - Bett
	and the second se	- I THE DOCUMENT AND ADDRESS OF			Contract of the local division of the local	and the second sec

3. Verify that the changed data on IED is reported to the Master by verifying the Outstation point list (middle bottom window) matches the Master point list (middle top window).

Control Commands

1. Right-click the Integrity Data Poll command.

Figure 242 Execute Control Command



2. Verify that the Control Command from the Control Center to the IED is updated.

IP Services





3. Verify that the control command is being sent out from the Master (first red box in the right-most window) and also verify that the control command executed successfully on the IED/outstation by looking for status=SUCCESS in the second red box in the right-hand window.

IP Services

This section describes QoS policy and NAT configuration on both the DA Gateways and the Mesh DA Gateways. The first section covers IP services applicable to the DA Gateways and the second section describes IP services applicable to DA Mesh Gateways. The QoS policy is configured on the DA Gateways while on DA Mesh Gateways only DSCP marking is applicable. The configurations and the necessary steps have been illustrated with the help of screenshots.

IP Services on Cellular DA Gateways

Quality of Service

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

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

QoS is a key feature when designing the multi-services Distribution Automation solution since traffic from AMI, DA, Remote Workforce, and network management use cases must be differentiated and prioritized. Estimated transport losses, delay, and jitter introduced by networking devices must be understood when forwarding sensitive data, particularly when a WAN backhaul link offers a limited amount of bandwidth.
In the case of dual-WAN interfaces with different bandwidth capabilities (that is, cellular), QoS policies must be applied to prioritize the traffic allowed to flow over these limited bandwidth links, to determine which traffic can be dropped, etc. A multi-services DA solution and QoS DiffServ can apply to traffic categorized as:

- IPv4 Traffic-Distribution Automation (FLISR), protocol translation (RTU monitoring), and network management
- IPv6 Traffic-IPV6 IED AMI and network management

Figure 211 lists the different priorities among Distribution Automation traffic.



Figure 244 DA Traffic Priority Chart

Following the IETF Differentiated Service model, the DA solution will deliver a service type that is based on the QoS specified by each packet. This specification can occur in different ways, for example, using the IP DSCP bit settings in IP packets or source and destination addresses. The QoS specification can be used to classify, mark, shape, and police traffic, and to perform intelligent queuing.

Cellular DA Gateways and FARs perform QoS actions on the Layer 3 (Cellular, Ethernet) interfaces. The sequencing of QoS actions on egress traffic is as follows:

- 1. Classification
- 2. Marking
- 3. Queuing

Upstream QoS: DA IED to SCADA

The DA IEDs perform the marking functionality. If the IED does not have capability to mark the IP packets, the DA Gateway or SSR can perform the marking functionality. On egress WAN interface, queuing will be performed. High priority FLISR and GOOSE traffic will be assigned in Low Latency Queue. Medium priority traffic like Volt/VAR and MMS will be assigned in Class-Based Weighted Fair Queue 1, and IOT FND Network management traffic will be assigned in Class-Based Weighted Fair Queue 2. The rest of the traffic will be treated with normal priority and will be assigned to a default queue. All QoS is done based on DSCP marking.

Note: It is recommended to define queuing bandwidth as a remaining percentage instead of in values so that the same policy can be applied across Cellular or Ethernet backhaul interfaces.

Headend Router–The ASR 1000, which supports a rich QoS feature set from Cisco IOS, provides DoS protection for applications like the FND and SCADA. Refer to the latest documentation link for complete details:

https://www.cisco.com/c/en/us/products/collateral/routers/asr-1002router/solution_overview_c22-449961.html



Figure 245 Upstream QoS IED to SCADA

Note: If the IEDs don't have the capability to perform the marking or if the marking done by IED needs to remarked, then the MQC policy on Ethernet can re-mark the DSCP values for the incoming traffic.

Note: A sample configuration to mark traffic on Ethernet interface:

```
class-map match-any dscp_ethernet
  match dscp default
  policy-map dscp_ethernet
      class dscp_ethernet
        set dscp af11
  interface GigabitEthernet 2/1
      service-policy input dscp_ethernet
```

Raw Socket QoS Marking

If RTU is connected to DA Gateway via the R232 async serial interface and if the Raw Socket feature is enabled, marking will be enabled on the serial line.

Class-based policy is not supported on serial interfaces. The packets received on the serial interface should be marked on the corresponding line of the serial interface. The following configurations should be applied on the line interface:

raw-socket tcp dscp <value>

After marking the packets from the serial interface, these marked packets can be prioritized at the WAN interface using the following class-map and policy-map. Since the SCADA traffic is encapsulated before it is sent out via the tunnel interface on the WAN interface, the QoS pre-classify command should be applied on the corresponding tunnel interface.

Queuing on DA Gateway WAN Port

policy-map SS class FLISR priority level 1

```
class volt-var
priority level 2
class NMS
priority level 1
class class-default
```

Network Address Translation

The IoT Gateway is capable of supporting both NAT and non-NAT scenarios described in the Design Guide. The NAT scenario has been implemented in this Implementation Guide.

Note: This configuration is pushed as part of ZTD (during device registration phase). The FND leverages the SCADA Application Traffic Enablement profiles discussed in Appendix E: HER and CGR Configurations, page 250.

Note: The Loopback address is assigned to the IoT Gateway during the Tunnel provisioning phase of ZTD and it uniquely represents the IoT Gateway in the solution.



Figure 246 Network Address Translation

In Figure 213, the SCADA Master communicates with the IP address of the IoT Gateway (represented by its loopback address-for example, 192.168.150.21) on port number 20000.

Once the communication reaches the IoT Gateway, the NAT table is referenced for the IoT Gateway IP (for example, 192.168.150.21) and port 20000, and the IP address and port number of the IED is derived.

Communication is then forwarded to IED IP (192.168.0.2) on port 20000. In summary:

- The SCADA communication on 192.168.150.21 on port 20000 is sent to IED1:20000.
- The SCADA communication on 192.168.150.22 on port 20000 is sent to IED2:20000.

In Figure 213 above, the SCADA Master communicates with the IP address of the IoT Gateway (represented by its loopback address, for example, 192.168.150.21) on port number 20000.

Once the communication reaches the IoT Gateway, the NAT table is referenced for the IoT Gateway IP (for example, 192.168.150.21) and port 20000, and the IP address and port number of the IED is derived.

Communication is then forwarded to IED IP (192.168.0.2) on port 20000. In summary:

- The SCADA communication on 192.168.150.21 on port 20000 is sent to IED1:20000.
- The SCADA communication on 192.168.150.22 on port 20000 is sent to IED2:20000.

NAT on IR1101

1

The Layer 3 port connected to the IED is VLAN1, which should be enabled as a NAT-inside interface. The Layer 3 port providing connectivity to the control center is the FlexVPN IPSec Tunnel interface, which should be enabled as a NAT-outside interface.

Note: The Fast Ethernet ports of IR1101 are Layer 2. The Layer 3 IP address is configured on the VLAN interface:

```
interface Loopback0
ip address 192.168.150.21 255.255.255.0 /* configured during ZTD */
!
interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
int FastEthernet 0/0/1
switchport access vlan 1
!
interface Tunne10
ip nat outside
!
! /* NAT the traffic on Loopback_IP:20000 to 192.168.0.2(IED_IP):2404 */ ip nat inside source
static tcp 192.168.0.2 2000 interface Loopback0 20000
```

NAT on IR807

The Layer 3 port connected to the IED is FastEthernet1, which should be enabled as a NAT-inside interface. The Layer 3 port providing connectivity to the control center is the FlexVPN IPSec Tunnel interface, which should be enabled as a NAT-outside interface.

Note: The Fast Ethernet ports of the IR807 are Layer 3:

```
!
interface Loopback0
ip address 192.168.150.22 255.255.255.0 /* configured during ZTD */
!
interface FastEthernet1
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in duplex auto speed auto
!
interface Tunne10
    ip nat outside
!
! /* NAT the traffic on Loopback_IP:20000 to 192.168.0.2(IED_IP):20000 */ ip nat inside source
static tcp 192.168.0.2 20000 interface Loopback0 20000
```

NAT configurations on other IoT Gateway platforms (such as CGR1000 and IR8xx platforms) would be similar to the ones captured above.

IP Services on Mesh DA Gateways

QoS on IR510

QoS is an IOS feature that is applicable to DA gateways. QoS on Mesh gateways isn't MQC based and they support only DSCP marking of the packets. This DSCP marking is available to the user and can be applied to the Ethernet interface or the serial interfaces. The marking can be easily done from FND. The following subsections describe how to enable marking on both Ethernet and serial interfaces.

Marking Ethernet Traffic on IR510

Marking on Ethernet interface can be performed in two ways:

First, all the traffic that is being transmitted on the Ethernet interfaces can be marked:

- 1. To mark all the packets, choose the CONFIG menu from the top bar.
- 2. Select Device Configuration from the drop-down config menu.
- 3. From the left menu, choose the ENDPOINT that was registered with FND.
- 4. Now select Edit Configuration Template, as shown in Figure 247. From the highlighted text, we can observe that DSCP settings can be changed according to the use case.
- 5. Once the DSCP marking has been defined, go to the push configuration and push the modified config to your device.

Figure 247 DSCP Marking on Ethernet Traffic

and the second in the second	B-beetCelgen: X		- 0
- C Q	A man 112 (K10) URD/012 provide the statistic t	@ Q	N (D) =
THE REPORT OF THE	RADINGAN CONCERNING CONCERNING CONCERNING		20
Depres - Devoirs connectivities			
and a second second second second			A CAR

Second, the DSCP marking can be set for packets from a particular source:

- 1. To mark the packets from a particular source, choose the CONFIG menu from the menu bar.
- 2. Select Device Configuration from the drop-down config menu.

- 3. From the left menu, choose the Config Profiles tab.
- 4. Now select **Default-DSCP-profile** or create a profile with a user-defined name by clicking the '+' button.
- 5. In the profile from the above step, add the **source address** and **DSCP marking value**. An example is shown in Figure 248.

The Default-DSCP-Profile or User defined profile should be added to the configuration template for the specific ENDPOINT. This shown at the end of this section.

Figure 248 DSCP Marking on Ethernet Traffic from a Source Address

In Life you signey partment fast gap		- 0 *
		N D 2
O Mathing & Impactant	17 (NR) - O U	W (D) =
	sessions second contactors conta-	= a.
ENVIOLE RECEPTION CONTRACTOR	CONTRACTOR CONTRACTOR	the bergin
Parign Derteit in ftreige Charge Derive Pressa Dieffault-D.DVD-Frieflit		
Receipt Carrilly Profiles		
Displayed in the line and a second se		
The second secon		
142 We 8.8 Mailing		
· Fail HOPLE		
Distant faiture		
* DESP PROFILS		
I Second Still Prome		
* HART PEOPLE		
By Map due to Mark 9.4		
CE Televis MART Produce		
* 1×12 51/1×1 0000 x.3:		
C Defend DeCP. Check Proline		
* 64744 PEDPAR		
The second matter Product		
* DICK GROUP PROFILE		
CD Tradeoff Dimiter-Barrier Protote		
1 9 9 9 9 4 POT N.K.		
Re stage das a filmitan T		
R Magnature Sector2		
The best of the set of		
# 2112-2114 Circu Symae, Ad. Add Adda Booth of Journal (192-79)	Salas II	11 A

Marking Serial Traffic on IR510

Similar to the marking of packets over Ethernet interface, packets from serial interface can be marked. To mark the packets from serial interface, complete the following steps:

- 1. Click CONFIG on the menu bar.
- 2. Select Device Configuration from the CONFIG drop-down menu.
- 3. Select the Config Profiles tab from the left menu.
- 4. Select Migrated Serial-1 or create a serial profile by clicking the '+' button.
- 5. Configure the Serial Properties and select the DSCP marking value, as shown in Figure 249.
- 6. Save the profile and add it to the correct ENDPOINT.

Figure 249 DSCP Marking on Serial Traffic



- 7. The Config Profiles modified or created should be added to the correct ENDPOINT under the EDIT Configuration Template present in the Groups tab in the left menu.
- 8. Scroll under the Edit Configuration Template.
- **9.** Add the **Ethernet DSCP marking profile**, **serial profile**, and any other profiles required under the respective sections. The highlighted part in Figure 250 shows the profiles that are added in the respective fields.
- **10.** After adding the **Config Profiles**, from **Push Configuration**, push the configs to the **Mesh DA Gateway**.

Figure 250 Adding Config Profiles in Edit Configuration Template

of Hit-benclonger: A. III of	10: Desertadipati-X 🔹 Nacia 🛛 🔺 🔶				
+ C Q 0	Content (172.16.123.128-144, provide the international of the first second seco			- 8 4	* 0
M Thus between consists			EVICES OPERADONS + COPIC - ADMIN + .		
THE + DEVICE CONTRACTOR			1 A A A A A A A A A A A A A A A A A A A		
mige become in Street 2 Street backer for	Britshin (1990)				
-	Taxa Memory and				
a sets	The States and States and States and States	away have been been been been			
Carl parameter the said is	•				
PERCEPTION.	 (1) more and (1) and (2) and (2)	5			
a real and instant in	404				
	- Adams building kritigt				
C Celaste sup spine (*)	Adaptive Adaptive (2)				
CI Debutto (198.12)	Active	to NET Charles			
CE Company and all	OCH BINGS IN 1995.10	100 CT			
a Bactercand	18 100.0	Name IV			
	idea et	and the second sec			
CI Origentation of	1794.0	lange -			
	(r)w.2	They a			
	uroe e	in the second			
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
	Note: This settings to supplication for 188-19 & 288-19 April and one only				
	Fill Purfac Ibana [2]				
	SSCP Prefix Default DSCP Prefix [16] E				
	Contraction of the second second				
	DICP Date Partie June In				
	collad Poplar (Datashilud bi Posta) (2)				
	terufation cost appressants i al la				
	All finite and and all finite				
	Taken In				
			<u>a</u>		
Scilic and free forms for all fight from	3-mm \$43.78	Saulas 75		water and the state	

NAT on IR510

NAT is required on the IR510. The IEDs are connected to the IR510 using a private IP addresses. These private addresses are not reachable from the Control Center. Therefore, the NAT-44 profile in the Config Profiles need to be set and pushed to the IR510 for the devices to be reachable from the Control Center.

To configure a NAT-44 profile, complete the following steps:

Note: Private IP addresses are considered so that all the IEDs could be configured with same IPv4 address 192.168.0.3, which causes the operational simplicity.

- 1. Select CONFIG from the Menu bar.
- 2. Select Device Configuration from the CONFIG menu bar.
- 3. Select Config Profiles from the left menu.
- 4. Select Default NAT-44 profile or create a user-defined NAT-44 profile by clicking the '+' button.
- 5. Add the source address and the respective source and destination port numbers for NAT to be configured on the IR510.
- 6. Save the profile and add the profile in the EDIT Configuration Template of the correct ENDPOINT, as shown in the previous subsection.

Figure 251 Modifying Default NAT-44 Profile



NTP

Services running on the FAN require time synchronization. The time synchronization for DA Gateways and Mesh DA Gateways are pushed from the FND while tunnel provisioning and Mesh Gateway registration occurs. For headend components such as the RA, CA, and FND, we use HER as the NTP server.

The NTP server on the HER is configured using the following command:

ntp server <server ip>

Note: The above command, which is part of ZTD process, is for reference only.

A similar command is used on DA gateways for time synchronization.

Appendix A: PnP Profiles

This appendix includes the following major topics:

- Bootstrapping Template for IPv4 Network, page 226
- Bootstrapping Template for IPv6 Network, page 229
- Bootstrapping Template for Provisioning and ZTD at the Deployed Location, page 230

Bootstrapping Template for IPv4 Network

Bootstrapping of the IoT Gateways that would NOT be deployed behind the NAT

These substitutions needs to be performed in the following bootstrapping template:

- fingerprint 'CFA2613029B11E461430A2DC5F624147CCEE6469' must be replaced by the fingerprint of the RSA CA server that issues the certificate to the FND, TPS and FAR.
- ip host entries of RA, TPS & NTP servers must be updated.

Bootstrap Profile Name: IPv4-BOOTSTRAP

```
</#if>
IPv6 unicast-routing
ntp server ntp.ipq.cisco.com !! Enable time-stamps
          localtime show-timezone
!
<#if pid?starts with("IR1101")> hostname IR1100 ${sn} <#elseif pid?starts with("IR807")> hostname
IR807 ${sn}
<#elseif pid?starts_with("IR809")> hostname IR809_${sn}
<#elseif pid?starts with("IR829")> hostname IR829 ${sn}
<#elseif pid?starts with("CGR1240")> hostname CGR1240 ${sn}
<#elseif pid?starts with("CGR1120")> hostname CGR1120 ${sn}
</#ifaaa authentication login default local
1
1
!username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}pki
profile enrollment LDevID enrollment url http://ra.ipg.cisco.com enrollment credential
CISCO IDEVID SUDIkey generate rsa label LDevID modulus 2048
serial-number noneip-address none password
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
revocation-check none 2048
cgna profile cg-nms-tunnel
add-command show hosts | 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 interval 10
url https://tps.ipg.cisco.com:9120/cgna/ios/tunneldo delete /force /recursive flash:
do mkdir flash:archive archive!
!! configure WSMA profiles
wsma profile listener exec profile!! mapping WSMA profile to WSMA agent configsÖ profile
config profile version 2
ip ssh rsa keypair-name LDevID
1
1
<#if pid?starts with("IR110")> ip http secure-port 443
<#else>
</#if>
```

```
!
!
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha ip http
secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
ip http max-connections 5
!
ip http secure-client-auth
ip http secure-trustpoint CISCO IDEVID SUDI
!ip http client connection timeout 5
!ip http client connection retry 5
!
! Disabling http server no ip http server
1
! Enabling http secure server. ip http secure-server
1
1
!
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 180 event manager
environment ZTD_SCEP_Debug TRUE
1
!sparrow event manager directory user policy "bootflash:/managed/scripts" event manager directory
user policy "flash:/eem"
!! The following command will activate the policy..
event manager policy tm_ztd_scep.tcl type system authorization bypass
1
1
!! When the config is applied, old applets can be removed. no event manager applet get-ca-cert no
event manager applet disable-pnp-sec-enf
```

Bootstrapping of IoT Gateways that would be Deployed behind NAT

These substitutions need to be performed in the following bootstrapping template:

- fingerprint 'CFA2613029B11E461430A2DC5F624147CCEE6469' must be replaced by the fingerprint of the RSA CA server that issues the certificate to the FND, TPS and FAR.
- ip host entries of RA, TPS & NTP servers must be updated.

Bootstrap Profile Name: IPv4-BOOTSTRAP-NAT

```
</#if>
boot-end-marker
</#if>
1
!! ip host configurations
ip host ra.ipg.cisco.com <ra-ipv4.ipg.cisco.com> ip host tps.ipg.cisco.com <tps-ipv4.ipg.cisco.com>
ip host ntp.ipg.cisco.com <public-ntp-server-ip>
!
<#if pid?starts with("IR8") || pid?starts with("CGR")> ntp update-calendar ip cef
</#if>
IPv6 unicast-routing
!! Enable time-stamps
localtime show-timezone !
<#if pid?starts with("IR1101")> hostname IR1100 ${sn}
<#elseif pid?starts with("IR807")> hostname IR807 ${sn}
<#elseif pid?starts_with("IR809")> hostname IR809_${sn}
```

```
<#elseif pid?starts with("IR829")> hostname IR829 ${sn}
<#elseif pid?starts with("CGR1240")> hostname CGR1240 ${sn}
<#elseif pid?starts with("CGR1120")> hostname CGR1120 ${sn}
</#if>
aaa authentication login default local
1
1
!username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
enrollment url http://ra.ipg.cisco.com enrollment credential CISCO IDEVID SUDI
!
crypto key generate rsa label LDevID modulus 2048
trustpoint LDevID enrollment mode ra enrollment profile LDevID fqdn none
ip-address none password
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
revocation-check none!
cgna gzip
1
1
interface loopback999
description workaround for CSCvb49055 ip address 169.254.1.1 255.255.255.255
1
cgna initiator-profile cg-nms-tunnel
callhome-url https://tps.ipq.cisco.com:9120/cqna/ios/config execution-url
https://169.254.1.1:8443/wsma/config
post-commands!
add-command show hosts | format flash:/managed/odm/FND.odm add-command show interfaces | format
flash:/managed/odm/FND.odm add-command show version | format flash:/managed/odm/FND.odm add-command
show IPv6 dhcp | format flash:/managed/odm/FND.odm
add-command show IPv6 interface | format flash:/managed/odm/FND.odm interval 10
1
do delete /force /recursive flash:archive do mkdir flash:archive archive
path flash:/archive maximum 8
!! configure WSMA profiles
wsma profile listener config profile transport https path /wsma/config wsma profile listener
exec_profile transport https path /wsma/exec
!! mapping WSMA profile to WSMA agent configs wsma agent config profile config_profile wsma agent
exec profile exec profile
!
1
1
<#if pid?starts_with("IR110")> ip http secure-port 443
<#else>
ip http secure-port 8443
</#if>
!
1
ip http authentication aaa login-authentication default
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
ip http timeout-policy idle 600 life 86400 requests 3 ip http max-connections 5
ip http secure-client-auth
ip http secure-trustpoint CISCO_IDEVID_SUDI
1
!ip http client connection timeout 5
!ip http client connection retry 5
1
! Disabling http server no ip http server
```

Bootstrapping Template for IPv6 Network

Bootstrapping of the IoT Gateways that would NOT be deployed behind the NAT

These substitutions need to be performed in the following bootstrapping template:

- fingerprint 'CFA2613029B11E461430A2DC5F624147CCEE6469' must be replaced by the fingerprint of the RSA CA server that issues the certificate to the FND, TPS and FAR.
- ip host entries of RA, TPS & NTP servers must be updated.

Bootstrap Profile Name: IPv6-BOOTSTRAP

```
<#elseif pid?starts with("CGR1240")> hostname CGR1240 ${sn}
<#elseif pid?starts_with("CGR1120")> hostname CGR1120_${s}
</#if>
new-model
aaa authentication login default local aaa authorization exec default local
!
!
username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
profile enrollment LDevID enrollment url http://ra.ipg.cisco.com enrollment credential
CISCO IDEVID SUDI
key generate rsa label LDevID modulus 2048
pki trustpoint LDevID enrollment mode ra enrollment profile LDevID none fqdn none
ip-address nonefingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
revocation-check none rsakeypair LDevID 2048
!
cgna gzip
1
cgna profile cg-nms-tunnel
add-command show hosts | 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 interval 10
url https://tps.ipg.cisco.com:9120/cgna/ios/tunnel gzip
1
!
1
do delete /force /recursive flash:archive do mkdir flash:archive archive
path flash:/archive maximum 8
I.
config profile transport https path /wsma/config wsma profile listener exec profile transport https
path /wsma/exec
wsma agent config profile config profile wsma agent exec profile exec profile
!
!
ip ssh version 2
ip ssh rsa keypair-name LDevID
<#if pid?starts with("IR110")> ip http secure-port 443
<#else>
ip http secure-port 8443
</#if>
!
```

!

```
!
1
ip http authentication aaa login-authentication default
ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
ip http timeout-policy idle 600 life 86400 requests 3 ip http max-connections 5
ip http secure-trustpoint CISCO_IDEVID_SUDI
1
!ip http client connection timeout 5
!ip http client connection retry 5
1
! Disabling http server no ip http server
1
! Enabling http secure server. ip http secure-server
   1
!sparrow event manager directory user policy "bootflash:/managed/scripts" event manager policy
no config replace.tcl type system authorization bypass
!! The following command will activate the policy..
1
!! When the config is applied, old applets can be removed. no event manager applet get-ca-cert no
event manager applet disable-pnp-sec-enf
1
1
event manager environment ZTD SCEP Enabled TRUE
!
event manager applet REMOVE IDEVID AS TP
event timer watchdog name remove-idevid-as-http-client-trustpoint time 30 maxrun 120 action 1.1 cli
command "enable"
action 1.2 cli command "show crypto pki trustpoints LDevID status" action 1.3 string match
"*Granted*" "$_cli_result"
action 1.4 puts "Match Result = $ string result" action 1.5 if $ string result eq "1"
action 1.6 puts "EEM:: FAR successfully retrieved LDevID certificate from CA" action 1.7 cli
command "configure terminal"
action 1.8 puts "EEM:: Removing CISCO IDEVID SUDI to enable Tunnel Provsioning" action 1.9 cli
```

```
command "no ip http client secure-trustpoint CISCO_IDEVID
```

Bootstrapping Template for Provisioning and ZTD at the Deployed Location

Bootstrapping of the IoT Gateways

These templates are used when the bootstrapping location and deployment location are the same. No manual intervention is need. Once the device is powered with a SIM card inserted, bootstrapping should begin and push the configuration from FND. The following template is an example of the template validated for IR1101. The template can be used for other platforms with minor changes such as the cellular interface.

!

ı

```
boot system flash:${far.bootimage}
      </#if>
     boot-end-marker
    </#if>
    1
    ip host ra.ipg.cisco.com 72.163.222.228
    ip host tps.ipg.cisco.com 72.163.222.227
   ip host ntp.ipg.cisco.com 123.108.200.124
    ip domain name ipg.cisco.com
 <#if pid?starts with("IR8") || pid?starts with("CGR")>
ntp update-calendar
ip cef
</#if>
ipv6 unicast-routing
   ntp server ntp.ipg.cisco.com
    clock timezone IST 5 30
    !! Enable time-stamps
    service timestamps debug datetime msec localtime show-timezone
    service timestamps log datetime msec localtime show-timezone
    1
    <#if pid?starts with("IR1101")>
    hostname IR1100 ${sn}
    ip forward-protocol nd
    <#elseif pid?starts_with("IR807")>
   hostname IR807_${sn}
    <#elseif pid?starts with("IR809")>
   hostname IR809 ${sn}
    <#elseif pid?starts_with("IR829")>
    hostname IR829_${sn}
    <#elseif pid?starts with("CGR1240")>
    hostname CGR1240 ${sn}
    <#elseif pid?starts_with("CGR1120")>
    hostname CGR1120 ${sn}
    </#if>
    1
    aaa new-model
    aaa authentication login default local
    aaa authorization exec default local
    1
    1
    username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
    username cisco privilege 15 algorithm-type sha256 secret Cisco@123
    1
    crypto pki profile enrollment LDevID
    enrollment url http://ra.ipg.cisco.com
    enrollment credential CISCO_IDEVID_SUDI
    1
    crypto key generate rsa label LDevID modulus 2048
    crypto pki trustpoint LDevID
    enrollment mode ra
    enrollment profile LDevID
    serial-number none
    fqdn none
    ip-address none
    password
    fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
    revocation-check none
    rsakeypair LDevID 2048
```

Ţ

```
cgna gzip
 1
interface cellular0/1/0
description Connection to DMZ UCS
 ip address negotiated
  dialer in-band
 dialer idle-timeout 0
  dialer watch-group 1
  dialer-group 1
  pulse-time 1
   ipv6 enable
 1
 !controller Cellular 0/1/0
 ! lte sim data-profile 1 attach-profile 1 slot 0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ip route 0.0.0.0 0.0.0.0 cellular 0/1/0
 1
 1
 1
 interface loopback999
description workaround for CSCvb49055
 ip address 169.254.1.1 255.255.255.255
 1
cgna initiator-profile cg-nms-tunnel
callhome-url https://tps.ipg.cisco.com:9120/cgna/ios/config
execution-url https://169.254.1.1:443/wsma/config
post-commands
active
1
!
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 version | 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
gzip
interval 10
1
 !
 !
 1
do delete /force /recursive flash:archive
do mkdir flash:archive
archive
path flash:/archive
maximum 8
 1
 !
 !
 1
wsma profile listener config_profile
transport https path /wsma/config
wsma profile listener exec profile
 transport https path /wsma/exec
 !
wsma agent config
profile config_profile
wsma agent exec
profile exec profile
 !
```

```
!
    1
    ip ssh version 2
    ip ssh rsa keypair-name LDevID
    1
    1
    <#if pid?starts with("IR110")>
    ip http secure-port 443
    <#else>
    ip http secure-port 8443
    </#if>
    1
    !
    1
    ip http authentication aaa login-authentication default
    !ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
    !ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
    ip http timeout-policy idle 600 life 86400 requests 3
    ip http max-connections 5
    ip http secure-client-auth
    ip http secure-trustpoint CISCO_IDEVID_SUDI
    1
    !ip http client connection timeout 5
    !ip http client connection retry 5
    1
! Disabling http server
no ip http server
!
! Enabling http secure server.
ip http secure-server
1
!
    1
    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 180
    event manager environment ZTD_SCEP_Debug TRUE
    1
    !sparrow event manager directory user policy "bootflash:/managed/scripts"
    event manager directory user policy "flash:/eem"
    event manager policy no_config_replace.tcl type system authorization bypass
    !! Below command will activate the policy..
    event manager policy tm_ztd_scep.tcl type system authorization bypass
    1
    1
    !! When the config is applied, old applets can be removed.
    no event manager applet get-ca-cert
    no event manager applet disable-pnp-sec-enf
    1
    1
    event manager environment ZTD SCEP Enabled TRUE
   event manager applet REMOVE IDEVID AS TP
     event timer watchdog name remove-idevid-as-http-client-trustpoint time 30 maxrun 1200
     action 1.1 cli command "enable"
     action 1.2 cli command "show crypto pki trustpoints LDevID status"
     action 1.3 string match "*Granted*" "$ cli result"
     action 1.4 puts "Match Result = $_string_result"
     action 1.5 if $_string_result eq "1"
     action 1.6 puts "EEM:: FAR successfully retrieved LDevID certificate from CA"
     action 1.7 cli command "configure terminal"
```

```
action 1.8 puts "EEM:: Removing CISCO IDEVID SUDI to enable Tunnel Provsioning"
     action 1.9 cli command "no ip http client secure-trustpoint CISCO IDEVID SUDI"
     action 2.0 puts "Cli result = $ cli result"
     action 2.1 cli command "do cgna exec profile cg-nms-tunnel"
    action 2.2 puts "EEM:: Removing the applet manager REMOVE_IDEVID_AS_TP as the CLI change is
done"
     action 2.3 cli command "no event manager applet REMOVE IDEVID AS TP"
     action 2.4 cli command "exit"
    action 2.5 else
    action 2.6 puts "EEM:: LDevID not Granted yet. Will check after 30 seconds"
    action 3.0 end
1
 ! track 1 interface Cellular0/1/0 line-protocol
 ! delay down 5 up 10
1
  ! event manager applet Default route via Cellular
      !event track 1 state up
!trigger delay 600
!action 1.0 cli command "enable"
!action 1.1 cli command "show run | sec ZTD SCEP Enabled"
!action 1.2 string match "*TRUE" "$ cli result"
!action 1.4 puts "Match Result = $_string_result"
   !action 1.5 if $_string_result eq "1"
!action 1.6 cli command "configure terminal"
!action 1.7 cli command "ip route 0.0.0.0 0.0.0.0 cellular 0/1/0"
!action 1.8 puts "Added Default route via Cellular"
!action 1.9 else
!action 2.0 puts "Could not added Default route via Cellular"
!action 2.1 end
1
no file prompt quiet
exit
 </#if>
  1
<#else>
 ${provisioningFailed("FAR is not running IOS")}
</#if>
```

Appendix B: FND Zero Touch Deployment Profiles

This appendix includes the following major topics:

- Tunnel Provisioning Profiles, page 235
- Tunnel Group for IPv6 Network, page 239

Tunnel Provisioning Profiles

The Tunnel Provisioning Profile could also be referred to as the "Tunnel Group." For steps to create a new Tunnel group, please refer to the "Creating Tunnel Groups" section of the Cisco IoT FND guide.

Once the tunnel group is created, move the IoT Gateways under the appropriate "Tunnel Group." For steps, please refer to the "Moving FARs to another group" section of the Cisco IoT FND guide.

Tunnel Group for IPv4 Network

Note: To have the IoT Gateway operate in Dual Control Center scenarios, populate the fields for **tunnelSrcInterface2** and **IPSecTunnelDestAddr2**. Leave them empty for single control center scenarios.

Note: Substitute the IP address with your FND IP address for fnd.ipg.cisco.com in the following template:

```
<#-- This template only supports FARs running IOS. -->
<#if !far.isRunningIos()>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

```
<#--
```

For FARs running IOS, configure a FlexVPN client in order to establish secure communications to the HER. This template expects that the HER has been appropriately pre-configured as a FlexVPN server:

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

<#-Configure a Loopback0 interface for the FARL</pre>

```
-->
interface Loopback0
<#--
```

If the loopback interface IPv4 address property has been set on the CGR, configure the interface with that address. Otherwise, obtain an address for the interface now using DHCP:

```
-->
<#if far.loopbackV4Address??>
<#assign loopbackIpv4Address=far.loopbackV4Address>
<#else>
<#--
```

Obtain an IPv4 address that can be used for this FAR's Loopback interface. The template API provides methods for requesting a lease from a DHCP server. The IPv4 address method requires a DHCP client ID and a link address to send in the DHCP request. The third parameter is optional and defaults to "IoT-FND." This value is sent in the DHCP user class

option. API also provides the method "dhcpClientld," which takes a DHCPv6 Identity association identifier (IAID) and a DHCP Unique IDentifier (DUID) and generates a DHCPv4 client identifier as specified in RFC 4361. This provides some consistency in how network elements are identified by the DHCP server.

```
-->
<#assign loopbackIpv4Address=far.ipv4Address(dhcpClientId(far.enDuid,0),far.dhcpV4LoopbackLink
).address>
</#if>
ip address ${loopbackIpv4Address} 255.255.255.255
<#--</pre>
```

If the loopback interface IPv6 address property has been set on the CGR, configure the interface with that address. Otherwise, obtain an address for the interface now using DHCP:

```
-->
<#if far.loopbackV6Address??>
<#assign loopbackIPv6Address=far.loopbackV6Address>
<#else>
<#--
```

Obtain an IPv6 address that can be used to for this FAR's loopback interface. The method is similar to the one used for IPv4, except clients in DHCPv6 are directly identified by their DUID and IAID. IAIDs used for IPv4 are separate from IAIDs used for IPv6, so we can use zero for both requests:

```
-->
<#assign loopbackIPv6Address=far.IPv6Address(far.enDuid,0,far.dhcpV6LoopbackLink).address>
</#if>
IPv6 address ${loopbackIPv6Address}/128 exit
```

Default to using FlexVPN for the tunnel configuration of FARs running IOS.

```
--> <#if (far.useFlexVPN!"true") = "true"> <#--
```

FlexVPN certificate map that matches if the peer (HER) presents a certificate whose issuer common name contains the string given in the FAR property **certissuerCommonName**:

```
-->
<#if !(far.certIssuerCommonName??)>
${provisioningFailed("FAR property certIssuerCommonName has not been set")}
</#if>
```

crypto pki certificate map FlexVPN_Cert_Map 1 issuer-name co cn = \${far.certIssuerCommonName} exit

<#--

<#--

IPv4 ACL, which specifies the route(s) FlexVPN will push to the HER. We want the HER to know the route to the CGR's loopback interface:

```
-->
ip access-list standard FlexVPN_Client_IPv4_LAN permit ${loopbackIpv4Address} exit
<#--
```

IPv6 ACL, which specifies the route(s) FlexVPN will push to the HER. We want the HER to know the route to the CGR's loopback interface. If a mesh has been configured on this CGR, we want the HER to know the route to the mesh:

```
IPv6 access-list FlexVPN_Client_IPv6_LAN
<#if far.meshPrefix??>
```

```
permit IPv6 ${far.meshPrefix}/64 any
</#if>
sequence 20 permit IPv6 host ${loopbackIPv6Address} any exit
<#-- Enable IKEv2 redirect mechanism on the FlexVPN client --> crypto ikev2 redirect client
<#--</pre>
```

Snapshot routing - for enabling connectivity between Control Center and IEDs:

```
-->
route-map snapshot permit 10
match ipv6 route-source snapshot
set tag 10
ipv6 access-list snapshot
permit ipv6 2001:DB8:267:1500::/56 any
ipv6 unicast-routing
```

<#--

FlexVPN authorization policy that configures FlexVPN to push the CGR LANs specified in the ACLs to the HER during the FlexVPN handshake:

```
-->

crypto ikev2 authorization policy FlexVPN_Author_Policy

route set access-list IPv6 FlexVPN_Client_IPv6_LAN exit

route set interface

route redistribute connected route-map snapshot

encryption aes-cbc-256 integrity sha256 exit

proposal FlexVPN_IKEv2_Proposal exit

<#-- FlexVPN authorization policy is defined locally. -->

crypto ikev2 profile FlexVPN_IKEv2_Profile

aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy authentication remote

rsa-sig

authentication local rsa-sig dpd 120 3 periodicmatch certificate FlexVPN_Cert_Map pki trustpoint

LDevID

exit
```

<#--

If the HER is an ASR, use a different configuration for the transform set since some ASR models are unable to support the set that we would prefer to use:

```
-->
<#if her.pid?contains("ASR")>
crypto IPSec transform-set FlexVPN_IPSec_Transform_Set esp-aes esp-sha-hmac mode tunnel exit
<#else>
crypto IPSec transform-set FlexVPN_IPSec_Transform_Set esp-aes esp-sha256-hmac mode tunnel
```

```
exit </#if>
```

crypto IPSec profile FlexVPN_IPSec_Profile set ikev2-profile FlexVPN_IKEv2_Profile set transform-set FlexVPN_IPSec_Transform_Set exit

<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")> interface Tunnel0
description IPSec tunnel to \${her.eid} ip unnumbered loopback0

```
IPv6 unnumbered loopback0tunnel protection IPSec profile FlexVPN_IPSec_Profile tunnel source
${wanInterface[0].name} exit
<#iif !(far.IPSecTunnelDestAddr1??)>
${provisioningFailed("FAR property IPSecTunnelDestAddr1 must be set to the destination address to
connect this FAR's FlexVPN tunnel to")}
</#if>
peer 1 ${far.IPSecTunnelDestAddr1} client connect Tunnel0
exit
<#else>
<#--</pre>
```

Configure the tunnel using DMVPN.

```
-->
router eigrp 1
network ${loopbackIpv4Address} exit IPv6 router eigrp 2 exit
interface Loopback0
IPv6 eigrp 2 exit
<#--
```

DMVPN certificate map that matches if the peer (HER) presents a certificate whose issuer's common name contains the string given in the FAR property:

```
certIssuerCommonName.
-->
<#if !(far.certIssuerCommonName??)>
${provisioningFailed("FAR property certIssuerCommonName has not been set")}
</#if>
crypto pki certificate map DMVPN_Cert_Map 1 issuer-name co cn = ${far.certIssuerCommonName} exit
crypto ikev2 proposal DMVPN_IKEv2_Proposal encryption aes-cbc-256
group 14 exit
crypto ikev2 policy DMVPN_IKEv2_Policy proposal DMVPN_IKEv2_Proposal exit
crypto ikev2 profile DMVPN_IKEv2_Profile authentication remote rsa-sig dpd 120 3 periodicmatch
certificate DMVPN_Cert_Mapexit
<#--</pre>
```

If the headend router is an ASR, use a different configuration for the transform set since some ASR models are unable to support the set that we would prefer to use:

```
- - >
<#if her.pid?contains("ASR")>
crypto IPSec transform-set DMVPN IPSec Transform Set esp-aes esp-sha-hmac mode tunnel exit
<#else>
crypto IPSec transform-set DMVPN IPSec Transform Set esp-aes 256 esp-sha256-hmac mode tunnel exit
</#if>
crypto IPSec profile DMVPN_IPSec_Profile set ikev2-profile DMVPN_IKEv2_Profile set transform-set
DMVPN IPSec Transform Set exit
<#if !(far.nbmaNhsV4Address??)>
${provisioningFailed("FAR property nbmaNhsV4Address has not been set")}
</#if>
<#if !(far.nbmaNhsV6Address??)>
${provisioningFailed("FAR property nbmaNhsV6Address has not been set")}
</#if>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")> interface Tunnel0
<#assign lease=far.ipv4Address(dhcpClientId(far.enDuid,1),far.dhcpV4TunnelLink)> ip address
${lease.address} ${lease.subnetMask}
ip nhrp map ${far.nbmaNhsV4Address} ${far.IPSecTunnelDestAddr1} ip nhrp map multicast
${far.IPSecTunnelDestAddr1}ip nhrp nhs ${her.interfaces("Tunnel0")[0].v4.addresses[0].address}
```

IPv6 address \${far.IPv6Address(far.enDuid,1,far.dhcpV6TunnelLink).address}/128 IPv6 eigrp 2 IPv6
nhrp map \${far.nbmaNhsV6Address}/128 \${far.IPSecTunnelDestAddr1} IPv6 nhrp map multicast
\${far.IPSecTunnelDestAddr1} IPv6 nhrp network-id 1
IPv6 nhrp nhs \${far.nbmaNhsV6Address} tunnel mode gre multipoint
tunnel protection IPSec profile DMVPN_IPSec_Profile tunnel source \${wanInterface[0].name} exit
router eigrp 1
network \${lease.address} exit
</#if>

Tunnel Group for IPv6 Network

Tunnel Group Name: IPv6_primary_tunnel_provision Sample csv file to import in FND: about csv file parameters.

Please refer to the following tech note Prepare .csv (Comma-Separated Value) Files to Import New Devices on FND

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/iot-field-network-director/210446-Prepa re-csv-Comma-Separated-Value-fil.html

Figure 252 Figure 151 Figure IoT-Gateway-deployment-over-IPv6-backhaul-csvfile

Note: Substitute the IP address for fnd.ipg.cisco.com with your FND IP address in the following template. Both the IPv4 and IPv6 address of the FND would be reachable from the IoT Gateway once the Tunnel is established. This template uses the IPv4 address of the FND for the IoT Gateway registration with the FND:

```
<#-- This template only supports FARs running IOS. -->
<#if !far.isRunningIos()>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

<#--

For FARs running IOS, configure a FlexVPN client in order to establish secure communications to the HER. This template expects that the HER has been appropriately pre-configured as a FlexVPN server:

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

Configure a Loopback0 interface for the FAR.

```
-->
interface Loopback0
<#--
```

If the loopback interface IPv4 address property has been set on the CGR, configure the interface with that address. Otherwise, obtain an address for the interface now using DHCP:

```
-->
<#if far.loopbackV4Address??>
<#assign loopbackIpv4Address=far.loopbackV4Address>
<#else>
```

<#--

Obtain an IPv4 address that can be used to for this FAR's Loopback interface. The template API provides methods for requesting a lease from a DHCP server. The IPv4 address method requires a DHCP client ID and a link address to send in the DHCP request. The third parameter is optional and defaults to "IoT-FND." This value is sent in the DHCP user class option.API also provides the method "dhcpClientld." This method takes a DHCPv6 Identity Association Identifier (IAID) and a DHCP Unique IDentifier (DUID) and generates a DHCPv4 client identifier as specified in RFC 4361. This provides some consistency in how network elements are identified by the DHCP server:

```
-->
<#assign loopbackIpv4Address=far.ipv4Address(dhcpClientId(far.enDuid,0),far.dhcpV4LoopbackLink
).address>
</#if>
ip address ${loopbackIpv4Address} 255.255.255.255
<#--</pre>
```

If the loopback interface IPv6 address property has been set on the CGR then configure the interface with that address. Otherwise obtain an address for the interface now using DHCP:

```
-->
<#if far.loopbackV6Address??>
<#assign loopbackIPv6Address=far.loopbackV6Address>
<#else>
<#--
```

Obtain an IPv6 address that can be used to for this FAR's loopback interface. The method is similar to the one used for IPv4, except clients in DHCPv6 are directly identified by their DUID and IAID. IAIDs used for IPv4 are separate from IAIDs used for IPv6, so we can use zero for both requests:

```
-->
<#assign loopbackIPv6Address=far.IPv6Address(far.enDuid,0,far.dhcpV6LoopbackLink).address>
</#if>
IPv6 address ${loopbackIPv6Address}/128 exit
<#--</pre>
```

Default to using FlexVPN for the tunnel configuration of FARs running IOS.

```
--> <#if (far.useFlexVPN!"true") = "true"> <#--
```

certIssuerCommonName.

FlexVPN certificate map that matches if the peer (HER) presents a certificate whose issuer's common name contains the string given in the FAR property:

```
-->
<#if !(far.certIssuerCommonName??)>
${provisioningFailed("FAR property certIssuerCommonName has not been set")}
</#if>
issuer-name co cn = ${far.certIssuerCommonName} exit
```

<#--

IPv4 ACL that specifies the route(s) FlexVPN will push to the HER. We want the HER to know the route to the CGR's loopback interface:

```
-->
ip access-list standard FlexVPN_Client_IPv4_LAN permit ${loopbackIpv4Address} exit
<#--
```

IPv6 ACL that specifies the route(s) FlexVPN will push to the HER. We want the HER to know the route to the CGR's loopback interface. If a mesh has been configured on this CGR, we want the HER to know the route to the mesh:

```
-->
IPv6 access-list FlexVPN_Client_IPv6_LAN
<#if far.meshPrefix??>
permit IPv6 ${far.meshPrefix}/64 any
</#if>
sequence 20 permit IPv6 host ${loopbackIPv6Address} any exit
<#-- Enable IKEv2 redirect mechanism on the FlexVPN client --> crypto ikev2 redirect client
```

<#--

Snapshot routing - For enabling connectivity between Control Center and IEDs

```
-->
route-map snapshot permit 10
match ipv6 route-source snapshot
set tag 10
ipv6 access-list snapshot
permit ipv6 2001:DB8:267:1500::/56 any
ipv6 unicast-routing
```

<#--

FlexVPN authorization policy that configures FlexVPN to push the CGR LAN's specified in the ACLs to the HER during the FlexVPN handshake:

```
-->
crypto ikev2 authorization policy FlexVPN Author Policy
route set access-list FlexVPN Client IPv4 LAN
route set access-list IPv6 FlexVPN_Client_IPv6_LAN
route set interface
route redistribute connected route-map snapshot
exit
exit
crypto ikev2 policy FLexVPN_IKEv2_Policy proposal FlexVPN_IKEv2_Proposal exit
<#-- FlexVPN authorization policy is defined locally. -->
aaa authorization network FlexVPN Author local
crypto ikev2 profile FlexVPN IKEv2 Profile
aaa authorization group cert list FlexVPN Author FlexVPN Author Policy
authentication local rsa-sig
identity local dn
pki trustpoint LDevID
exit
<#--
```

If the HER is an ASR, use a different configuration for the transform set since some ASR models are unable to support the set that we'd prefer to use:

-->

```
<#if her.pid?contains("ASR")>
   crypto IPSec transform-set FlexVPN IPSec Transform Set esp-aes esp-sha-hmac
   mode tunnel
   exit
   <#else>
   crypto IPSec transform-set FlexVPN IPSec Transform Set esp-aes esp-sha256-hmac exit
   </#if>
   crypto IPSec profile FlexVPN IPSec Profile set ikev2-profile FlexVPN IKEv2 Profile set pfs group14
   set transform-set FlexVPN IPSec Transform Set exit
   <#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")> interface Tunnel0
   description IPSec tunnel to ${her.eid} ip unnumbered loopback0
   IPv6 unnumbered loopback0 tunnel destination dynamic
   tunnel protection IPSec profile FlexVPN IPSec Profile tunnel source ${wanInterface[0].name} tunnel
   mode gre IPv6 exit
   <#if !(far.IPSecTunnelDestAddr1??)>
   ${provisioningFailed("FAR property IPSecTunnelDestAddr1 must be set to the destination address to
   connect this FAR's FlexVPN tunnel to") }
   </#if>
   crypto ikev2 client flexVpn FlexVPN_Client peer 1 ${far.IPSecTunnelDestAddr1} client connect
   Tunnel0
   exit
   ip host fnd.ipg.cisco.com 172.16.103.100
   <#else>
   <#--
Configure the tunnel using DMVPN:
```

-->

```
router eigrp 1
network ${loopbackIpv4Address} exit IPv6 router eigrp 2 no shutdown exit
IPv6 eigrp 2 exit
<#--</pre>
```

DMVPN certificate map that matches if the peer (HER) presents a certificate whose issuer common name contains the string given in the FAR property:

```
certIssuerCommonName.
--->
<#if !(far.certIssuerCommonName??)>
${provisioningFailed("FAR property certIssuerCommonName has not been set")}
</#if>
crypto pki certificate map DMVPN_Cert_Map 1 issuer-name co cn = ${far.certIssuerCommonName} exit
crypto ikev2 proposal DMVPN_IKEv2_Proposalgroup 14 exit
crypto ikev2 policy DMVPN_IKEv2_Policy
proposal DMVPN_IKEv2_Proposal exit
crypto ikev2 profile DMVPN_IKEv2_Profile authentication remote rsa-sig authentication local rsa-sig
dpd 120 3 periodic identity local dn match certificate DMVPN_Cert_Map pki trustpoint LDevID
exit
<#--</pre>
```

If the HER is an ASR, then use a different configuration for the transform set since some ASR models are unable to support the set we'd prefer to use:

```
--> <#if her.pid?contains("ASR")> crypto IPSec transform-set DMVPN IPSec Transform Set esp-aes esp-sha-hmac exit
```

```
<#else>
crypto IPSec transform-set DMVPN IPSec Transform Set esp-aes 256 esp-sha256-hmac mode tunnel exit
</#if>
crypto IPSec profile DMVPN IPSec Profile set ikev2-profile DMVPN IKEv2 Profile set pfs group14 set
transform-set DMVPN_IPSec_Transform_Set exit
<#if !(far.nbmaNhsV4Address??)>
${provisioningFailed("FAR property nbmaNhsV4Address has not been set")}
</#if>
<#if !(far.nbmaNhsV6Address??)>
${provisioningFailed("FAR property nbmaNhsV6Address has not been set")}
</#if>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")> interface Tunnel0
<#assign lease=far.ipv4Address(dhcpClientId(far.enDuid,1),far.dhcpV4TunnelLink)>
ip address ${lease.address} ${lease.subnetMask}
ip nhrp map ${far.nbmaNhsV4Address} ${far.IPSecTunnelDestAddr1} ip nhrp map multicast
${far.IPSecTunnelDestAddr1} ip nhrp network-id 1
ip nhrp nhs ${her.interfaces("Tunnel0")[0].v4.addresses[0].address}
IPv6 address ${far.IPv6Address(far.enDuid,1,far.dhcpV6TunnelLink).address}/128 IPv6 eigrp 2 IPv6
nhrp map ${far.nbmaNhsV6Address}/128 ${far.IPSecTunnelDestAddr1} IPv6 nhrp map multicast
${far.IPSecTunnelDestAddr1} IPv6 nhrp network-id 1
IPv6 nhrp nhs ${far.nbmaNhsV6Address} tunnel mode gre multipoint
tunnel protection IPSec profile DMVPN_IPSec_Profile tunnel source ${wanInterface[0].name} exit
router eigrp 1
network ${lease.address} exit
</#if>
!
no event manager environment ZTD_SCEP_Debug
1
ip host fnd.ipq.cisco.com 172.16.103.100
1
!
</#if>
```

Appendix C: Device Configuration Profiles

Appendix C: Device Configuration Profiles

This appendix contains the following major topic:

CGR Device Configuration Template, CR Mesh enabled, page 244

CGR Device Configuration Template, CR Mesh enabled

```
<#if far.isRunningIos()>
  <#--
   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 and SNMP traps. 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>
          </#if>
  <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
   cgna profile cg-nms-periodic
      interval 60
   exit
  <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
   cona heart-beat interval 15
  <#-- Enable the following configurations for the nms host to receive informs instead of traps -->
  <#-- no snmp-server host ${nms.host} traps version 3 priv ${far.adminUsername} -->
  <#-- snmp-server engineID remote ${nms.host} ${nms.localEngineID} -->
  <#-- snmp-server user ${far.adminUsername} cgnms remote ${nms.host} v3 auth sha</pre>
${far.adminPassword} priv aes 256 ${far.adminPassword} -->
  <#-- snmp-server host ${nms.host} informs version 3 priv ${far.adminUsername} -->
  <#--
       Enable the following configurations to generate events that track if the router
      moves by a certain distance (unit configurable) or within a certain time (in minutes)
   -->
  <#-- cgna geo-fence -->
  <#-- cgna geo-fence distance-threshold 30 -->
  <#-- cgna geo-fence threshold-unit foot -->
  <#-- cqna geo-fence -->
  <#-- Enable the battery backup unit if one is present -->
  <#if far.hasActiveBattery()>
   do battery charge-discharge enable
 </#if>
< # -
Enable WPAN configurations
-->
!
address prefix ${far.meshPrefix}/64 lifetime infinite infinite
interface wpan 4/1
 ieee154 phy-mode 149
ieee154 panid ${far.meshPanidConfig}
 ieee154 ssid mesh-cellular
ipv6 address ${far.meshPrefix}1/64
  exit
<#elseif far.isRunningCgOs()>
  <#-- Enable periodic inventory notification every 6 hours to report metrics. -->
  callhome
   periodic-inventory notification frequency 360
```

Appendix C: Device Configuration Profiles

```
exit
  <#-- Enable periodic configuration (heartbeat) notification every 1 hour. -->
  <#if far.supportsHeartbeat()>
  callhome
   periodic-configuration notification frequency 60
  exit
  </#if>
  <#-- Enable the battery backup unit if one is present -->
  <#if device.bbuPresent = "true">
   backup-battery un-inhibit discharge
  </#if>
  <#-- Enable gzip compression on devices running CG3 and higher versions of the firmware -->
  <#if far.supportsCallhomeCompression()>
  callhome
   destination-profile nms compress-message
 exit
  </#if>
<#else>
  ${provisioningFailed("FAR is not running CG-OS or IOS")}
</#if>
```

Appendix D: SCADA ICT Enablement Profiles

This appendix contains the following major topics:

- IR1101: IP + Raw Socket Profile, page 246
- IR1101: IP + Protocol Translation Profile, page 247
- IR807: IP + Raw Socket Profile, page 248
- IR807: IP + Protocol Translation Profile, page 249

IR1101: IP + Raw Socket Profile

```
<#if far.isRunningIos()>
  <#if far.interfaces("Loopback0")?size != 0>
   ip http client source-interface Loopback0
   snmp-server trap-source Loopback0
  </#if>
  <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
   cgna profile cg-nms-periodic
     interval 60
   exit
  <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
  cgna heart-beat interval 15
  <#if far.hasActiveBattery()>
   do battery charge-discharge enable
  </#if>
<#-- Beginning of Custom addition of configuration -->
interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
int fastEthernet 0/0/1
switchport access vlan 1
1
interface Tunnel0
ip nat outside
1
interface Tunnel1
ip nat outside
1
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
interface Async0/2/0
no ip address
encapsulation raw-tcp
T.
line 0/2/0
raw-socket tcp client 172.16.107.11 25000 192.168.150.42 25000
databits 8
stopbits 1
speed 9600
parity none
!
<#-- End of custom addition of configuration -->
<#else>
```

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

IR1101: IP + Protocol Translation Profile

```
<#if far.isRunningIos()>
  <#if far.interfaces("Loopback0")?size != 0>
    ip http client source-interface Loopback0
    snmp-server trap-source Loopback0
  </#if>
  <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
    cgna profile cg-nms-periodic
     interval 60
    exit
  <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
  cgna heart-beat interval 15
  <#if far.hasActiveBattery()>
   do battery charge-discharge enable
  </#if>
<#-- Beginning of Custom addition of configuration -->
interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
int fastEthernet 0/0/1
switchport access vlan 1
1
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
interface Async0/2/0
no ip address
encapsulation scada
1
line 0/2/0
databits 8
stopbits 1
speed 9600
parity none
1
scada-gw protocol dnp3-serial
channel dnp3 ch1
 link-addr source 4
 bind-to-interface Async0/2/0
session dnp3_session1
 attach-to-channel dnp3_ch1
scada-gw protocol dnp3-ip
channel dnp3ip ch1
 tcp-connection local-port 21000 remote-ip any
 session dnp3ip_session1
 attach-to-channel dnp3ip_ch1
```

```
link-addr source 4
map-to-session dnp3_session1
scada-gw enable
<#-- End of custom addition of configuration -->
<#else>
  ${provisioningFailed("FAR is not running IOS")}
</#if>
```

IR807: IP + Raw Socket Profile

```
<#if far.isRunningIos()>
  <#if far.interfaces("Loopback0")?size != 0>
   ip http client source-interface Loopback0
    snmp-server trap-source Loopback0
  </#if>
  <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
   cgna profile cg-nms-periodic
      interval 60
   exit
  <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
  cgna heart-beat interval 15
  <#if far.hasActiveBattery()>
   do battery charge-discharge enable
  </#if>
<#-- Beginning of Custom addition of configuration -->
interface FastEthernet1
ip address 192.168.0.1 255.255.255.0
ip nat inside
duplex auto
speed auto
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
interface Async1
no ip address
encapsulation raw-tcp
!
line 1
raw-socket tcp client 172.16.107.11 25000 192.168.150.42 25000
databits 8
stopbits 1
speed 9600
parity none
1
<#-- End of custom addition of configuration -->
<#else>
  ${provisioningFailed("FAR is not running IOS")}
</#if>
```

IR807: IP + Protocol Translation Profile

```
<#if far.isRunningIos()>
  <#if far.interfaces("Loopback0")?size != 0>
    ip http client source-interface Loopback0
    snmp-server trap-source Loopback0
  </#if>
  <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
    cgna profile cg-nms-periodic
      interval 60
    exit
  <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
  cgna heart-beat interval 15
  <#if far.hasActiveBattery()>
   do battery charge-discharge enable
  </#if>
<#-- Beginning of Custom addition of configuration -->
interface FastEthernet1
ip address 192.168.0.1 255.255.255.0
ip nat inside
duplex auto
speed auto
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
interface Async1
no ip address
encapsulation scada
1
line 4
databits 8
stopbits 1
speed 9600
parity none
!
scada-gw protocol dnp3-serial
channel dnp3_ch1
 link-addr source 4
 bind-to-interface Async1
session dnp3 session1
 attach-to-channel dnp3_ch1
scada-gw protocol dnp3-ip
channel dnp3ip_ch1
 tcp-connection local-port 21000 remote-ip any
session dnp3ip session1
 attach-to-channel dnp3ip_ch1
  link-addr source 4
  map-to-session dnp3_session1
scada-gw enable
<#-- End of custom addition of configuration -->
<#else>
```

Appendix E: HER and CGR Configurations

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

Appendix E: HER and CGR Configurations

This appendix contains the following major topics:

- HER Running Configuration, page 250
- CGR Running Configuration, page 257

HER Running Configuration

```
FAN-PHE-HER#
version 16.6
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
1
hostname FAN-PHE-HER
!
boot-start-marker
boot system bootflash:asr1000rpx86-universalk9.16.06.05.SPA.bin
boot-end-marker
1
1
vrf definition DMZ VRF
rd 100:100
address-family ipv4
exit-address-family
I.
vrf definition Mgmt-intf
1
address-family ipv4
exit-address-family
1
address-family ipv6
exit-address-family
!
vrf definition temp
rd 80:80
1
address-family ipv4
exit-address-family
1
logging buffered 21474836
enable secret 4 <hex code removed>
aaa new-model
!
1
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
aaa authorization network FlexVPN_Author_v6 local
1
aaa session-id common
clock timezone IST 5 30
!
```

Appendix E: HER and CGR Configurations

```
ip host rsaca.ipg.cisco.com 172.16.102.2
ip host rsaca.ipg.cisco.comB 172.16.102.2
no ip domain lookup
ip domain name ipg.cisco.com
!
subscriber templating
ipv6 unicast-routing
1
multilink bundle-name authenticated
!
crypto pki trustpoint LDevID
enrollment retry count 10
enrollment retry period 2
enrollment mode ra
enrollment profile LDevID
 serial-number
ip-address none
password
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
revocation-check none
rsakeypair LDevID
!
crypto pki profile enrollment LDevID
enrollment url http://rsaca.ipq.cisco.com/certsrv/mscep/mscep.dll
!
crypto pki certificate map FlexVPN Cert Map 1
issuer-name co cn = ipg-rsa-root-ca
I.
crypto pki certificate map FlexVPN v6 Cert Map 1
issuer-name co dc = ipg
!
crypto pki certificate chain LDevID
certificate <hex code removed for clarity>
!
license udi pid ASR1004 sn NWG16060A8C
license accept end user agreement
license boot level adventerprise
spanning-tree extend system-id
diagnostic bootup level minimal
!
!
!
username cisco privilege 15 password 0 <password>
1
redundancy
mode none
1
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface
route set access-list FlexVPN Client Default IPv4 Route
route set access-list ipv6 FlexVPN Client Default IPv6 Route
crypto ikev2 redirect gateway init
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
crypto ikev2 proposal FlexVPN_v6_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
```

Appendix E: HER and CGR Configurations

```
Ţ
crypto ikev2 policy FlexVPN IKEv2 Policy
proposal FlexVPN IKEv2 Proposal
1
!
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
dpd 30 3 periodic
aaa authorization group cert list FlexVPN Author FlexVPN Author Policy
virtual-template 1
1
1
crypto ikev2 cluster
standby-group CLUSTER0
Slave priority 90
Slave max-session 100
no shutdown
1
!
cdp run
1
class-map match-all serial-packets
match dscp af11
class-map match-all serial-packets-af33
match dscp af33
!
policy-map test-policy
class serial-packets
class serial-packets-af33
I.
!
crypto isakmp invalid-spi-recovery
1
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 512
1
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha-hmac
mode tunnel
crypto ipsec transform-set FlexVPN v6 IPsec Transform Set esp-aes esp-sha-hmac
mode transport
!
crypto ipsec profile FlexVPN IPsec Profile
set transform-set FlexVPN_IPsec_Transform_Set
set pfs group14
set ikev2-profile FlexVPN IKEv2 Profile
responder-only
1
1
interface Loopback0
ip address 192.168.150.1 255.255.255.255
ipv6 address 2001:DB8:BABA:FACE::1/64
ipv6 enable
!
interface Loopback6
no ip address
ipv6 address 2001:DB8:168:150::1/64
ipv6 enable
!
interface GigabitEthernet0/0/0
description connected to Gi0/0/0 of SWITCH DMZ IE5K RR07
 ip address 10.10.100.101 255.255.255.0
```
```
ip nat outside
 standby version 2
 standby 0 ip 10.10.100.100
standby 0 priority 110
standby 0 preempt
standby 0 name CLUSTER0
negotiation auto
cdp enable
1
interface GigabitEthernet0/0/1
no ip address
negotiation auto
cdp enable
!
interface GigabitEthernet0/0/1.101
description ** To Jump Host of FAN PHE DC **
encapsulation dot1Q 101
 ip address 172.16.101.1 255.255.255.0
ip ospf 1 area 0
nat64 enable
ipv6 address 2001:DB8:16:101::1/64 anycast
ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0/1.102
description RSA CA SERVER NPS AD
encapsulation dot1Q 102
 ip address 172.16.102.1 255.255.255.0
ntp broadcast
I.
interface GigabitEthernet0/0/1.103
description FND
encapsulation dot1Q 103
ip address 172.16.103.2 255.255.255.0
ip nat inside
 standby version 2
 standby 103 ip 172.16.103.1
standby 163 ipv6 2001:DB8:16:103::1/64
 standby 163 priority 253
standby 163 preempt
ntp broadcast
nat64 enable
ipv6 address 2001:DB8:16:103::11/64
ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0/1.104
description FND-DB
encapsulation dot1Q 104
ip address 172.16.104.1 255.255.255.0
!
interface GigabitEthernet0/0/1.105
description CPNR
encapsulation dot1Q 105
ip address 172.16.105.1 255.255.255.0
ipv6 address 2001:DB8:16:105::1/64
1
interface GigabitEthernet0/0/1.106
description ECC-CA-Server-NPS-AD
encapsulation dot1Q 106
ip address 172.16.106.1 255.255.255.0
!
interface GigabitEthernet0/0/1.107
description to-SCADA-Master
encapsulation dot1Q 107
```

```
ip address 172.16.107.101 255.255.255.0
standby version 2
standby 107 ip 172.16.107.1
standby 107 priority 253
standby 107 preempt
standby 107 name SCADA MASTER1
nat64 enable
!
interface GigabitEthernet0/0/1.241
description ISR4451-Physical-RA
encapsulation dot1Q 241
ip address 172.16.241.1 255.255.255.0
1
interface GigabitEthernet0/0/1.242
description DMZ-UCS-TPS-Ethernet
encapsulation dot1Q 242
ip address 172.16.242.1 255.255.255.0
ntp broadcast
ipv6 address 2001:DB8:16:242::1/64
!
interface GigabitEthernet0/0/2
no ip address
negotiation auto
cdp enable
!
interface GigabitEthernet0/0/3
no ip address
negotiation auto
cdp enable
!
interface GigabitEthernet0/0/4
ip address 11.1.1.3 255.255.255.0
negotiation auto
cdp enable
service-policy output test-policy
!
interface GigabitEthernet0/0/5
no ip address
negotiation auto
cdp enable
!
interface GigabitEthernet0/0/6
no ip address
negotiation auto
!
interface GigabitEthernet0/0/7
description To be connected to Gi 1/7 of IE5K_RR07 switch (on access vlan 601)
no ip address
shutdown
negotiation auto
cdp enable
ipv6 address 2001:DB8:1010:903::2/64
!
interface GigabitEthernet0/3/0
no ip address
negotiation auto
!
interface GigabitEthernet0/3/1
no ip address
negotiation auto
1
interface GigabitEthernet0/3/2
no ip address
negotiation auto
 !
```

```
interface GigabitEthernet0/3/3
no ip address
negotiation auto
1
interface GigabitEthernet0/3/4
description Connected to IXIA for QOS oversubscription test
 ip address 172.16.177.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:172:16:177::1/80
ipv6 enable
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1300
ip nhrp network-id 1
ip nhrp redirect
ip tcp adjust-mss 1260
nat64 enable
ipv6 unnumbered Loopback0
ipv6 enable
ipv6 mtu 1280
tunnel protection ipsec profile FlexVPN IPsec Profile
1
interface Virtual-Template2 type tunnel
no ip address
shutdown
ipv6 unnumbered Loopback0
ipv6 enable
ipv6 mtu 1362
 ipv6 tcp adjust-mss 1302
 tunnel source GigabitEthernet0/0/7
tunnel mode gre ipv6
tunnel path-mtu-discovery
tunnel protection ipsec profile FlexVPN_IPsec_Profile
1
!
router eigrp 99
network 172.16.200.0 0.0.0.255
!
!
router eigrp 100
network 111.16.200.1 0.0.0.0
!
router ospf 1
router-id 192.168.150.1
redistribute connected subnets
redistribute static subnets
1
ip nat inside source list fnd_ips interface GigabitEthernet0/0/0 overload
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 10.10.100.1 100 name DEFAULT ROUTE TO WAN ROUTER ASR903
ip route vrf DMZ_VRF 0.0.0.0 0.0.0.0 173.39.13.81 240
1
ip ssh time-out 30
ip ssh rsa keypair-name FAN-PHE-HER.ipg.cisco.com
```

```
ip ssh version 2
ip scp server enable
1
1
ip access-list standard FlexVPN_Client_Default_IPv4_Route
permit 172.16.177.11
permit 172.16.177.1
permit 172.16.101.200
permit 172.16.103.243
permit 172.16.106.175
permit 172.16.103.100
permit 192.168.150.1
permit 172.16.107.0 0.0.0.255
permit 11.1.1.0 0.0.0.255
permit 199.199.0.0 0.0.255.255
permit 192.168.150.0 0.0.0.255
ip access-list standard fnd_ips
permit 172.16.103.100
1
ip access-list extended allow dmz and esp to her only
permit ip any host 10.10.100.100
permit ip any host 10.10.100.101
permit ip any host 10.10.100.102
permit ip any 172.16.241.0 0.0.0.255
permit ip any 172.16.242.0 0.0.0.255
permit esp any host 10.10.100.100
permit esp any host 10.10.100.101
permit esp any host 10.10.100.102
permit ip 192.168.150.0 0.0.0.255 host 10.0.0.243
permit ip any any
1
ip access-list extended permit dmz ips only
permit ip any host 10.10.100.100
permit ip any 10.10.100.0 0.0.0.255
permit ip any 172.16.241.0 0.0.0.255
permit ip any 172.16.242.0 0.0.0.255
deny ip any any log
1
ipv6 route 2001:DB8:10:62::/64 2001:DB8:1010:903::22
ipv6 router ospf 1
router-id 192.168.150.1
passive-interface GigabitEthernet0/0/1.103
redistribute connected
redistribute static
!
ipv6 access-list FlexVPN Client Default IPv6 Route
sequence 5 permit ipv6 any host 2001:DB8:16:103::100
sequence 6 permit ipv6 host 2001:DB8:16:103::243 any
sequence 10 permit ipv6 2001:DB8:367:BABA::/64 any
sequence 15 permit ipv6 host 2001:DB8:16:101::200 any
1
ipv6 access-list FlexVPN_v6_Client_IPv6_LAN_Secondary
permit ipv6 host 2001:DB8:16:103::100 any
permit ipv6 host 2001:DB8:16:101::200 any
sequence 40 permit ipv6 host 2001:DB8:172:16:177::1 any
permit ipv6 host 2001:DB8:172:16:177::11 any
1
control-plane
!
1
line con 0
exec-timeout 60 0
escape-character 3
stopbits 1
line vty 0 4
```

```
password <password>
transport preferred ssh
!
1
monitor session 1 type erspan-source
shutdown
destination
 mtu 1464
1
!
ntp Master 5
nat64 settings fragmentation header disable
nat64 map-t domain 1
default-mapping-rule 2001:DB8:367:BABA::/64
basic-mapping-rule
 ipv6-prefix 2001:DB8:267:1500::/56
 ipv4-prefix 10.153.10.0/24
 port-parameters share-ratio 1 start-port 1
netconf max-sessions 16
netconf ssh
!
!
end
```

FAN-PHE-HER#

CGR Running Configuration

```
CGR1240_JAD20410B2Z#
```

```
version 15.8
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
1
hostname CGR1240 JAD20410B2Z
boot-start-marker
boot-end-marker
I.
1
aaa new-model
1
!
aaa group server radius ms-aaa
server name aaa server
1
aaa authentication login default local
aaa authentication dot1x default group ms-aaa
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
1
!
aaa session-id common
clock timezone IST 5 30
1
ip domain name ipq.cisco.com
ip host ra.ipg.cisco.com 172.16.241.2
ip host tps.ipg.cisco.com 172.16.242.2
ip host ntp.ipg.cisco.com 10.10.100.100
```

```
ip host fnd-san.ipg.cisco.com 172.16.103.243
ip cef
ipv6 unicast-routing
ipv6 dhcp pool dhcpd6-pool
address prefix 2001:DB8:ABCD:1::/64 lifetime infinite infinite
vendor-specific 26484
  suboption 1 address 2001:DB8:16:103::243
!
ipv6 cef
1
multilink bundle-name authenticated
1
1
crypto pki trustpoint LDevID
enrollment retry count 4
enrollment retry period 2
enrollment mode ra
enrollment profile LDevID
serial-number none
fgdn none
ip-address none
password
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
subject-name serialNumber=PID:CGR1240/K9 SN:JAD20410B2Z,CN=CGR1240 JAD20410B2Z.ipg.cisco.com
revocation-check none
rsakeypair LDevID 2048
I.
crypto pki trustpoint fnd-pnp
enrollment mode ra
enrollment url http://172.16.102.2:80/certsrv/mscep/mscep.dll
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
revocation-check none
1
crypto pki profile enrollment LDevID
enrollment url http://ra.ipg.cisco.com
!
1
1
crypto pki certificate map FlexVPN Cert Map 1
issuer-name co cn = ipg-rsa-root-ca
!
crypto pki certificate chain LDevID
certificate <hex code removed for clarity>
!
1
license udi pid CGR1240/K9 sn JAD20410B2Z
license accept end user agreement
license boot module cgr1000 technology-package securityk9
license boot module cgr1000 technology-package datak9
dot1x system-auth-control
1
1
archive
path flash:/archive
maximum 8
username cg-nms-administrator privilege 15 secret 8 <hex code removed>
username cisco privilege 15 secret 8 <hex code removed>
1
redundancy
1
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface
route set access-list FlexVPN Client IPv4 LAN
route set access-list ipv6 FlexVPN_Client_IPv6_LAN
```

```
route redistribute connected route-map snapshot
!
crypto ikev2 proposal FlexVPN IKEv2 Proposal
encryption aes-cbc-256
integrity sha256
group 14
1
crypto ikev2 policy FLexVPN_IKEv2_Policy
proposal FlexVPN IKEv2 Proposal
1
!
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
dpd 120 3 periodic
aaa authorization group cert list FlexVPN Author FlexVPN Author Policy
!
crypto ikev2 client flexvpn FlexVPN Client
 peer 1 10.10.100.100
  client connect Tunnel0
1
1
crypto ipsec transform-set FlexVPN IPsec Transform Set esp-aes esp-sha-hmac
mode tunnel
1
crypto ipsec profile FlexVPN_IPsec_Profile
set transform-set FlexVPN IPsec Transform Set
set pfs group14
set ikev2-profile FlexVPN IKEv2 Profile
!
interface Loopback0
ip address 192.168.150.36 255.255.255.255
ipv6 address 2001:DB8:BABA:FACE:4447:B1E8:5748:B32D/128
1
interface Tunnel0
description IPsec tunnel to FAN-PHE-HER
ip unnumbered Loopback0
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet2/1
tunnel destination dynamic
tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
1
interface Dot11Radio2/1
no ip address
shutdown
no mop enabled
no mop sysid
I.
interface FastEthernet2/3
no ip address
!
interface FastEthernet2/4
no ip address
!
```

```
interface FastEthernet2/5
no ip address
!
interface FastEthernet2/6
no ip address
1
interface GigabitEthernet2/1
no switchport
ip address dhcp
duplex auto
speed auto
1
interface GigabitEthernet2/2
no switchport
no ip address
shutdown
duplex auto
speed auto
1
interface GigabitEthernet3/1
no ip address
shutdown
duplex auto
speed auto
1
interface GigabitEthernet3/2
no ip address
shutdown
duplex auto
speed auto
1
interface Vlan1
no ip address
1
interface Async1/1
no ip address
encapsulation scada
1
interface Async1/2
no ip address
encapsulation scada
1
interface Wpan4/1
no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 10 max-interval 20 suppression-coefficient 1
ieee154 dwell window 12400 max-dwell 400
 ieee154 panid 1
 ieee154 ssid mesh-ha-s
outage-server 2001:DB8:16:103::243
rpl dag-lifetime 60
rpl dio-dbl 5
 rpl dio-min 16
 rpl version-incr-time 120
 rpl storing-mode
 authentication host-mode multi-auth
authentication port-control auto
 ipv6 address 2001:DB8:ABCD:1::1/64
 ipv6 dhcp server dhcpd6-pool rapid-commit
no ipv6 pim
dot1x pae authenticator
!
!
ip forward-protocol nd
```

```
!
no ip http server
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
ip http secure-client-auth
ip http secure-port 8443
ip http secure-trustpoint LDevID
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection forceclose
ip http client source-interface Loopback0
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
1
ip ssh rsa keypair-name LDevID
ip ssh version 2
ip access-list standard FlexVPN_Client_IPv4_LAN
permit 192.168.150.36
1
ipv6 ioam timestamp
1
route-map snapshot permit 10
match ipv6 route-source snapshot
set tag 10
!
!
snmp-server group cgnms v3 priv
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps flash removal
snmp-server enable traps flash low-space
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps auth-framework auth-fail
snmp-server enable traps c3g
snmp-server enable traps envmon status
snmp-server enable traps wpan
snmp-server enable traps aaa_server
snmp-server enable traps entity-ext
snmp-server enable traps fru-ctrl
snmp-server enable traps mempool
snmp-server host 172.16.103.243 version 3 priv cg-nms-administrator
1
radius server aaa_server
address ipv4 172.16.106.175 auth-port 1812 acct-port 1813
key <secret key>
!
!
ipv6 access-list FlexVPN Client IPv6 LAN
permit ipv6 2001:DB8:ABCD:1::/64 any
permit ipv6 host 2001:DB8:BABA:FACE:4447:B1E8:5748:B32D any
1
ipv6 access-list snapshot
permit ipv6 2001:DB8:267:1500::/56 any
!
control-plane
L
vstack
!
line con 0
length 0
line 1/1 1/2
transport preferred none
```

```
stopbits 1
line 1/3 1/6
transport preferred none
transport output none
stopbits 1
line vty 0 4
length 0
transport input none
1
ntp update-calendar
ntp server ntp.ipg.cisco.com
no iox hdm-enable
iox client enable interface GigabitEthernet0/1
iox client enable interface GigabitEthernet0/2
iox client enable interface GigabitEthernet3/1
iox client enable interface GigabitEthernet3/2
wsma agent exec
profile exec profile
1
wsma agent config
profile config profile
1
1
wsma profile listener exec profile
transport https path /wsma/exec
!
wsma profile listener config profile
transport https path /wsma/config
!
cgna gzip
1
cgna heart-beat interval 15
cgna heart-beat active
1
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.ipg.cisco.com:9120/cgna/ios/tunnel
qzip
1
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 platform gps location | format flash:/managed/odm/cg-nms.odm
add-command show platform hypervisor | format flash:/managed/odm/cg-nms.odm
 add-command show sd-card password status | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show iox host list detail | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 10
url https://fnd-san.ipg.cisco.com:9121/cgna/ios/registration
qzip
!
cgna profile cg-nms-periodic
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show environment temperature | 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 platform hypervisor | format flash:/managed/odm/cg-nms.odm
 add-command show sd-card password status | format flash:/managed/odm/cg-nms.odm
 add-command show platform gps location | format flash:/managed/odm/cg-nms.odm
 add-command show raw-socket tcp sessions | format flash:/managed/odm/cg-nms.odm
 add-command show raw-socket tcp statistics | format flash:/managed/odm/cg-nms.odm
 add-command show scada tcp | format flash:/managed/odm/cg-nms.odm
add-command show scada statistics | format flash:/managed/odm/cg-nms.odm
add-command show iox host list detail | format flash:/managed/odm/cg-nms.odm
add-command show wpan 4/1 hardware version | format flash:/managed/odm/cg-nms.odm
add-command show wpan 4/1 rpl brief | format flash:/managed/odm/cg-nms.odm
add-command show wpan 4/1 ha-detail | format flash:/managed/odm/cg-nms.odm
add-command show wpan 4/1 conf | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 4/1 packet-count | format flash:/managed/odm/cg-nms.odm
 add-command show platform door | format flash:/managed/odm/cg-nms.odm
 add-command show platform battery short | format flash:/managed/odm/cg-nms.odm
 interval 60
url https://fnd-san.ipg.cisco.com:9121/cgna/ios/metrics
qzip
active
1
!
cgna exec-profile CGNA-default-exec-profile
add-command cqna exec profile cq-nms-register
 interval 1
exec-count 1
1
T
!
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 180
event manager environment ZTD SCEP Debug TRUE
event manager directory user policy "flash:/eem"
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm ztd scep.tcl type system authorization bypass
I.
end
CGR1240 JAD20410B2Z#
```

Appendix F: FLISR Simulation using DTM

Fault Location, Isolation, and Service Restoration

Fault Location, Isolation, and Service Restoration (FLISR) is the process for dealing with fault conditions on the electrical grid. When a fault occurs in a section of the grid, first identify fault location and isolate the smallest possible section affected by the fault. Then restore the power to larger possible section of the grid.

The goal of the FLISR to minimize the fault affected area with very short turnaround time by identifying the fault location, isolating the fault section, and restoring the power to the remaining section of the grid within a short turnaround time.

Event Sequence Diagram



Figure 253 Semi-automatic Sequence Diagram

Use Case Steps

- 1. Remote Fault Indicator (RFI) 1 reports to the DMS whenever it encounters a fault.
- 2. Re-closer 2 opens and sends a report to the DMS when it encounters a temporary fault.
- 3. Remote Control Switch (RCS) 2 reports no voltage status to the DMS.
- 4. RCS 2 closes after 15 seconds and re-opens immediately.
- 5. RFI 1 reports fault for the second time.
- 6. RCS 2 opens after 40 seconds and reports status.
- 7. Re-closer 2 closes after 40 seconds, reopens and locks out permanently, and report status to the DMS.
- 8. The DMS decides to issue a close command to RCS 3.
- 9. The DMS issues a close command to RCS 3.

FLISR Use Case Simulation

- 1. Load the FLISR workspace by importing into DTM. The FLISR workspace can be found in Appendix E: HER and CGR Configurations, page 196.
- 2. Start all the host machines.

Figure 254 DTM FLISR Start All Hosts



3. Start the FLISR DTM Simulation script.

Figure 255 DTM FLISR Start the Script

	B +000 +000 +000 +0	No E Maria	6.				ම යාග යාග යාග	100			
04-campe 0593-s10_84503.84	Day a state i want with Day 1 is		atoma .				Page a sum to basis into		to the second		
a l'attente	Name	T Nature	T Point Tape	T 4 T	Quality	T Timest	Name	T Value	T. Point Spec T 1	T Quality	Y Develop
And Barrantine	ACS 2 - Sine Yotage Statue	04	(1) Binary Inputs	4	Drive	2.2.0079	ACS 2 - Line Voltage To	No 109	(Clinesy hours d	Drive	3/2/2018 12:40:39 1
and seconds	RCL1 - Carer State	(De	[10] Broary Output Statuant	+	Other	2/5/0191	RCL2-Com Tate	04	[10] Brwy Output Statuses 3	Orline	21022181340381
eni Gereje	ACE 3 - Live Verleté Status	0#	(1) Broary Inputs	1	Online	2/5/38191	RC3.3 - Line Voltage Dr	tei DP	(1) Browy Inguist (1)	Online	3/4/2019 10415 A
	RCS 1 - Open State	On .	[10] Browy Output Statuses		Other	2/1/2019 1	ACLE-Types states	08	[15] Browy Output Statutes: S	Drive	3/4/2018 1/04/15 A
lainge -	Art 1, Fault Instantor	De	[1] Birwy Inpuls		Orine	2/3/2019 (RFLE - Fault Indicator	09	112 Briary Inputs 2	Online	314/2019 104/36 A
an Data Pulinto	Re-Court 1 - Open State	Die .	[10] Briany Cyliput Thatuaes	1.00	Othe	2/5/00191	Re-Closer 3 - Coard and	09	[10] Broary Curpol Statutes 3	Drive	216 2018 1 (MAZ A
es/Leuis licente	4										
and and a	Sentiles + Departy 6	and an even of the					Send Your * Dages	ing if ut it states	045		
	Manual or an in-										
	Provide Land Contraction of Contract										
1 1 100.]	1 10:43/25,125,124 2 10:43/25,427 10:43/25,447 10:43/25,447 10:43/25,447 10:43/25,447 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25,35 10:43/25 10:45/25 10	OffeetLL com Channell (Out DiffeetL) com Channell (Out Channell (Out OffeetR) com Channell (Out	ertei station:NLLINGE const station:NLLINGE const station:NLLINGE const station:NLINGE const station:Necleor_1/NDE c	ad ed ed errected							
L))) Dawe_] + tat:the Mag.	The Language 1 (1944) (27, 15%, 1987) 1 (1944) (27, 15%, 1987) 1 (1944) (27, 45%, 1984) 1 (1944) (27, 45%, 1984) 1 (1944) (27, 15%, 1984) 1 (Offeetil com Channel (Okt Ditentit can Disnet com Channel (Okt Ottentit Com Channel (Okt	ected Microsoft, Julius cannot the Microsoft, Julius cannot ected distinguistic, Julius cannot distinguistic cannot can distinguistic can distinguistic can distinguistic cannot can distinguistic	ni ed ed edrestaal	-						
r Basja . 1	European 1 (1942) 27.55 mem 2 (1942) 27.45 mem 1 (1942) 27.45 mem 1 (1942) 27.45 mem 1 (1942) 27.55 m	Offeet2 com Chaned /Oct Difeet2 com Chaned /Oct Difeet3 com Chaned /Oct	nted setted setted that (see Not.) / the second setted that (see Not.) / the second setted that (see Not.) / the second that (see Not.) / the second setted that (see Not.) / the second setted	al of al official							
T Naja	European 1 (1944) 25, 125 (1997) 1 (1944) 25, 126 (1997) 1 (1944) 25	Urhesti com Chandi /bit Urhesti com Chandi /bit Urhesti com Chandi /bit Urhesti com Chandi /bit	nted setted setted that (see Note,) / (the second setted that (see Note,) / (the second setted that (see Note,) / (the second that (see Note,) / (the sec	al el el							
2 CDr Maja . Line	Exclusion 1 (1942) (2.15% merry 1 (2.146) (2.15% merry 1 (2.146) (2.146) (2.146) 1 (2.146) (2.146) (2.146) (2.146) 1 (2.146) (2.146) (2.146) (2.146) 1 (2.146) (2.146) (2.146) (2.146) (2.146) 1 (2.146) (2.146) (2.146) (2.146) (2.146) (2.146) 1 (2.146)	Ufwatti sem Utwatd, Joh Ufwatti sen Osmali Joh Sfeets sen Osmali An Ufwati sen Osmali Joh	actad Station (RL_1) (BW (asset) Station (RL_1) (BW (asset) station (WL_1) (BW (asset) station (WL_1) (BW (asset) station (WL_1) (BW (asset) station (RL_1))	ni ni ni ni ni							
cð LCDV Haga . Maine	1044.2(25.55) 1044.3(25.55) 1044.3(24.65) 1044.3(24.65) 1044.3(24.65) 1044.3(24.65) 1044.3(25.26) 1044.3	Ufwatil see Ufwatil see Ufwatil op Ufwatil op Ufwatil op Ufwatil op Ufwatil op Ufwatil op	actad solution the solution solu	ni el el ennectad							
j J J J J J J J J J J J J J J J J J J J	European 1 (1942) 25.05 mem 2 (1942) 25.45 mem 1 (1942) 25.45 mem 1 (1942) 25.45 mem 1 (1942) 25.45 mem 1 (1942) 25.55 m	Urnatti sere Channil, Ant Ufnetti sere Shansii Oko Urbandi Ada Urbandi Ada Urbandi Ada Urbandi Ada	nted setted stations/httpl/state stations/httpl/stations/httpl/state stations/httpl/	nd ed ad administration							
ver, 3 NF Kol Christian Histori Angt	1. 1942.228.526. 21.44535.477.69 21.244535.477.69 21.244535.477.69 21.244535.255.269 21.244535.255.269 21.244535.269 21.24535.255.269 21.24535.255.269 21.24535.255.269 21.24535.255.269 21.24535.255.269 21.24555.255 21.24555.255 21.24555.255 21.2455555.255 21.2455555.255 21.2455555.255 21.2455555.255 21.2455555.255 21.2455555.255 21.2455555.255 21.2455555555555.25555555555555555555555	Ufmatti som Channel (Joh Disardi Anto Disardi Anto Disardi Anto Disardi Anto Disardi Anto Disardi Anto Disardi Anto Disardi Anto Disardi Anto	actad actad Mationality_JoidW (asset) Mationality_JoidW (asset) stationalWJoidW (asset) station	ni ed ad administration	-						
CLJ P CLJ P Clower,J Clower,Clowe	1. 1944 (2), 455 1. 1944 (2), 457 1. 1944 (2), 447 1. 1944 (2), 447 1. 1944 (2), 477 1. 1944 (2),	Ofmentia serve Observational control officers and control officers of the control officers of the control officers of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the cont	ntad vielionini, julium isenati vielionini, julium isenati vielioni, vielioni, vielioni, julium isenati vielioni, vielioni, vi								

4. Simulate the fault by changing the RFI1 data once. Click on Change Data Once on the RFI1 outstation device.

256452

Figure 256 DTM FLISR Execute the RFI Script Once



Note: The FLISR use case steps 1 to 9 are fully automated by the scripts.



interest of the second s	B with with with all	C B Maran					B 54.04 04 04							
B	Ding a solution frames and plays if have to group by that obtains						Dag a second basis and their from to group to the second							
Centre Connected p	1000	Waturn T	Paint Type	7.4	T Quality	T Finned	Aure 1.1	Value	T	Point Type	7 . 1	Cuality	Y. Ilenstone	
AMERIC S. 104 Data Accessia	MITT, Fault Indicator	(Dec	111 Binary Install		Deve.	2,5,9778	MIT-Not toliane	04		TEBriary houts	1.0	O-line .	214/2018 186-44	
	Ar-Door J -Opei Sale	(On	[11] Browy Output Transm	- 4	Online	2/5/00191	Re-Closer 3 - Cipier State	08		12 Browy Output State	(m) ()	Online	2420191072	
TQ-3-10K Matter and Taveya	RC3 1 - Oper Sate	0+	[10] Broary Dylaut Steware		Other	2/5/2019 1	NCL 2 - Daver states	OP:		10 Brwy Output State	er: 0	Online	3/4/2019 1/07/21	
rlantsiji	ACE 3 - Love Voltate Status	Ow	(1) Binary Inputs		(Drive)	2/4/2019	RCL3 - size Votage Status	De:		TE Binery Inputs		Dalling	3(4:00)+9 1(r).1	
	NCS.2 - Open State	On .	[10] Brivey Curput Statutes		Oritinal	2/5/2019	RC1.2 - Openi 2044	00		20 Brary Output Strip	im: 0	Orient	210/0219 13:400	
	AC3.2 - Lore Voltage Status	0.0	[1] Binary Inputs		Orite .	2/5/2019	NCS 2 - Low Voltage Status	D#		1) Brieg Houts	. 6	Gebia	215-0019 12-423	
	1						1		_					
	Interface + Destantial of Advances						Same Time + Designed	of the state law	-					
5.114 Carenarda, A							International Action of the International Action		-					
	Dident	111					10							
nga Dariya Matta di Kata Kata Maya	 IP 10+5126, 204: 264 IP+5126, 204: 264 IP+6427, 2251; 847 IP+6427, 2251; 847 IP+6427, 2251; 847 IP+6427, 2091; 634 IP+6427, 2091; 634 IP+6427, 2091; 756 IP+6427, 2091; 756 IP+6427, 2091; 756 IP+6427, 2091; 756 IP+6427, 2091; 766 IP+6427, 2091; 766 IP+6427, 2091; 766 IP+6427, 2091; 766 IP+644, 10, 8091; 766 IP+644, 10, 8091; 766 	Calling defails Calling defails Taling the same reging the same to face 1 Status for reging the SCL 2.1 mean 1 Openitate Desar 1 Specifies 3 reports faults	values in all HDs in, charing tacloser J lower J, Operlant + Ta e + True int Charged. So, Dang Deviding Torth point NUCDE ATTOR ISSUES IN CONSTAN Investigated, for the UCDED time tec	lae Ing the I to F4, Insporter r efter	ta padre. NCL_2_Librari M y opening Disect tamp	altege_itetus. mary sporting								

5. Verify that the DTM logs are in line with the FLISR Event Sequence diagram of this document. Confirm the Control Command is sent from the control center to RCS3 in the last lines of the log. All Outstation data is updated to SCADA Control Center (Master) data points.