Distribution Automation—Secondary Substation Implementation Guide

This *Distribution Automation - Secondary Substation Implementation Guide* provides a comprehensive explanation of the Cisco Smart Grid Field Area Network solution implementation for Secondary Substation monitoring and Distribution Automation use cases such as Fault Location, Isolation, and Service Restoration (FLISR) and Volt/VAR.

This document includes implementation information about the solution's architecture, possible deployment models, and guidelines for deployment. It also recommends best practices and potential issues when deploying the reference architecture.

Navigator

The following table describes the content of the chapters in this document.

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, Supervisory Control and Data Acquisition (SCADA) protocols, and have been exposed to Field Area Networks.

Introduction

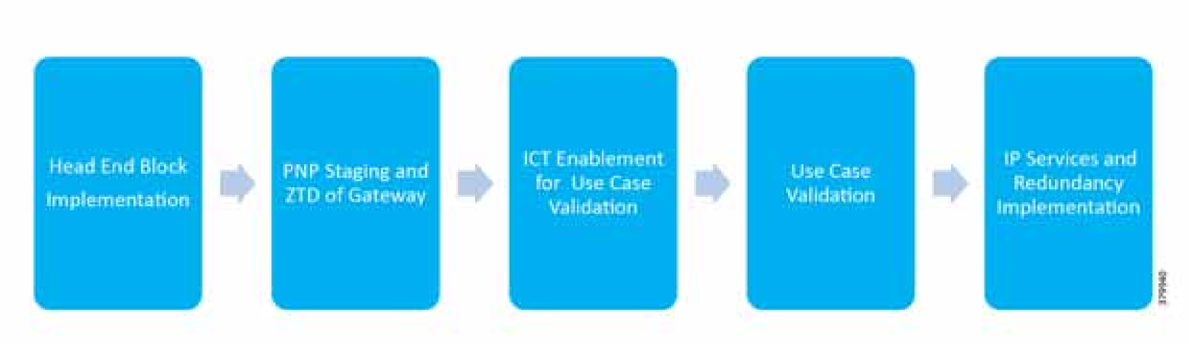
This implementation guide details the implementation of Distribution Automation use cases like FLISR, Volt/VAR and Secondary Substation monitoring for the Europe region. Therefore, the focus of this document is on IEC 60870-5-104 or T104 and IEC 60870-5-101 or T101 Supervisory Control and Data Acquisition (SCADA) protocols. We have planned a separate implementation guide that focuses on the North American Region distribution automation use cases.

Secondary Substation monitoring covers both SCADA transport and SCADA translation scenarios. SCADA protocol translations are enabled on Cisco routers such as the Cisco IR1101, Cisco IR809, Cisco IR807, Cisco IR829, and CGR 1120. These routers are referred to as Secondary Substation Routers (SSR) or Distribution Automation Gateways (DA Gateways) throughout this document. Solution implementation is based on the design recommended in the *Distribution Automation - Secondary Substation Design Guide* that can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG.html

The flow of this implementation guide is depicted in Figure 1:

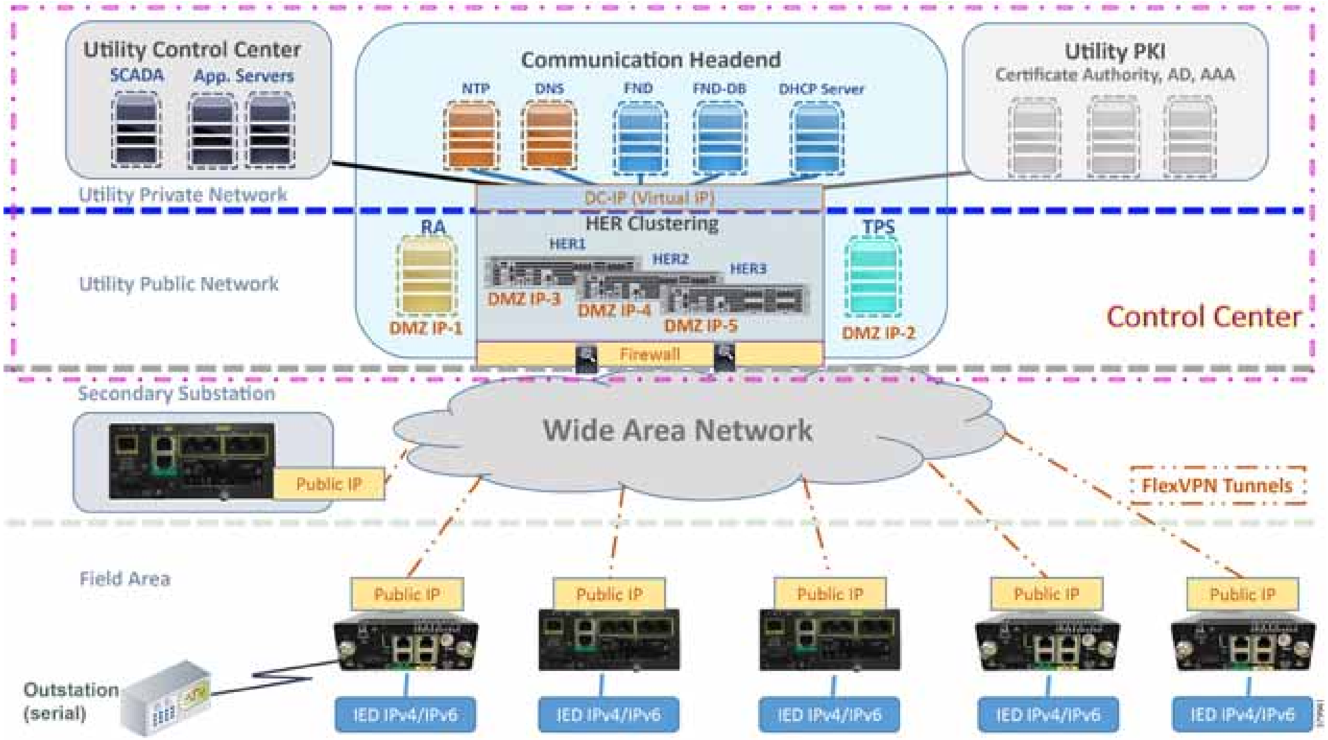
Figure 1 Implementation Flow


Head End Block Implementation
PNP Staging and ZTD of Gateway
ICT Enablement for Use Case Validation
Use Case Validation
IP Services and Redundancy Implementation
379960

The Cisco Distribution Automation Solution is a two-tier architecture where the headend block is connected to the Field Area Network or Secondary Substation block using the WAN tier. The Gateway aggregates application traffic from the Field Area block and routes to the Headend block where the application resides. For a detailed description of different elements in the Field Area block and their implementation, please refer to the *Cisco FAN - Headend Deep Dive Implementation and FAN Use Cases* at the following URL:

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

Figure 2 Distribution Automation Solution Architecture



Gateways connect various outstation IEDs (IPV4/IPV6 or serial) in the Field Area or Secondary Substation via Ethernet and RS232/RS485 asynchronous serial interfaces. Solution Network Topology and Addressing, page 4 discusses in detail the solution implementation topology, various IP address schemes used in different blocks, and VLAN segmentation across services. The gateway can be onboarded, staged, and deployed in Zero Touch fashion, which is the preferred and scalable way for deploying gateways.

The various stages involved in Zero Touch Deployment (ZTD) and best practices to be followed during ZTD implementation are discussed in detail in IoT Gateway Onboarding and Management, page 14 discusses in detail. Once the gateways are registered to the Network Management Systems (NMS) Field Network Director (FND), gateways are provisioned with various features that will enable the secure bidirectional flow between IEDs in the field to SCADA applications in the Headend of the Distribution System Operator (DSO). Some of the application flow from the IEDs is via the Remote Terminal Unit (RTU) residing in the Secondary Substation to the SCADA.

Features can be broadly classified into *horizontal* ones like IP routing, network encryption, time synchronization (like NTP), QoS, NAT, and DHCP and *vertical* features like protocol translation, raw sockets, and IED-based ACLs. Appendix A: PnP Profiles, page 174 provides customized and well-tested use case-based NMS templates, which is key for faster field deployment of Distribution Automation use cases.

Application Use Cases

This document addresses the following technology use cases:

- Secondary Substation Monitoring
- Volt/VAR
- FLISR

Solution Network Topology and Addressing

This chapter, which discusses the various topologies used for solution validation and implementation in this guide, includes the following major topics:

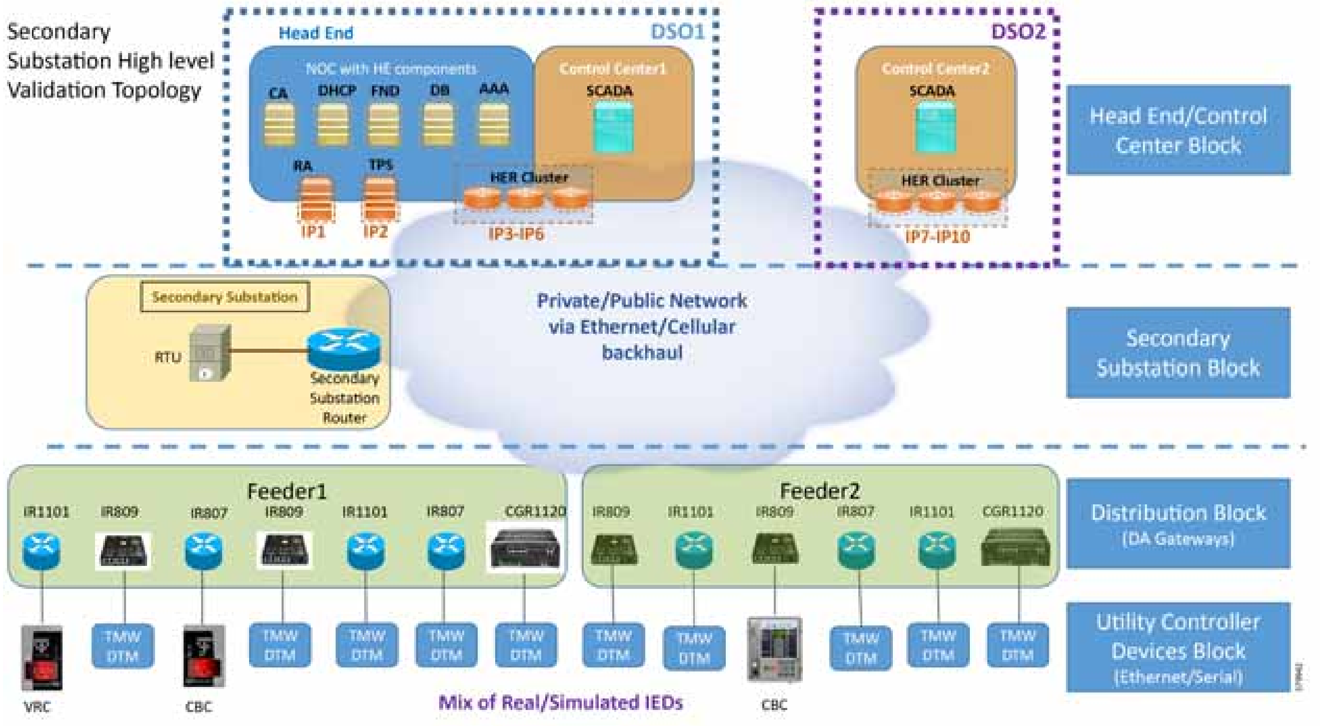
Topology Diagram

This section describes the high-level solution validation topology that has been used in this Secondary Substation Implementation Guide.

High Level Solution Validation Topology

Figure 3 depicts the high level solution validation topology:

Figure 3 Secondary Substation High Level Solution Validation Topology



The multiple layers of topology include:

1. Head End/Control Center Block, which hosts the DSO Control Center1 (DSO1) and DSO Control Center2 (DSO2):
   a. Both Control Centers host the SCADA application server. They could also host other application servers.
   b. Of the two Control Centers, DSO1 hosts the following additional components:
      - CA, Active Directory (AD), Dynamic Host Configuration Protocol (DHCP), Field Network Director (FND), Authentication, Authorization, and Accounting (AAA), Registration Authority (RA), and Tunnel Provisioning Server (TPS).

- These components are essential for the ZTD of the SSRs that are positioned in the Secondary Substation and DA Gateways that are positioned along the Distribution Feeder.

2. Secondary Substation Block
3. Distribution Block
4. Utility Controller Devices Block. Utility controller devices (real/simulated) are connected to the DA Gateways over a Ethernet/Serial interface.

The following components are simulated using the Triangle MicroWorks (Distributed Test Manager or DTM) tool:

1. SCADA Master located in DSO1
2. SCADA Master located in DSO2
3. IEDs located in the Utility Controller Devices Block layer

Two Instances of the Solution Validation Topology

Two instances of this topology have been used during this implementation:

1. One instance is located in Cisco Engineering lab premises, with validation done over the Ethernet backhaul:
   a. No public internet connectivity
   b. WAN Network is simulated inside the engineering lab
   c. Is referred to as the *Engineering Lab Topology* throughout this document
2. The second instance is located in the Cisco DMZ premises, with validation done over the cellular backhaul, along with Ethernet WAN:
   a. Over public internet connectivity using Cellular SIM Cards, as well as over Ethernet
   b. WAN Network is the service provider's network
   c. Is referred to as *Cisco DMZ Headend* throughout this document.

'

Table 1 Differences in Validation between Engineering Lab Headend and Cisco DMZ Headend

Block	With Engineering Lab Topology	With Cisco DMZ Headend
Headend/Control Center Block	■ Positioned in Engineering Lab	■ Positioned in Cisco DMZ space
Secondary Substation Block	■ Positioned in Engineering Lab ■ Connectivity is over simulated WAN ■ Both IPv4 and IPv6 backhauls are validated	■ Can be positioned anywhere ■ Connectivity is over service provider cellular network ■ IPv4 backhaul is validated as cellular provider allocated IPv4 address only ■ IPv6 backhaul is validated as part of the Engineering Lab Topology
Distribution Gateway Block	■ Positioned in Engineering Lab ■ Ethernet uplink of DA Gateway has been validated	■ Can be positioned anywhere ■ Two uplink networks are validated on the DA Gateway: – Cellular uplink validated predominantly – Along with Ethernet uplink
Utility Controller Devices Block	■ Agnostic to the positioning of the headend. Ethernet and serial connectivity to simulated IEDs have been validated.	

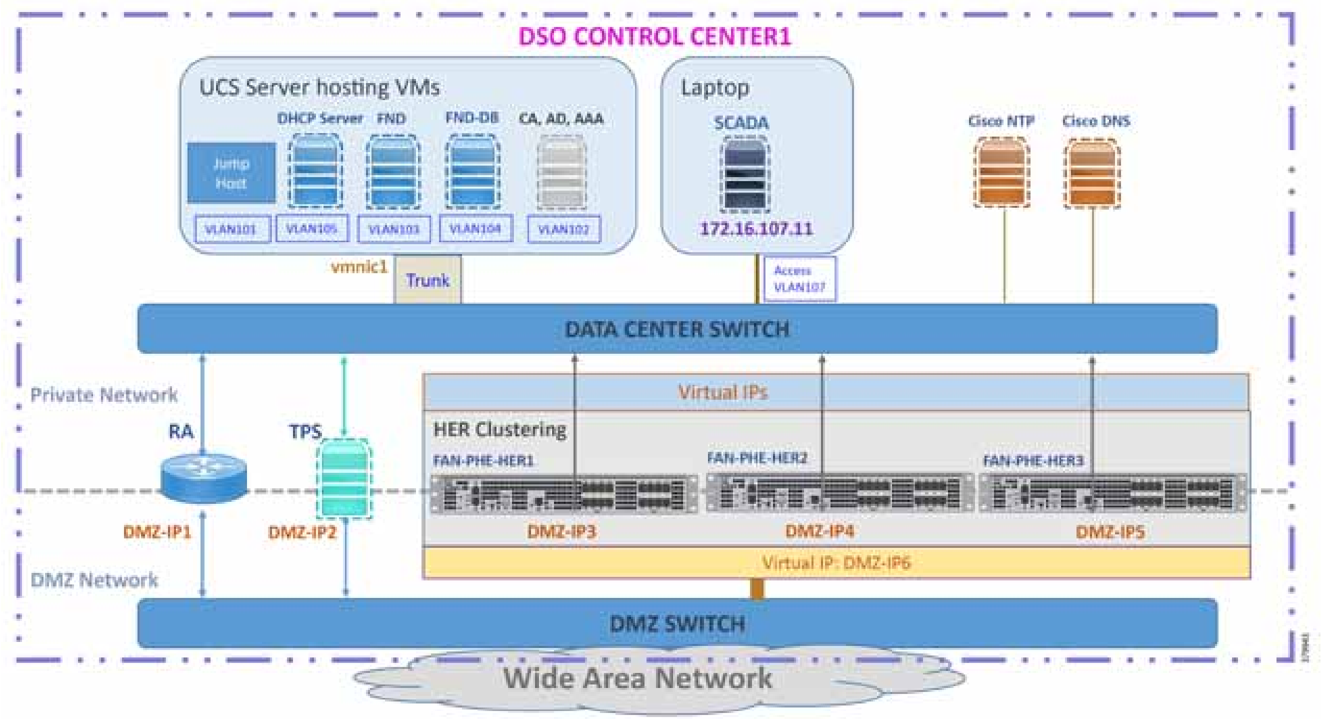
Note: The following sections of this guide capture the IP addressing used only in the Engineering Lab topology. For security reasons, Cisco DMZ IP addresses are referred to with abstract names instead of actual IP addresses.

IPv4 and IPv6 Addressing

Addressing in DSO Control Center1

Zooming in on the DSO1 part of the Head End/Control Center block, Figure 4 captures the granular details of the DSO Control Center1:

Figure 4 DSO Control Center 1–Implementation Topology



The DSO Control Center1 is composed of two different networks:

- Addressing in the DMZ Network
- Addressing in the Private Network

Addressing Convention Followed in the Private Network Subnet Selection

Two prefixes are used in the private network of the Control Center:

- 172.16.X.yy in the Engineering Lab Topology
- 192.168.X.yy in the Cisco DMZ Headend

Table 2 Addressing Convention Followed with Third Octet of IP Address

Third Octet	Component Connected by the Subnet	Sample Address
101	Jump Host	172.16.**101**.2
102	Certificate Authority, Active Directory, AAA	172.16.**102**.2 192.168.**102**.100
103	Field Network Director	172.16.**103**.100 192.168.**103**.100
104	Field Network Director - Database	172.16.**104**.100 192.168.**104**.100
105	DHCP Server	172.16.**105**.100 192.168.**105**.100
106	SCADA Server	172.16.**106**.100 192.168.**106**.100

For example, 172.16.103.X represents the network connecting to FND. 172.16.107.X represents the network connecting to the SCADA server.

Note: The third octet also signifies the VLAN used to connect to the corresponding component. For example, VLAN 103 is used for communication with the FND component and VLAN 107 is used for communication with the SCADA server component.

DSO Control Center1: Addressing in the DMZ Network

The topology in Figure 4 on the previous page 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—Cluster of ASR 1000 series of routers.

CC1: Addressing in the Simulated DMZ Network with Engineering Lab Topology

Table 3 and Table 4 capture the IPv4 and IPv6 addresses of the RA, TPS, and HER Cluster (represented in Figure 4) in the "Engineering Lab Topology":

Table 3 Control Center1—IPv4 and IPv6 Addressing—Simulated DMZ Network with Engineering Lab Topology

Component Name	Address Type (IPv4/IPv6)	IP Address (with Engineering Lab Topology)
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::242
FAN-PHE-HER1	IPv4	10.10.100.101
	IPv6	2001:DB8:1010:903::2

Table 3 Control Center1–IPv4 and IPv6 Addressing–Simulated DMZ Network with Engineering Lab Topology

Component Name	Address Type (IPv4/IPv6)	IP Address (with Engineering Lab Topology)
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 10.10.100.150 in the Engineering Lab Topology.

CC1: Addressing in the Real DMZ Network with Cisco DMZ Headend

This section captures the addressing details of the control center components located in the real DMZ network.

For security reasons, instead of referencing real Cisco DMZ IPv4 and IPv6 addresses, the following representations are used throughout this document:

Table 4 Control Center1: IPv4 and IPv6 Addressing–Real DMZ Network with Cisco DMZ Headend

DMZ Component	Address Type	Is represented in this document as:
Registration Authority	IPv4	ra-ipv4.ipg.cisco.com
	IPv6	ra-ipv6.ipg.cisco.com
Tunnel Provisioning Server	IPv4	tps-ipv4.ipg.cisco.com
	IPv6	tps-ipv6.ipg.cisco.com
Headend Router 1	IPv4	her1-ipv4.ipg.cisco.com
	IPv6	her1-ipv6.ipg.cisco.com
Headend Router 2	IPv4	her2-ipv4.ipg.cisco.com
	IPv6	her2-ipv6.ipg.cisco.com
HER Cluster (Virtual IP)	IPv4	her-ipv4.ipg.cisco.com
	IPv6	her-ipv6.ipg.cisco.com

DSO Control Center1: Addressing in the Private Network

Table 5 captures the addressing details of the components located in the Private Network of Control Center1:

Table 5 DSO Control Center1: Addressing in the Private Network

Component	Address Type	In Engineering Lab Topology	In Cisco DMZ Headend
CA/AD/AAA	IPv4	172.16.102.2	192.168.102.100
FND	IPv4	172.16.103.100	192.168.103.100
	IPv6	2001:db8:16:103::100	2001:db8:192:168:103::100
FND DB	IPv4	172.16.104.100	192.168.104.100
DHCP Server	IPv4	172.16.105.2	192.168.105.100
	IPv6	2001:db8:16:105::2	2001:db8:192:168:105::100
SCADA	IPv4	172.16.107.11	192.168.107.11
	IPv6	2001:db8:16:107::11	2001:db8:192:168:107::11
RA	IPv4	172.16.241.2	192.168.102.75

Table 5 DSO Control Center1: Addressing in the Private Network (continued)

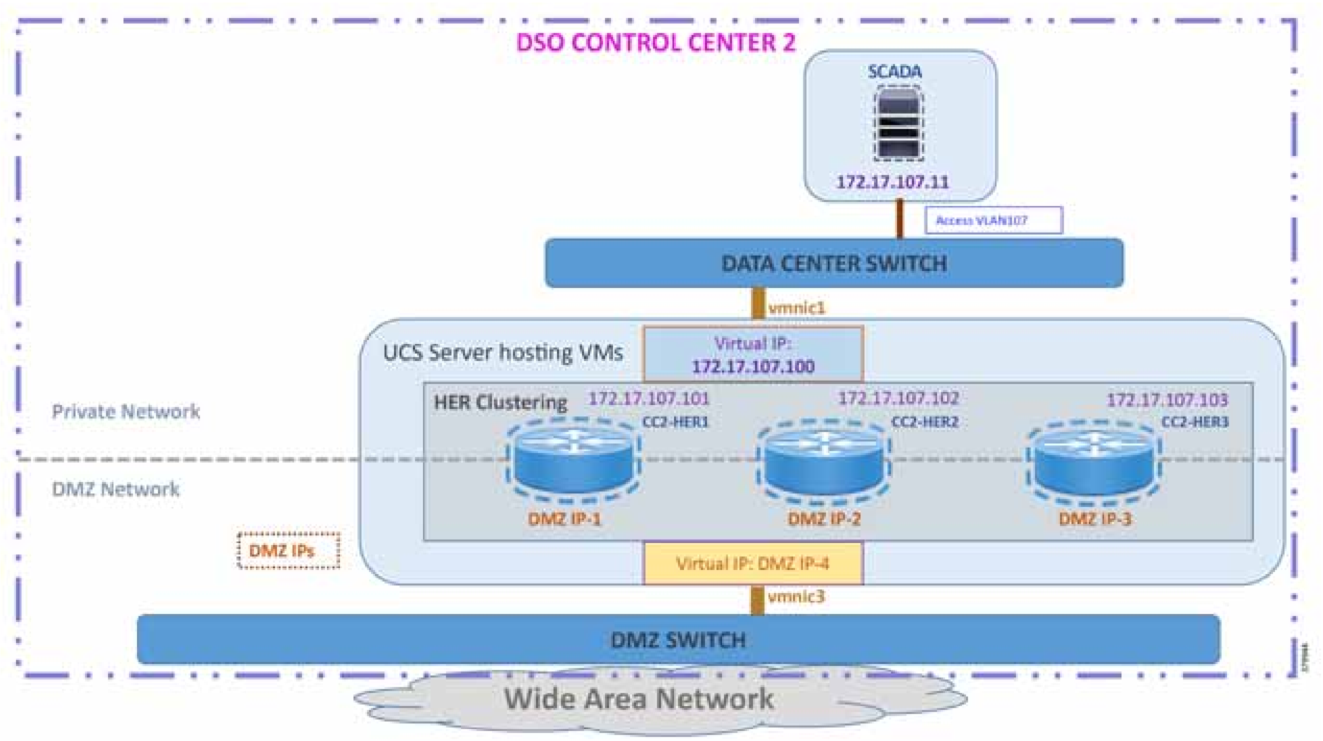
Component	Address Type	In Engineering Lab Topology	In Cisco DMZ Headend
TPS	IPv4	172.16.242.242	192.168.103.242
	IPv6	2001:db8:16:242::242	2001:db8:192:168:103::242
HER1	IPv4	172.16.101.251 172.16.102.251 172.16.103.251 172.16.104.251 172.16.105.251 172.16.107.251 172.16.241.251 172.16.242.251	192.168.103.251 192.168.105.251
	IPv6	2001:DB8:16:103::251 2001:DB8:16:105::251 2001:DB8:16:242::251	2001:DB8:192:168:103::251 2001:DB8:192:168:105::251
HER2	IPv4	172.16.101.252 172.16.102.252 172.16.103.252 172.16.104.252 172.16.105.252 172.16.107.252 172.16.241.252 172.16.242.252	192.168.103.252 192.168.105.252
	IPv6	2001:DB8:16:103::252 2001:DB8:16:105::252 2001:DB8:16:242::252	2001:DB8:192:168:103::252 2001:DB8:192:168:105::252
HER3	IPv4	172.16.101.253 172.16.102.253 172.16.103.253 172.16.104.253 172.16.105.253 172.16.107.253 172.16.241.253 172.16.242.253	N/A
	IPv6	2001:DB8:16:103::253 2001:DB8:16:105::253 2001:DB8:16:242::253	N/A
HER Cluster (Virtual IP)	IPv4	172.16.101.1 172.16.102.1 172.16.103.1 172.16.104.1 172.16.105.1 172.16.107.1 172.16.241.1 172.16.242.1	192.168.103.75
	IPv6	2001:DB8:16:103::1 2001:DB8:16:105::1 2001:DB8:16:242::1	2001:DB8:192:168:103::75 2001:DB8:192:168:105::75
NTP	IPv4	ntp.esl.cisco.com (Cisco's NTP server)	ntp.esl.cisco.com
DNS	IPv4	Cisco's DNS server	Cisco's DNS server

Addressing in DSO Control Center2

Either the Cisco ASR 1000 series of physical routers or CSR1000v series of virtual routers could be used to serve the role of headend routers (HERs). In high scale deployments, the ASR 1000 is recommended while CSR1000v might be sufficient for low scale deployment. Scale is a metric of the number of SSRs or DA Gateways that needs to be aggregated at the control center.

The ASR 1000 has been validated as part of Control Center1 and CSR1000v has been validated as part of Control Center2.

Figure 5 DSO Control Center 2–Implementation Topology



The DSO Control Center2 is comprised of two types of networks:

- DMZ Network:
  - Simulated DMZ in the Engineering Lab Topology
  - Real DMZ in the Cisco DMZ headend
- Private Network

DSO Control Center2: Addressing in the DMZ Network

Similar to the DSO Control Center1, the DMZ Switch is the entry point of the WAN into the DSO Control Center2. The following components are located in the DMZ Network (reachable over WAN):

- HER Cluster—implemented using CSR1000v series of virtual routers on UCS platform:
  - The HER Cluster performs the role of aggregating the secure tunnels from the DA Gateways and SSRs and provides connectivity to the SCADA server and other application servers.

CC2: Addressing in the Simulated DMZ Network with Engineering Lab Topology

Table 6 and Table 7 capture the IPv4 and IPv6 addresses of the HER Cluster with the instance of the solution validation topology positioned in the Engineering Lab Topology:

Table 6 CC2–IPv4 and IPv6 Addressing–DMZ Network with Engineering Lab Topology

Component Name	Address Type (IPv4/IPv6)	IP Address (With Engineering Lab Topology)
CC2-HER1	IPv4	10.10.101.101
	IPv6	2001:DB8:1011:903::2
CC2-HER2	IPv4	10.10.101.102
	IPv6	2001:DB8:1011:903::5
CC2-HER3	IPv4	10.10.101.103
	IPv6	2001:DB8:1011:903::6

Note: The Virtual IP for HER1, HER2, and HER3 is 10.10.101.100 in the Engineering Lab Topology.

CC2: Addressing in the Real DMZ Network with Cisco DMZ Headend

Table 7 captures the addressing details of the Control Center2 components located in the real DMZ network. For security reasons, instead of referencing real Cisco DMZ IPv4 and IPv6 addresses, the following representations are used throughout this document:

Table 7 CC2–IPv4 and IPv6 Addressing–Real DMZ Network with Cisco DMZ Headend

DMZ Component	Address Type	Is represented in this document as:
Head End Router1	IPv4	cc2-her1-ipv4.ipg.cisco.com
	IPv6	cc2-her1-ipv6.ipg.cisco.com
Head End Router2	IPv4	cc2-her2-ipv4.ipg.cisco.com
	IPv6	cc2-her2-ipv6.ipg.cisco.com
HER Cluster (Virtual IP)	IPv4	cc2-her-ipv4.ipg.cisco.com
	IPv6	cc2-her-ipv6.ipg.cisco.com

DSO Control Center2: Addressing in the Private Network

Table 8 captures the addressing details of the components located in the Private Network of the Control Center2:

Table 8 DSO Control Center2–Addressing in the Private Network

Component	Address Type	In Engineering Lab Topology	In Cisco DMZ Headend
SCADA	IPv4	172.17.107.11	192.168.117.11
	IPv6	2001:db8:17:107::11	2001:db8:192:168:117::11
HER1	IPv4	172.17.107.251	192.168.117.251
	IPv6	2001:DB8:17:107::251	2001:DB8:192:168:117::251
HER2	IPv4	172.17.107.252	192.168.117.252
	IPv6	2001:DB8:17:107::252	2001:DB8:192:168:117::252
HER3	IPv4	172.17.107.253	N/A
	IPv6	2001:DB8:17:107::253	N/A

Table 8 DSO Control Center2–Addressing in the Private Network (continued)

Component	Address Type	In Engineering Lab Topology	In Cisco DMZ Headend
HER Cluster (Virtual IP)	IPv4	172.17.107.1	192.168.117.75
	IPv6	2001:DB8:17:107::1	2001:DB8:192:168:117::75
NTP	IPv4	ntp.esl.cisco.com (Cisco's NTP server)	ntp.esl.cisco.com
DNS	IPv4	Cisco's DNS server	Cisco's DNS server

IoT Gateway Onboarding and Management

This chapter includes the following major topics:

This chapter corresponds to the “Zero Touch Onboarding of Cisco IOS Routers” chapter in the *Distribution Automation - Secondary Substation Design Guide*. Field Network Director (FND) is used as the NMS in this solution.

IoT Gateway Onboarding has been made very simple:

1. The brand new IoT Gateway could be unpacked from the box.
2. It could be subjected to bootstrapping using plug-and-play (PnP) infrastructure.
3. After bootstrapping, the IoT Gateway could be powered off and deployed at the desired deployment location. In some cases, bootstrapping could occur directly out of the deployment location itself.
4. When powered on, ZTD then happens with the IoT Gateway.
5. As a result, the device could be made fully operational with zero manual configuration.

As part of IoT Gateway onboarding with ZTD, the IoT Gateways are registered with the FND. From that point onwards, the FND located in the Control Center could be used to remotely monitor/manage/troubleshoot the IoT Gateways (which are spread across the entire Distribution Automation Network) and the Secondary Substations.

This process has three phases:

1. Bootstrapping of the IoT Gateway
2. Deployment of the IoT Gateway
3. Remote Monitoring/Management/Troubleshooting of the IoT Gateway.

The design guide talks about the following two different approaches for **bootstrapping** versus **deployment** of the IoT Gateway:

- **Approach 1**—IoT Gateway Bootstrapped in staging location, deployed in a different location
- **Approach 2**—IoT Gateway Bootstrapped straight out of deployed location

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

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,

Two Logical Categories of Tunnel Provisioning Server/Field Network Director

Bootstrapping TPS/FND

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

Network Operating Center TPS/FND

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 upon the chosen approach. With Approach 1, two different pairs of TPS/FND have been implemented. They are referred to as:

- Bootstrapping TPS/FND
- NOC TPS/FND

With Approach 2, the same pair of TPS/FND serves the purpose of bootstrapping TPS/FND and 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 IoT 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.

Note: Please refer to the “Certificate/Considerations for PnP and ZTD**”** section in the *Distribution Automation - Secondary Substation Design Guide* for Common Name and Subject Alternate Name requirements while creating certificates for the Bootstrapping TPS/FND and NOC TPS/FND.

Bootstrapping of 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 9:

Table 9 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. 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. ■ Dynamic approaches, in which any of the following actors provides the PnP server detail: – DHCP server – DNS server – Cisco PnP Cloud Redirection Service ■ Manual approach, in which the PnP server detail is configured manually in the profile: – Custom PnP server profile configuration.
PnP Proxy	Tunnel Provisioning Server	Responsible for mediating the bootstrapping request between the IoT Gateway and the FND. 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 (also called as bootstrapping configuration) could be created as a Template in FND.

This section is discussed in the following phases:

- Prerequisites, page 18
- Certificate Creation and Installation, page 18
- Installation of Bootstrapping TPS, page 20
- Installation of Bootstrapping FND, page 21
- Configuration of Bootstrapping TPS, page 21
- Configuration of Bootstrapping FND, page 24

Prerequisites

Prerequisites include the following:

- TPS and FND server must be up and running.
- This section focuses only on the incremental portions to make the regular TPS/FND as 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* at the following URL:

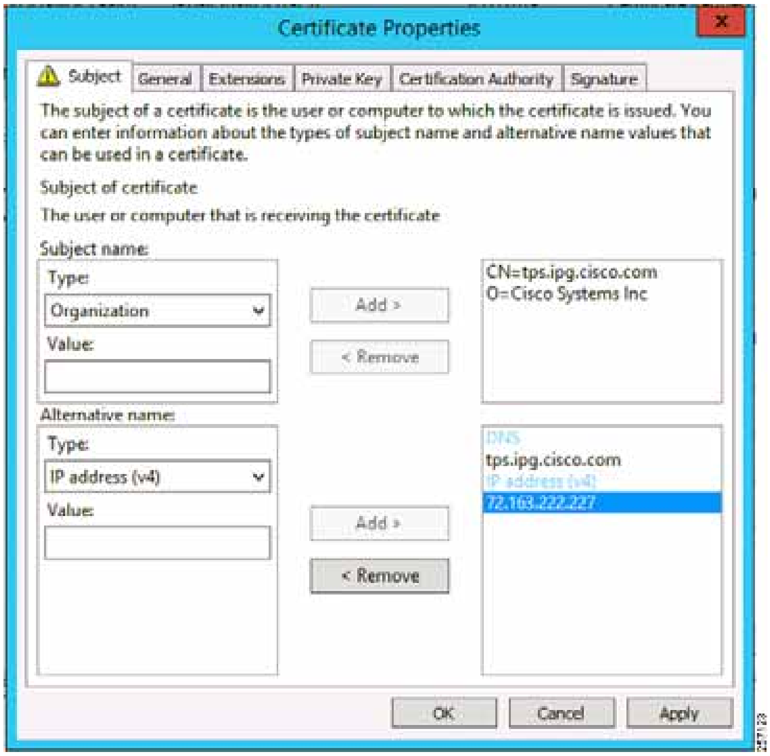
- https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872

Implementation and FAN Use Cases are available under Cisco SalesConnect.

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.

Figure 6 TPS Certificate Parameters for PnP Bootstrapping



Certificate Properties

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 certificate

The user or computer that is receiving the certificate

Subject name:

Type: Organization

Value:

CN=tps.ipg.cisco.com
O=Cisco Systems Inc

Alternative name:

Type: IP address (v4)

Value:

DNS
tps.ipg.cisco.com
IP address (v4)
72.163.222.227

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

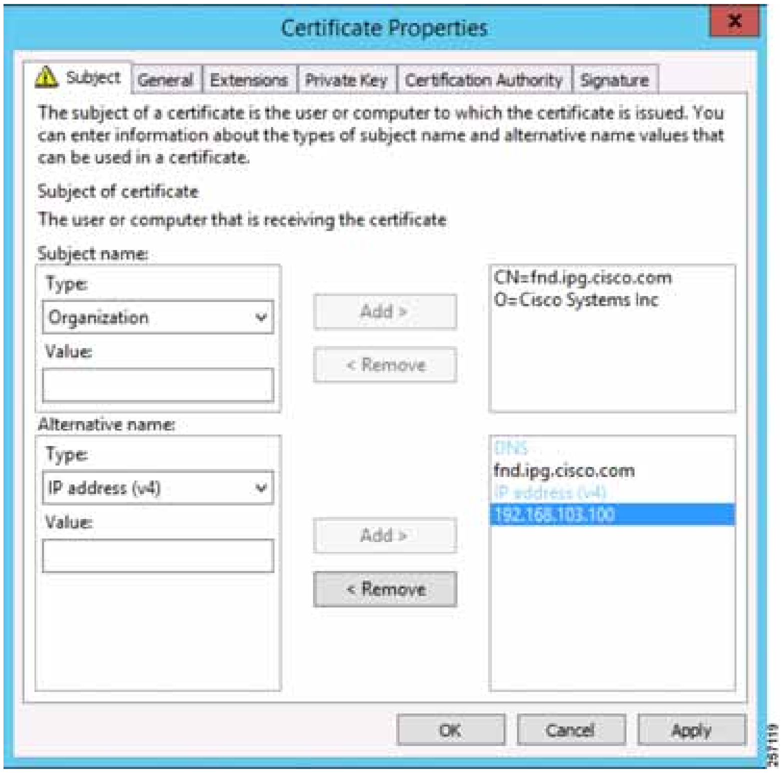
The Subject Alternative Name must be set to the FQDN of the PnP Proxy, along with the optional IP address. The Subject Alternative Name is required for PnP to work.

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.

Figure 7 FND Certificate Parameters for FND Bootstrapping



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 certificate

The user or computer that is receiving the certificate

Subject name:

Type: Organization

Value:

CN=fnd.ipg.cisco.com
O=Cisco Systems Inc

Alternative name:

Type: IP address (v4)

Value:

DNS
fnd.ipg.cisco.com
IP address (v4)
192.168.103.100

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 at the following URL:

- https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872

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** instead of **TPS.pfx** while enrolling the certificate on the TPS.

Following are the crisp 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.

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* at the following URL:

- https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872

FND Certificate Installation on the Bootstrapping FND

For installation of 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** instead of **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+TrDWqh1w==

## 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 tps-san.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:

***************** WARNING WARNING WARNING *****************
*   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.*
***************** WARNING WARNING WARNING *****************

Keystore type: JKS Keystore provider: SUN

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, 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 ~]#
```

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 of 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.xxx # DNS2=xxx.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+TrDWqh1w==
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=<Cisco DMZ IP>
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.

The IOT gateway should be able to communicate with the value given against the proxy-bootstrap-ip. IF IPv4 is used, it must be reachable from the IOT gateway. If FQDN is used, it must be DNS resolvable and reachable from the IoT gateway.

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
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6 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:

***************** WARNING WARNING WARNING *****************
*   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.*
***************** WARNING WARNING WARNING *****************

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-san conf]#
```

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]# 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]#
```

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.xxx
# DNS2=xxx.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
ir800,IR807G-LTE-GA-K9+FCW2231004T,FastEthernet0,cg-nms-
administrator,<encrypted_pwd>,IR807_BS1,ipg.cisco.com,flash:/ir800l-
universalk9-mz.SPA.157-3.M2.bin
ir1100,IR1101-K9+FCW222700K0,GigabitEthernet0/0/0,cg-nms-
administrator,<encrypted_pwd>,IR1100_FCW222700K0,ipg.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/ima
ges/cgr1000-universalk9-mz.SPA.157-3.M2
ir800,IR829GW-LTE-GA-EK9+FGL195024PP,Vlan1,cg-nms-
administrator,<encrypted_pwd>,IR829_FGL195024PP,ipg.cisco.com,flash:/ir8
00-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
```

Table 10 Fields 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
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.
adminPassword	<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.

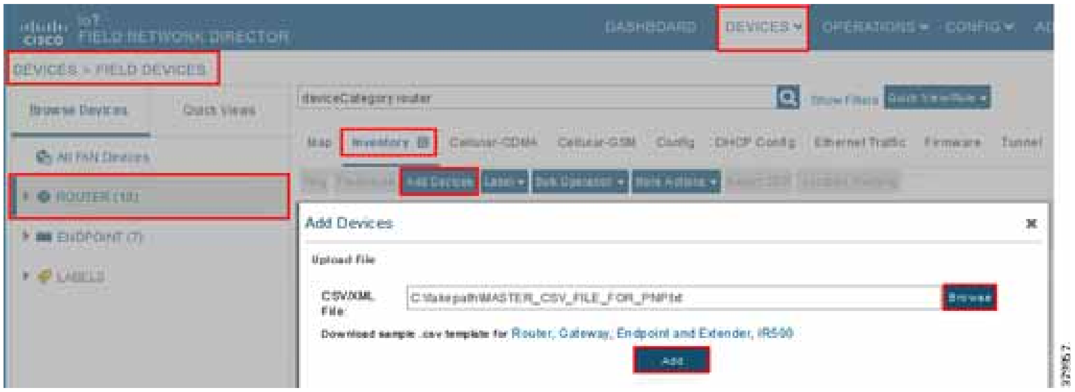
Obtain the *<encrypted_pwd>* for the adminPassword field using the following step (from FND Linux shell prompt):

/opt/cgms-tools/bin/signature-tool encrypt /opt/cgms/server/cgms/conf/cgms_keystore password-file.txt

For more details, please refer to the following URL:

- https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/iot-field-network-director/210446-Prepare-csv-Comma-Separated-Value-fil.html

Figure 8 Bootstrapping CSV Import at Bootstrapping FND



CSV/XML File: C:\fakepath\MASTER_CSV_FILE_FOR_PNP.txt

Download sample .csv template for Router, Gateway, Endpoint and Extender, IR500

In bootstrapping FND, from **Devices > Field Devices**, click **Router** in the left pane, click the **Inventory** tab on the middle pane, click **Add Devices**, browse the csv file created in the previous step, and then click **Add** to import the IoT Gateway CSV list into the bootstrapping FND.

PnP Server Discovery through DHCP and Bootstrapping

This section is discussed in the following phases:

- Prerequisites, page 28
- Bootstrapping in the IPv4 Network, page 28
- Bootstrapping in the IPv6 Network, page 29
- Logical Call Flow, page 35

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.

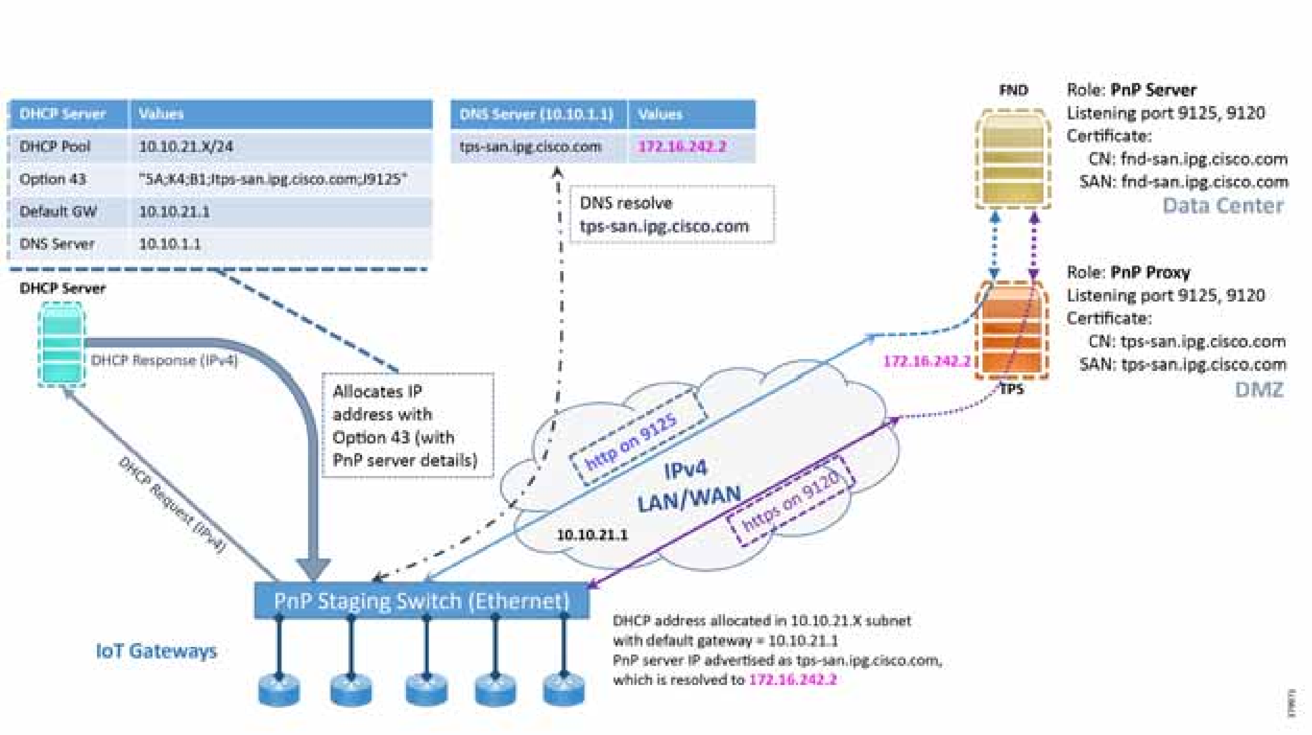
Bootstrapping in the IPv4 Network

This section discusses the DHCP server-assisted bootstrapping of the IoT Gateways over the IPv4 network.

In Figure 9, 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 9 DHCP Server-Assisted Bootstrapping of IoT Gateways over IPv4 Network



DHCP Server	Values
DHCP Pool	10.10.21.X/24
Option 43	"5A;K4;B1;Itps-san.ipg.cisco.com;J9125"
Default GW	10.10.21.1
DNS Server	10.10.1.1

DNS Server (10.10.1.1)	Values
tps-san.ipg.cisco.com	172.16.242.2

DHCP Server
DHCP Response (IPv4)
DHCP Request (IPv4)
Allocates IP address with Option 43 (with PnP server details)
DNS resolve tps-san.ipg.cisco.com
http on 9125
IPv4 LAN/WAN
https on 9120
10.10.21.1
PnP Staging Switch (Ethernet)
IoT Gateways
DHCP address allocated in 10.10.21.X subnet
with default gateway = 10.10.21.1
PnP server IP advertised as tps-san.ipg.cisco.com,
which is resolved to 172.16.242.2
FND
Role: PnP Server
Listening port 9125, 9120
Certificate:
CN: fnd-san.ipg.cisco.com
SAN: fnd-san.ipg.cisco.com
Data Center
Role: PnP Proxy
Listening port 9125, 9120
Certificate:
CN: tps-san.ipg.cisco.com
SAN: tps-san.ipg.cisco.com
DMZ
172.16.242.2
TPS

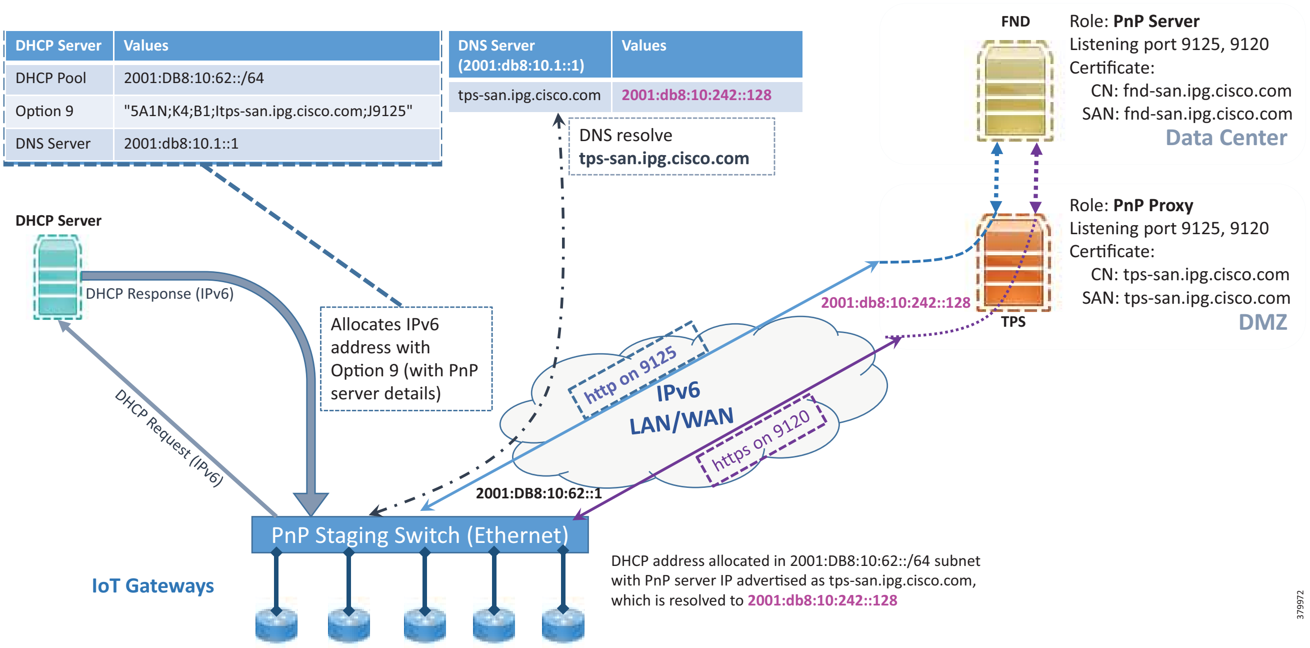
Bootstrapping in the IPv6 Network

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

In Figure 10:

- 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.

Figure 10 DHCP Server-Assisted Bootstrapping of IoT Gateways over IPv6 Network



DHCP Server	Values
DHCP Pool	2001:DB8:10:62::/64
Option 9	"5A1N;K4;B1;Itps-san.ipg.cisco.com;J9125"
DNS Server	2001:db8:10.1::1

DNS Server (2001:db8:10.1::1)	Values
tps-san.ipg.cisco.com	2001:db8:10:242::128

DHCP address allocated in 2001:DB8:10:62::/64 subnet with PnP server IP advertised as tps-san.ipg.cisco.com, which is resolved to 2001:db8:10:242::128

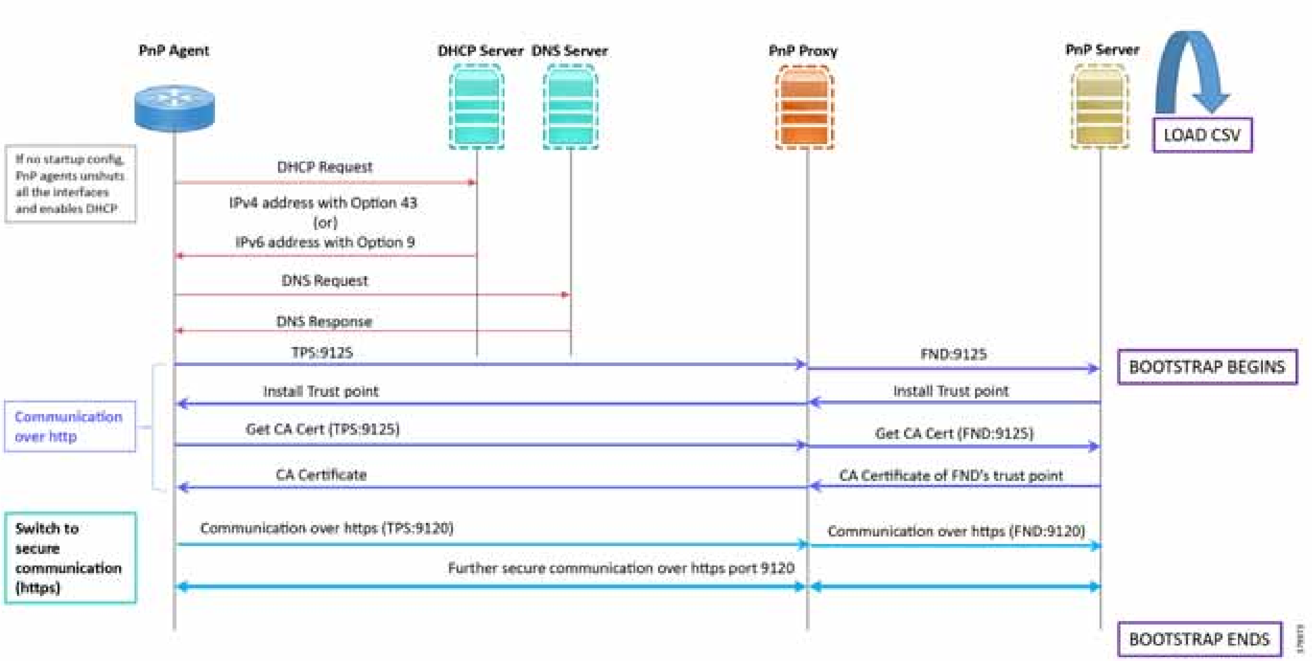
Logical Call Flow

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 10 are the following:

- PnP Agent (IoT Gateway)
- DHCP Server
- DNS Server
- PnP Proxy (TPS)
- PnP Server (FND)

Figure 11 DHCP Server-Assisted Bootstrapping of IoT Gateways—Logical Call Flow


PnP Agent
DHCP Server
DNS Server
PnP Proxy
PnP Server
LOAD CSV
If no startup config, PnP agents unshuts all the interfaces and enables DHCP
DHCP Request
IPv4 address with Option 43 (or) IPv6 address with Option 9
DNS Request
DNS Response
TPS:9125
FND:9125
BOOTSTRAP BEGINS
Install Trust point
Install Trust point
Communication over http
Get CA Cert (TPS:9125)
Get CA Cert (FND:9125)
CA Certificate
CA Certificate of FND's trust point
Switch to secure communication (https)
Communication over https (TPS:9120)
Communication over https (FND:9120)
Further secure communication over https port 9120
BOOTSTRAP ENDS

1. 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 interfaces and enables DHCP on all of them.

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, and placing the IoT gateway under the respective “Tunnel Group” on FND (which contains the bootstrapping template under the Router Bootstrap Configuration tab).

6. The FND installs the trust point on the IoT Gateway.

7. 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 addressed:

   - For example, if https://<TPS_FQDN>:9120 is attempted, then the certificate installed on the TPS must have CN/SAN configured with <TPS_FQDN>.
   - Similarly, if the 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 message from IoT 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.

PnP Server Definition through Manual PnP Profile and Bootstrapping

This section is discussed in the following phases:

- Prerequisites, page 32
- Bootstrapping over IPv4 Network, page 33
- Bootstrapping over IPv6 Network, page 34
- Logical Call Flow, page 35

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

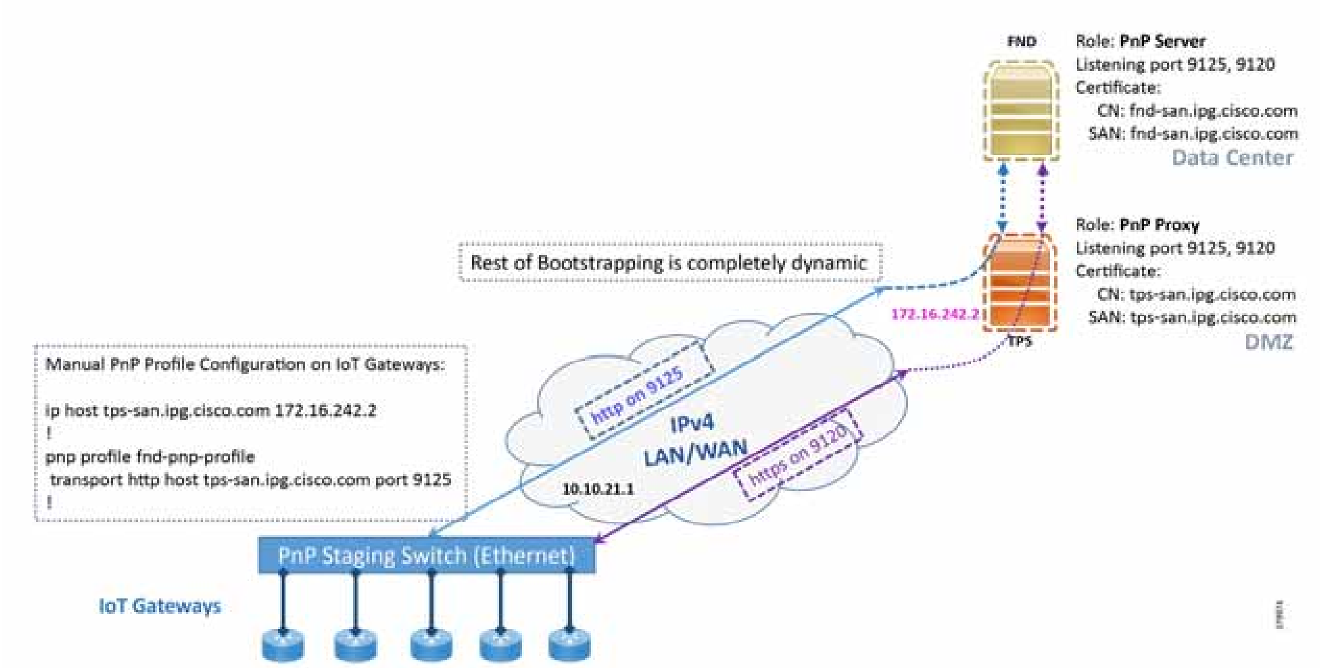
- The PnP server must be reachable either over the LAN or over the WAN/Internet.
- As TPS is used in this implementation, TPS acts as a PnP server for the IoT Gateways.

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 12, 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 12 Custom PnP Profile-Assisted Bootstrapping of IoT Gateways over IPv4 Network



Manual PnP Profile Configuration on IoT Gateways:

```
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
!
```

FND
Role: PnP Server
Listening port 9125, 9120
Certificate:
CN: fnd-san.ipg.cisco.com
SAN: fnd-san.ipg.cisco.com
Data Center
Role: PnP Proxy
Listening port 9125, 9120
Certificate:
CN: tps-san.ipg.cisco.com
SAN: tps-san.ipg.cisco.com
DMZ
TPS
172.16.242.2
Rest of Bootstrapping is completely dynamic
http on 9125
IPv4
LAN/WAN
https on 9120
10.10.21.1
PnP Staging Switch (Ethernet)
IoT Gateways

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

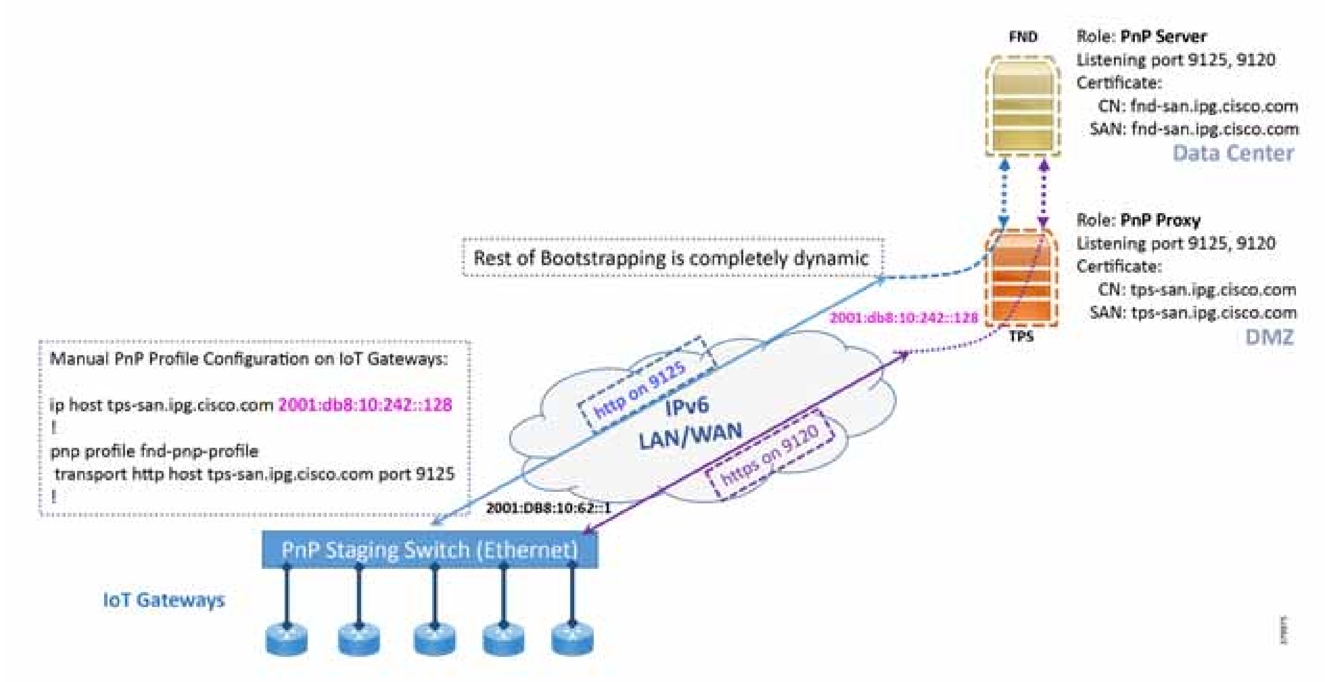
This section focuses on the bootstrapping of the IoT Gateways over the IPv6 network in the absence of the DHCP server, DNS server, and Cisco Cloud Redirector Server to provide the PnP server details. IoT Gateways are informed about the PnP server detail directly through the Cisco IOS configuration commands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

In Figure 13, 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 13 Custom PnP Profile-Assisted Bootstrapping of IoT Gateways over IPv6 Network



Manual PnP Profile Configuration on IoT Gateways:

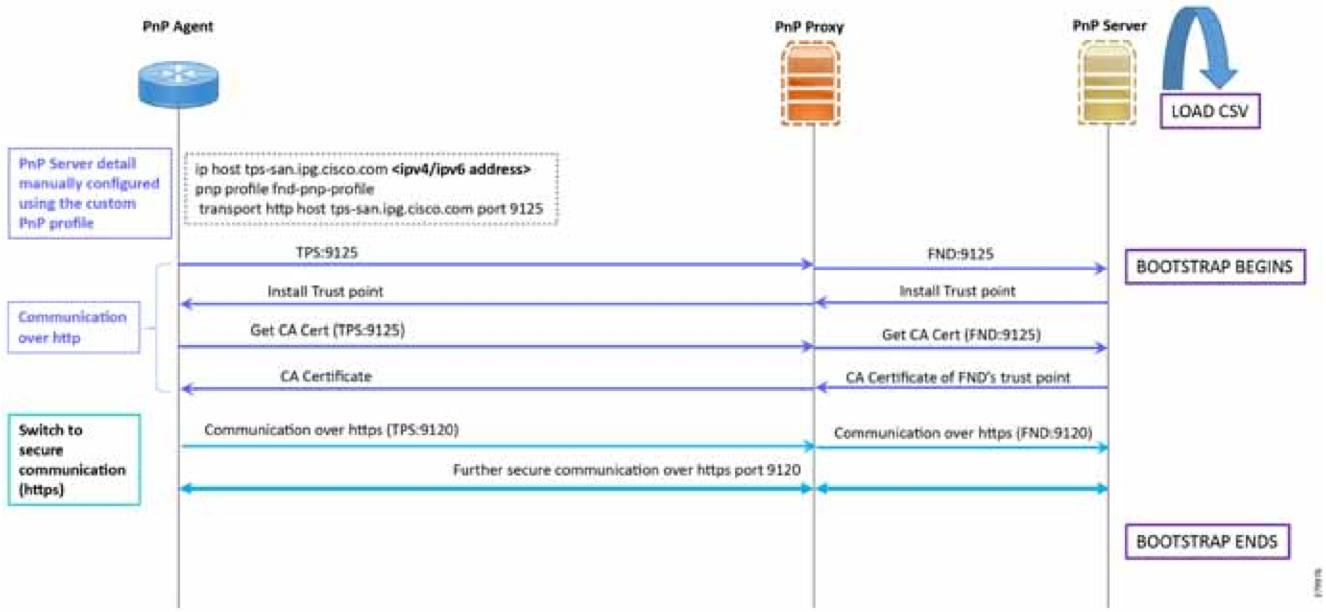
```
ip host tps-san.ipg.cisco.com 2001:db8:10:242::128
!
pnp profile fnd-pnp-profile
 transport http host tps-san.ipg.cisco.com port 9125
!
```

FND
Role: PnP Server
Listening port 9125, 9120
Certificate:
CN: fnd-san.ipg.cisco.com
SAN: fnd-san.ipg.cisco.com
Data Center
Role: PnP Proxy
Listening port 9125, 9120
Certificate:
CN: tps-san.ipg.cisco.com
SAN: tps-san.ipg.cisco.com
DMZ
TPS
2001:db8:10:242::128
Rest of Bootstrapping is completely dynamic
http on 9125
IPv6
LAN/WAN
https on 9120
2001:DB8:10:62::1
PnP Staging Switch (Ethernet)
IoT Gateways

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


PnP Agent
PnP Proxy
PnP Server
LOAD CSV
PnP Server detail manually configured using the custom PnP profile
TPS:9125
FND:9125
BOOTSTRAP BEGINS
Install Trust point
Install Trust point
Communication over http
Get CA Cert (TPS:9125)
Get CA Cert (FND:9125)
CA Certificate
CA Certificate of FND's trust point
Switch to secure communication (https)
Communication over https (TPS:9120)
Communication over https (FND:9120)
Further secure communication over https port 9120
BOOTSTRAP ENDS

```
ip host tps-san.ipg.cisco.com <ipv4/ipv6 address>
pnp profile fnd-pnp-profile
 transport http host tps-san.ipg.cisco.com port 9125
```

In Figure 14:

- 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

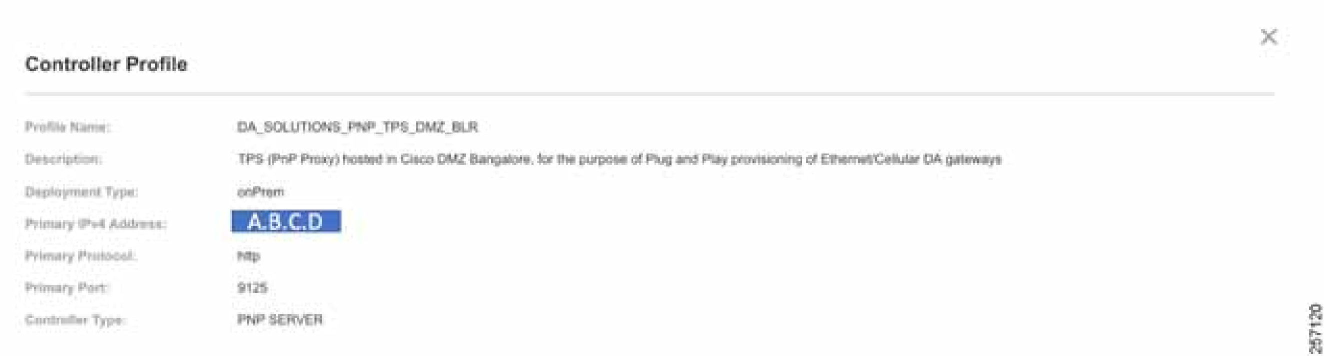
Prerequisites

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 tool bar and add the details.

Figure 15 shows the controller profile added on software.cisco.com:

Figure 15 Controller Profile

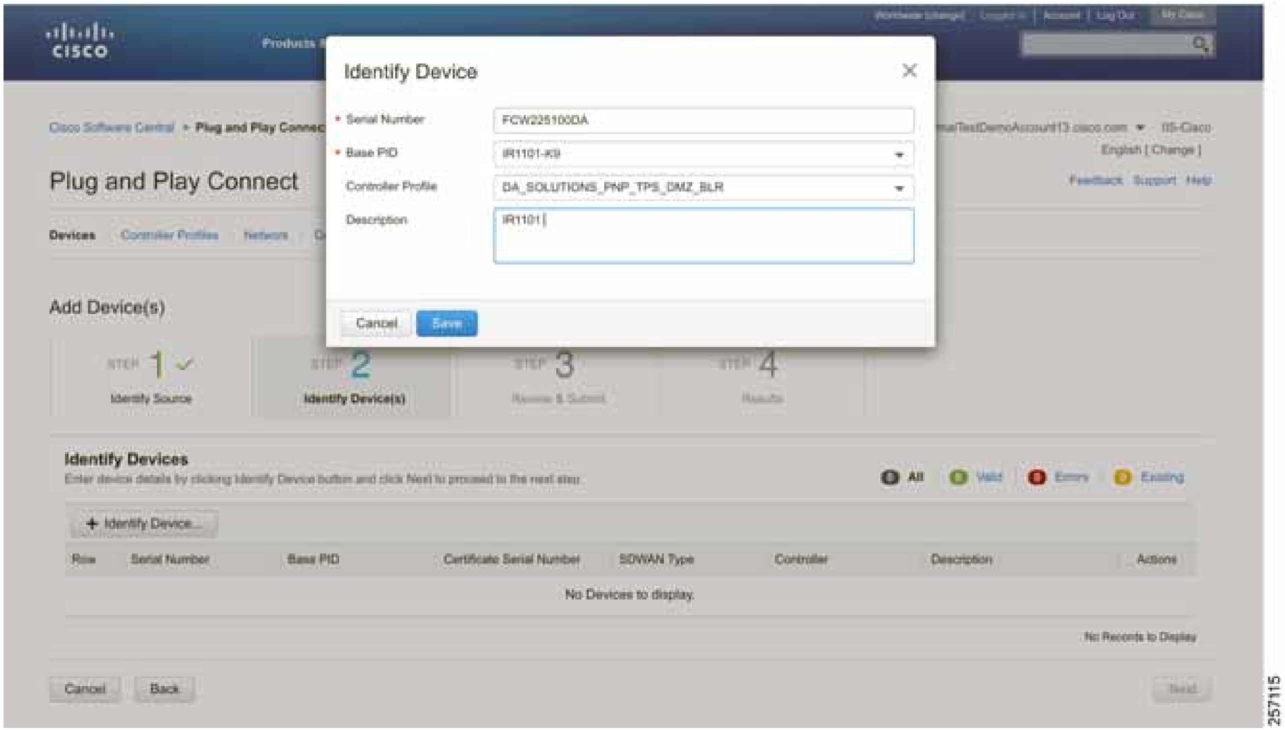


Controller Profile

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
Primary 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 Secondary Substation Design Guide*. Figure 16 shows adding a device manually:

Figure 16 Manual Addition of Device



Identify Device

* Serial Number	FCW225100DA
* Base PID	IR1101-K9
Controller Profile	DA_SOLUTIONS_PNP_TPS_DMZ_BLR
Description	IR1101

Identify Devices

Enter device details by clicking Identify Device button and click Next to proceed to the next step.

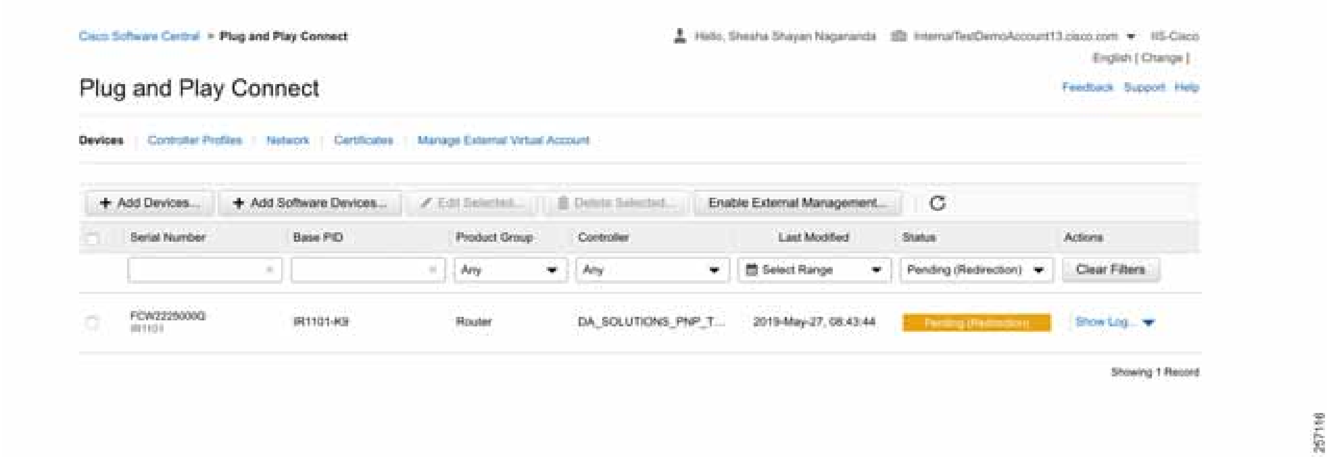
Row	Serial Number	Base PID	Certificate Serial Number	SDWAN Type	Controller	Description	Actions

No Devices to display.

No Records to Display

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 17:

Figure 17 PnP Redirect Pending after Manual Device Addition



Cisco Software Central » Plug and Play Connect

Hello, Shesha Shayan Naganarda | InternalTestDemoAccount13.cisco.com | IIS-Cisco

English [Change]

Plug and Play Connect

Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account

+ Add Devices... | + Add Software Devices... | Edit Selected... | Delete Selected... | Enable External Management...

	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
			Any	Any	Select Range	Pending (Redirection)	Clear Filters
○	FCW22250000 IR1101	IR1101-K9	Router	DA_SOLUTIONS_PNP_T...	2019-May-27, 08:43:44	Pending (Redirection)	Show Log...

Showing 1 Record

257116

Finally, when the device is added successfully, it should be populated in the devices list as shown in Figure 17, which lists the devices for when the Redirect was successful.

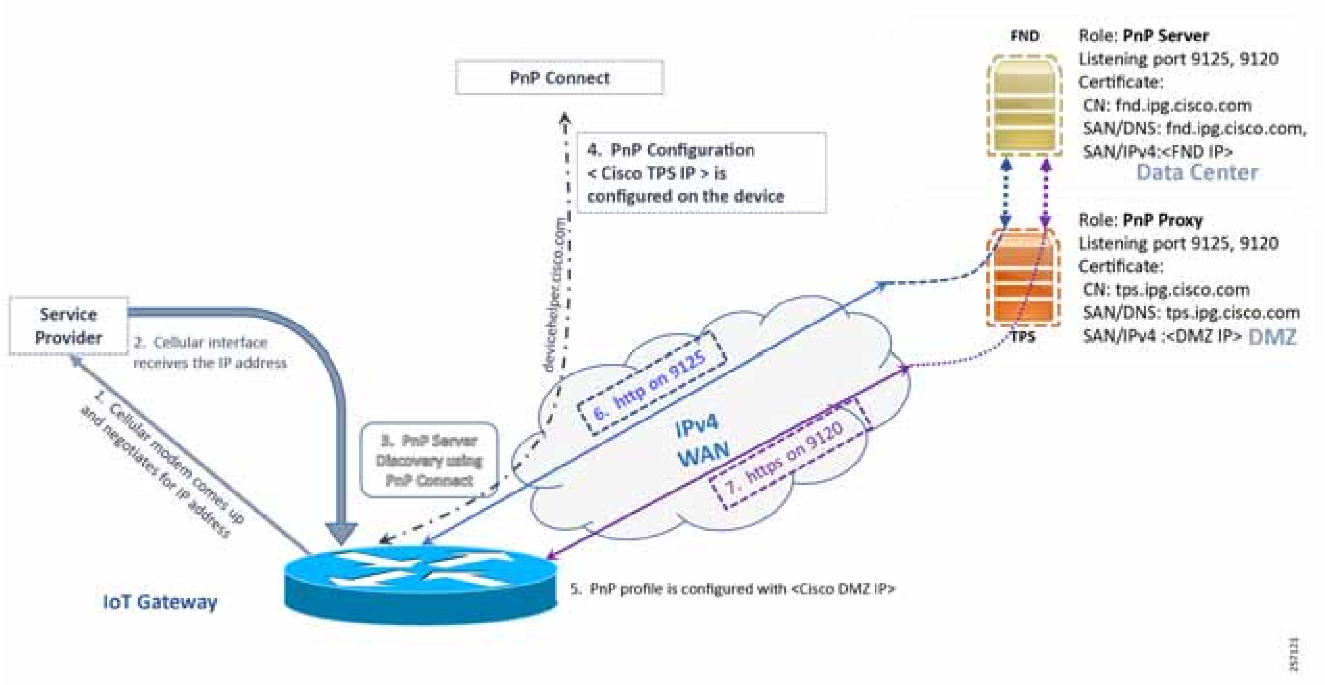
Bootstrapping

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

In Figure 18, 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.

Figure 18 PnP Connect—Assisted Bootstrapping of IoT Gateways


PnP Connect
4. PnP Configuration < Cisco TPS IP > is configured on the device
devicehelper.cisco.com
FND
Role: PnP Server
Listening port 9125, 9120
Certificate:
CN: fnd.ipg.cisco.com
SAN/DNS: fnd.ipg.cisco.com,
SAN/IPv4:<FND IP>
Data Center
Role: PnP Proxy
Listening port 9125, 9120
Certificate:
CN: tps.ipg.cisco.com
SAN/DNS: tps.ipg.cisco.com
SAN/IPv4 :<DMZ IP>
DMZ
TPS
Service Provider
2. Cellular interface receives the IP address
1. Cellular modem comes up and negotiates for IP address
3. PnP Server Discovery using PnP Connect
6. http on 9125
IPv4 WAN
7. https on 9120
IoT Gateway
5. PnP profile is configured with <Cisco DMZ IP>
257121

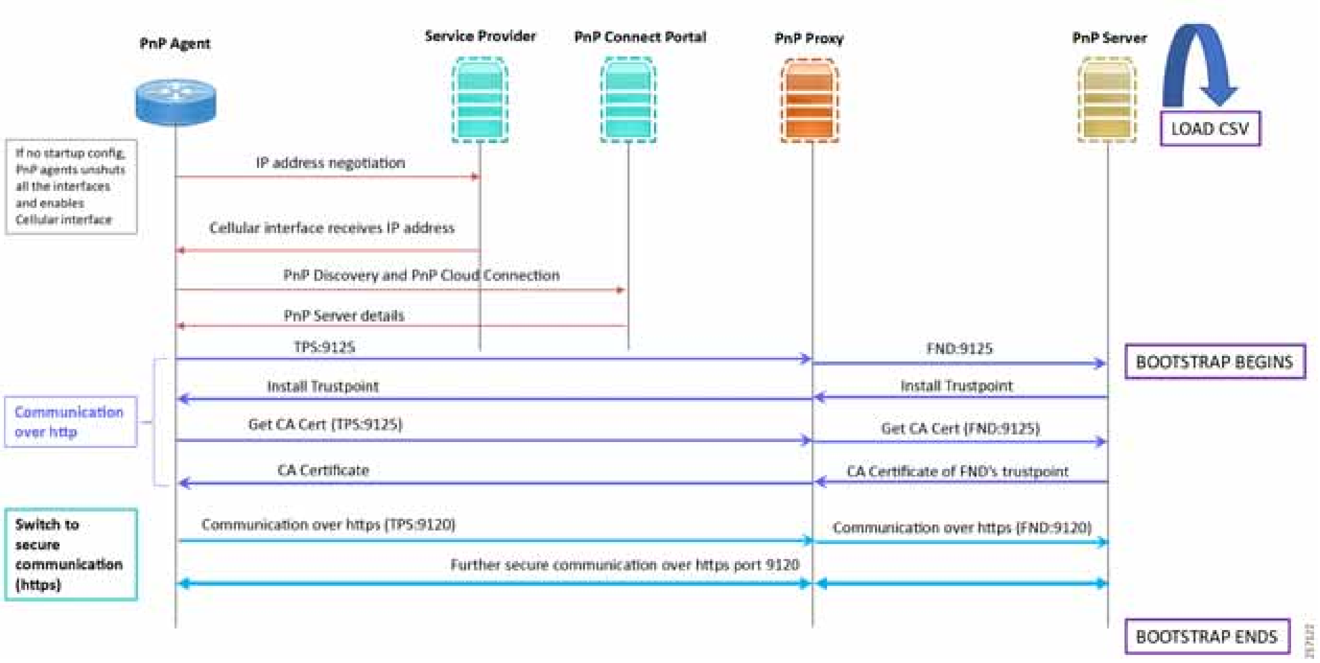
Logical Call Flow

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 19 are the following:

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

Figure 19 PnP Connect–Assisted Bootstrapping of IoT Gateways–Logical Call Flow


PnP Agent
Service Provider
PnP Connect Portal
PnP Proxy
PnP Server
LOAD CSV
If no startup config, PnP agents unshuts all the interfaces and enables Cellular interface
IP address negotiation
Cellular interface receives IP address
PnP Discovery and PnP Cloud Connection
PnP Server details
TPS:9125
FND:9125
BOOTSTRAP BEGINS
Communication over http
Install Trustpoint
Install Trustpoint
Get CA Cert (TPS:9125)
Get CA Cert (FND:9125)
CA Certificate
CA Certificate of FND's trustpoint
Switch to secure communication (https)
Communication over https (TPS:9120)
Communication over https (FND:9120)
Further secure communication over https port 9120
BOOTSTRAP ENDS

1. 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.

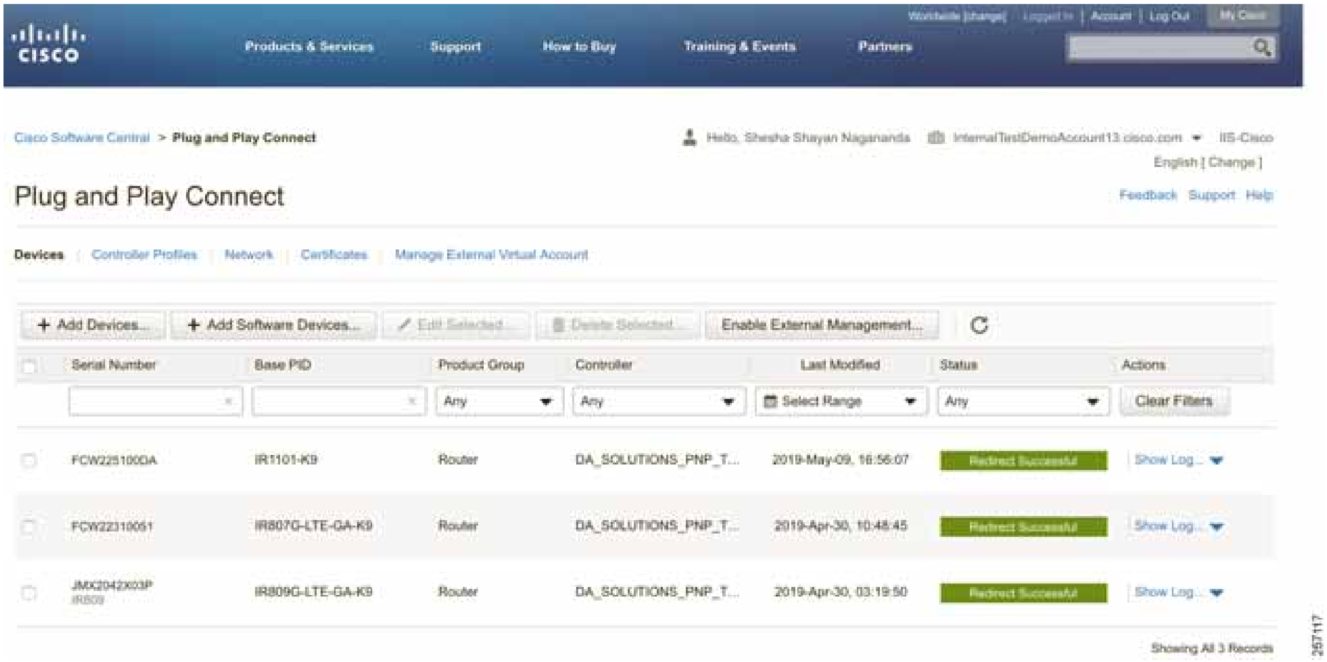
3. The service provider responds back with the IPv4 address.

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. Figure 20 shows that the PnP redirection is 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.

Figure 20 PnP Redirection Successful


Products & Services
Support
How to Buy
Training & Events
Partners
Worldwide [change]
Logged In | Account | Log Out
My Cisco
Cisco Software Central > Plug and Play Connect
Hello, Shesha Shayan Naganandа
InternalTestDemoAccount13.cisco.com
IIS-Cisco
English [Change]
Feedback Support Help
Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account
+ Add Devices...
+ Add Software Devices...
Edit Selected...
Delete Selected...
Enable External Management...
Select Range
Clear Filters
Showing All 3 Records
257117

Plug and Play Connect

Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
		Any	Any	Select Range	Any	Clear Filters
FCW225100DA	IR1101-K9	Router	DA_SOLUTIONS_PNP_T...	2019-May-09, 16:56:07	Redirect Successful	Show Log...
FCW22310051	IR807G-LTE-GA-K9	Router	DA_SOLUTIONS_PNP_T...	2019-Apr-30, 10:48:45	Redirect Successful	Show Log...
JMX2042X03P IR809	IR809G-LTE-GA-K9	Router	DA_SOLUTIONS_PNP_T...	2019-Apr-30, 03:19:50	Redirect Successful	Show Log...

Bootstrapping Configuration Template on Bootstrapping FND

Like the tunnel provisioning template, the bootstrapping template has to be defined on FND. This template initiates the deployment process when the gateway is deployed in the desired location.

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 translated into the Cisco IOS configuration, which is then pushed onto the IoT Gateway.

In the previous section, we discussed three PnP server discovery methods. In this section, we will discuss the bootstrapping template creation for enabling the gateway to undergo the deployment process without any manual intervention.

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.

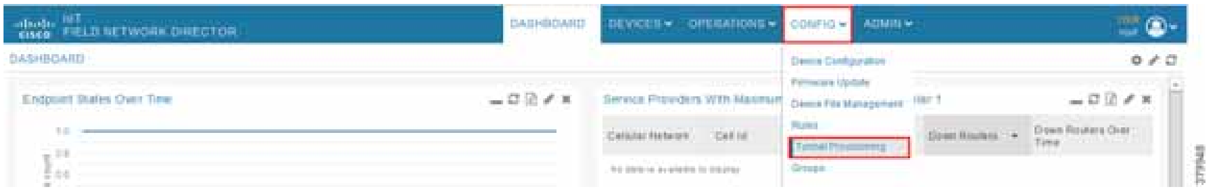
This implementation section includes the following sections:

- Creation of Bootstrap Configuration Template Group, page 41
- Router Bootstrap Configuration Groups—Populating Templates, page 44

Creation of Bootstrap Configuration Template Group

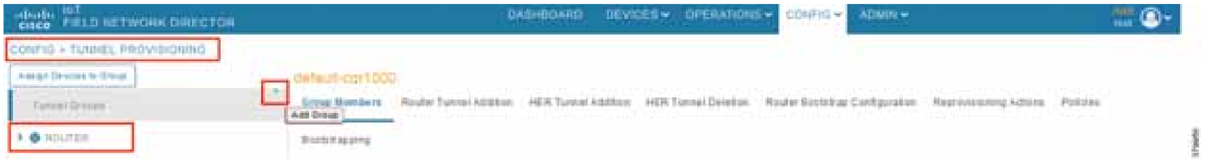
This section covers the steps required for configuring the bootstrapping group.

Figure 21 CREATE Bootstrap–CONFIG–Tunnel Provisioning



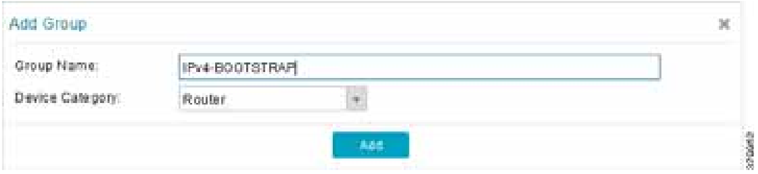
1. From the **CONFIG** Menu, select the **Tunnel Provisioning** option.

Figure 22 CREATE Bootstrap–Add Group



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

Figure 23 CREATE Bootstrap–Add IPv4 Group

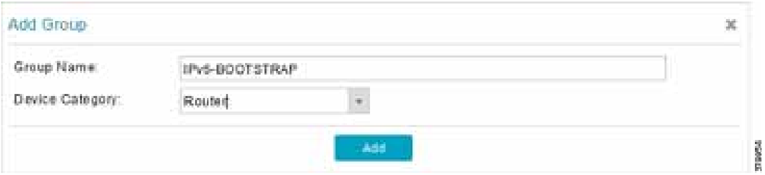


Group Name: IPv4-BOOTSTRAP

Device Category: Router

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

Figure 24 CREATE Bootstrap–Add IPv6 Group

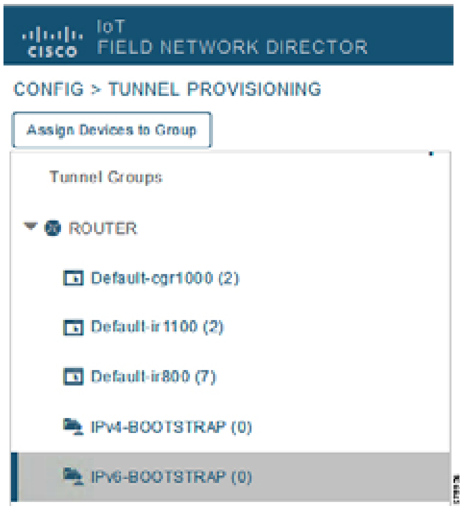


Group Name: IPv6-BOOTSTRAP

Device Category: Router

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

Figure 25 CREATE Bootstrap–List of Bootstrap Groups



CONFIG > TUNNEL PROVISIONING

Assign Devices to Group

Tunnel Groups

- ROUTER
  - Default-cgr1000 (2)
  - Default-ir1100 (2)
  - Default-ir800 (7)
  - IPv4-BOOTSTRAP (0)
  - IPv6-BOOTSTRAP (0)

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:

1. In Figure 26, 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 26 CHANGE Tunnel Group–Device Under Default Group

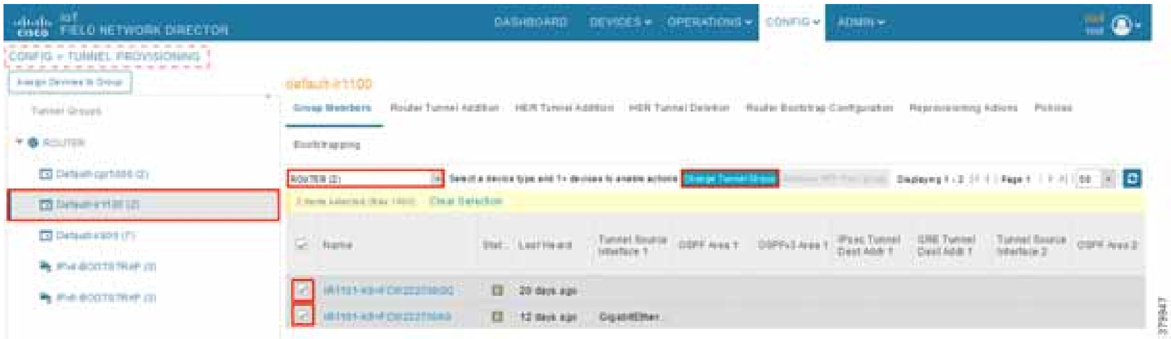
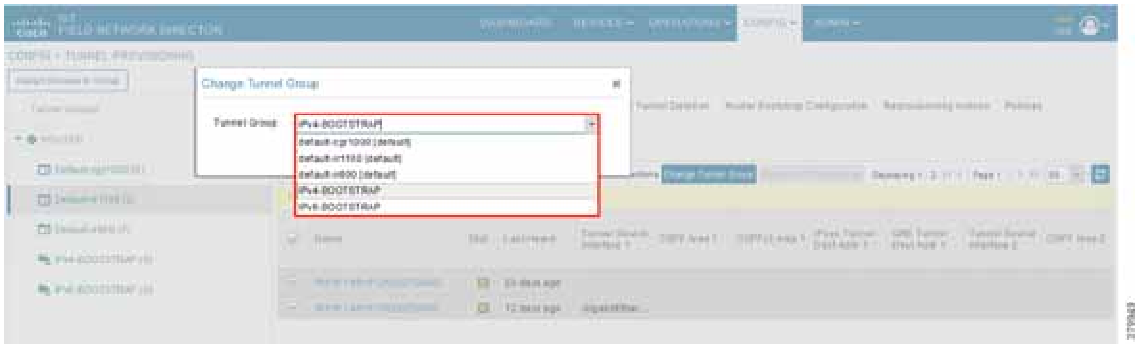
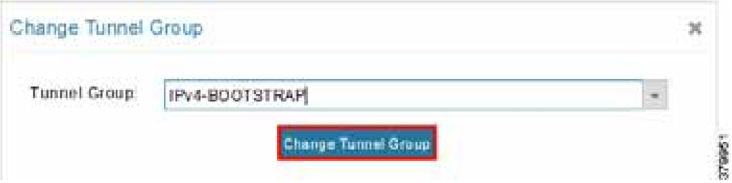


Figure 27 CHANGE Tunnel Group–Pull-Down Menu



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

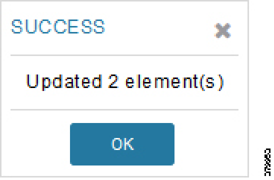
Figure 28 CHANGE Tunnel Group–Select IPv4 Group


Change Tunnel 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.

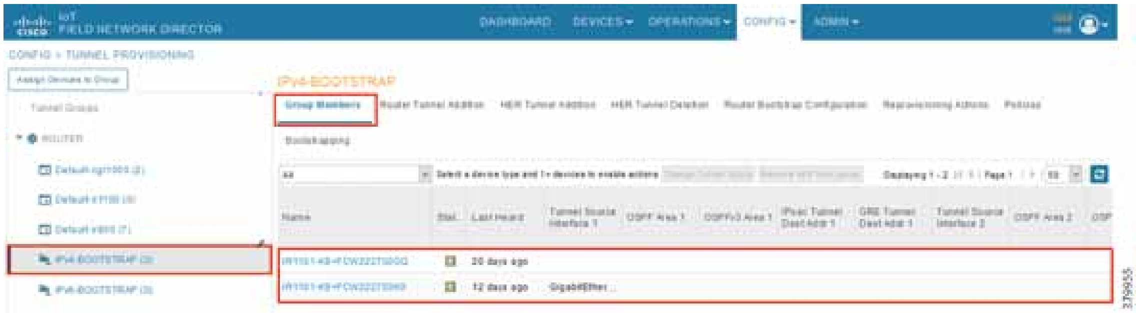
Figure 29 CHANGE Tunnel Group–Updated IPv4 Group


SUCCESS

Updated 2 element(s)

4. Device migration to the desired group was successful.

Figure 30 CHANGE Tunnel Group–Devices Moved under IPv4 Group



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

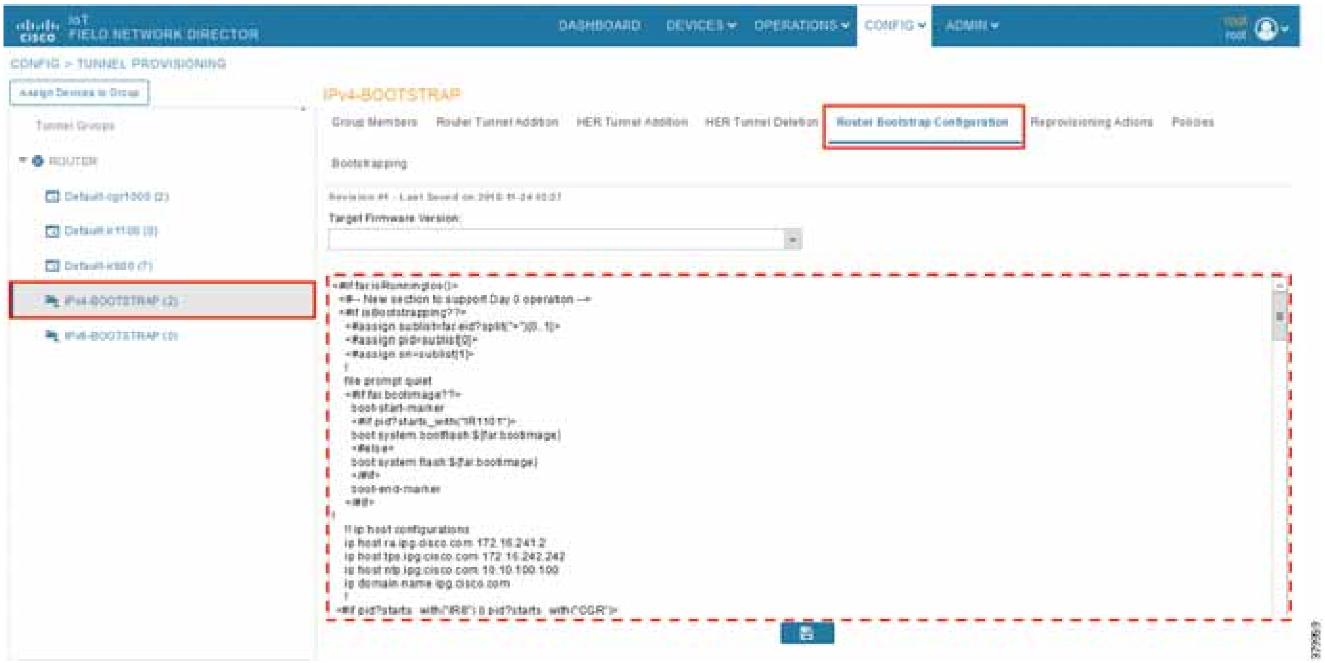
Router Bootstrap Configuration Groups–Populating Templates

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 174.

Figure 31 captures the **Router Bootstrap Configuration** section that needs to be populated for the purpose of bootstrapping:

Figure 31 Router Bootstrap Configuration



Revision #1 - Last Saved on 2018-11-24 02:27

Target Firmware Version:

```
<#if far.isRunningIos()>
 <#-- New section to support Day 0 operation -->
 <#if isBootstrapping??>
  <#assign sublist=far.eid?split("+")[0..1]>
  <#assign pid=sublist[0]>
  <#assign sn=sublist[1]>
  !
  file prompt quiet
  <#if far.bootImage??>
   boot-start-marker
   <#if pid?starts_with("IR1101")>
   boot system bootflash:${far.bootImage}
   <#else>
   boot system flash:${far.bootImage}
   </#if>
   boot-end-marker
  </#if>
!
  !! ip host configurations
  ip host ra.ipg.cisco.com 172.16.241.2
  ip host tps.ipg.cisco.com 172.16.242.242
  ip host ntp.ipg.cisco.com 10.10.100.100
  ip domain-name ipg.cisco.com
  !
 <#if pid?starts_with("IR8") || pid?starts_with("CGR")>
```

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

Table 11 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 11, 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

- Cisco IoT Gateway should have gone through the bootstrapping procedure mentioned in Bootstrapping of the IoT Gateway, page 16, with the device being part of the appropriate bootstrapping group.
- The CSV file should be imported for the IoT Gateways at the Control Center FND. Refer to Figure 171 available in Appendix B: FND Zero Touch Deployment Profiles, page 188, which shows the CSV file.

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.
- 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 Center1.
- NOC TPS, RA, and HERs must have static IP addresses configured and should be reachable from the Cisco IoT Gateways that are located in the secondary substation or along the Distribution network.

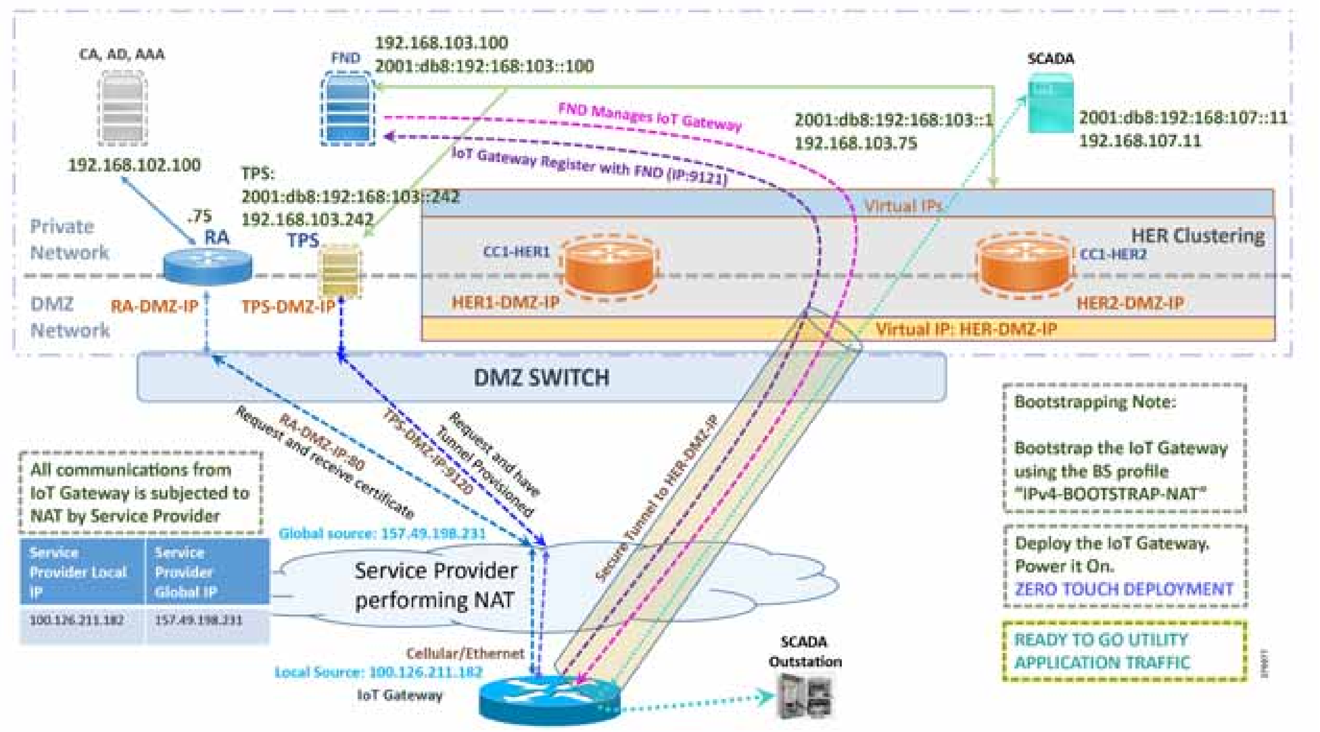
Note: If the prerequisites for deployment are addressed, ZTD of the IoT Gateways should happen successfully after the gateway is deployed at the desired location and powered on, with the Ethernet cable connected or the LTE SIM card inserted.

Deployment over IPv4 Cellular Network with NAT

Note: This section has no implementation steps. As the name “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 32 captures the deployment steps for IoT Gateway over LTE Cellular:

Figure 32 Deployment over IPv4 Cellular Network with Cisco DMZ Headend


CA, AD, AAA
192.168.102.100
FND
192.168.103.100
2001:db8:192:168:103::100
SCADA
2001:db8:192:168:107::11
192.168.107.11
FND Manages IoT Gateway
IoT Gateway Register with FND (IP:9121)
2001:db8:192:168:103::1
192.168.103.75
TPS:
2001:db8:192:168:103::242
192.168.103.242
Private Network
.75
RA
TPS
Virtual IPs
HER Clustering
CC1-HER1
CC1-HER2
DMZ Network
RA-DMZ-IP
TPS-DMZ-IP
HER1-DMZ-IP
HER2-DMZ-IP
Virtual IP: HER-DMZ-IP
DMZ SWITCH
RA-DMZ-IP:80
Request and receive certificate
TPS-DMZ-IP:9120
Request and have Tunnel Provisioned
Secure Tunnel to HER-DMZ-IP
All communications from IoT Gateway is subjected to NAT by Service Provider
Service Provider Local IP
Service Provider Global IP
100.126.211.182
157.49.198.231
Global source: 157.49.198.231
Service Provider performing NAT
Cellular/Ethernet
Local Source: 100.126.211.182
IoT Gateway
SCADA Outstation
Bootstrapping Note:
Bootstrap the IoT Gateway using the BS profile "IPv4-BOOTSTRAP-NAT"
Deploy the IoT Gateway. Power it On.
ZERO TOUCH DEPLOYMENT
READY TO GO UTILITY APPLICATION TRAFFIC
279071

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.

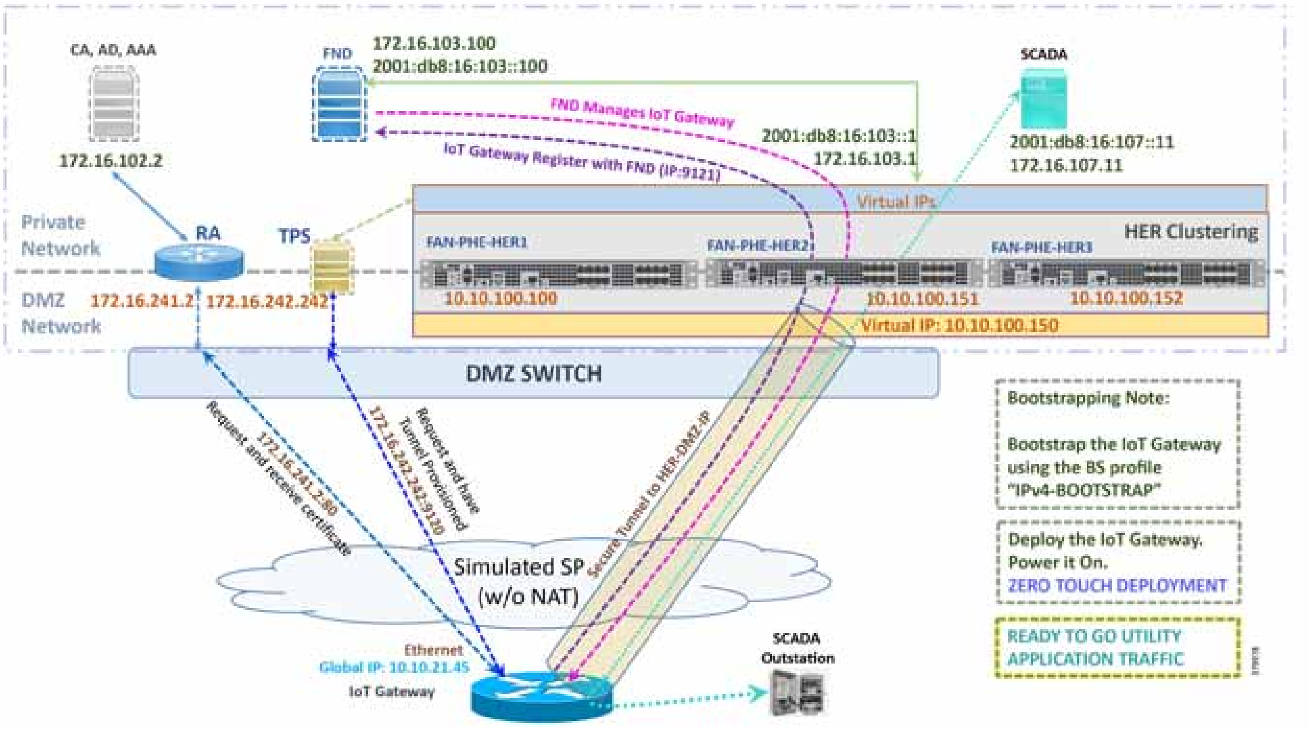
7. As part of the device registration with the FND, FND also pushes SCADA Traffic enablement configurations to the IoT Gateway, which enables the communication between the SCADA Master in the Control Center and the SCADA Outstation located in the Secondary Substation/Distribution Network.
8. ZTD of the 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 name "ZTD" suggests, 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 33 Deployment over IPv4 Ethernet Network in Engineering Lab Topology



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

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.

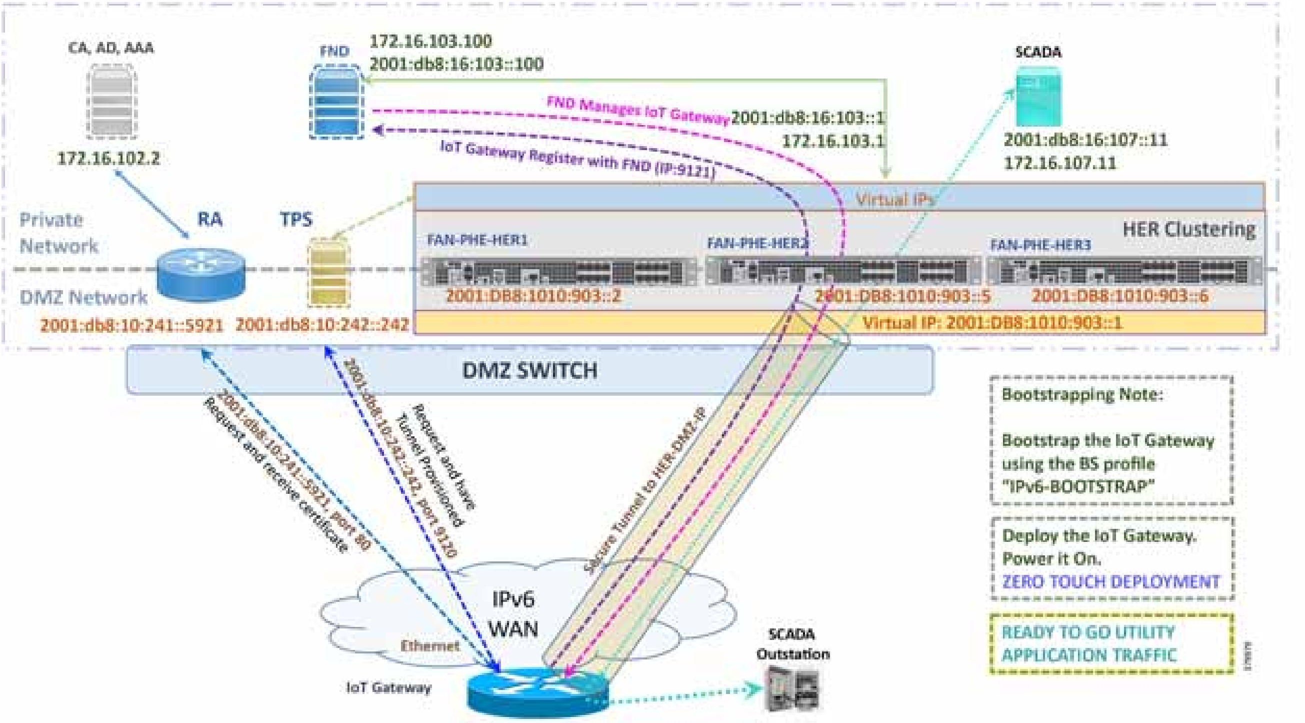
4. As an overlay routing, FND (172.16.103.100 and 2001:db8:16:103::100) and SCADA (172.16.107.11 and 2001:db8:16:107::11) routes are advertised (by HER) to the IoT Gateway through the secure FlexVPN tunnel.
5. IoT Gateway sends out a registration request to FND IPv4 address 172.16.103.100 (or) IPv6 address 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 SCADA Traffic enablement configurations to the IoT Gateway, which enables the communication between SCADA Master in the Control Center and the SCADA Outstation located in the Secondary Substation/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 name “ZTD” suggests, 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 being synchronized.

Figure 34 captures the deployment steps for the IoT Gateway over the Native IPv6 network:

Figure 34 Deployment over Native IPv6 Ethernet Network in Engineering Lab Topology



Note: This scenario has been validated with the headend located in the Engineering Lab Topology 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 Center1, 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.
7. 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 SCADA Traffic enablement configurations to the IoT Gateway, which enables the communication between SCADA Master in the Control Center and the SCADA Outstation located in the secondary substation/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 188.

Device Configuration Template Profiles

Device Configuration Template profiles, which are needed for ICT SCADA Traffic enablement, are captured in Appendix B: FND Zero Touch Deployment Profiles, page 188.

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 are 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 for successful deployment.

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

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.

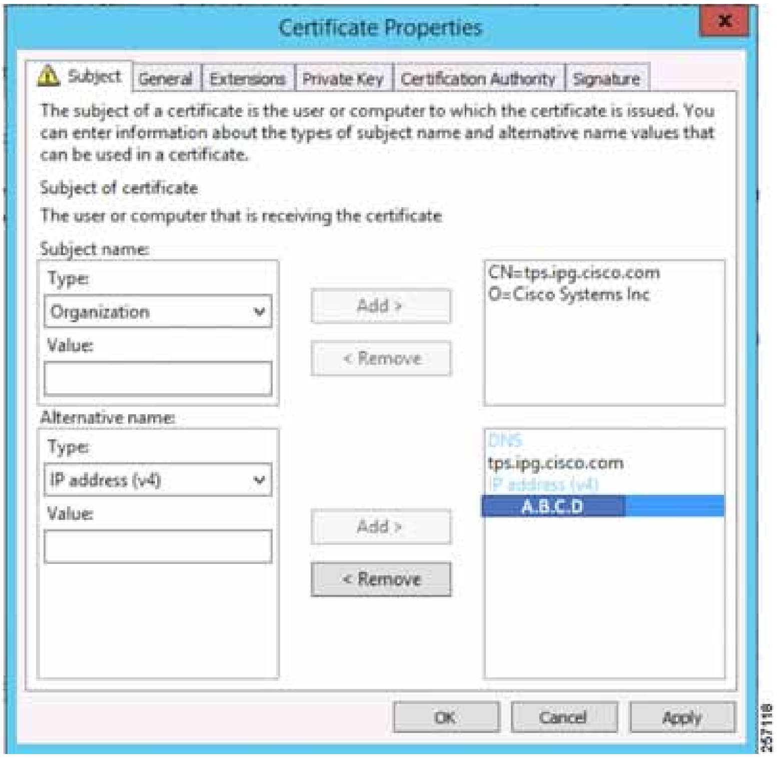
Note: For detailed instructions about certificate creation, please refer to the section “Creation of Certificate Templates and Certificates” of the *Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases Guide* at the following URL:

- 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.

Figure 35 TPS Certificate Parameters



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 certificate

The user or computer that is receiving the certificate

Subject name:

Type: Organization

Value:

CN=tps.ipg.cisco.com
O=Cisco Systems Inc

Alternative name:

Type: IP address (v4)

Value:

DNS
tps.ipg.cisco.com
IP address (v4)
A.B.C.D

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

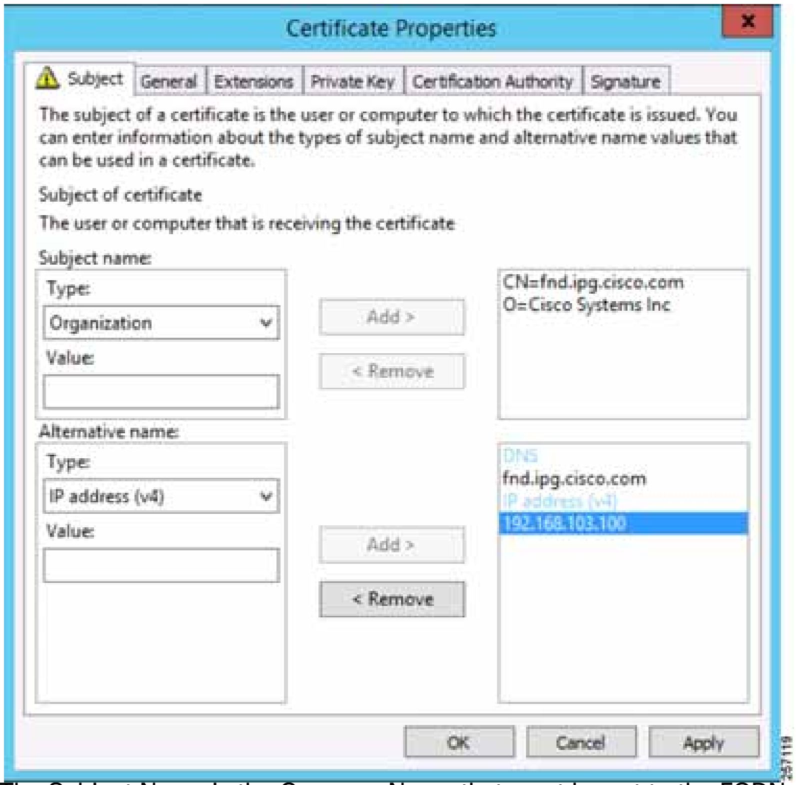
The Subject Alternative Name must be set to the FQDN - tps.ipg.cisco.com of the TPS, along with the IP address (A.B.C.D - Public reachable DMZ IP). The Subject Alternative Name is required for PnP to work. The IP address must be reachable from the IoT Gateway. TPS is located in DMZ. The IP address is 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.

Figure 36 FND Certificate Parameters



Certificate Properties

Subject | General | Extensions | Private Key | Certification Authority | Signature

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 certificate

The user or computer that is receiving the certificate

Subject name:

Type: Organization

Value:

CN=fnd.ipg.cisco.com
O=Cisco Systems Inc

Alternative name:

Type: IP address (v4)

Value:

DNS
fnd.ipg.cisco.com
IP address (v4)
192.168.103.100

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 36 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 52.

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+TrDWqh1w==

## 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:

```
Enter keystore password:

***************** WARNING WARNING WARNING *****************
*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.*
***************** WARNING WARNING WARNING *****************

Keystore type: JKS Keystore provider: SUN

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 ~]# 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.xxx # DNS2=xxx.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+TrDWqh1w==
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:
***************** WARNING WARNING WARNING *****************
*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.*
***************** WARNING WARNING WARNING *****************

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, O=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.xxx
# DNS2=xxx.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+HVhF36G0ORerMcg7N5Vh77RH18Fg/SctLRta0gBD4PdcdJeQI0R5UVQpoU3dlPtefC
Z4LAOh4gitQJ72avXzygsofG17CPk4ZDdc9cQ9jrpV2fzpzS/Wyv2ryzIkKVMUYDCr9fLBITPtWUwCuX/bylZHaH
vBnsq5ZwTC3uaSTzd2LDXvk+iRtynjLXJRcWdaRqnIGVCDp0C8l3du3fxHInJ69jjob924tIH3YjZ101D6gt4VxK
dtCA==,IPG-RSA-ROOT-
CA,HER1.ipg.cisco.com,IR1100_FCW225100DA,ipg.cisco.com,flash:/ir1101-
universalk9.16.11.01.SPA.bin
```

Table 12 Fields 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
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>	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

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 35.

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 46, elucidates the ZTD process that would begin as soon as bootstrapping using Cisco PnP Connect is complete.

IoT Gateway Validation Matrix

Table 13 captures the Bootstrapping and ZTD validation matrix across the various platform types, supported as IoT Gateways:

Table 13 IoT Gateway Validation Matrix

Platforms	IP Protocol Type (IPv4/IPv6)	Network Type (Ethernet/Cellular)	Bootstrapping over Ethernet using IP Protocol Type	Bootstrapping over Cellular	Zero Touch Deployment over Network Type and IP Protocol Type
IR1101	IPv6	Ethernet	Validated	N/A	Validated
	IPv4	Ethernet	Validated	Validated	Validated
		Cellular			Validated
IR807	IPv4	Ethernet	Validated	Validated	Validated
		Cellular			Validated
IR809	IPv4	Ethernet	Validated	Validated	Validated
IR829	IPv4	Ethernet	Validated		Validated
CGR1120	IPv4	Ethernet	Validated	Validated	Validated
CGR1240	IPv4	Ethernet	Validated		Validated

From Table 13, 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 and Cellular
- ZTD over IPv4 Ethernet/Cellular

Similarly, Platform IR807 has been validated for:

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

All other platform types have been validated for:

- Bootstrapping over IPv4 Ethernet and Cellular
- ZTD over IPv4 Ethernet network

ICT Enablement for SCADA Use Case Validation

This chapter includes the following major topics:

In order to ensure the proper functioning of substations and related equipment such as line-mounted switches and capacitors, most utilities use SCADA systems to automate monitoring and control.

New sites typically implement a SCADA system to monitor and control substations and related equipment. However, older facilities can also benefit by adding a SCADA system or by upgrading an existing SCADA system to take advantage of newer technologies.

The Distributed Automation Solution supports the SCADA service models shown in Table 14:

Table 14 SCADA Service Models

Service	Connectivity	Service Model
Legacy SCADA (DNP3, Modbus, T101)	Point-to-Point (Master Slave) Single Control Center	Raw Socket over FlexVPN
Legacy SCADA (DNP3, Modbus, T101)	P2MP Multi-drop Dual Control Center	Raw Socket over FlexVPN
SCADA Gateway (DNP3, T101) to IP Conversion (DN3-IP, T104)	Point-to-Point Multi-drop Single Control Center	Protocol Translation over FlexVPN
SCADA Gateway (DNP3, T101) to IP Conversion (DN3-IP, T104)	Multi-Master Dual Control Center	Protocol translation over FlexVPN
SCADA (DNP3-IP, Modbus-TCP, T104)	Point-to-Point (Master Slave) Single Control Center	FlexVPN - Single Control Center

SCADA Single Control Center Point-to-Point Implementation Scenarios

In this scenario, the DSO will be hosting SCADA applications (Master) in a single Control Center. The SCADA Slave is connected to the DA Gateway or SSR via the serial or Ethernet interface. The SCADA Master residing in the DSO Control Center can communicate with the Slave using the IEC 60870-5-104 or IEC 60870-5-101 protocol.

The operations that can be executed when the communication protocol is T104 or T101 or T101-T104 translation are as follows:

- Poll (Master > Slave)
- Control (Master > Slave)
- Report by Exception (Slave > Master) - Notification

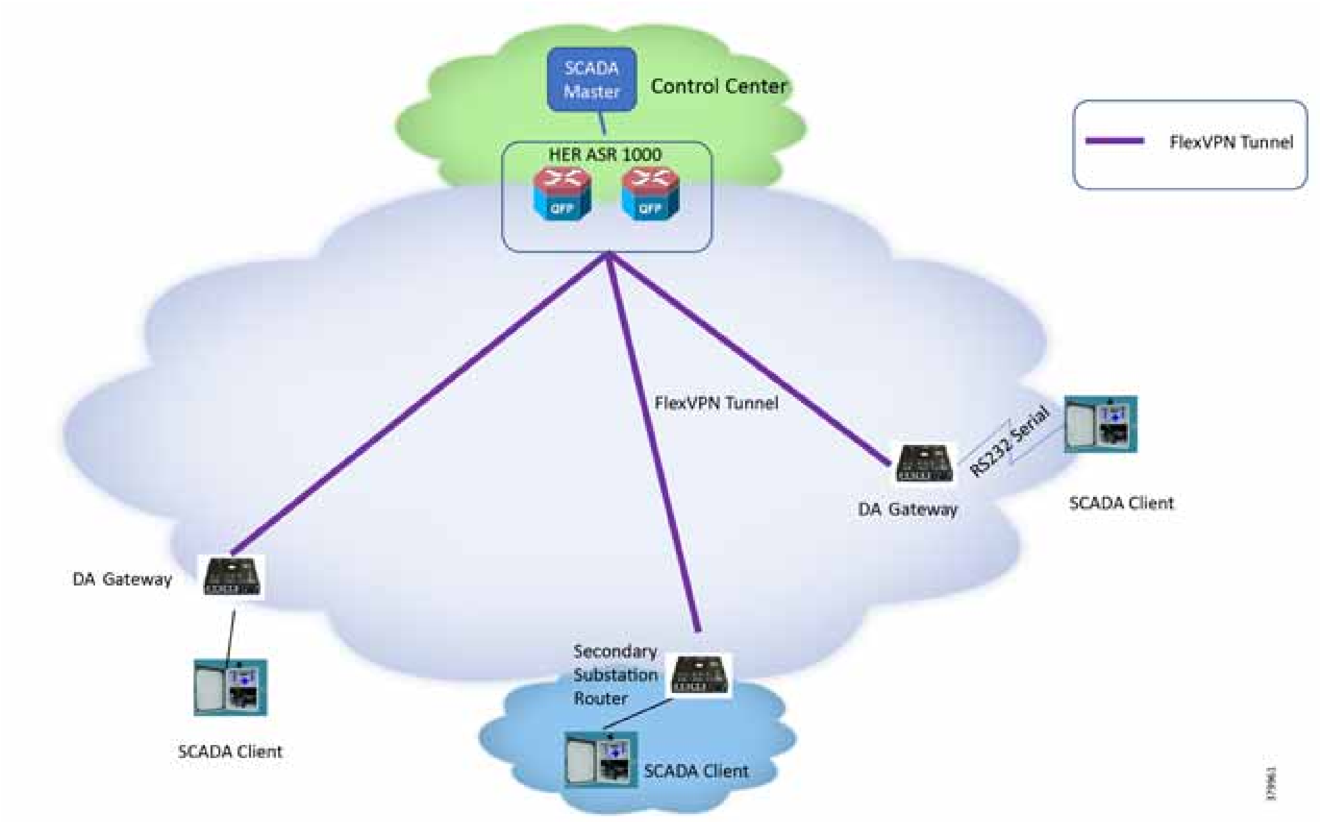
The operations have been executed using a SCADA simulator known as the Distributed Test Manager (DTM), which has the capability of simulating both the Master and the Slave devices.

If the endpoint is connected to the SSR/ 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 reused. 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 or protocol translation (T101 to T104) must happen at the gateway.

This document focuses on SCADA protocols such as T101 and T104 and the T101-T104 translation protocols widely used in the Europe Region with a single Control Center.

Figure 37 Single Control Center Topology



IR110 and IR807 are implemented as DA Gateways and SSRs. ASR 1000s implemented in clustering mode act as a HER, which terminates FlexVPN tunnels from DA Gateways and SSRs.

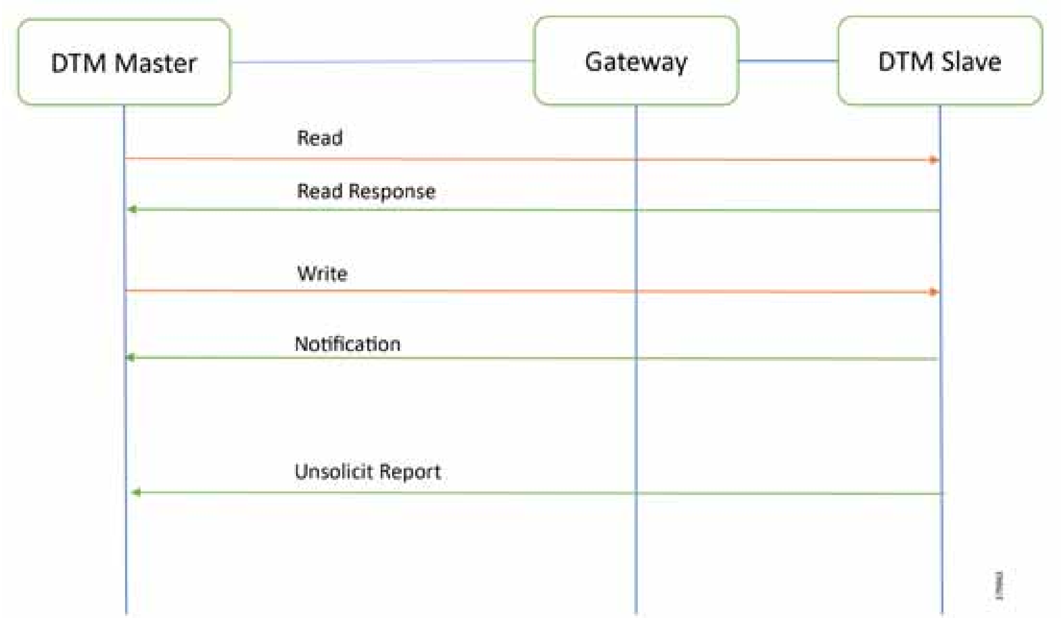
IP-Based SCADA

Protocol Validated

The protocol we have validated for this release is IEC 60870-5-104.

Flow Diagram

Figure 38 T104 Control Flow



As shown in Figure 38, the SCADA Master DTM can perform a read and write operation to a remote Slave via the DA Gateway. The Slave can send the Report by Exception to the SCADA Master via DA Gateway over the IP network.

IR807 DA Gateway Configuration

```
interface FastEthernet1
/* Interface connecting to IED SCADA Slave */ ip address 192.168.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in duplex auto
speed auto

interface Tunnel0 ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
int fastEthernet 0/0/1
/* Interface connecting to IED SCADA Slave */ switchport access vlan 1
!

interface Tunnel0 ip nat outside
!
interface Tunnel1 ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
```

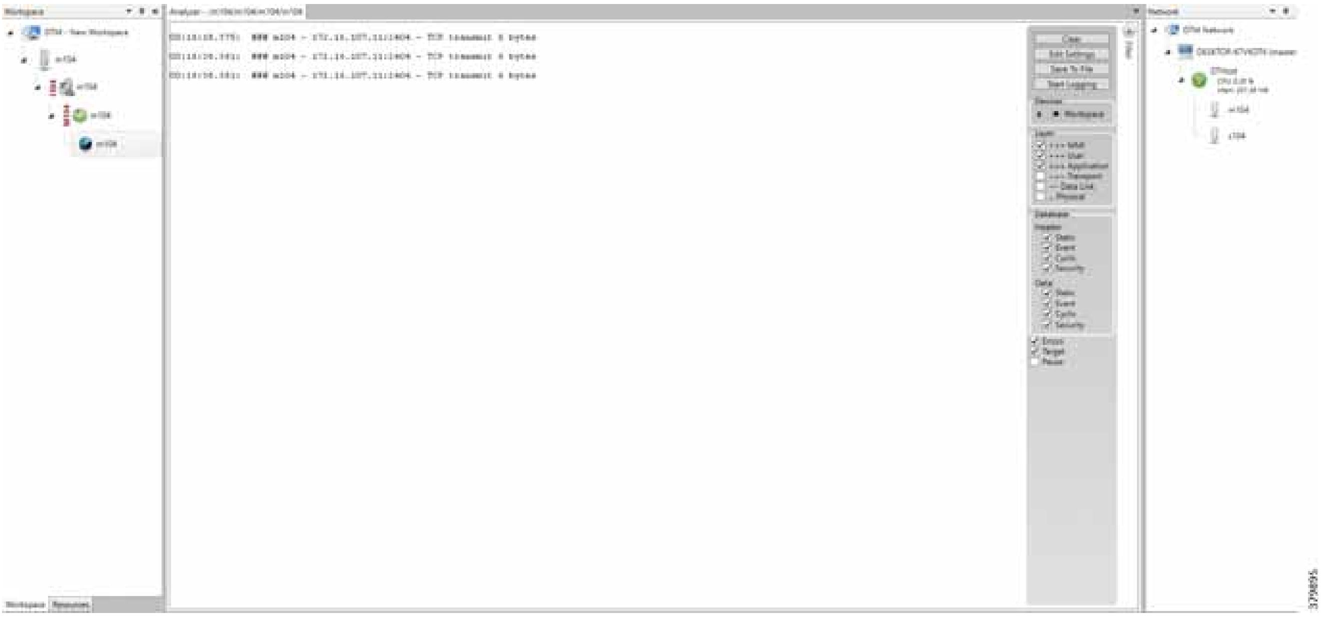
SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Report by Exception is sent to the Master from the Slave. Figure 39 and Figure 40 show the Poll operation from the SCADA Master. Similarly, Control and Report by Exception can also be seen on the Master Analyzer logs.

Poll

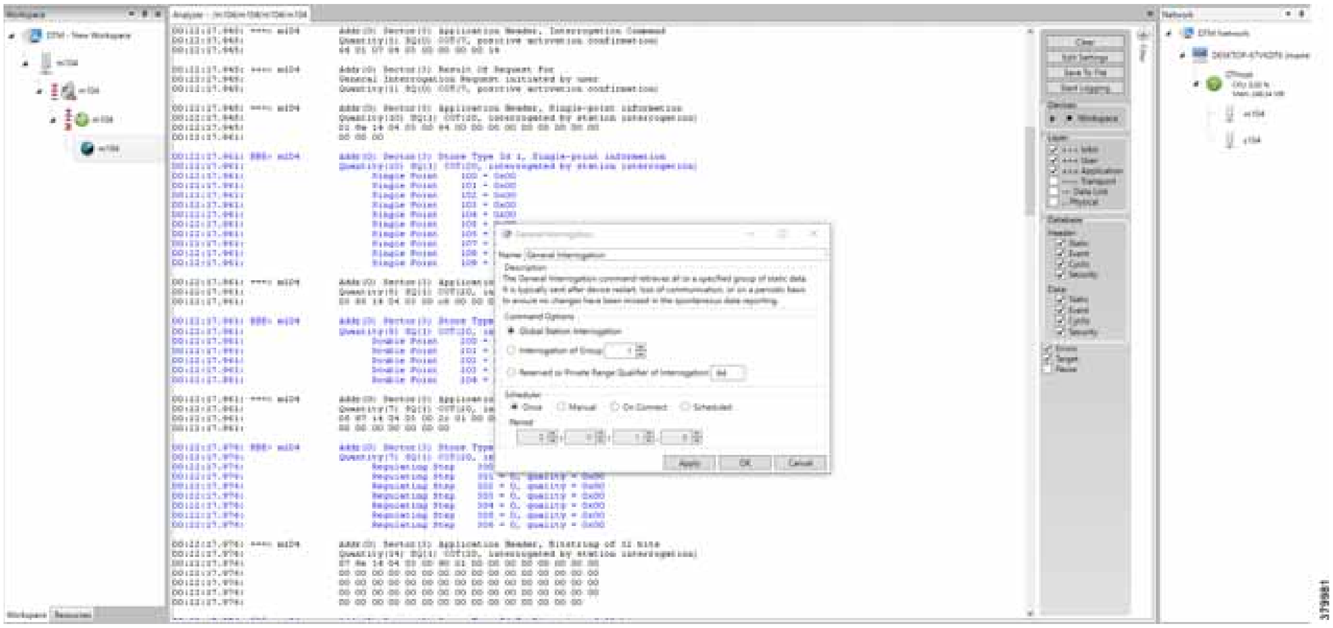
The Poll operation is performed by the Master. The Master can execute a general Poll in which all the register values are read and sent to the Master, a Poll on a set of registers or a Poll on a single register. In Figure 39 and Figure 40, we see a general Poll executed on the Slave side. Initially, the Master Analyzer is empty; however, when the *General Interrogation* command is executed, the values of all the registers are displayed on the Master Analyzer of DTM.

Figure 39 Master Analyzer Logs before Poll Operation



```
00:18:18.775:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
00:18:28.141:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
00:18:58.181:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

Figure 40 Master Analyzer Logs after Poll Operation



```
00:22:27.965: <--- m104      Addr(0) Sector(1) Application Header, Interrogation Command
00:22:27.965:                Quantity(1) SQ(0) COT(7, positive activation confirmation)
00:22:27.965:                64 01 07 04 00 00 00 00 00 14

00:22:27.965: <--- m104      Addr(0) Sector(1) Result Of Request for
00:22:27.965:                General Interrogation Request initiated by user
00:22:27.965:                Quantity(1) SQ(0) COT(7, positive activation confirmation)

00:22:27.965: <--- m104      Addr(0) Sector(1) Application Header, Single-point information
00:22:27.965:                Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:27.965:                01 8a 14 04 00 00 64 00 00 00 00 00 00 00 00 00
00:22:27.961:                00 00 00

00:22:27.961: DDD> m104      Addr(0) Sector(1) Store Type Id 1, Single-point information
00:22:27.961:                Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:27.961:                     Single Point    100 = 0x00
00:22:27.961:                     Single Point    101 = 0x00
00:22:27.961:                     Single Point    102 = 0x00
00:22:27.961:                     Single Point    103 = 0x00
00:22:27.961:                     Single Point    104 = 0x00
00:22:27.961:                     Single Point    105 =
00:22:27.961:                     Single Point    106 =
00:22:27.961:                     Single Point    107 =
00:22:27.961:                     Single Point    108 =
00:22:27.961:                     Single Point    109 =

00:22:27.961: <--- m104      Addr(0) Sector(1) Application
00:22:27.961:                Quantity(5) SQ(1) COT(20, in
00:22:27.961:                03 85 14 04 00 00 c8 00 00 0

00:22:27.961: DDD> m104      Addr(0) Sector(1) Store Type
00:22:27.961:                Quantity(5) SQ(1) COT(20, in
00:22:27.961:                     Double Point    200 =
00:22:27.961:                     Double Point    201 =
00:22:27.961:                     Double Point    202 =
00:22:27.961:                     Double Point    203 =
00:22:27.961:                     Double Point    204 =

00:22:27.961: <--- m104      Addr(0) Sector(1) Application
00:22:27.961:                Quantity(7) SQ(1) COT(20, in
00:22:27.961:                05 87 14 04 00 00 2c 01 00 0
00:22:27.961:                00 00 00 00 00 00 00

00:22:27.976: DDD> m104      Addr(0) Sector(1) Store Type
00:22:27.976:                Quantity(7) SQ(1) COT(20, in
00:22:27.976:                     Regulating Step    300
00:22:27.976:                     Regulating Step    301 = 0, quality = 0x00
00:22:27.976:                     Regulating Step    302 = 0, quality = 0x00
00:22:27.976:                     Regulating Step    303 = 0, quality = 0x00
00:22:27.976:                     Regulating Step    304 = 0, quality = 0x00
00:22:27.976:                     Regulating Step    305 = 0, quality = 0x00
00:22:27.976:                     Regulating Step    306 = 0, quality = 0x00

00:22:27.976: <--- m104      Addr(0) Sector(1) Application Header, Bitstring of 32 bits
00:22:27.976:                Quantity(14) SQ(1) COT(20, interrogated by station interrogation)
00:22:27.976:                07 8e 14 04 00 00 90 01 00 00 00 00 00 00 00 00
00:22:27.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:27.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:27.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:27.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

General Interrogation

Name: General Interrogation

Description

The General Interrogation command retrieves all or a specified group of static data. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure no changes have been missed in the spontaneous data reporting.

Command Options

● Global Station Interrogation

○ Interrogation of Group 1

○ Reserved or Private Range Qualifier of Interrogation 84

Schedule

● Once ○ Manual ○ On Connect ○ Scheduled

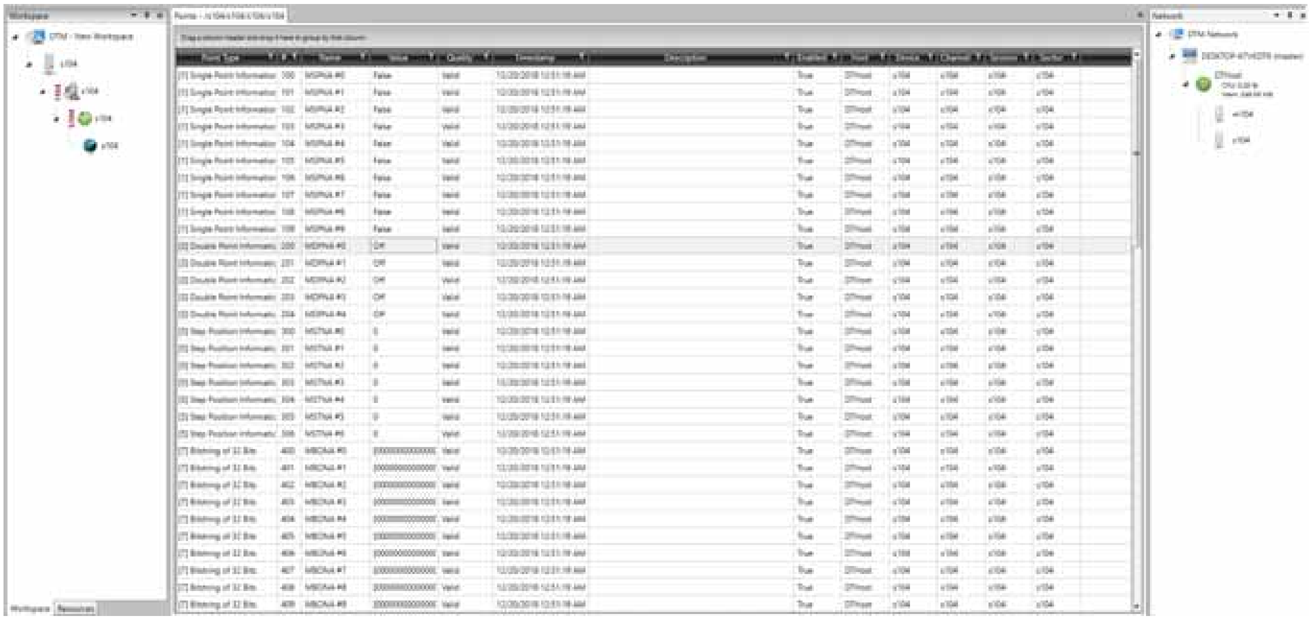
Period 1 : 0 : 1 : 0

Apply OK Cancel

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 Double Point Register (#200) is changed and the same is reported to the Master. Figure 41, Figure 42, and Figure 43 show the Report by Exception sent to the Master for a particular register:

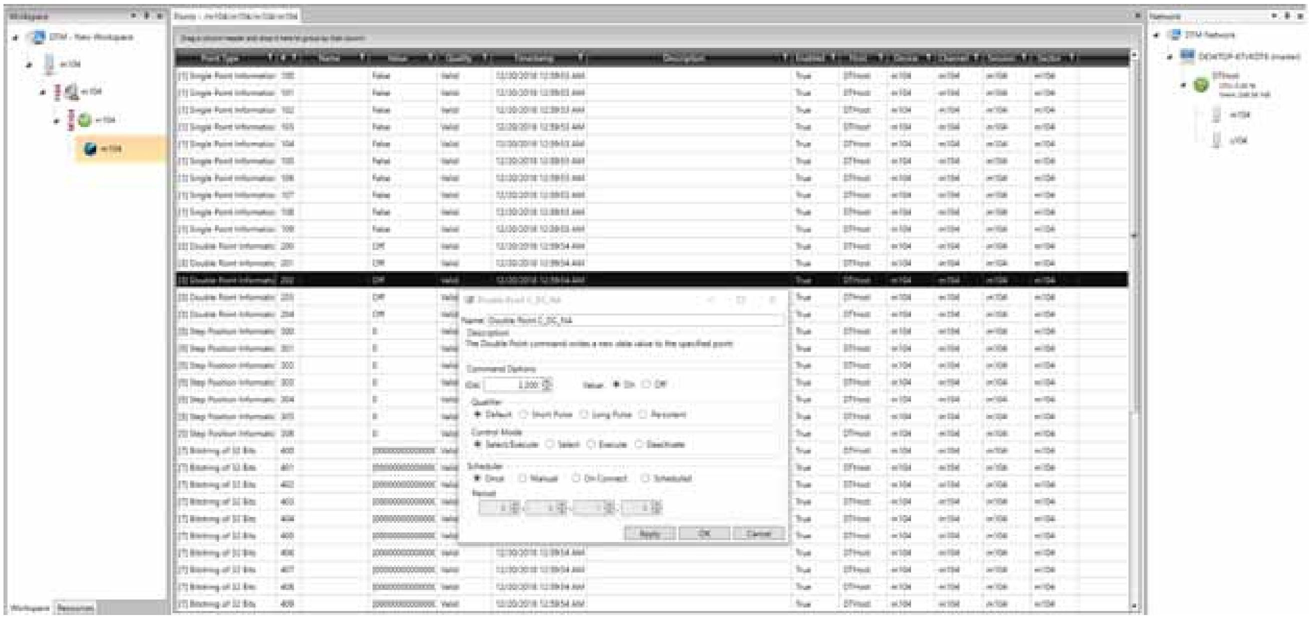
Figure 41 Slave Register before Control Operation



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

Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	M_SP_NA #0	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	101	M_SP_NA #1	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	102	M_SP_NA #2	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	103	M_SP_NA #3	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	104	M_SP_NA #4	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	105	M_SP_NA #5	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	106	M_SP_NA #6	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	107	M_SP_NA #7	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	108	M_SP_NA #8	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	109	M_SP_NA #9	False	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	200	M_DP_NA #0	Off	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	201	M_DP_NA #1	Off	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	202	M_DP_NA #2	Off	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	203	M_DP_NA #3	Off	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	204	M_DP_NA #4	Off	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	300	M_ST_NA #0	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	301	M_ST_NA #1	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	302	M_ST_NA #2	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	303	M_ST_NA #3	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	304	M_ST_NA #4	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	305	M_ST_NA #5	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	306	M_ST_NA #6	0	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	M_BO_NA #0	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	M_BO_NA #1	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	M_BO_NA #2	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	M_BO_NA #3	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	M_BO_NA #4	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	M_BO_NA #5	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	M_BO_NA #6	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	M_BO_NA #7	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	M_BO_NA #8	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	M_BO_NA #9	[0000000000000000	Valid	12/20/2018 12:51:19 AM		True	DTHost	s104	s104	s104	s104

Figure 42 Master Control Control Operation



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

Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	101		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	102		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	103		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	104		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	105		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	106		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	107		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	108		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	109		False	Valid	12/20/2018 12:39:53 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	200		Off	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	201		Off	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	202		Off	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	203		Off	Valid			True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	204		Off	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	300		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	301		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	302		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	303		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	304		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	305		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	306		0	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	400		[0000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	401		[0000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	402		[0000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	403		[0000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	404		[0000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	405		[0000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	406		[0000000000000000	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	407		[0000000000000000	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	408		[0000000000000000	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	409		[0000000000000000	Valid	12/20/2018 12:39:54 AM		True	DTHost	m104	m104	m104	m104

Double Point C_DC_NA

Name: Double Point C_DC_NA

Description

The Double Point command writes a new state value to the specified point.

Command Options

IOA: 1,200 Value: ● On ○ Off

Qualifier

● Default ○ Short Pulse ○ Long Pulse ○ Persistent

Control Mode

● Select/Execute ○ Select ○ Execute ○ Deactivate

Scheduler

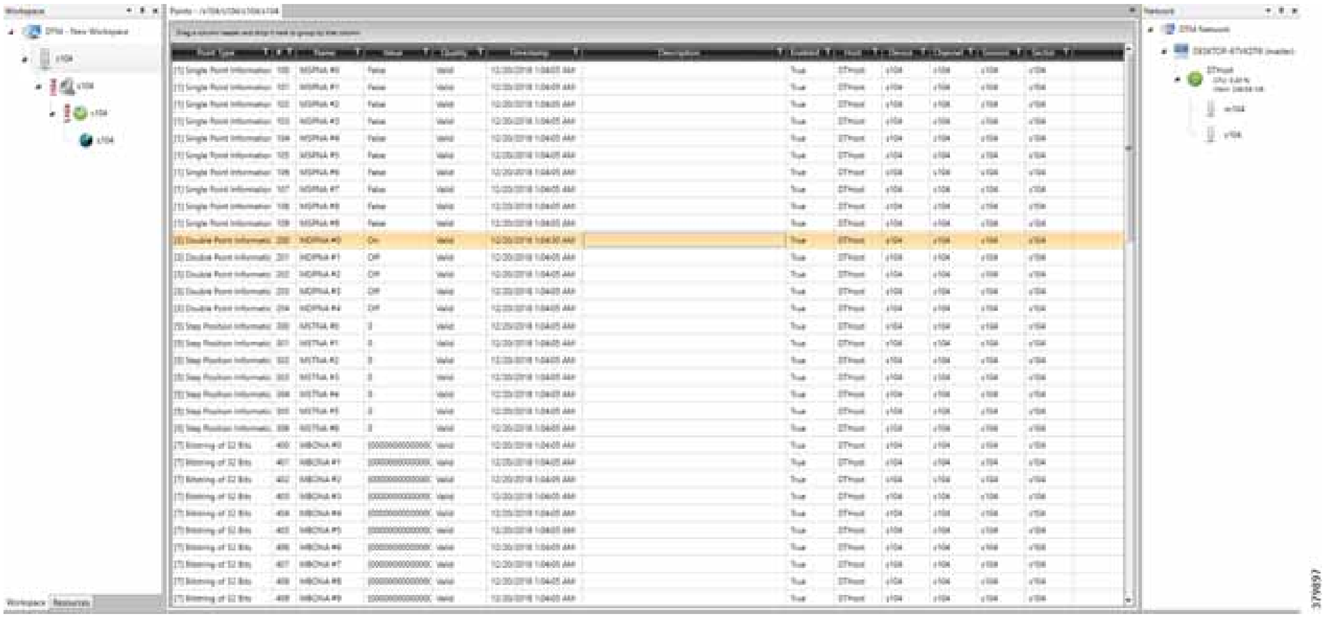
● Once ○ Manual ○ On Connect ○ Scheduled

Period

0 0 0 0

Apply OK Cancel

Figure 43 Slave Register after Control Operation

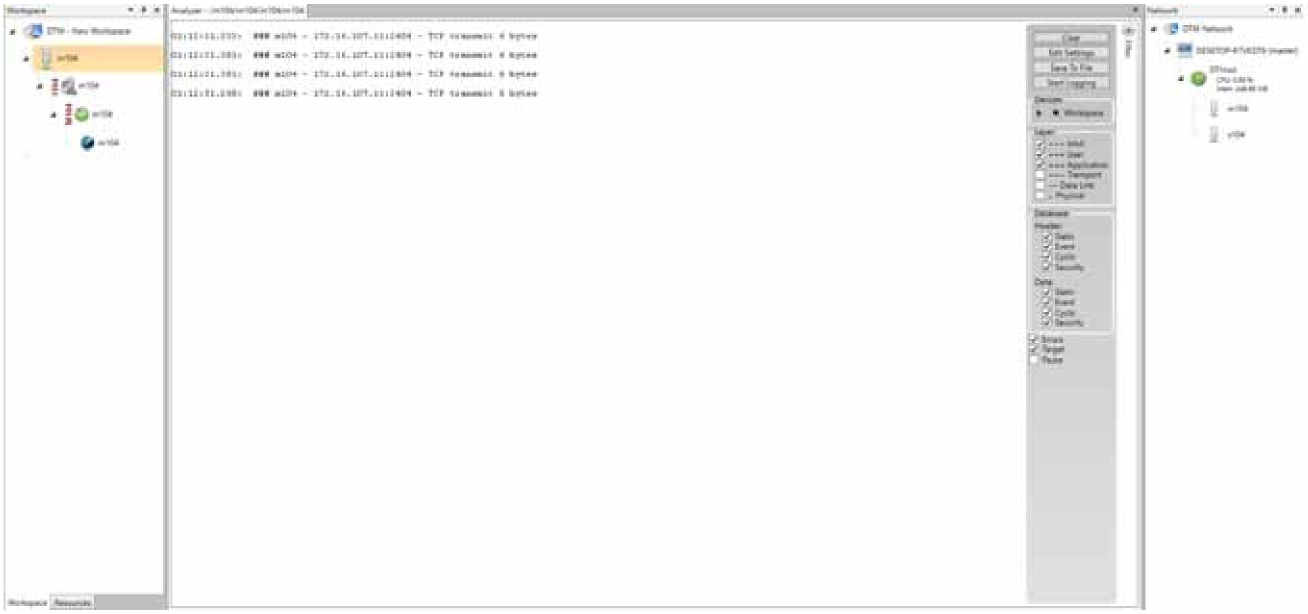

Workspace
DTM - New Workspace
s104
s104
s104
s104
Points - /s104/s104/s104/s104
Drag a column header and drop it here to group by that column
Network
DTM Network
DESKTOP-[illegible] (master)
DTHost
s104
s104
Workspace
Resources
379897

Point Type		Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	MSPNA #0	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	101	MSPNA #1	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	102	MSPNA #2	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	103	MSPNA #3	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	104	MSPNA #4	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	105	MSPNA #5	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	106	MSPNA #6	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	107	MSPNA #7	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	108	MSPNA #8	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	109	MSPNA #9	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	On	Valid	12/20/2018 1:04:30 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104

Report by Exception

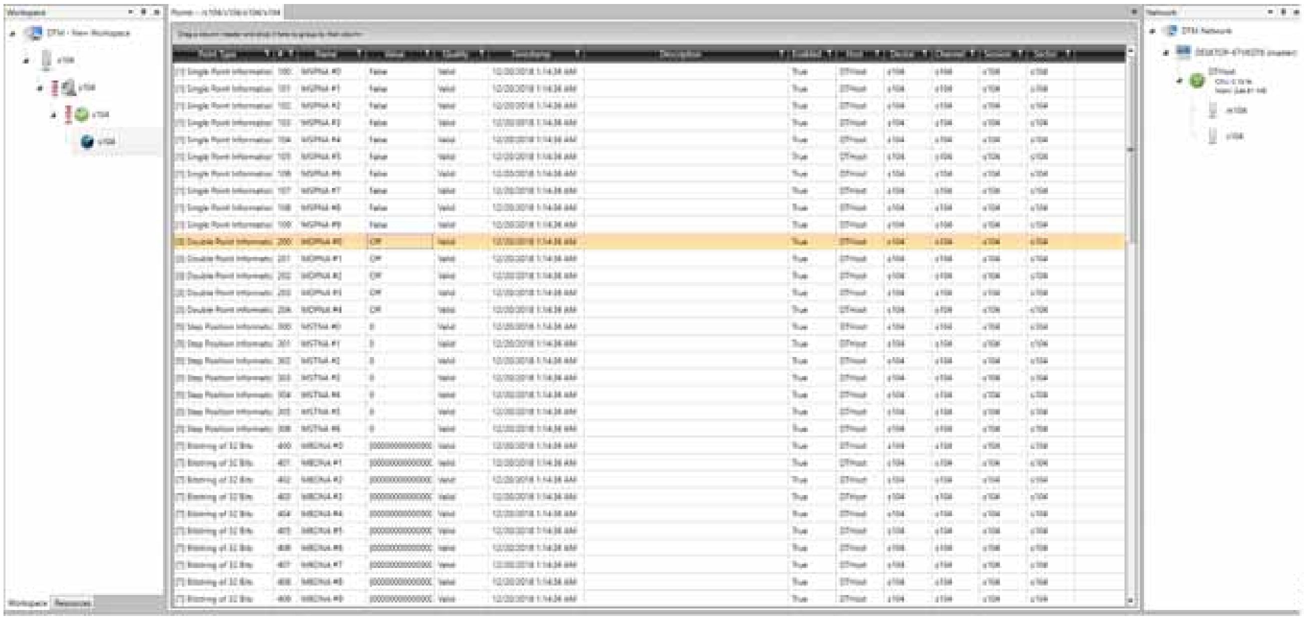
Report by Exception is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register changes are reported to the SCADA Master. This notification can be seen on the Master Analyzer of DTM software. Figure 44, Figure 45, Figure 46, and Figure 47 show the Report by Exception on the analyzer. The other operations such as Poll and Control can be executed, and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to the Master. Figure 44, Figure 45, Figure 46, and Figure 47 how the Report by Exception sent to the Master for a particular register:

Figure 44 Master Analyzer



```
01:13:11.333:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:13:21.383:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:13:21.393:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:13:21.398:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

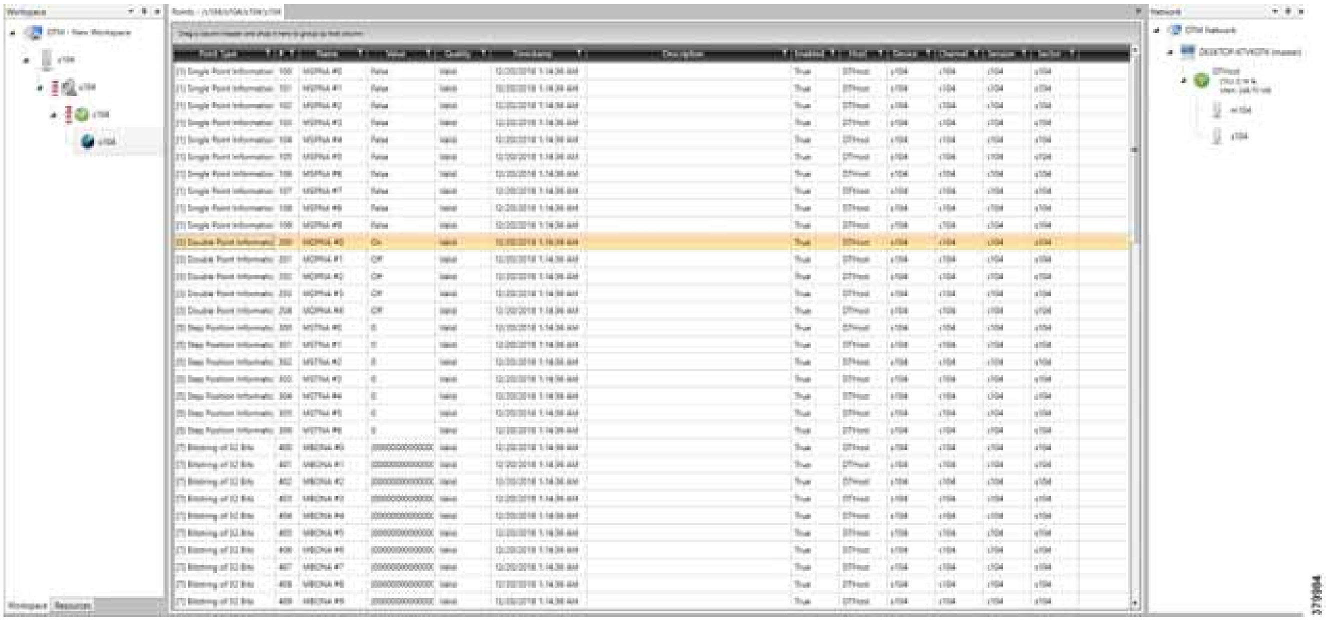
Figure 45 Slave Registers



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

Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	[0000000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104

Figure 46 Change in Slave Register Value



Point Type		Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	MSPNA #0	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	101	MSPNA #1	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	102	MSPNA #2	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	103	MSPNA #3	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	104	MSPNA #4	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	105	MSPNA #5	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	106	MSPNA #6	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	107	MSPNA #7	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	108	MSPNA #8	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	109	MSPNA #9	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	On	Valid	12/20/2018 1:19:39 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104

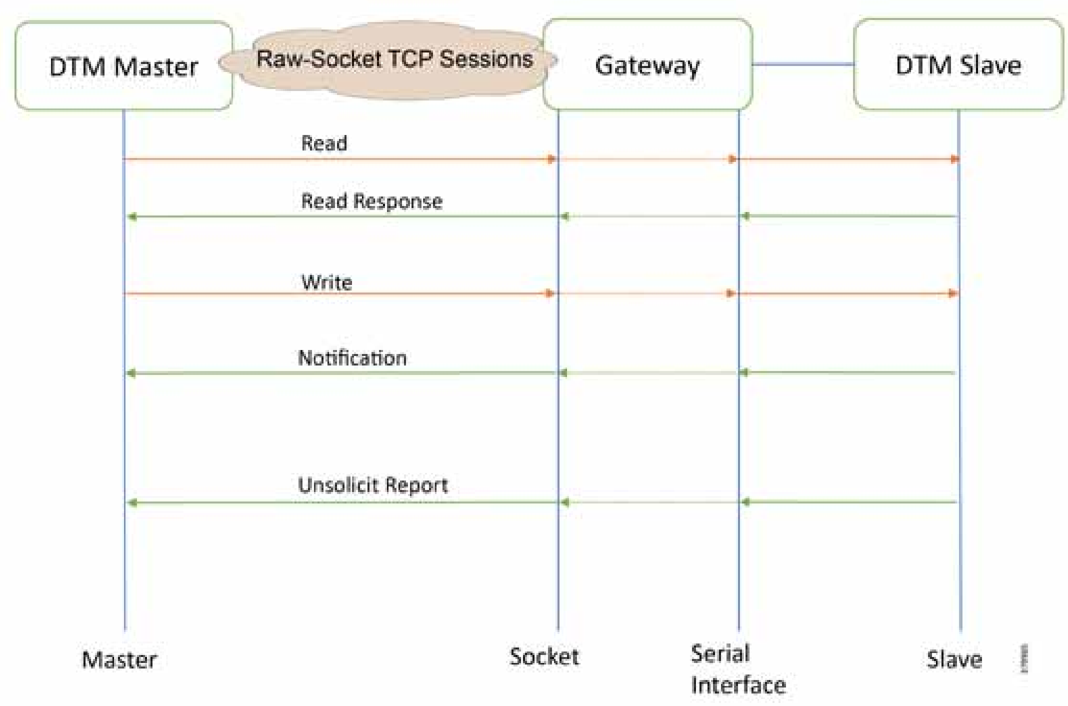
Legacy SCADA (Raw-Socket TCP)

Protocol Validated

The protocol we have validated for this release is IEC 60870-5-101.

Flow Diagram

Figure 47 T101 Control Flow



As shown in Figure 47, the DTM Master can read and write the Slave via the DA Gateway using TCP Raw Socket. And the Slave can send the Report by Exception to the Master via the DA Gateway using TCP Raw-Socket. For more details about Raw Socket, refer to the *Distribution Automation - Secondary Substation Design Guide.*

IR807 DA Gateway Raw Socket Configuration

```
interface Async1
    no ip address
    /*TCP Raw socket implementation*/ encapsulation raw-tcp
!
line 4
    raw-socket tcp client 172.16.107.11 25000
    databits 8
    stopbits 1
    speed 9600 parity none
!
```

IR1101 DA Gateway Raw Socket Configuration

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

SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Report by Exception is sent to the Master from the Slave. Figure 48 and Figure 49 show the Poll operation from the SCADA-Master. Similarly, Control and Report by Exception 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, a Poll on a set of registers or a Poll on a single register. In Figure 48 and Figure 49, we see a general Poll executed on the Slave side. Initially, the Master Analyzer is empty; however, when the *General Interrogation* command is executed, the values of all the registers are displayed on the Master Analyzer of DTM.

Figure 48 Master Analyzer Logs before Poll Operation

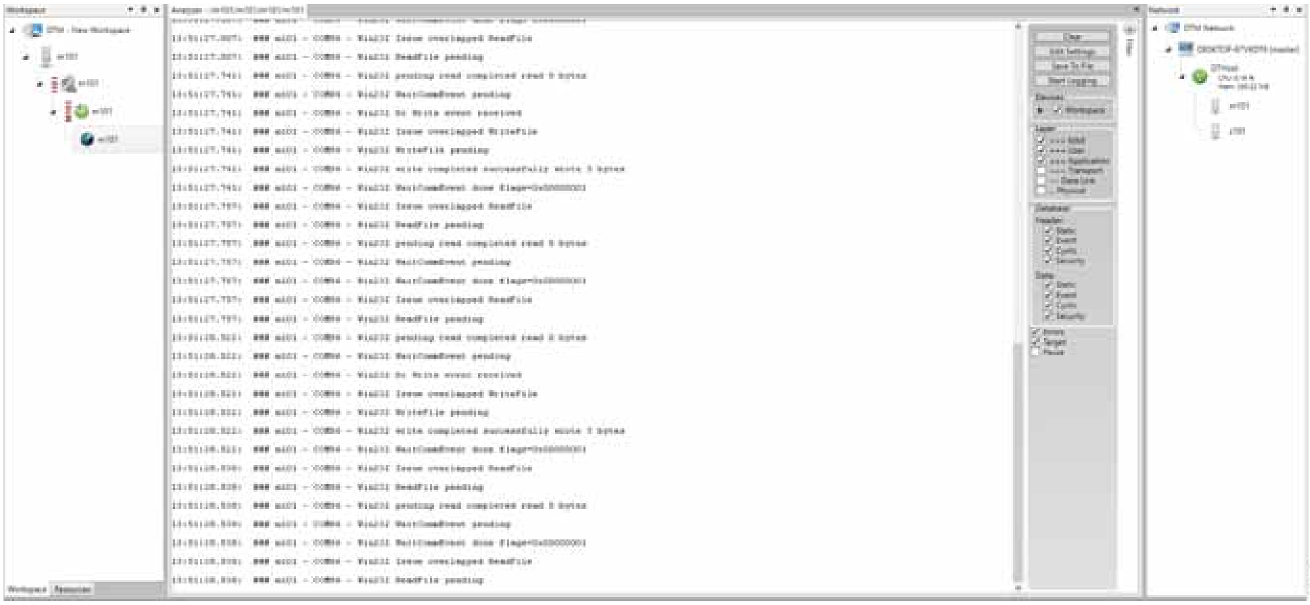
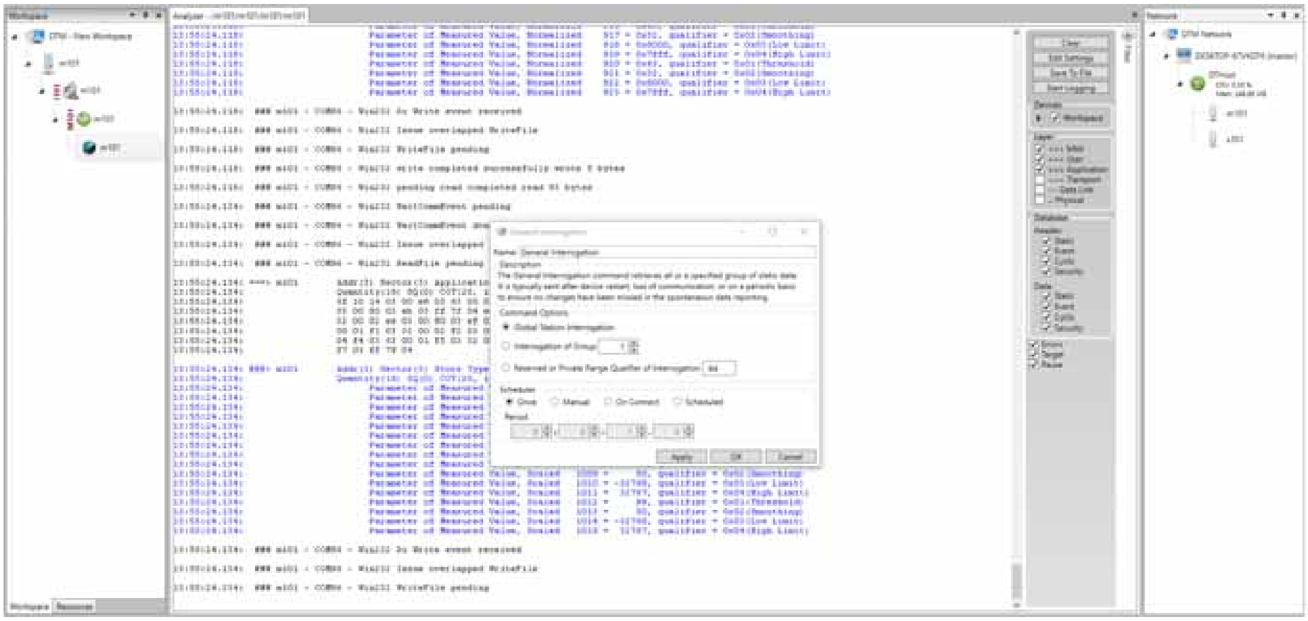


Figure 49 Master Analyzer Logs after Poll Operation



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 Double Point Register (#200) is changed and the same is reported to the Master. Figure 50, Figure 51, and Figure 52 show the Report by Exception sent to the Master for a particular register:

Figure 50 Slave Register before Control Operation

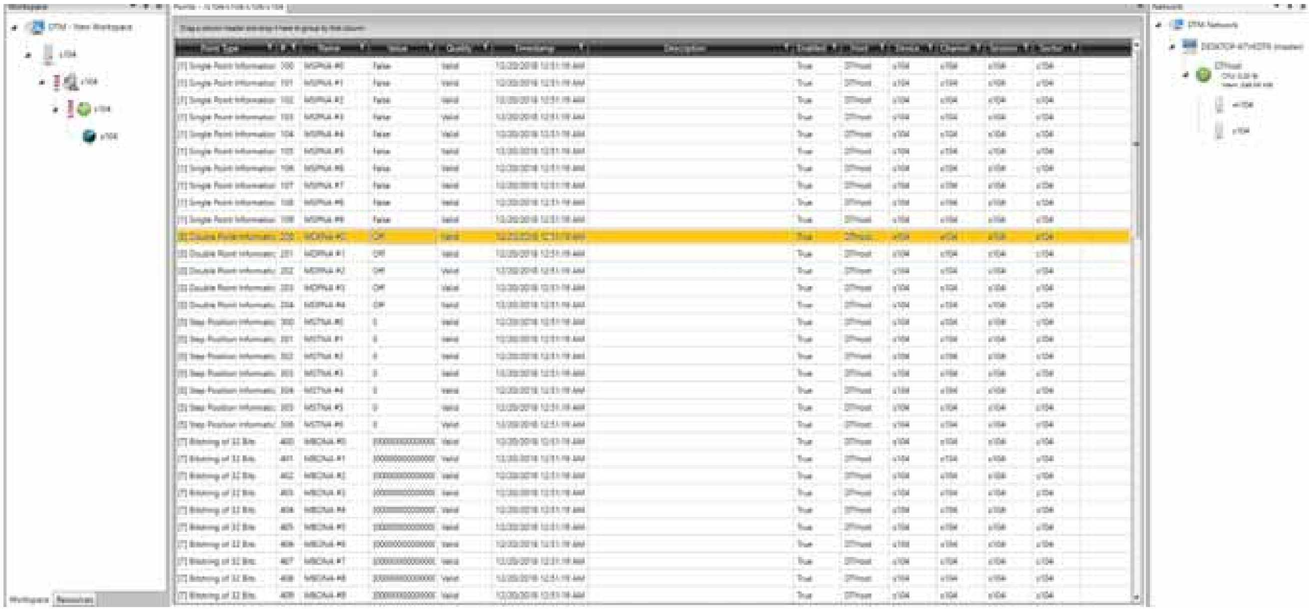
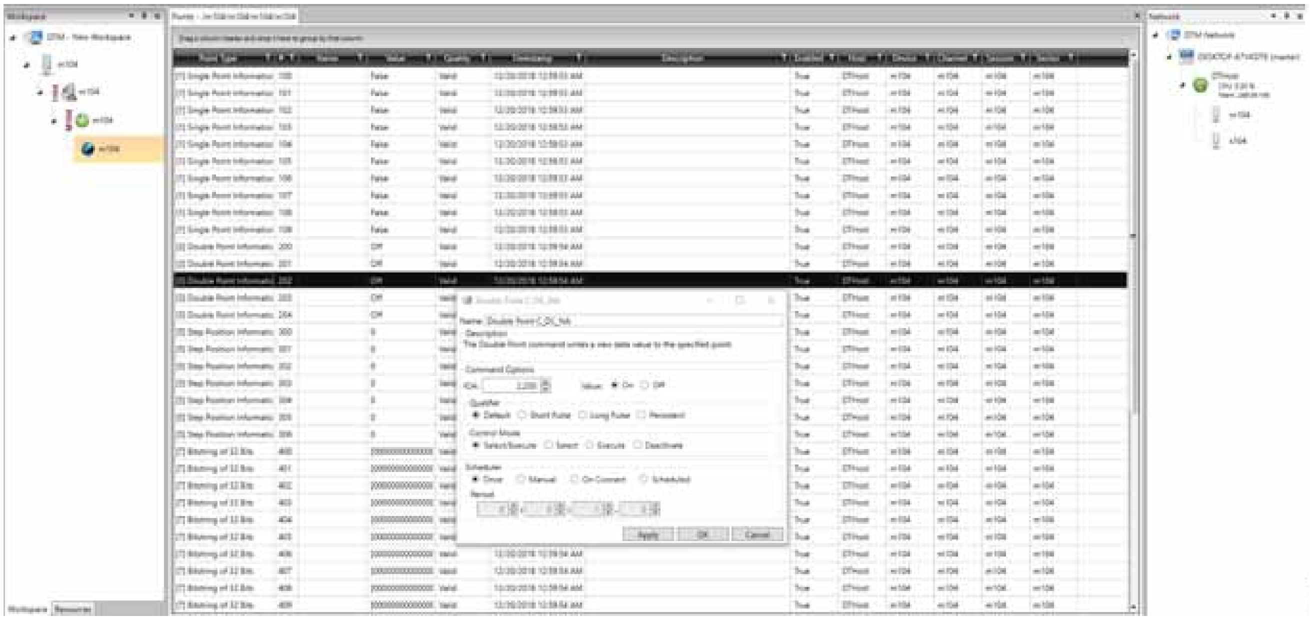


Figure 51 Master Control Control Operation



Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	101		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	102		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	103		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	104		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	105		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	106		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	107		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	108		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Informatio	109		False	Valid	12/20/2018 12:59:03 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	200		Off	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	201		Off	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	202		Off	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	203		Off	Valid			True	DTHost	m104	m104	m104	m104
[3] Double Point Informatic	204		Off	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	300		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	301		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	302		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	303		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	304		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	305		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatic	306		0	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	400		{000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	401		{000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	402		{000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	403		{000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	404		{000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	405		{000000000000000	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	406		{000000000000000	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	407		{000000000000000	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	408		{000000000000000	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	409		{000000000000000	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104

Double Point C_DC_NA

Name: Double Point C_DC_NA

Description

The Double Point command writes a new state value to the specified point.

Command Options

IOA: 2,200 Value: ● On ○ Off

Qualifier

● Default ○ Short Pulse ○ Long Pulse ○ Persistent

Control Mode

● Select/Execute ○ Select ○ Execute ○ Deactivate

Scheduler

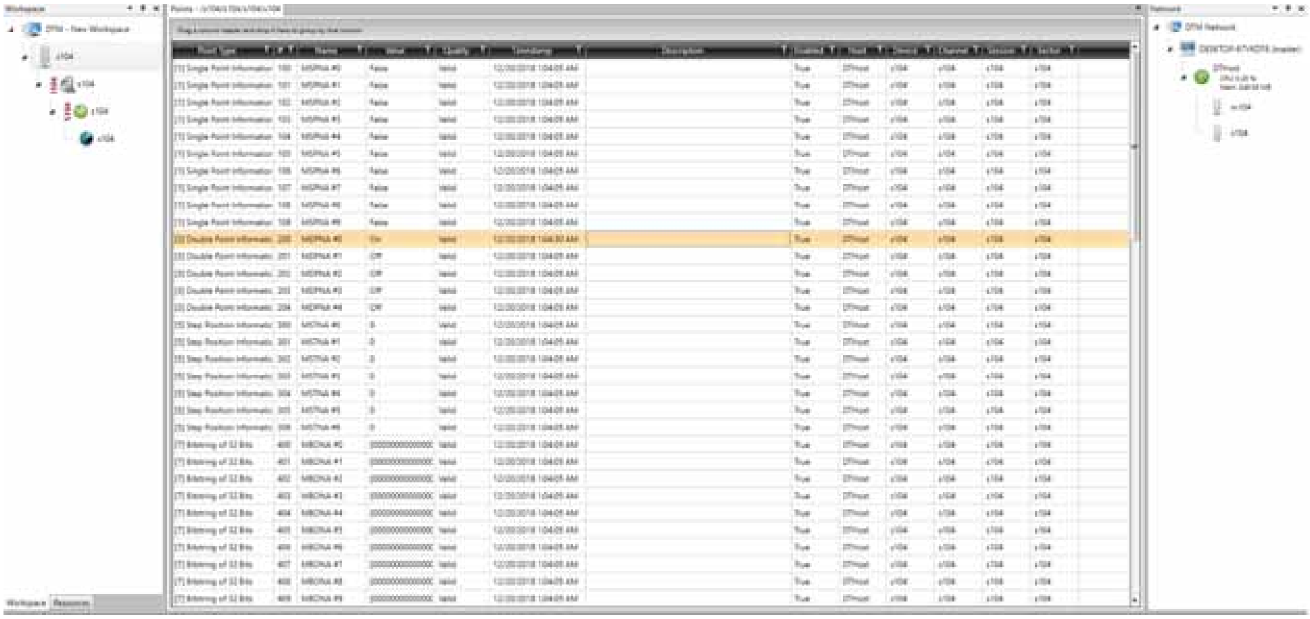
● Once ○ Manual ○ On Connect ○ Scheduled

Period

0 : 0 : 0 . 0

Apply OK Cancel

Figure 52 Slave Register after Control Operation

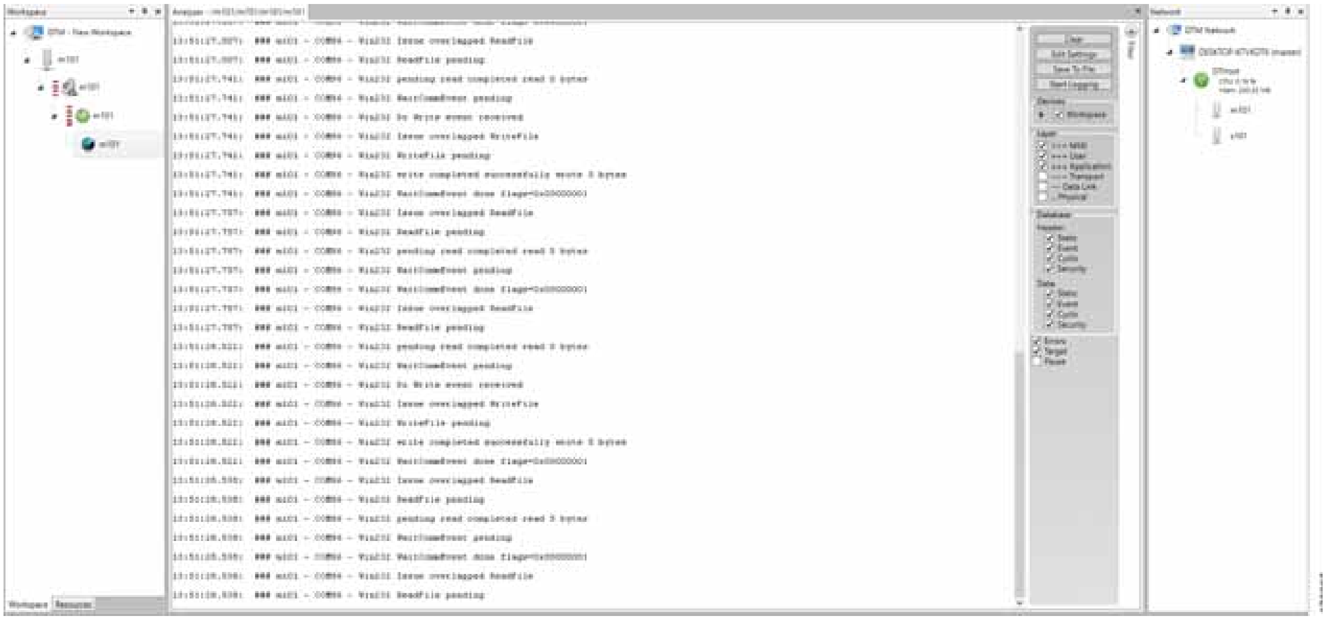


Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	M_SP_NA #0	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	M_SP_NA #1	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	M_SP_NA #2	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	M_SP_NA #3	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	M_SP_NA #4	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	M_SP_NA #5	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	M_SP_NA #6	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	M_SP_NA #7	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	M_SP_NA #8	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	M_SP_NA #9	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	200	M_DP_NA #0	On	Valid	12/20/2018 1:04:30 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	201	M_DP_NA #1	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	202	M_DP_NA #2	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	203	M_DP_NA #3	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	204	M_DP_NA #4	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	300	M_ST_NA #0	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	301	M_ST_NA #1	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	302	M_ST_NA #2	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	303	M_ST_NA #3	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	304	M_ST_NA #4	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	305	M_ST_NA #5	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	306	M_ST_NA #6	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	M_BO_NA #0	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	M_BO_NA #1	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	M_BO_NA #2	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	M_BO_NA #3	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	M_BO_NA #4	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	M_BO_NA #5	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	M_BO_NA #6	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	M_BO_NA #7	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	M_BO_NA #8	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	M_BO_NA #9	{00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104

Report by Exception

Report by Exception is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register changes are reported to SCADA-Master. This notification can be seen on the Master Analyzer of DTM software. Figure 53, Figure 54, Figure 55, and Figure 56 show the Report by Exception on the analyzer. The other operations such as Poll and Control can be executed, and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to the Master. Figure 53, Figure 54, Figure 55, and Figure 56 show the Report by Exception sent to the Master for a particular register:

Figure 53 Master Analyzer



```
13:51:27.727: ### m101 - COM56 - Win32 Issue overlapped ReadFile
13:51:27.727: ### m101 - COM56 - Win32 ReadFile pending
13:51:27.741: ### m101 - COM56 - Win32 pending read completed read 3 bytes
13:51:27.741: ### m101 - COM56 - Win32 WaitCommEvent pending
13:51:27.741: ### m101 - COM56 - Win32 Rx Write event received
13:51:27.741: ### m101 - COM56 - Win32 Issue overlapped WriteFile
13:51:27.741: ### m101 - COM56 - Win32 WriteFile pending
13:51:27.741: ### m101 - COM56 - Win32 write completed successfully wrote 3 bytes
13:51:27.741: ### m101 - COM56 - Win32 WaitCommEvent done flags=0x00000001
13:51:27.757: ### m101 - COM56 - Win32 Issue overlapped ReadFile
13:51:27.757: ### m101 - COM56 - Win32 ReadFile pending
13:51:27.757: ### m101 - COM56 - Win32 pending read completed read 3 bytes
13:51:27.757: ### m101 - COM56 - Win32 WaitCommEvent pending
13:51:27.757: ### m101 - COM56 - Win32 WaitCommEvent done flags=0x00000001
13:51:27.757: ### m101 - COM56 - Win32 Issue overlapped ReadFile
13:51:27.757: ### m101 - COM56 - Win32 ReadFile pending
13:51:28.522: ### m101 - COM56 - Win32 pending read completed read 3 bytes
13:51:28.522: ### m101 - COM56 - Win32 WaitCommEvent pending
13:51:28.522: ### m101 - COM56 - Win32 Rx Write event received
13:51:28.522: ### m101 - COM56 - Win32 Issue overlapped WriteFile
13:51:28.522: ### m101 - COM56 - Win32 WriteFile pending
13:51:28.522: ### m101 - COM56 - Win32 write completed successfully wrote 3 bytes
13:51:28.522: ### m101 - COM56 - Win32 WaitCommEvent done flags=0x00000001
13:51:28.538: ### m101 - COM56 - Win32 Issue overlapped ReadFile
13:51:28.538: ### m101 - COM56 - Win32 ReadFile pending
13:51:28.538: ### m101 - COM56 - Win32 pending read completed read 3 bytes
13:51:28.538: ### m101 - COM56 - Win32 WaitCommEvent pending
13:51:28.538: ### m101 - COM56 - Win32 WaitCommEvent done flags=0x00000001
13:51:28.538: ### m101 - COM56 - Win32 Issue overlapped ReadFile
13:51:28.538: ### m101 - COM56 - Win32 ReadFile pending
```

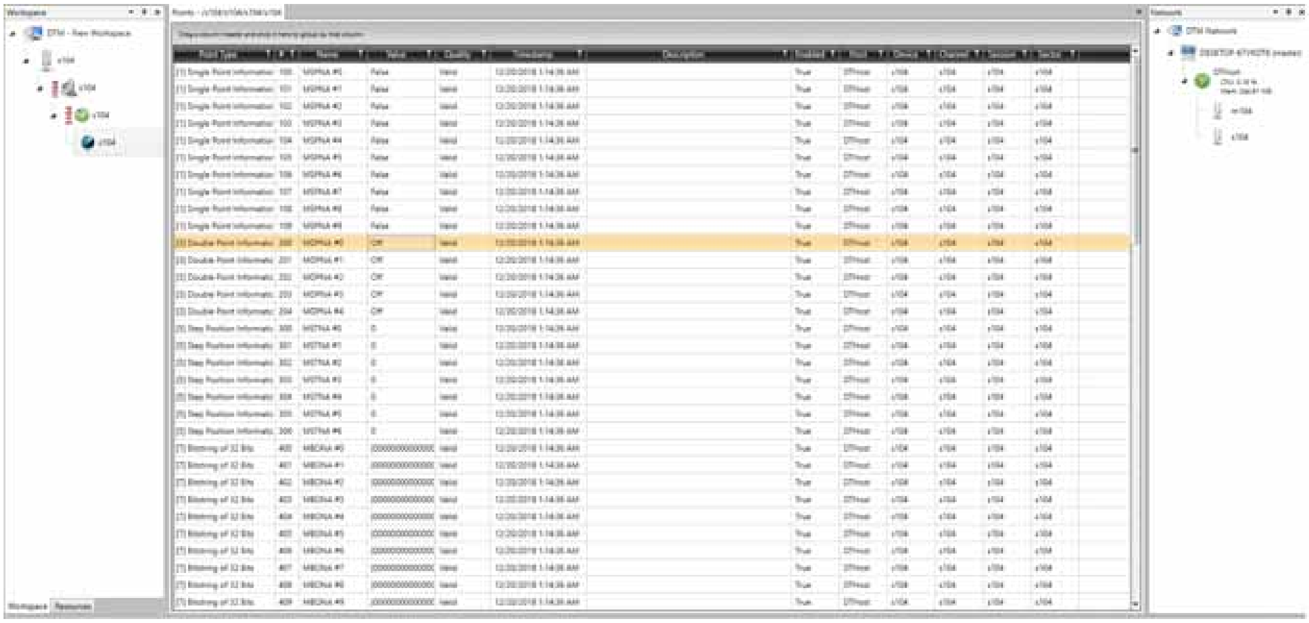
Clear
Edit Settings
Save To File
Start Logging

Layer
☑ MMI
☑ User
☑ Application
□ Transport
□ Data Link
□ Physical

Database
Header
☑ Static
☑ Event
☑ Cyclic
☑ Security
Data
☑ Static
☑ Event
☑ Cyclic
☑ Security

☑ Errors
☑ Target
□ Pause

Figure 54 Slave Registers



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

Point Type	Id	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	MSPNA #0	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	101	MSPNA #1	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	102	MSPNA #2	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	103	MSPNA #3	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	104	MSPNA #4	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	105	MSPNA #5	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	106	MSPNA #6	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	107	MSPNA #7	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	108	MSPNA #8	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[1] Single Point Informatio	109	MSPNA #9	False	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[3] Double Point Informatic	200	MDPNA #0	Off	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[3] Double Point Informatic	201	MDPNA #1	Off	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[3] Double Point Informatic	202	MDPNA #2	Off	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[3] Double Point Informatic	203	MDPNA #3	Off	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[3] Double Point Informatic	204	MDPNA #4	Off	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	300	MSTNA #0	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	301	MSTNA #1	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	302	MSTNA #2	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	303	MSTNA #3	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	304	MSTNA #4	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	305	MSTNA #5	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[5] Step Position Informatic	306	MSTNA #6	0	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	000000000000000	Valid	12/20/2018 1:14:36 AM		True	DTMroot	s104	s104	s104	s104

Figure 55 Change in Slave Register Value

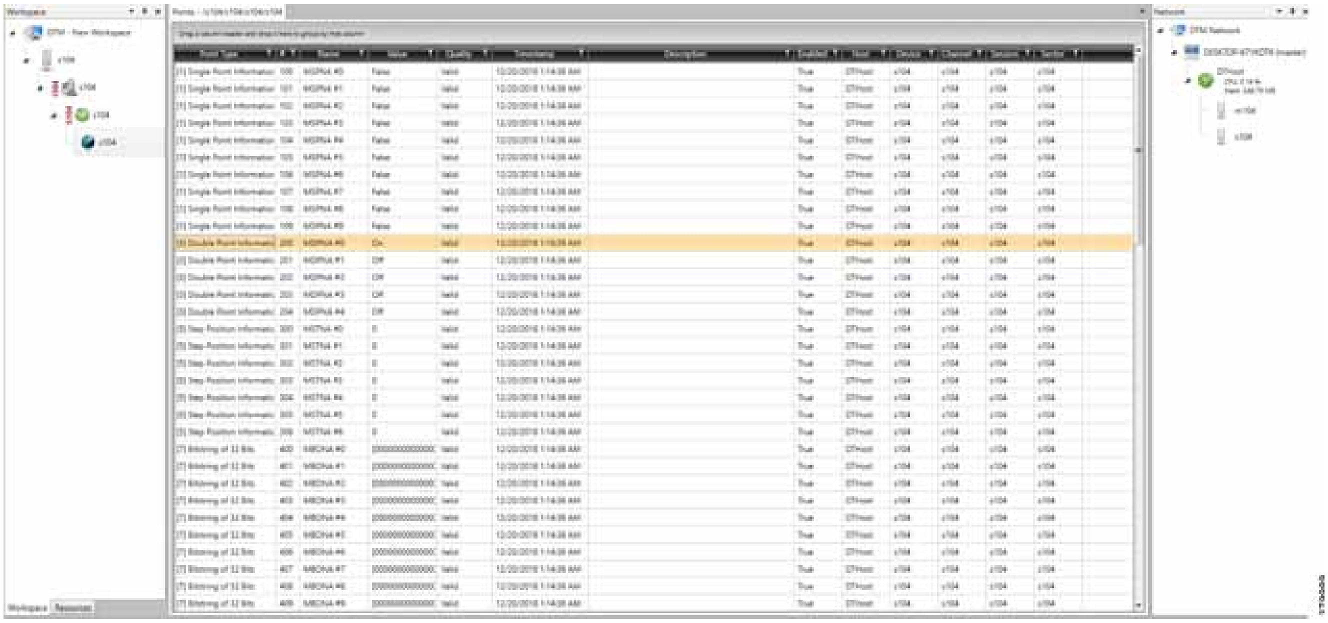
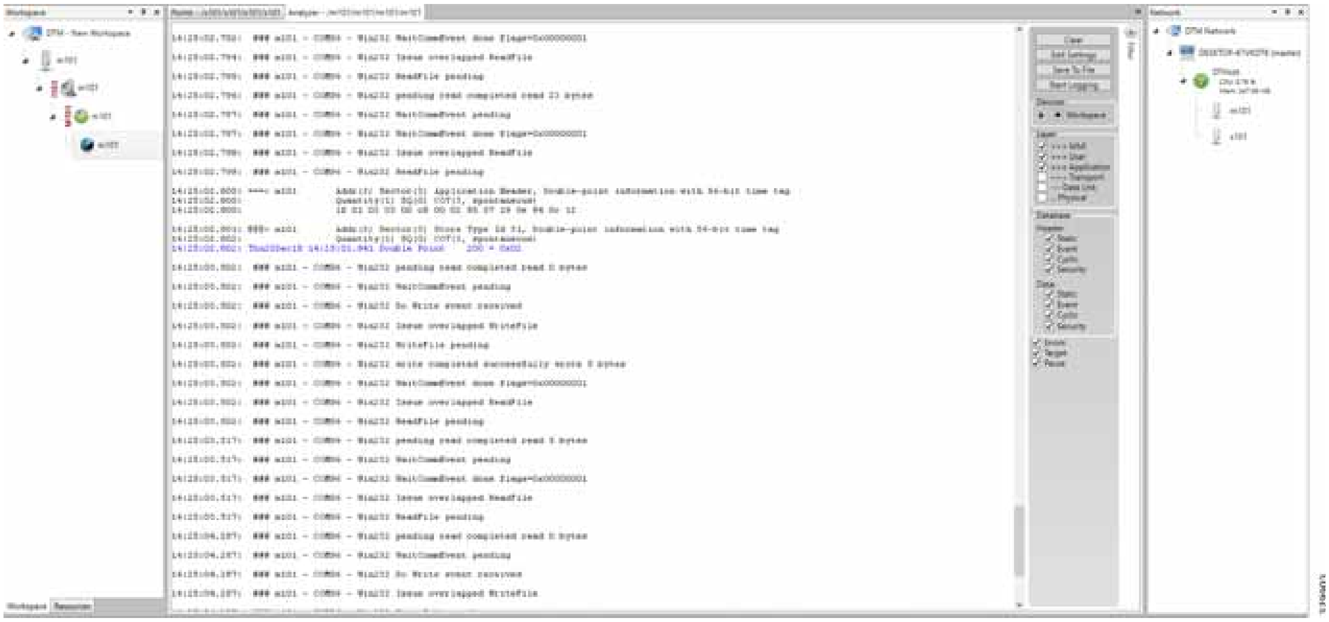


Figure 56 Master Analyzer after Change in Register Value



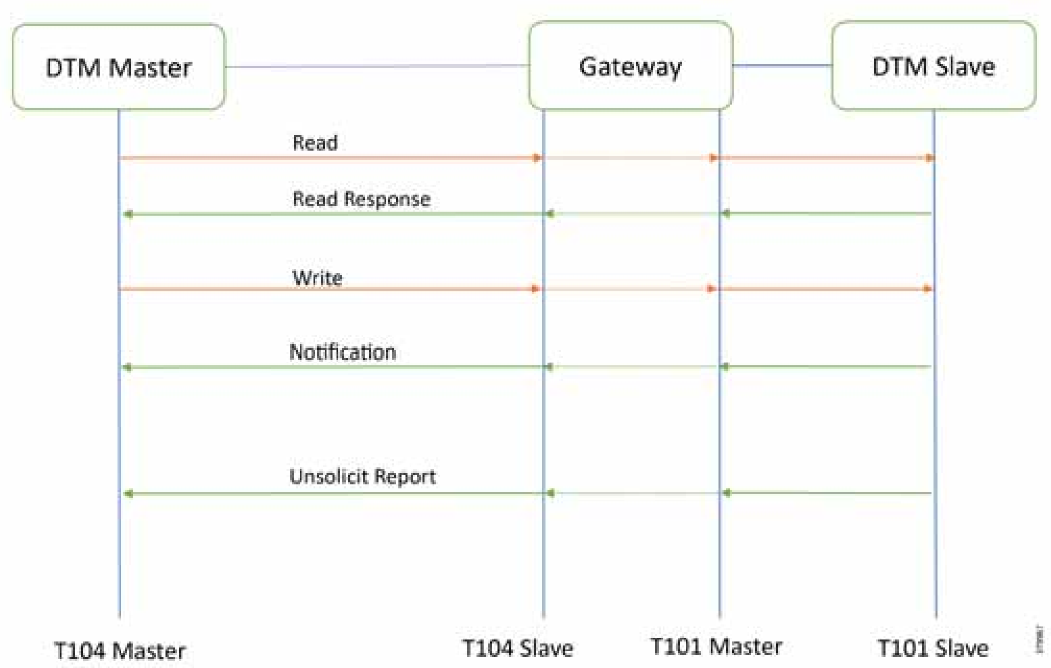
SCADA Gateway

Protocol Validated

The protocol we have validated for this release is IEC 60870-5-101 and IEC 60870-5-104.

Flow Diagram

Figure 57 T101 to T104 Protocol Translation Control Flow



As shown in Figure 57, the DTM Master can read and write the Slave via the DA Gateway using protocol translation. The Slave can send the Report by Exception to the Master via the DA Gateway using protocol translation.

IR807 SCADA Gateway Configuration

```
line 4
    databits 8
    stopbits 1
    speed 9600
parity none
!
interface Async1
no ip address
    encapsulation scada
!
scada-gw protocol t101 channel t101_ch1

link-addr-size two
    bind-to-interface Async1
session t101_session1
    attach-to-channel t101_ch1
sector t101_sector1
    attach-to-session t101_session1
scada-gw protocol t104
    channel t104_ch1
    t3-timeout 20
    tcp-connection 0 local-port 25000 remote-ip any
session t104_session1
    attach-to-channel
    t104_ch1
sector t104_sector1
    attach-to-session t104_session1
    map-to-sector t101_sector1
scada-gw enable
```

IR1101 SCADA Gateway Configuration

```
line 0/2/0
    databits 8
    stopbits 1
    speed 9600
    parity none
!
interface Async0/2/0
    no ip address
    encapsulation scada
!
scada-gw protocol t101
    channel t101_ch1
    link-addr-size two
    bind-to-interface Async 0/2/0
session t101_session1
    attach-to-channel t101_ch1
sector t101_sector1
    attach-to-session t101_session1

scada-gw protocol t104
    channel t104_ch1
    t3-timeout 20
    tcp-connection 0 local-port 25000 remote-ip any
session t104_session1
    attach-to-channel t104_ch1
sector t104_sector1
    attach-to-session t104_session1
    map-to-sector t101_sector1
scada-gw enable
```

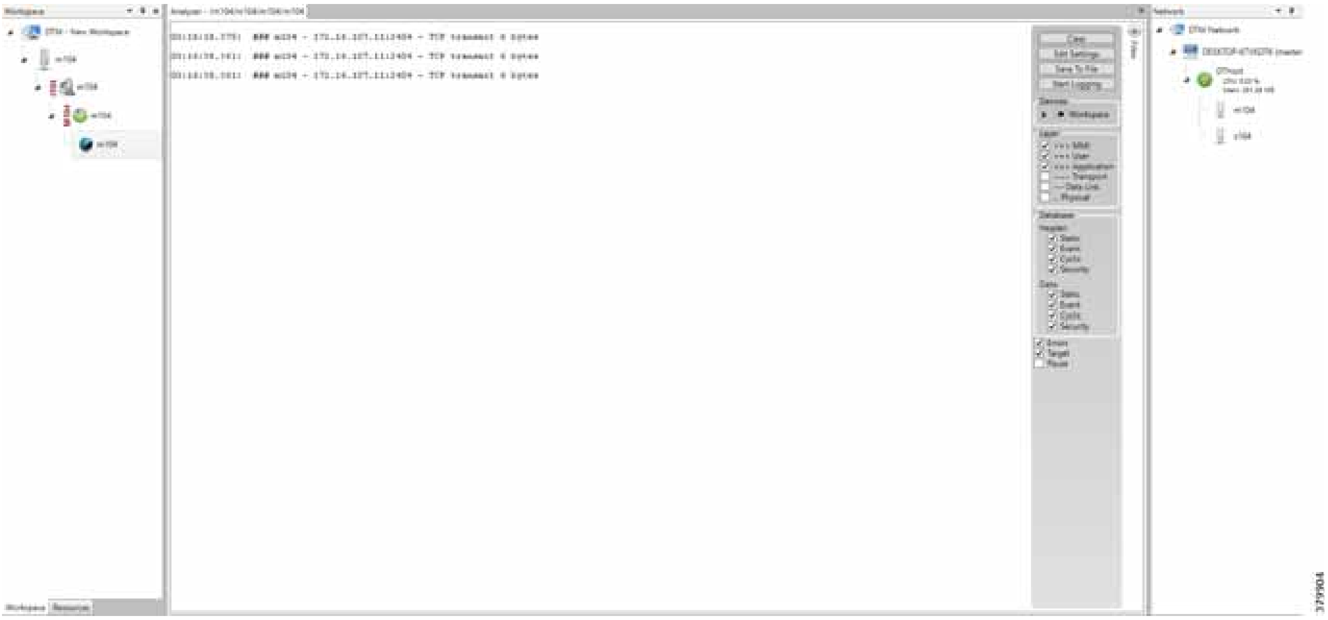
SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Report by Exception is sent to the Master from the Slave. Figure 59 and Figure 60 show the Poll operation from SCADA-Master. Similarly, Control and Report by Exception can also be seen on the Master Analyzer logs.

Poll

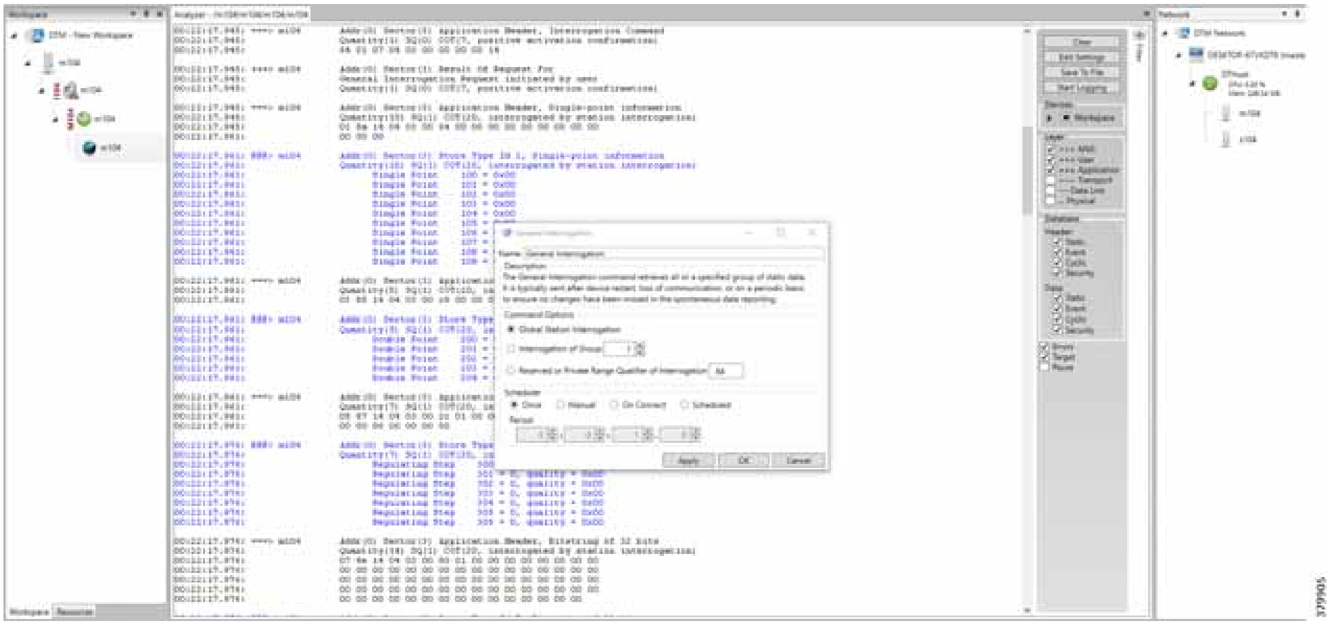
The Poll operation is performed by the Master. The Master can execute a general Poll in which all the register values are read and sent to the Master, a Poll on a set of registers, or a Poll on a single register. In Figure 59 and Figure 60, we see a general Poll executed on the Slave side. Initially the Master Analyzer is empty; however, when the *General Interrogation* command is executed, the values of all the registers are displayed on the Master Analyzer of DTM.

Figure 58 Master Analyzer Logs before Poll Operation



```
00:18:18.775:  ### m104 - 172.16.107.111:2404 - TCP transmit 6 bytes
00:18:38.781:  ### m104 - 172.16.107.111:2404 - TCP transmit 6 bytes
00:18:58.781:  ### m104 - 172.16.107.111:2404 - TCP transmit 6 bytes
```

Figure 59 Master Analyzer Logs after Poll Operation



```
00:22:17.945: <--- m104      ADDR(0) Sector(1) Application Header, Interrogation Command
00:22:17.945:                Quantity(1) SQ(0) COT(7, positive activation confirmation)
00:22:17.945:                64 01 07 00 00 00 00 00 00 14

00:22:17.945: <+++ m104      ADDR(0) Sector(1) Result Of Request For
00:22:17.945:                General Interrogation Request initiated by user
00:22:17.945:                Quantity(1) SQ(0) COT(7, positive activation confirmation)

00:22:17.945: <--- m104      ADDR(0) Sector(1) Application Header, Single-point information
00:22:17.945:                Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.945:                01 8a 14 00 00 00 64 00 00 00 00 00 00 00 00 00
00:22:17.961:                00 00 00

00:22:17.961: ###> m104      ADDR(0) Sector(1) Store Type 1D 1, Single-point information
00:22:17.961:                Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.961:                       Single Point    100 = 0x00
00:22:17.961:                       Single Point    101 = 0x00
00:22:17.961:                       Single Point    102 = 0x00
00:22:17.961:                       Single Point    103 = 0x00
00:22:17.961:                       Single Point    104 = 0x00
00:22:17.961:                       Single Point    105 = [illegible]
00:22:17.961:                       Single Point    106 = [illegible]
00:22:17.961:                       Single Point    107 = [illegible]
00:22:17.961:                       Single Point    108 = [illegible]
00:22:17.961:                       Single Point    109 = [illegible]

00:22:17.961: <--- m104      ADDR(0) Sector(1) Applicatio[illegible]
00:22:17.961:                Quantity(5) SQ(1) COT(20, in[illegible]
00:22:17.961:                03 85 14 04 00 00 c8 00 00 [illegible]

00:22:17.961: ###> m104      ADDR(0) Sector(1) Store Type[illegible]
00:22:17.961:                Quantity(5) SQ(1) COT(20, in[illegible]
00:22:17.961:                       Double Point    200 = [illegible]
00:22:17.961:                       Double Point    201 = [illegible]
00:22:17.961:                       Double Point    202 = [illegible]
00:22:17.961:                       Double Point    203 = [illegible]
00:22:17.961:                       Double Point    204 = [illegible]

00:22:17.961: <--- m104      ADDR(0) Sector(1) Applicatio[illegible]
00:22:17.961:                Quantity(7) SQ(1) COT(20, in[illegible]
00:22:17.961:                05 87 14 04 00 00 2c 01 00 0[illegible]
00:22:17.961:                00 00 00 00 00 00 00

00:22:17.976: ###> m104      ADDR(0) Sector(1) Store Type[illegible]
00:22:17.976:                Quantity(7) SQ(1) COT(20, in[illegible]
00:22:17.976:                       Regulating Step    300[illegible]
00:22:17.976:                       Regulating Step    301 = 0, quality = 0x00
00:22:17.976:                       Regulating Step    302 = 0, quality = 0x00
00:22:17.976:                       Regulating Step    303 = 0, quality = 0x00
00:22:17.976:                       Regulating Step    304 = 0, quality = 0x00
00:22:17.976:                       Regulating Step    305 = 0, quality = 0x00
00:22:17.976:                       Regulating Step    306 = 0, quality = 0x00

00:22:17.976: <--- m104      ADDR(0) Sector(1) Application Header, Bitstring of 32 bits
00:22:17.976:                Quantity(16) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.976:                07 8e 14 04 00 00 90 01 00 00 00 00 00 00 00 00
00:22:17.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.976:                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

General Interrogation

Name: General Interrogation

Description

The General Interrogation command retrieves all or a specified group of static data. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure no changes have been missed in the spontaneous data reporting.

Command Options

● Global Station Interrogation

○ Interrogation of Group 1

○ Reserved or Private Range Qualifier of Interrogation AA

Scheduler

● Once ○ Manual ○ On Connect ○ Scheduled

Period

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 Double Point Register (#200) is changed and the same is reported to the Master. Figure 60, Figure 61, and Figure 62 show the Report by Exception sent to the Master for a particular register:

Figure 60 Slave Register before Control Operation

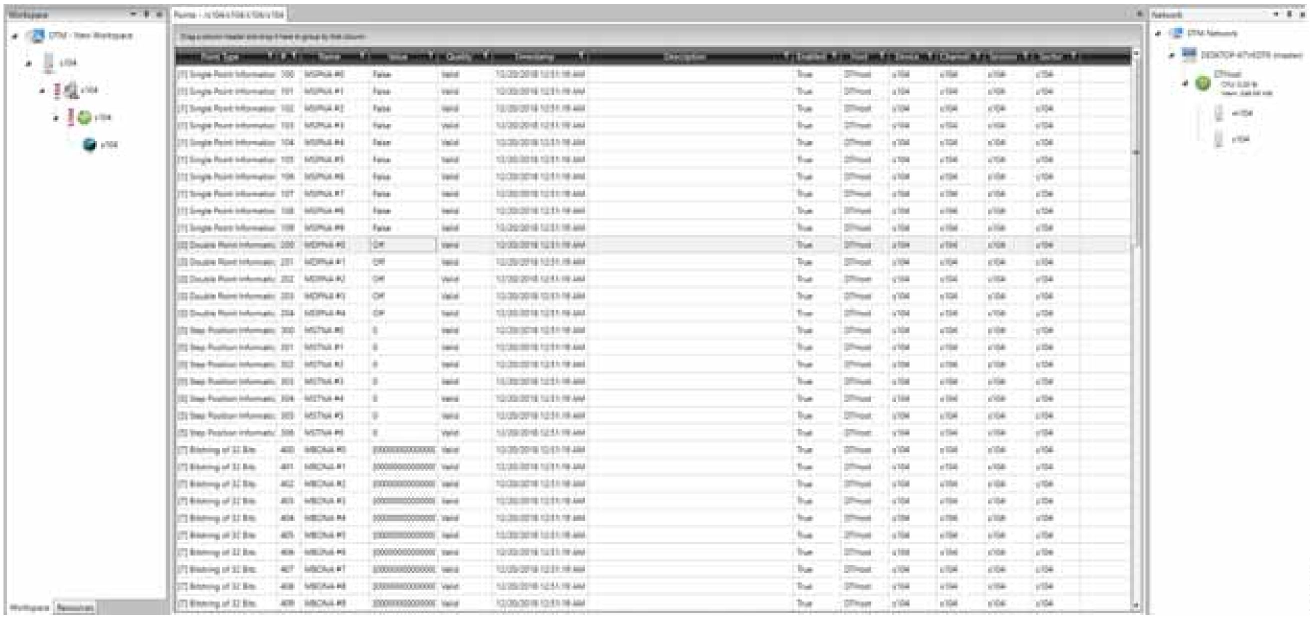


Figure 61 Master Control Control Operation

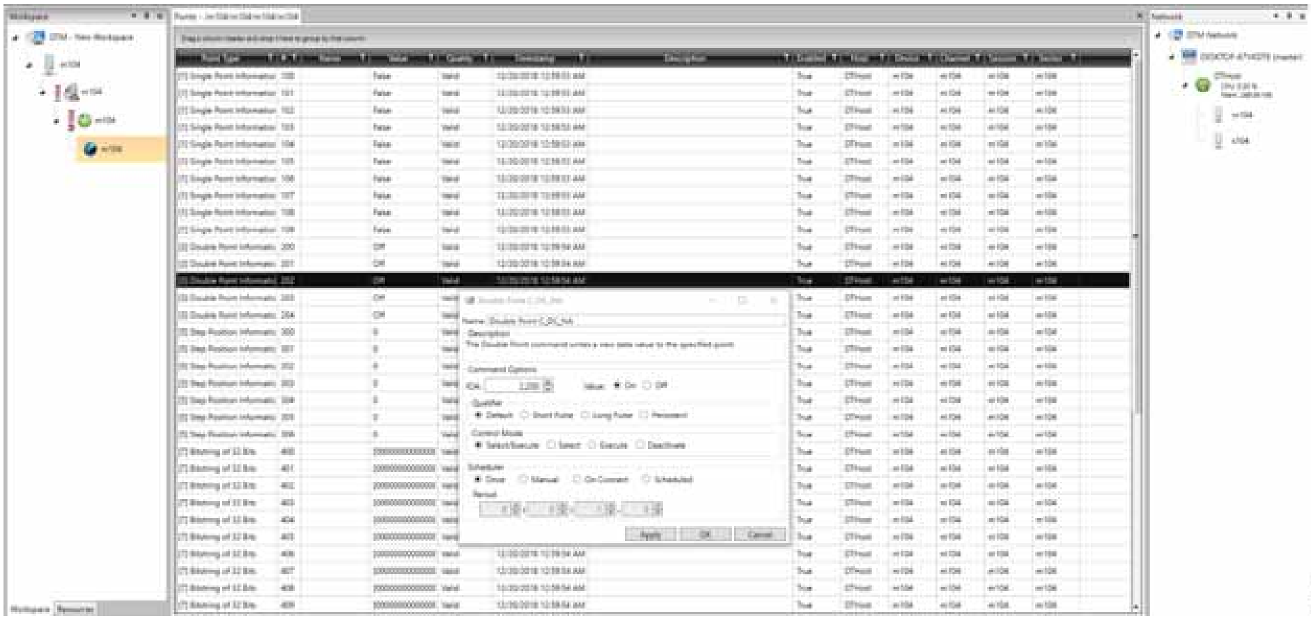
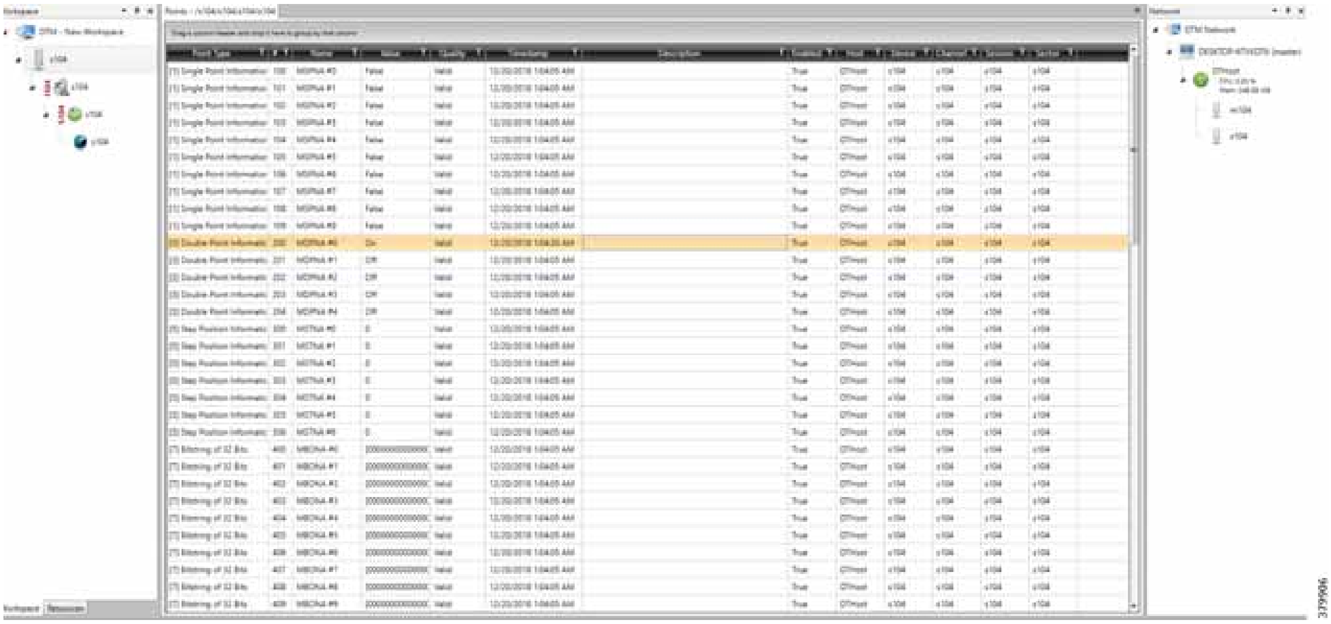


Figure 62 Slave Register after Control Operation

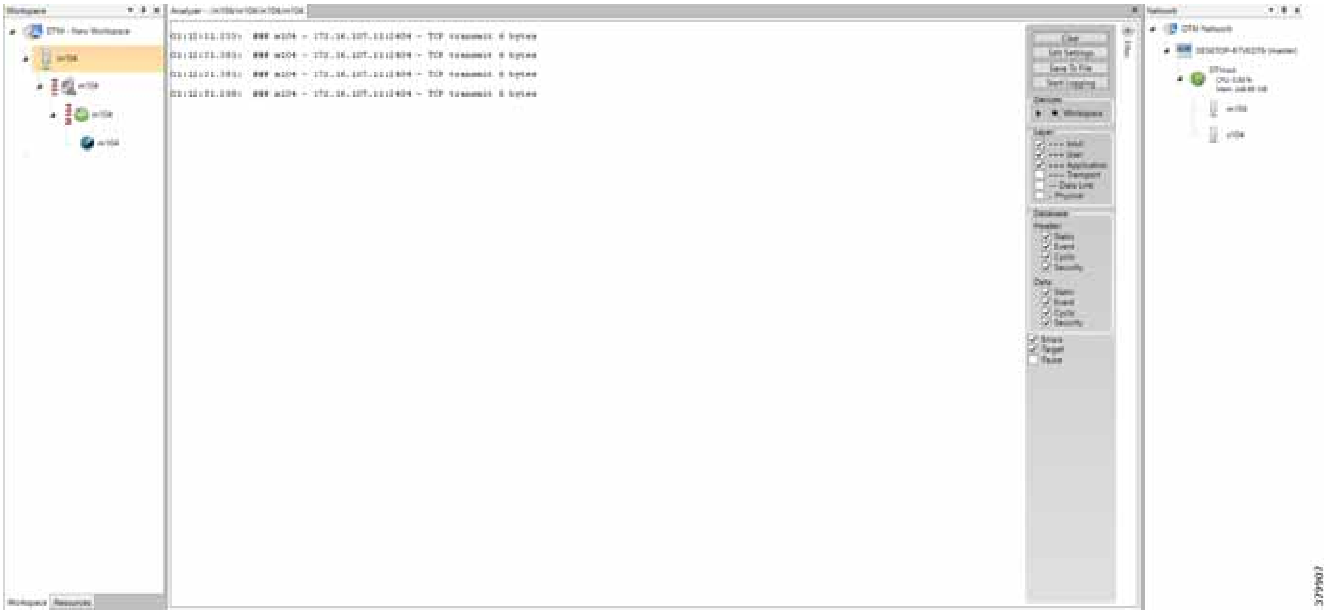


Point Type	#	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	MSPNA #0	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	101	MSPNA #1	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	102	MSPNA #2	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	103	MSPNA #3	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	104	MSPNA #4	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	105	MSPNA #5	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	106	MSPNA #6	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	107	MSPNA #7	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	108	MSPNA #8	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	109	MSPNA #9	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	On	Valid	12/20/2018 1:04:20 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104

Report by Exception

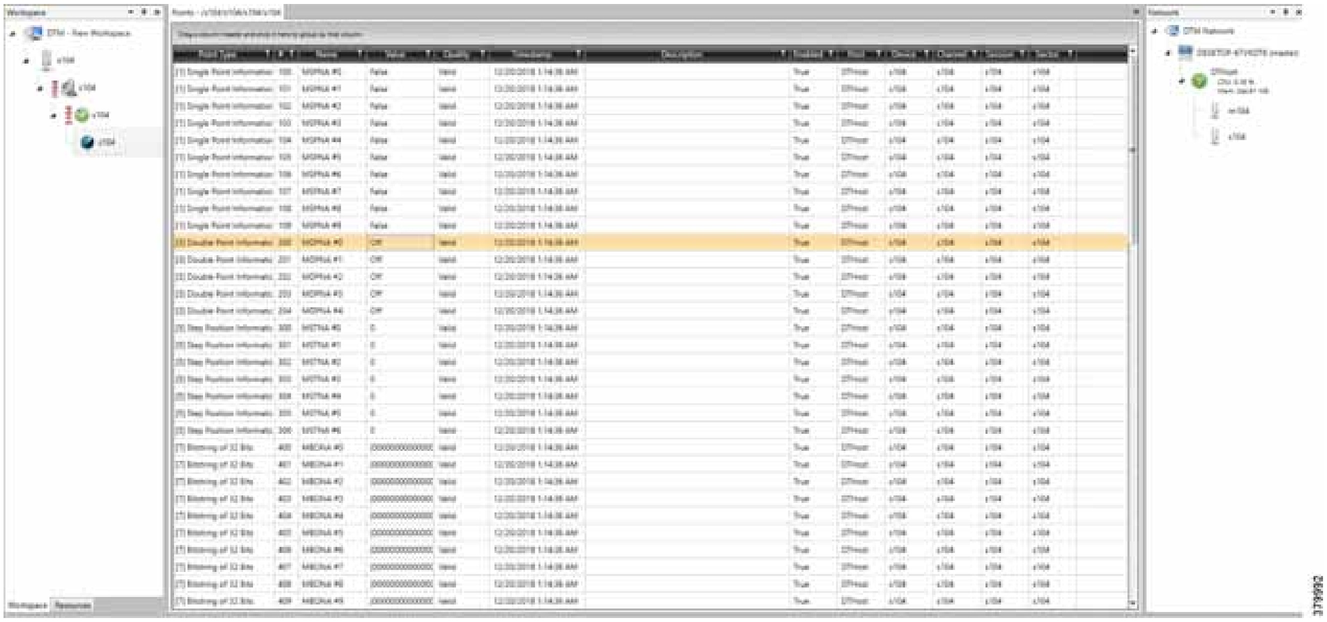
Report by Exception is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are reported to SCADA-Master. This notification can be seen on the Master Analyzer of DTM software. Figure 63, Figure 64, Figure 65, and Figure 66 show the Report by Exception on the analyzer. The other operations such as Poll and Control can be executed, and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to the Master. Figure 63, Figure 64, Figure 65, and Figure 66show the Report by Exception sent to the Master for a particular register:

Figure 63 Master Analyzer



```
01:12:11.233: ### s104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:12:21.383: ### s104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:12:21.383: ### s104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:12:21.238: ### s104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

Figure 64 Slave Registers



Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	Off	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	00000000000000	Valid	12/20/2018 1:14:26 AM		True	DTHost	s104	s104	s104	s104

Figure 65 Change in Slave Register Value

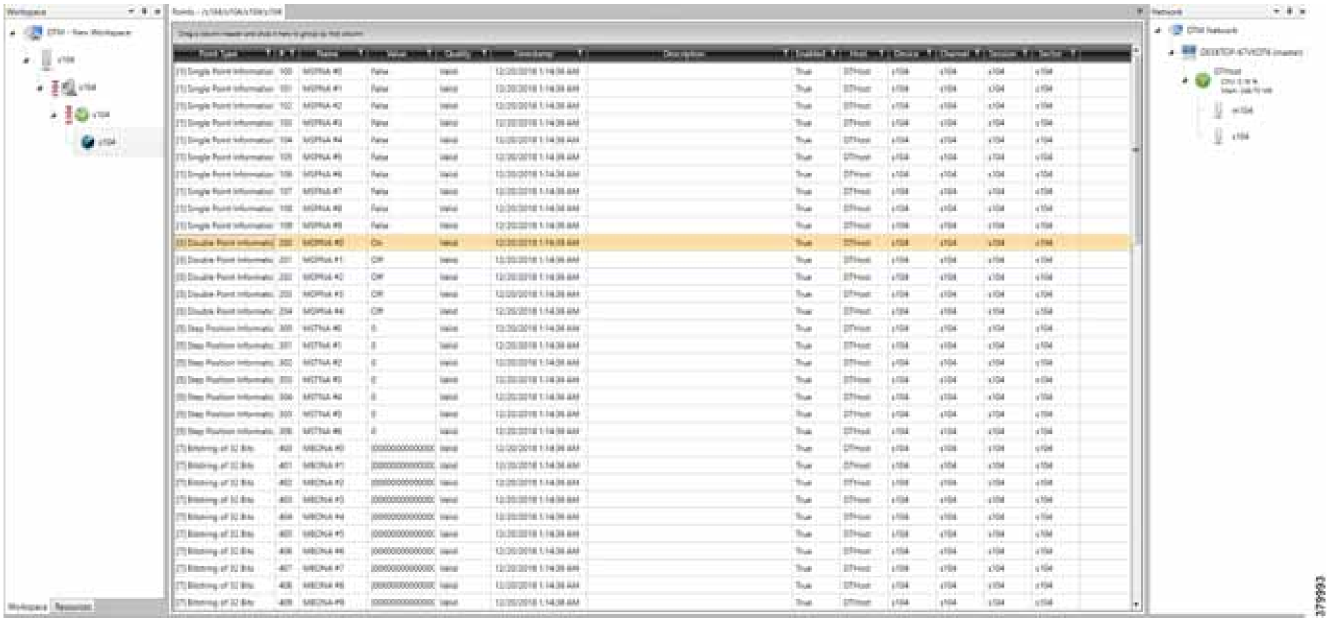
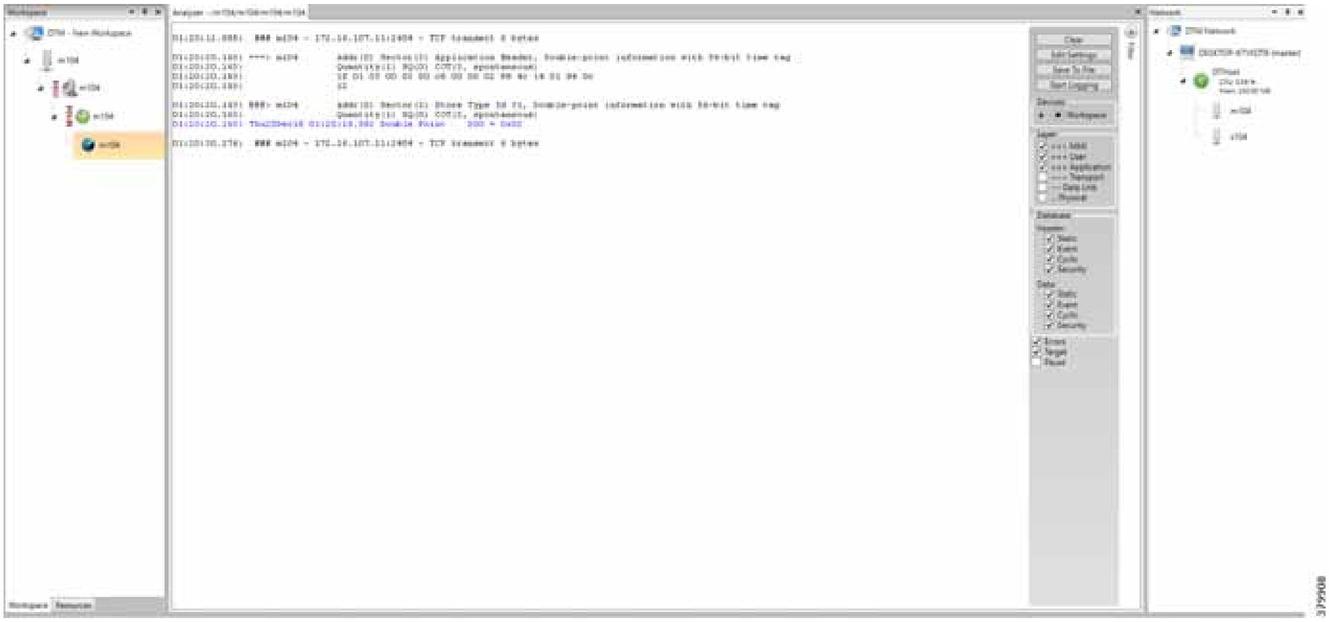


Figure 66 Master Analyzer after Change in Register Value



Dual Control Center

When a Slave is connected to the DA Gateway via the serial or Ethernet port, then the Master and the Slave can communicate using the T104 or T101 protocol to the dual Control Center. The communication between the Slave and Master can be Ethernet based (T104) or RS232 serial communication (T101) or by means of protocol translation.

Operations that can be executed when the communication protocol is T104 or T101 or T101- T104 translation are as follows:

- Poll (Master > Slave)
- Control (Master > Slave)
- Report by Exception (Slave > Master) - Notification

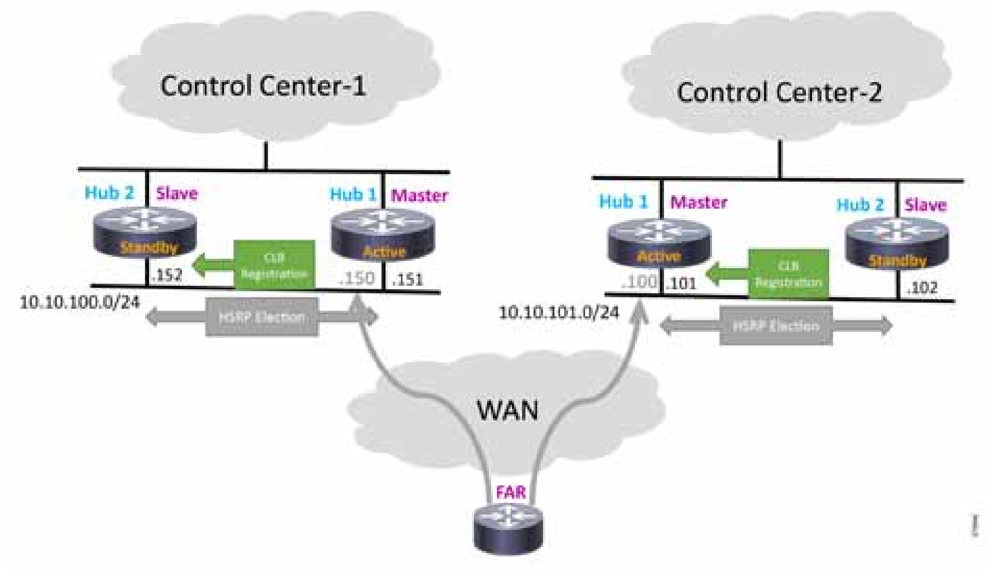
The operations have been executed using a SCADA simulator known as DTM, which has the capability of simulating both Master and the Slave device.

Implementation Overview

This document focuses on SCADA protocols such as T101 and T104 and the T101-T104 translation protocols widely used in the Europe Region with Primary and Secondary DSO Control Centers.

Topology Diagram

Figure 67 Dual Control Center



IP-Based SCADA

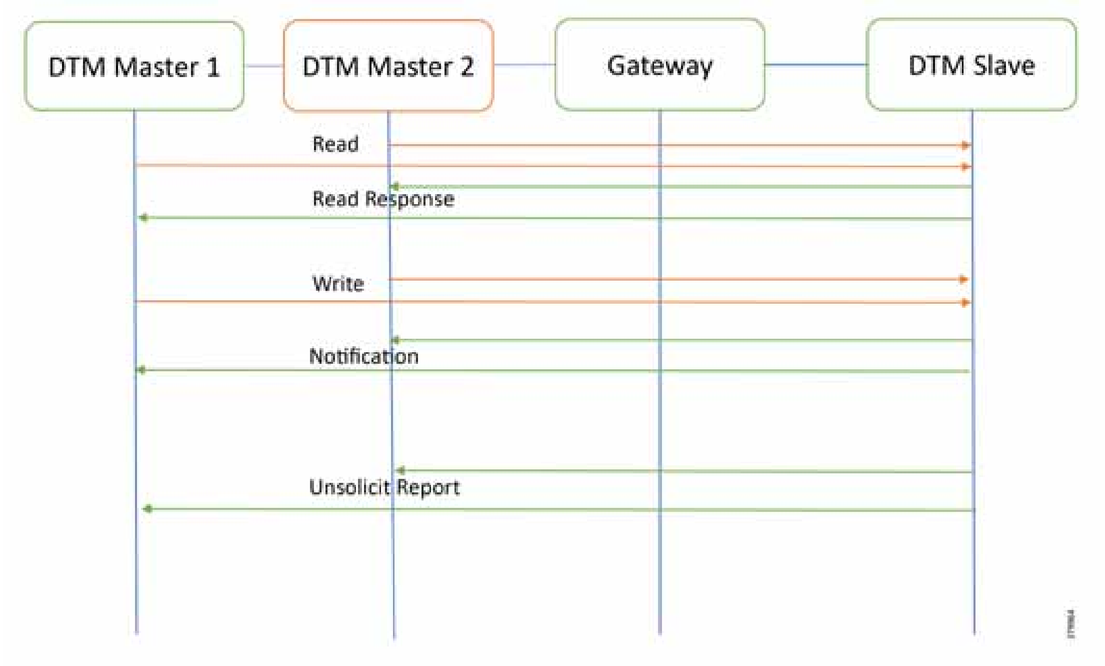
Protocol Validated

The protocol we have validated for this release is IEC 60870-5-104.

Flow Diagram

As shown in Figure 68, both the DTM Master can read and write the Slave via the DA Gateway, and the Slave can send the Report by Exception to both Master via the DA Gateway over the IP network:

Figure 68 T104 Control Flow



IR807 as DA Gateway or Secondary Substation Router

```
interface FastEthernet1
    ip address 192.168.0.1 255.255.255.0
    ip nat inside
    ip virtual-reassembly in
    duplex auto
    speed auto

interface Tunnel0
/*Tunnel to primary control center*/
    ip nat outside
!
interface Tunnel1
/*Tunnel to primary control center*/
    ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
ip nat inside source static tcp 192.168.0.2 26000 interface Loopback0 26000
```

IR1101 as DA Gateway or Secondary Substation Router

```
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 Tunnel0 ip nat outside
!
interface Tunnel1 ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
ip nat inside source static tcp 192.168.0.2 26000 interface Loopback0 26000
```

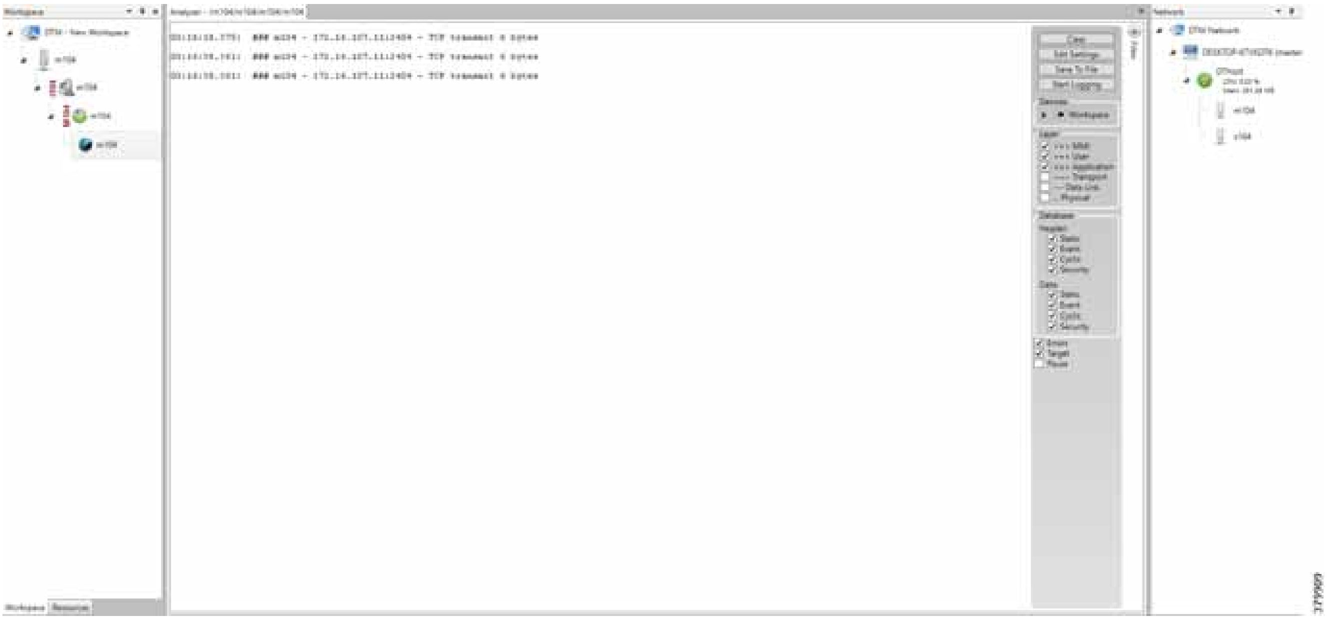
The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Report by Exception is sent to the Master from the Slave. Figure 69 and Figure 70 show the Poll operation from Dual SCADA-Master belongs to a different control center. Similarly, Control and Report by Exception can also be seen on the Master Analyzer logs.

SCADA Operations

Poll

The Poll operation is performed by the dual Masters. The Masters can execute a general Poll in which all the register values are read and sent to the Master, a Poll on a set of registers, or a Poll on a single register. In Figure 69, Figure 70, Figure 71, and Figure 72, we see a general Poll executed on the Slave side. Initially the Master Analyzer is empty; however, when the *General Interrogation* command is executed, the values of all the registers are displayed on the Master Analyzer of DTM.

Figure 69 CC-1 Master Analyzer Logs before Poll Operation



```
[illegible]   ### m104 - 172.16.107.11:2404 - TCP transmit 0 bytes
[illegible]   ### m104 - 172.16.107.11:2404 - TCP transmit 0 bytes
[illegible]   ### m104 - 172.16.107.11:2404 - TCP transmit 0 bytes
```

Figure 70 CC-2 Master Analyzer Logs before Poll Operation

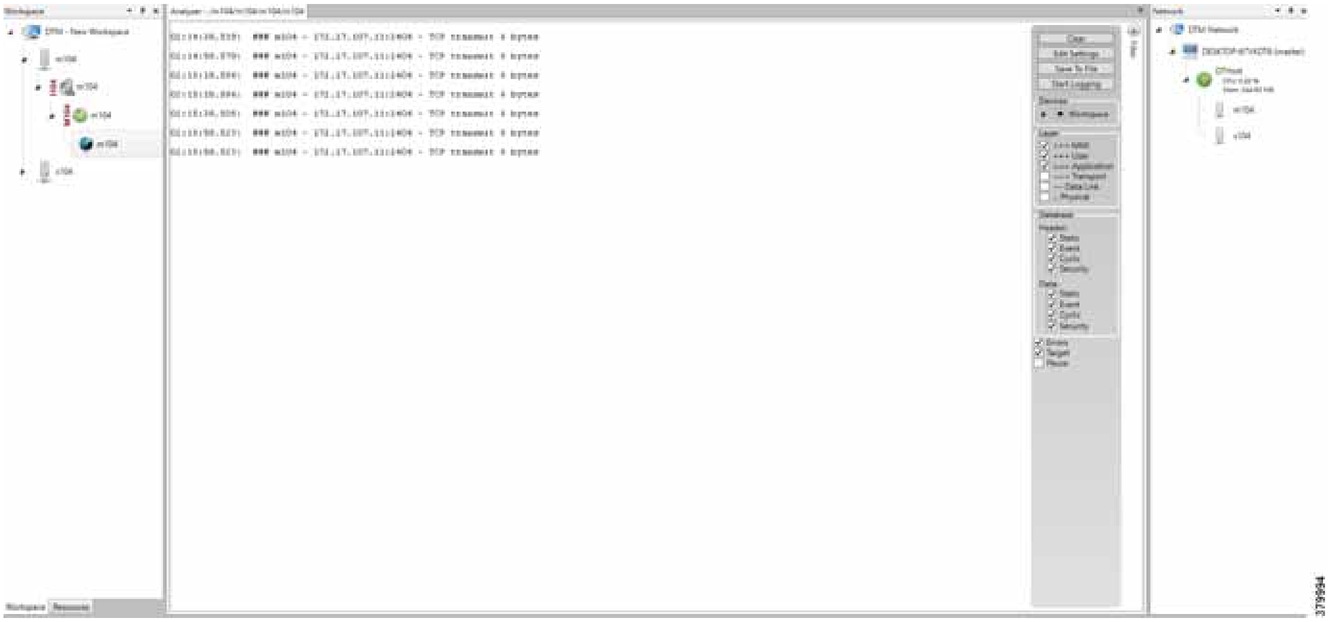


Figure 71 CC-1 Master Analyzer Logs after Poll Operation

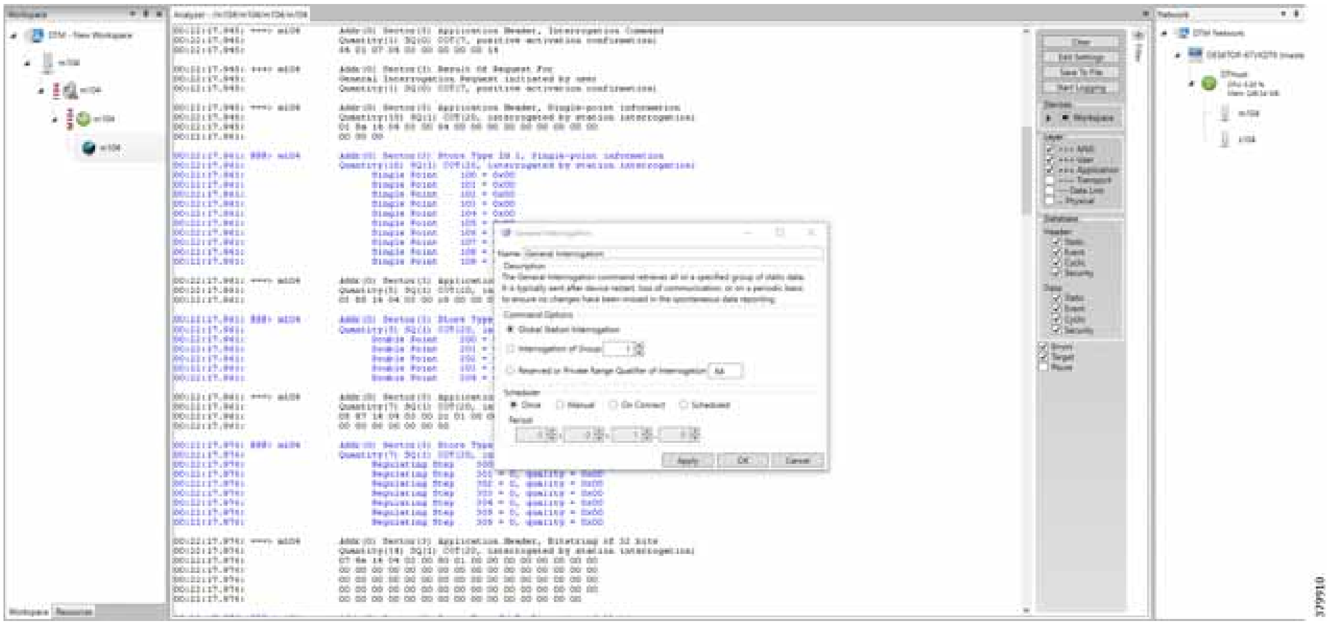
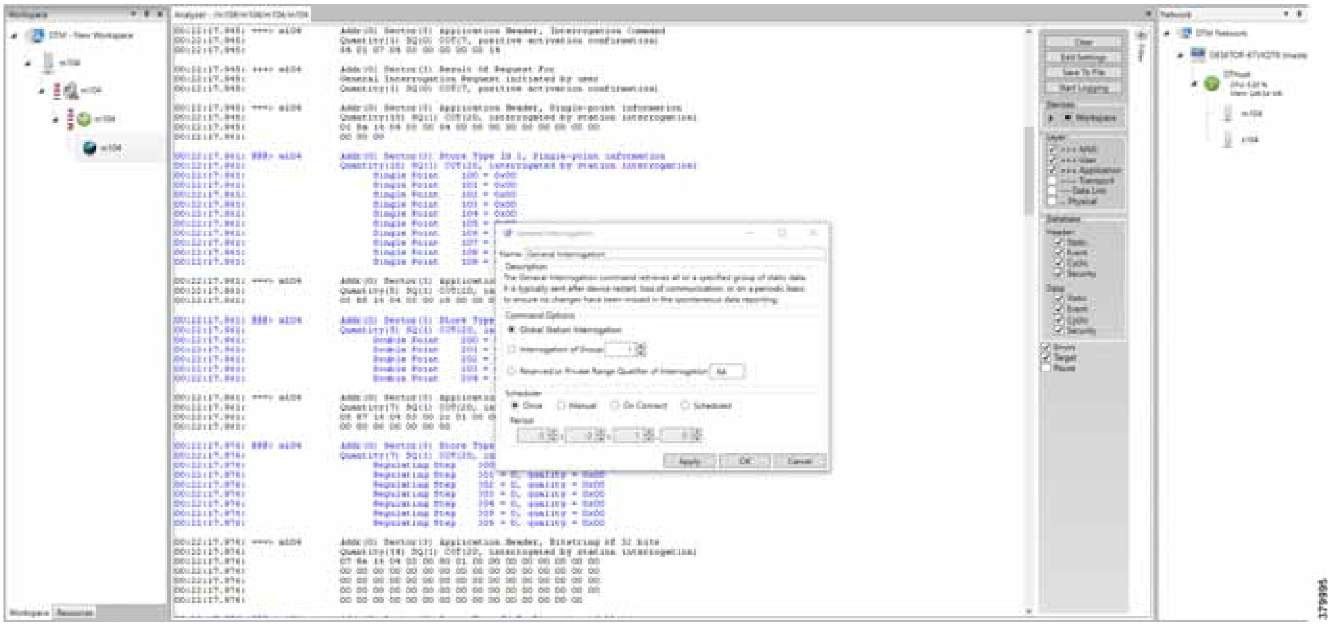


Figure 72 CC-2 Master Analyzer Logs after Poll Operation



```
00:22:17.945: ---> m104       Addr(0) Sector(1) Application Header, Interrogation Command
00:22:17.945:                 Quantity(1) SQ(0) COT(7, positive activation confirmation)
00:22:17.945:                 64 01 07 04 00 00 00 00 00 14

00:22:17.945: <--- m104       Addr(0) Sector(1) Result Of Request For
00:22:17.945:                 General Interrogation Request initiated by user
00:22:17.945:                 Quantity(1) SQ(0) COT(7, positive activation confirmation)

00:22:17.945: ---> m104       Addr(0) Sector(1) Application Header, Single-point information
00:22:17.945:                 Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.945:                 01 8a 14 04 00 00 64 00 00 00 00 00 00 00 00
00:22:17.961:                 00 00 00

00:22:17.961: ### m104        Addr(0) Sector(1) Store Type ID 1, Single-point information
00:22:17.961:                 Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.961:                      Single Point    100 = 0x00
00:22:17.961:                      Single Point    101 = 0x00
00:22:17.961:                      Single Point    102 = 0x00
00:22:17.961:                      Single Point    103 = 0x00
00:22:17.961:                      Single Point    104 = 0x00
00:22:17.961:                      Single Point    105 =
00:22:17.961:                      Single Point    106 =
00:22:17.961:                      Single Point    107 =
00:22:17.961:                      Single Point    108 =
00:22:17.961:                      Single Point    109 =

00:22:17.961: ---> m104       Addr(0) Sector(1) Applicatio
00:22:17.961:                 Quantity(5) SQ(1) COT(20, in
00:22:17.961:                 03 85 14 04 00 00 c8 00 00 0

00:22:17.961: ### m104        Addr(0) Sector(1) Store Type
00:22:17.961:                 Quantity(5) SQ(1) COT(20, in
00:22:17.961:                      Double Point    200 =
00:22:17.961:                      Double Point    201 =
00:22:17.961:                      Double Point    202 =
00:22:17.961:                      Double Point    203 =
00:22:17.961:                      Double Point    204 =

00:22:17.961: ---> m104       Addr(0) Sector(1) Applicatio
00:22:17.961:                 Quantity(7) SQ(1) COT(20, in
00:22:17.961:                 05 87 14 04 00 00 2c 01 00 0
00:22:17.961:                 00 00 00 00 00 00 00

00:22:17.976: ### m104        Addr(0) Sector(1) Store Type
00:22:17.976:                 Quantity(7) SQ(1) COT(20, in
00:22:17.976:                      Regulating Step    300
00:22:17.976:                      Regulating Step    301 = 0, quality = 0x00
00:22:17.976:                      Regulating Step    302 = 0, quality = 0x00
00:22:17.976:                      Regulating Step    303 = 0, quality = 0x00
00:22:17.976:                      Regulating Step    304 = 0, quality = 0x00
00:22:17.976:                      Regulating Step    305 = 0, quality = 0x00
00:22:17.976:                      Regulating Step    306 = 0, quality = 0x00

00:22:17.976: ---> m104       Addr(0) Sector(1) Application Header, Bitstring of 32 bits
00:22:17.976:                 Quantity(16) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.976:                 07 8a 14 04 00 00 90 01 00 00 00 00 00 00 00 00
00:22:17.976:                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.976:                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.976:                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.976:                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

General Interrogation

Name: General Interrogation

Description

The General Interrogation command retrieves all or a specified group of static data. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure no changes have been missed in the spontaneous data reporting.

Command Options

● Global Station Interrogation

○ Interrogation of Group: 1

○ Reserved or Private Range Qualifier of Interrogation: 64

Scheduler

● Once ○ Manual ○ On Connect ○ Scheduled

Period

0 : 0 : 1 : 0

Apply | OK | Cancel

Control

The control operation basically sends the control command from the Dual SCADA Masters 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 Double Point Register (#200) is changed and the same is reported to both Masters. Figure 73, Figure 74, Figure 75, Figure 76, and Figure 77 show the Report by Exception sent to the dual Masters for a particular register:

Figure 73 Slave Register before Control Operation

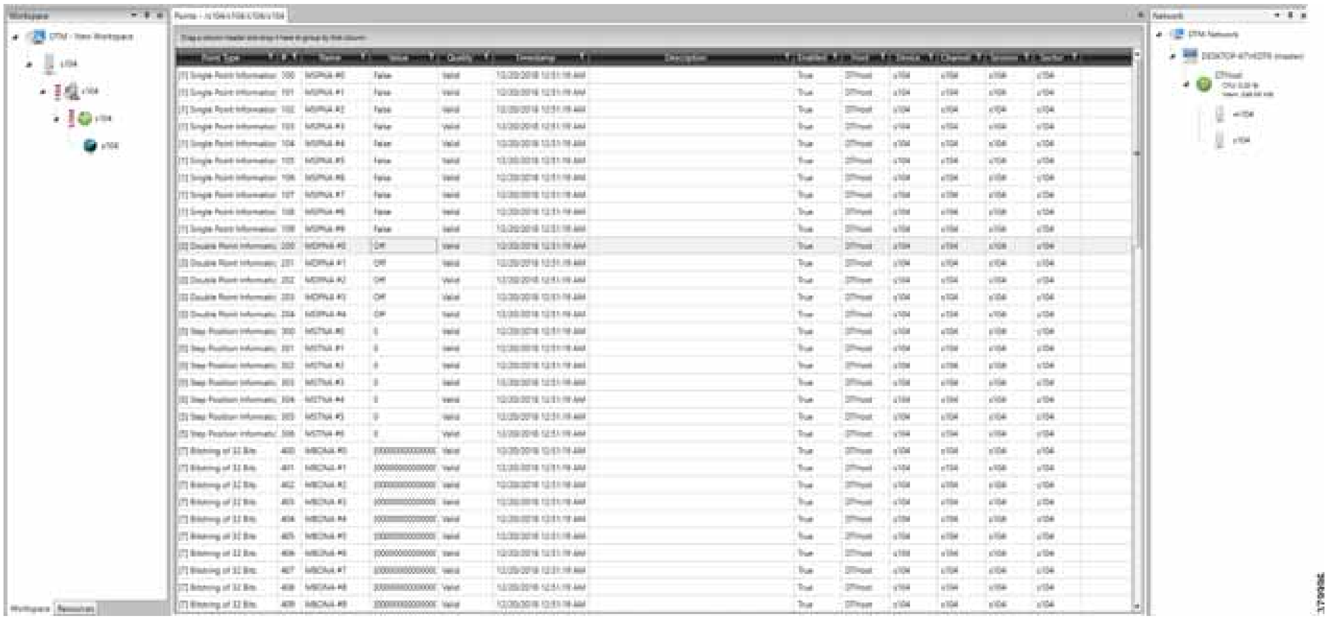


Figure 74 CC-1 Master Control Control Operation

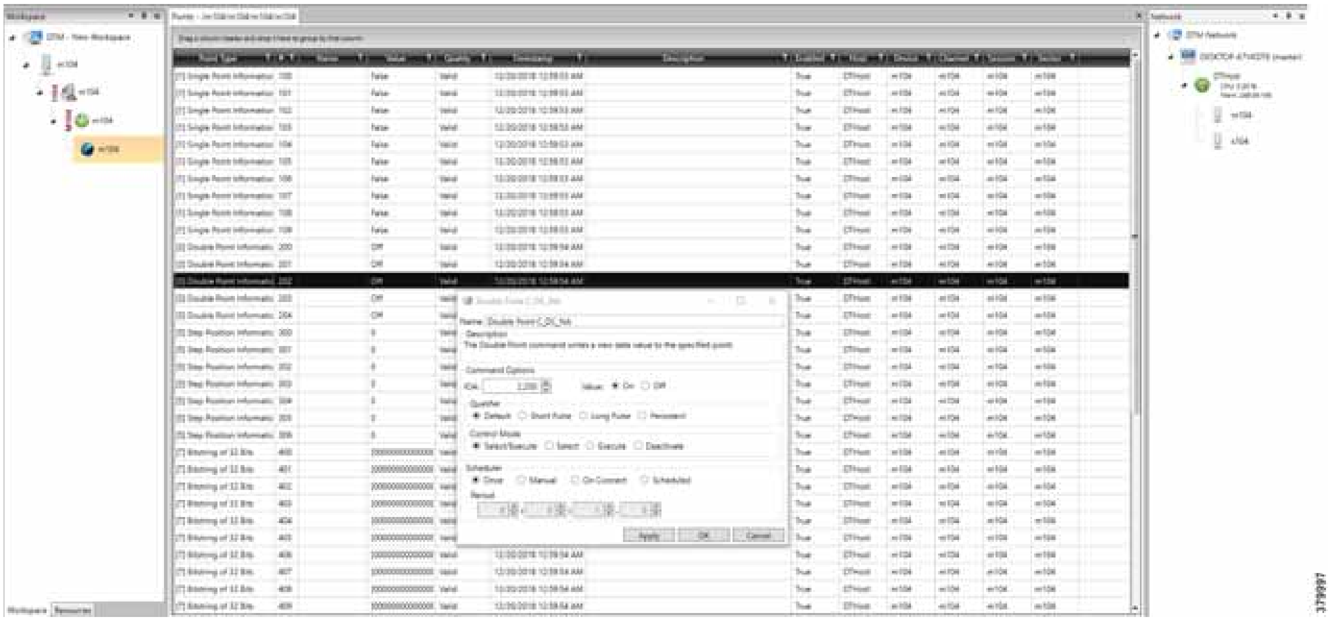


Figure 75 CC-2 Master Control Control Operation

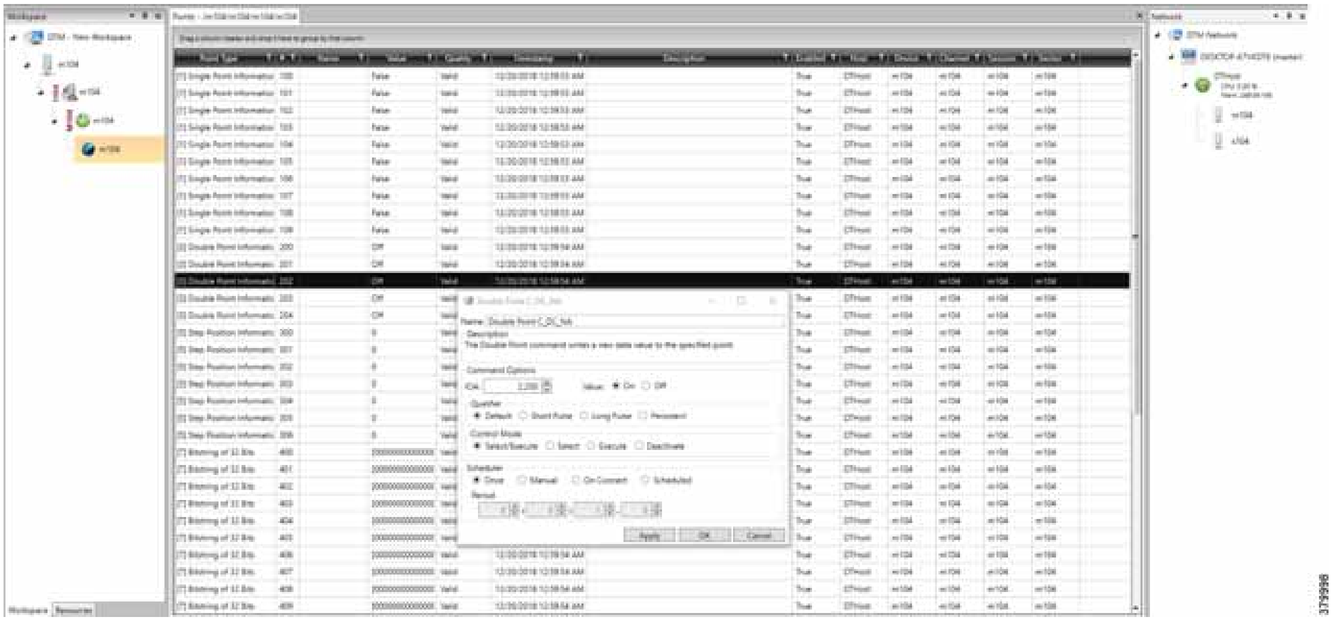


Figure 76 CC-1 Slave Register after Control Operation

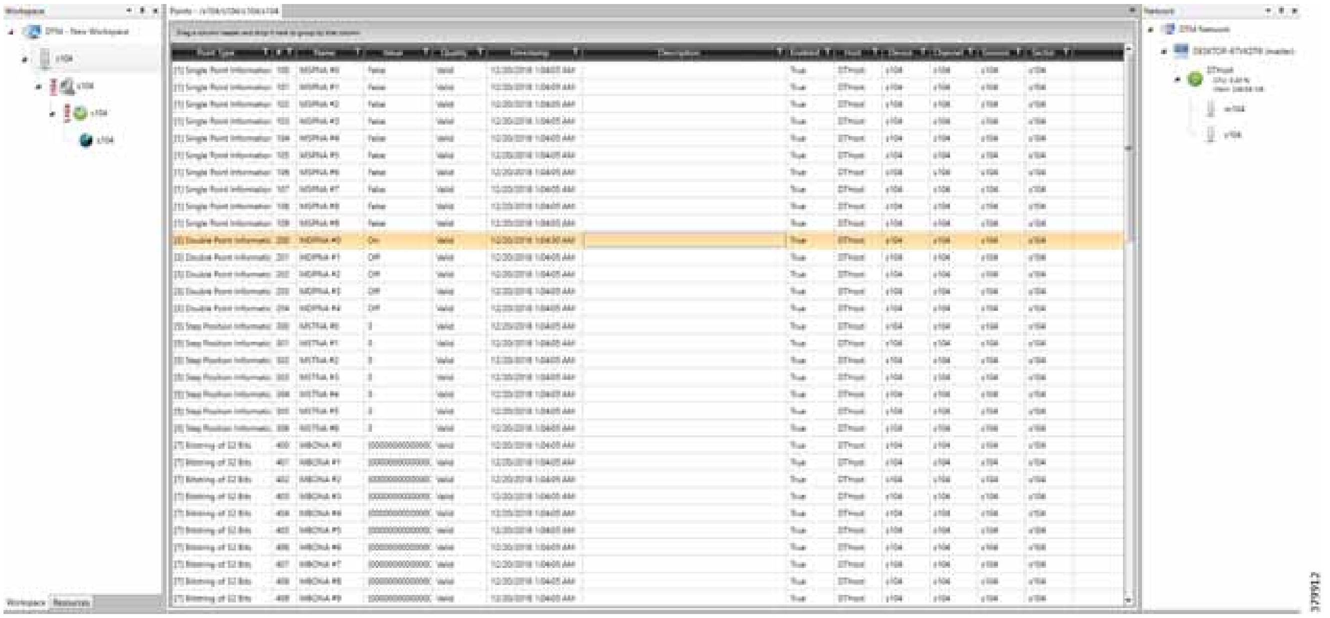
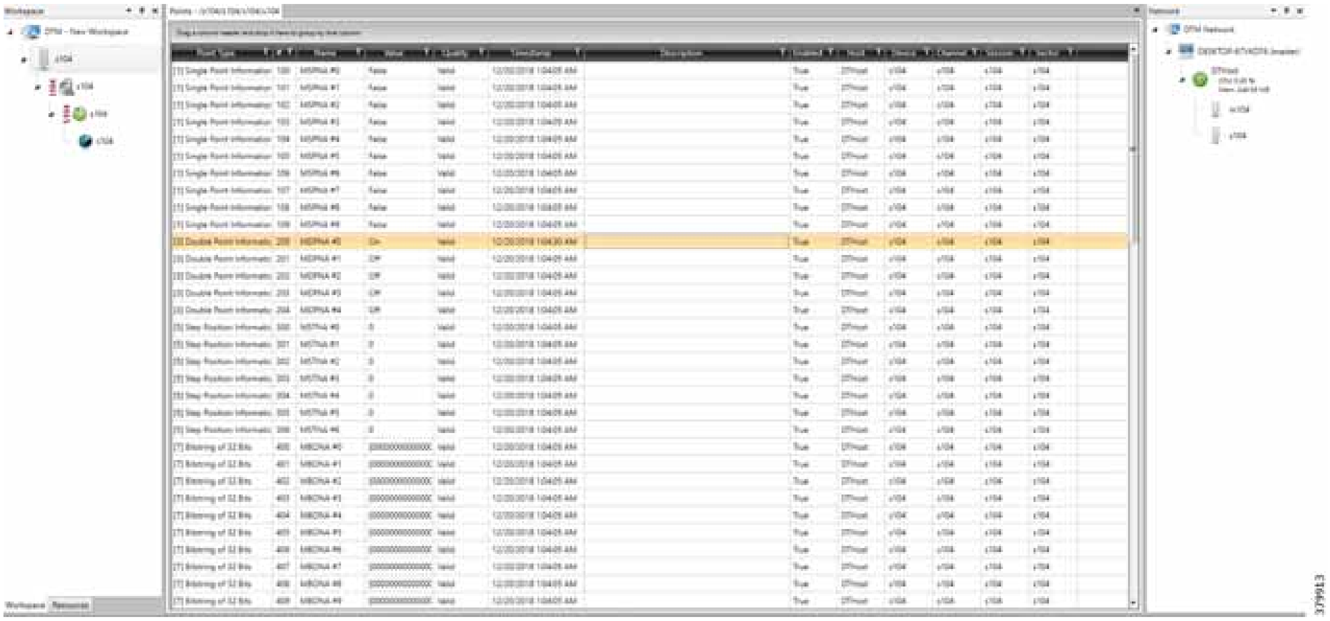


Figure 77 CC-2 Slave Register after Control Operation

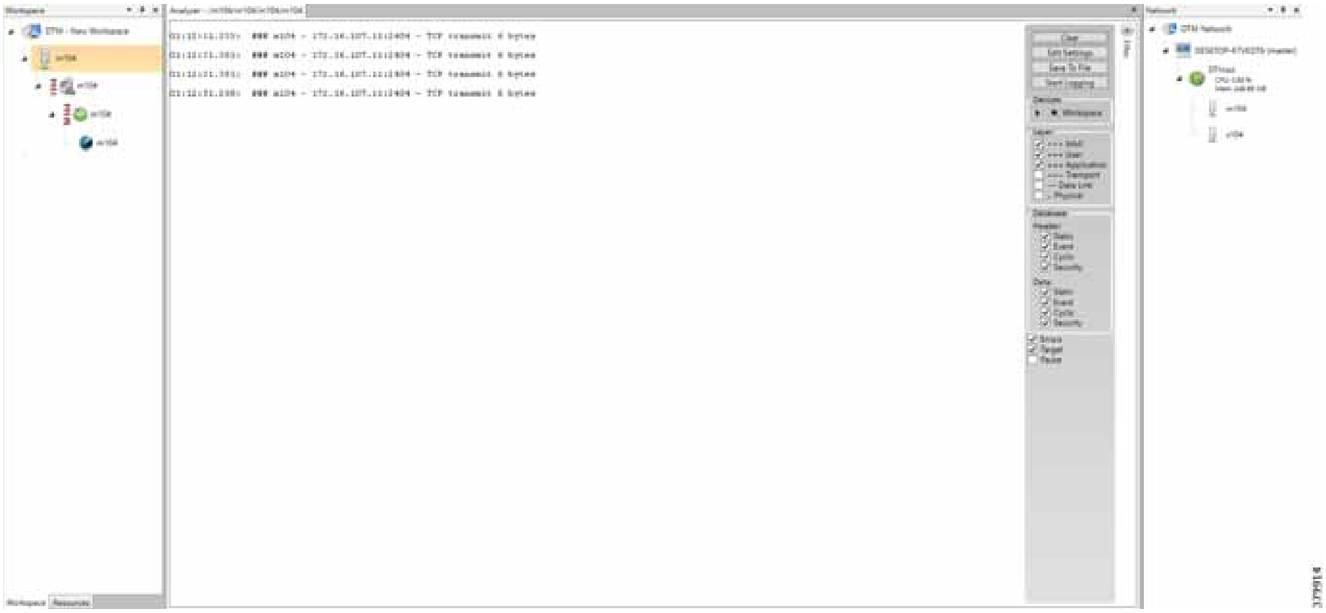


Point Type	#	Name	Value	Quality	TimeStamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	200	MDPNA #0	On	Valid	12/20/2018 10:04:30 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	201	MDPNA #1	Off	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	202	MDPNA #2	Off	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	203	MDPNA #3	Off	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	204	MDPNA #4	Off	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	300	MSTNA #0	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	301	MSTNA #1	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	302	MSTNA #2	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	303	MSTNA #3	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	304	MSTNA #4	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	305	MSTNA #5	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	306	MSTNA #6	0	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	[00000000000000	Valid	12/20/2018 10:04:05 AM		True	DTHost	s104	s104	s104	s104

Report by Exception

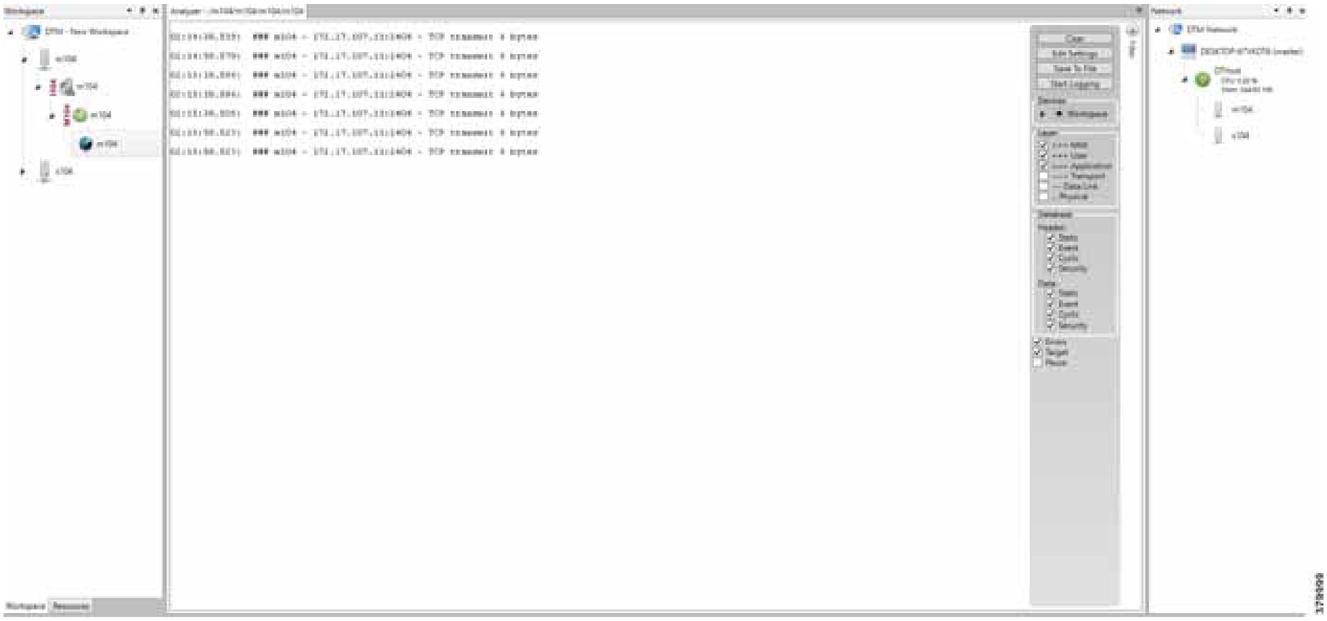
Report by Exception is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are reported to Dual SCADA-Masters. This notification can be seen on the Master Analyzer of DTM software. Figure 78, Figure 79, Figure 80, Figure 81, Figure 82, and Figure 83 show the Report by Exception on the analyzer. The other operations such as Poll and Control can be executed and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to both Masters. Figure 78, Figure 79, Figure 80, Figure 81, Figure 82, and Figure 83 show the Report by Exception sent to both Masters for a particular register:

Figure 78 CC-1 Master Analyzer



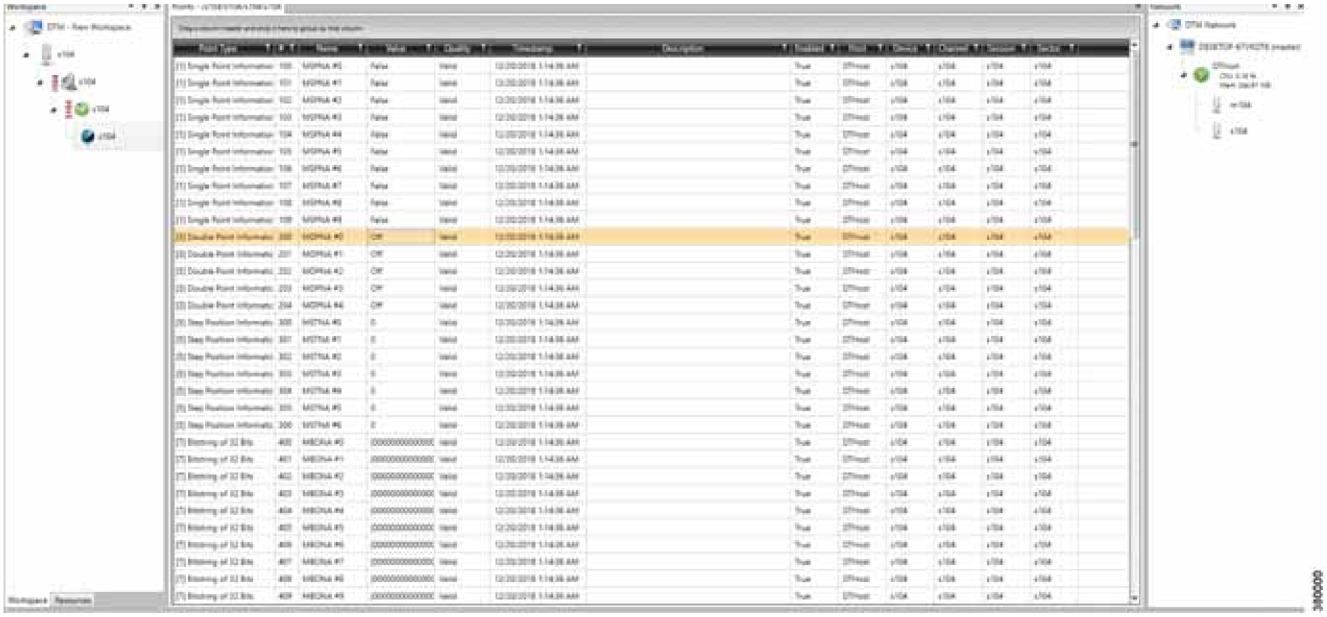
```
01:12:11.233:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:12:21.383:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:12:21.381:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
01:12:21.338:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

Figure 79 CC-2 Master Analyzer



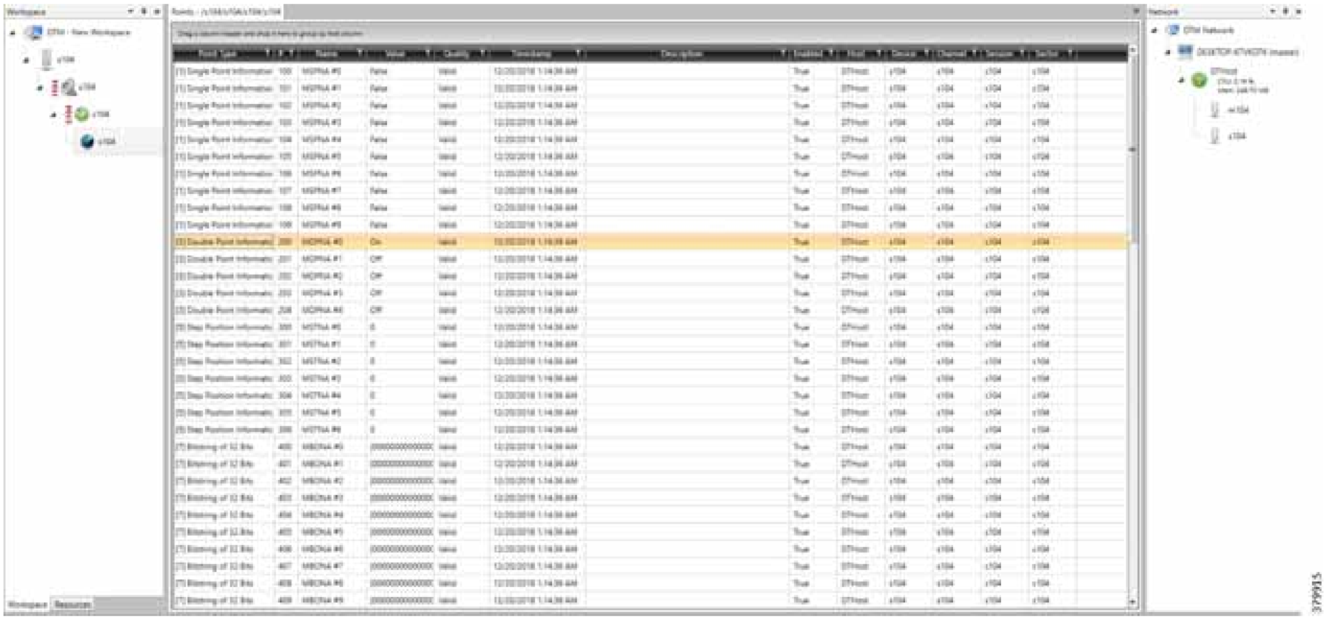
```
02:14:38.533:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
02:14:58.879:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
02:15:18.886:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
02:15:38.884:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
02:15:38.805:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
02:15:58.823:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
02:15:58.823:  ### m104 - 172.17.107.11:2404 - TCP transmit 4 bytes
```

Figure 80 Slave Registers



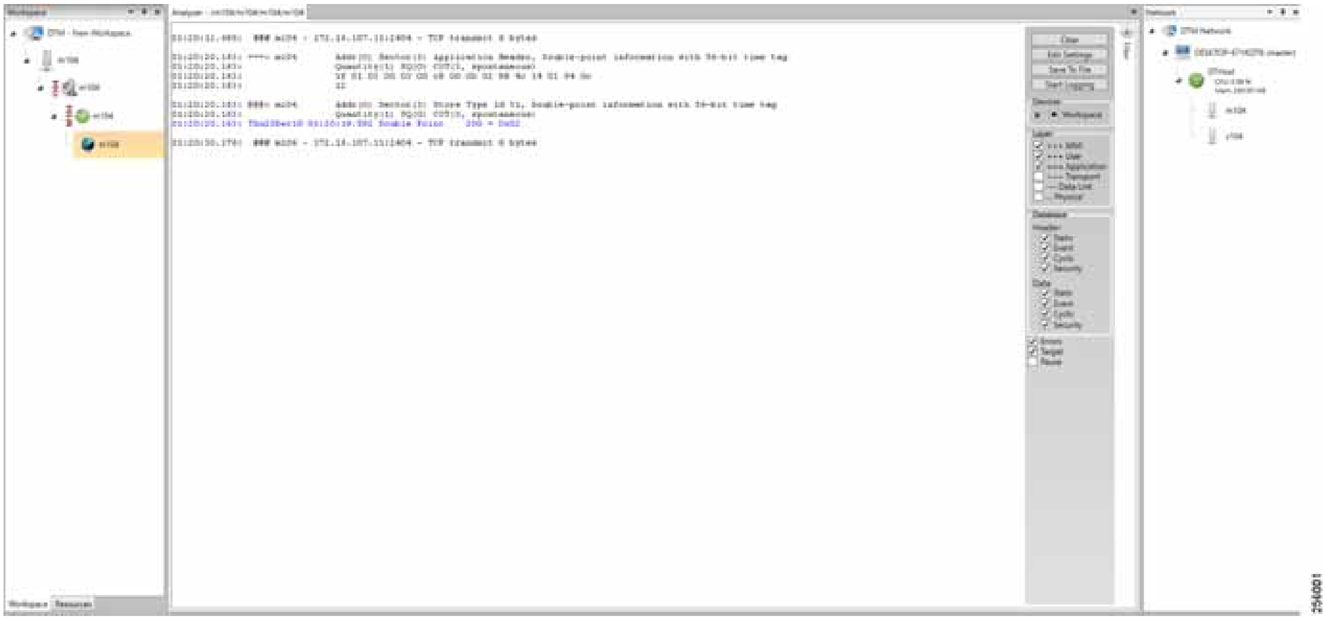
Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104

Figure 81 Change in Slave Register Value



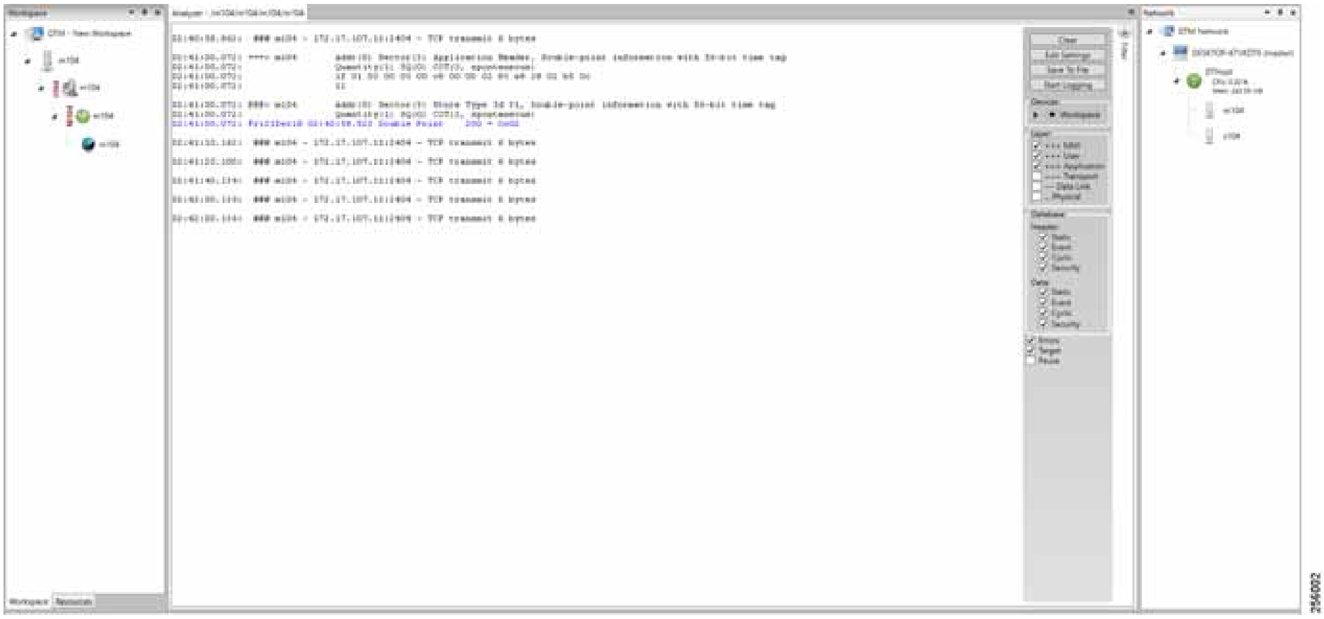
Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	On	Valid	12/20/2018 1:14:39 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	00000000000000	Valid	12/20/2018 1:14:38 AM		True	DTHost	s104	s104	s104	s104

Figure 82 CC-1 Master Analyzer after Change in Register Value



```
21:20:11.085:  ### m104 - 172.16.107.11:2404 - TCP transmit 0 bytes

21:20:20.143: ---> m104        ASDU(0) Sector(1) Application Header, Double-point information with 56-bit time tag
21:20:20.143:                  Quantity(1) SQ(0) COT(3, spontaneous)
21:20:20.143:                  [illegible]
21:20:20.143:                  [illegible]

21:20:20.143: ###> m104        ASDU(0) Sector(1) [illegible] Double-point information with 56-bit time tag
21:20:20.143:                  Quantity(1) SQ(0) COT(3, spontaneous)
21:20:20.143: [illegible] Double Point    200 = [illegible]

21:20:30.179:  ### m104 - 172.16.107.11:2404 - TCP transmit 0 bytes
```

Figure 83 CC-2 Master Analyzer after Change in Register Value



```
22:40:58.042:  ### m104 - 172.17.107.11:2404 - TCP transmit 0 bytes

22:41:00.072: ---> m104        ASDU(0) Sector(1) Application Header, Double-point information with 56-bit time tag
22:41:00.072:                  Quantity(1) SQ(0) COT(3, spontaneous)
22:41:00.072:                  [illegible]
22:41:00.072:                  [illegible]

22:41:00.072: ###> m104        ASDU(0) Sector(1) [illegible] Double-point information with 56-bit time tag
22:41:00.072:                  Quantity(1) SQ(0) COT(3, spontaneous)
22:41:00.072: [illegible] Double Point    200 = [illegible]

22:41:10.142:  ### m104 - 172.17.107.11:2404 - TCP transmit 0 bytes

22:41:20.100:  ### m104 - 172.17.107.11:2404 - TCP transmit 0 bytes

22:41:40.114:  ### m104 - 172.17.107.11:2404 - TCP transmit 0 bytes

22:42:00.114:  ### m104 - 172.17.107.11:2404 - TCP transmit 0 bytes

22:42:20.114:  ### m104 - 172.17.107.11:2404 - TCP transmit 0 bytes
```

Legacy SCADA (Raw Socket TCP)

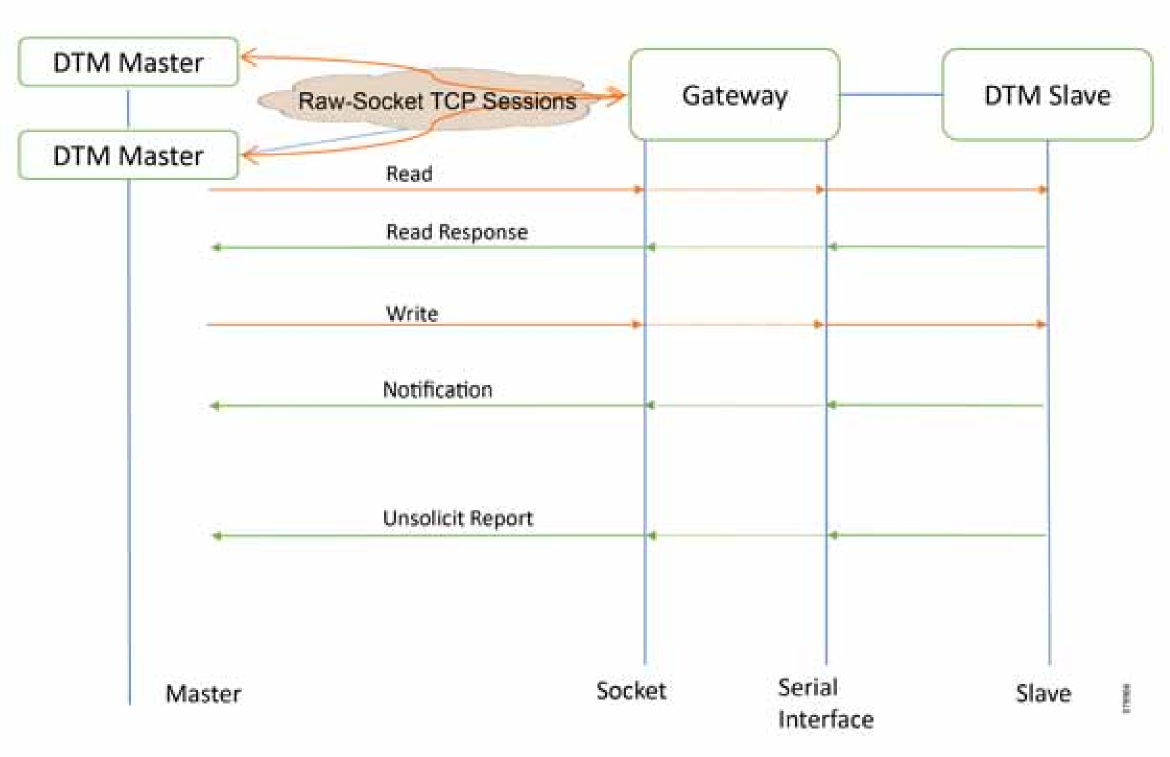
Protocol Validated

The protocol we have validated for this release is IEC 60870-5-101.

Flow Diagram

As shown in Figure 84, both the DTM Master can read and write the Slave via the DA Gateway over TCP Raw Socket, and the Slave can send the Report by Exception to both Masters via the DA Gateway over TCP Raw Socket:

Figure 84 T101 Control Flow



IR807 as Raw Socket Client

```
interface Async1
    no ip address
    encapsulation raw-tcp
!

line 4
/* Raw sockets to two different control centers */
    raw-socket tcp client 172.16.107.11 25000

    raw-socket tcp client 172.17.107.11 25000
    databits 8
    stopbits 1
    speed 9600 parity none
!
```

IR1101 as Raw Socket Client

```
interface Async0/2/0
   no ip address
   encapsulation raw-tcp
!

line 0/2/0
   raw-socket tcp client 172.16.107.11 25000
   raw-socket tcp client 172.17.107.11 25000
   databits 8
   stopbits 1
   speed 9600 parity none
!
```

SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Master. Report by Exception is sent to both Masters from the Slave.

Figure 85, Figure 86, Figure 87, and Figure 88 show the Poll operation from Dual SCADA Masters. Similarly, Control and Report by Exception can also be seen on both Master Analyzer logs.

Poll

The Poll operation is performed by both Masters. The Masters can execute a general Poll in which all the register values are read and sent to the Masters, a Poll on a set of registers or a Poll on a single register. In Figure 85, Figure 86, Figure 87, and Figure 88, we see a general Poll executed on the Slave side. Initially the Master Analyzer is empty; however, when the *General Interrogation* command is executed, the values of all the registers are displayed on both Masters+ analyzer of DTM.

Figure 85 CC-1 Master Analyzer Logs before Poll Operation

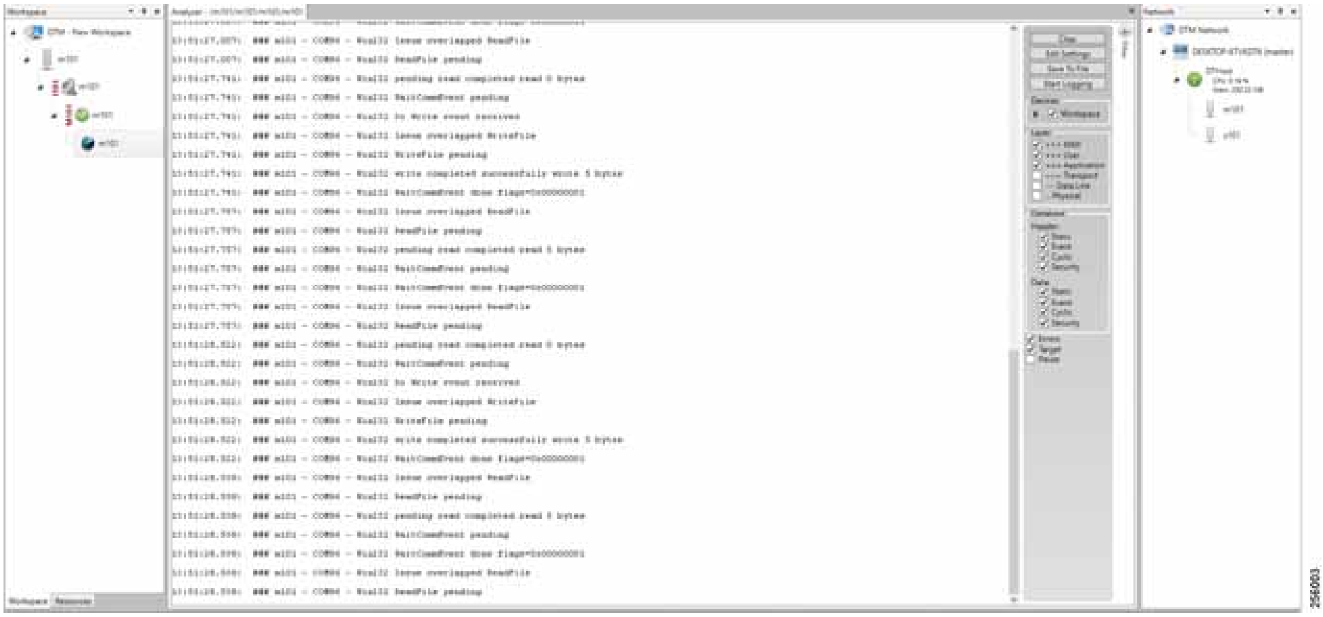
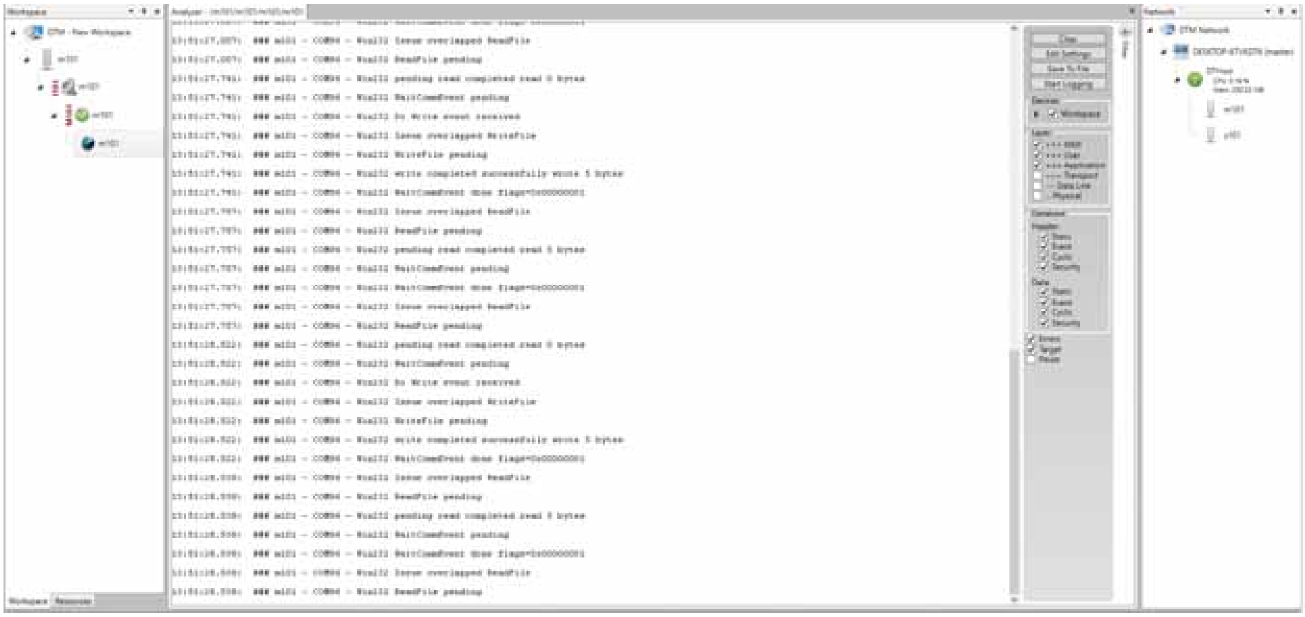


Figure 86 CC-2 Master Analyzer Logs before Poll Operation



```
13:51:27.707: ### m101 - COM84 - Win32 Issue overlapped ReadFile
13:51:27.707: ### m101 - COM84 - Win32 ReadFile pending
13:51:27.745: ### m101 - COM84 - Win32 pending read completed read 5 bytes
13:51:27.745: ### m101 - COM84 - Win32 WaitCommEvent pending
13:51:27.745: ### m101 - COM84 - Win32 Do Write event received
13:51:27.745: ### m101 - COM84 - Win32 Issue overlapped WriteFile
13:51:27.745: ### m101 - COM84 - Win32 WriteFile pending
13:51:27.745: ### m101 - COM84 - Win32 write completed successfully wrote 5 bytes
13:51:27.745: ### m101 - COM84 - Win32 WaitCommEvent done flags=0x00000001
13:51:27.787: ### m101 - COM84 - Win32 Issue overlapped ReadFile
13:51:27.787: ### m101 - COM84 - Win32 ReadFile pending
13:51:27.787: ### m101 - COM84 - Win32 pending read completed read 5 bytes
13:51:27.787: ### m101 - COM84 - Win32 WaitCommEvent pending
13:51:27.787: ### m101 - COM84 - Win32 WaitCommEvent done flags=0x00000001
13:51:27.787: ### m101 - COM84 - Win32 Issue overlapped ReadFile
13:51:27.787: ### m101 - COM84 - Win32 ReadFile pending
13:51:28.522: ### m101 - COM84 - Win32 pending read completed read 5 bytes
13:51:28.522: ### m101 - COM84 - Win32 WaitCommEvent pending
13:51:28.522: ### m101 - COM84 - Win32 Do Write event received
13:51:28.522: ### m101 - COM84 - Win32 Issue overlapped WriteFile
13:51:28.522: ### m101 - COM84 - Win32 WriteFile pending
13:51:28.522: ### m101 - COM84 - Win32 write completed successfully wrote 5 bytes
13:51:28.522: ### m101 - COM84 - Win32 WaitCommEvent done flags=0x00000001
13:51:28.538: ### m101 - COM84 - Win32 Issue overlapped ReadFile
13:51:28.538: ### m101 - COM84 - Win32 ReadFile pending
13:51:28.538: ### m101 - COM84 - Win32 pending read completed read 5 bytes
13:51:28.538: ### m101 - COM84 - Win32 WaitCommEvent pending
13:51:28.538: ### m101 - COM84 - Win32 WaitCommEvent done flags=0x00000001
13:51:28.538: ### m101 - COM84 - Win32 Issue overlapped ReadFile
13:51:28.538: ### m101 - COM84 - Win32 ReadFile pending
```

Clear | Edit Settings | Save To File | Start Logging

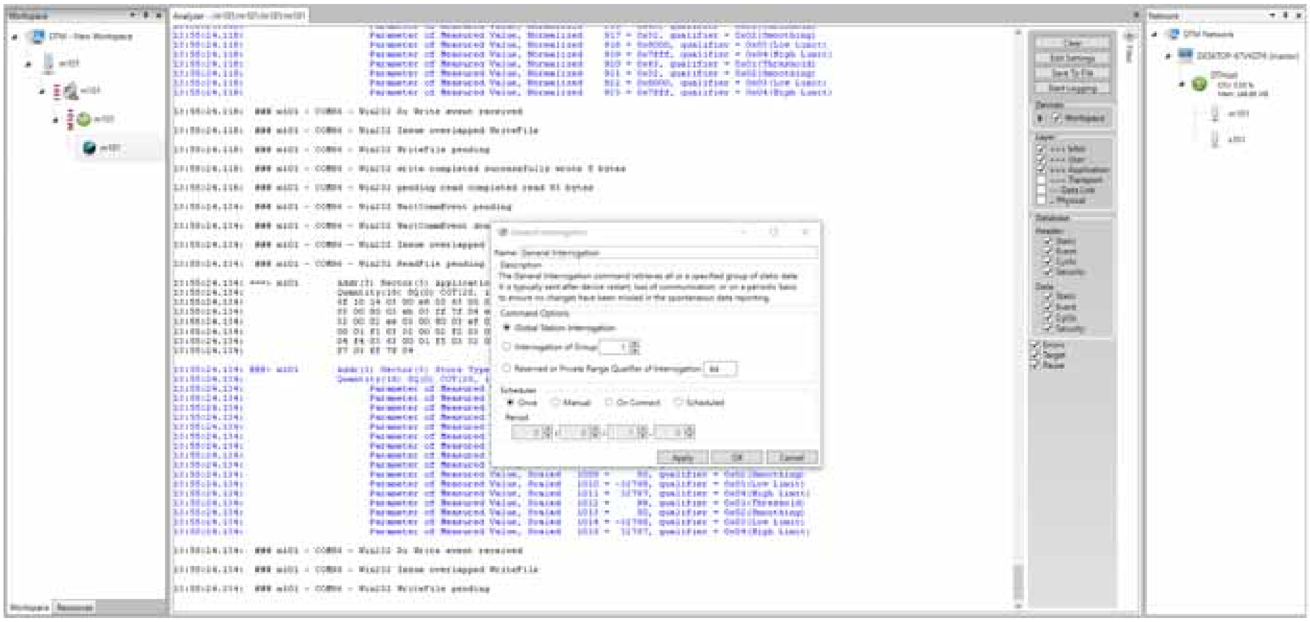
Devices: ☑ Workspace

Layer: ☑ <<-> Info ☑ <<-> User ☑ <<-> Application ☐ ---- Transport ☐ -- Data Link ☐ - Physical

Database — Header: ☑ Static ☑ Event ☑ Cyclic ☑ Security; Data: ☑ Static ☑ Event ☑ Cyclic ☑ Security

☑ Errors ☑ Target ☐ Pause

Figure 87 CC-1 Master Analyzer Logs after Poll Operation



```
13:55:24.118:                     Parameter of Measured Value, Normalized   917 = 0x01,   qualifier = 0x02(Smoothing)
13:55:24.118:                     Parameter of Measured Value, Normalized   918 = 0x8000, qualifier = 0x03(Low Limit)
13:55:24.118:                     Parameter of Measured Value, Normalized   919 = 0x7fff, qualifier = 0x04(High Limit)
13:55:24.118:                     Parameter of Measured Value, Normalized   920 = 0x01,   qualifier = 0x01(Threshold)
13:55:24.118:                     Parameter of Measured Value, Normalized   921 = 0x01,   qualifier = 0x02(Smoothing)
13:55:24.118:                     Parameter of Measured Value, Normalized   922 = 0x8000, qualifier = 0x03(Low Limit)
13:55:24.118:                     Parameter of Measured Value, Normalized   923 = 0x7fff, qualifier = 0x04(High Limit)

13:55:24.118: ### m101 - COM84 - Win32 Do Write event received
13:55:24.118: ### m101 - COM84 - Win32 Issue overlapped WriteFile
13:55:24.118: ### m101 - COM84 - Win32 WriteFile pending
13:55:24.118: ### m101 - COM84 - Win32 write completed successfully wrote 7 bytes
13:55:24.118: ### m101 - COM84 - Win32 pending read completed read 93 bytes
13:55:24.134: ### m101 - COM84 - Win32 WaitCommEvent pending
13:55:24.134: ### m101 - COM84 - Win32 WaitCommEvent don
13:55:24.134: ### m101 - COM84 - Win32 Issue overlapped
13:55:24.134: ### m101 - COM84 - Win32 ReadFile pending

13:55:24.134: <<<- m101       ASDU(1) Sector(1) Applicatio
13:55:24.134:                 Quantity(18) SQ(0) COT(20, 
13:55:24.134:                 68 10 14 01 00 a8 00 41 00 0
13:55:24.134:                 f0 00 00 01 eb 01 ff 7f 04 e
13:55:24.134:                 f2 00 02 ee 03 00 80 03 ef 0
13:55:24.134:                 00 01 f1 03 02 00 02 f2 03 0
13:55:24.134:                 04 f4 03 42 00 01 f5 03 02 0
13:55:24.134:                 f7 03 ff 7f 04

13:55:24.134: ###- m101       Addr(1) Sector(1) Store Type
13:55:24.134:                 Quantity(18) SQ(0) COT(20, 
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured
13:55:24.134:                     Parameter of Measured Value, Scaled   1009 =     50, qualifier = 0x02(Smoothing)
13:55:24.134:                     Parameter of Measured Value, Scaled   1010 = -32768, qualifier = 0x03(Low Limit)
13:55:24.134:                     Parameter of Measured Value, Scaled   1011 =  32767, qualifier = 0x04(High Limit)
13:55:24.134:                     Parameter of Measured Value, Scaled   1012 =     99, qualifier = 0x01(Threshold)
13:55:24.134:                     Parameter of Measured Value, Scaled   1013 =     50, qualifier = 0x02(Smoothing)
13:55:24.134:                     Parameter of Measured Value, Scaled   1014 = -32768, qualifier = 0x03(Low Limit)
13:55:24.134:                     Parameter of Measured Value, Scaled   1015 =  32767, qualifier = 0x04(High Limit)

13:55:24.134: ### m101 - COM84 - Win32 Do Write event received
13:55:24.134: ### m101 - COM84 - Win32 Issue overlapped WriteFile
13:55:24.134: ### m101 - COM84 - Win32 WriteFile pending
```

General Interrogation

Name: General Interrogation

Description

The General Interrogation command retrieves all or a specified group of static data. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure no changes have been missed in the spontaneous data reporting.

Command Options

● Global Station Interrogation

○ Interrogation of Group 1

○ Reserved or Private Range Qualifier of Interrogation 64

Schedule

● Once ○ Manual ○ On Connect ○ Scheduled

Period

Apply | OK | Cancel

Clear | Edit Settings | Save To File | Start Logging

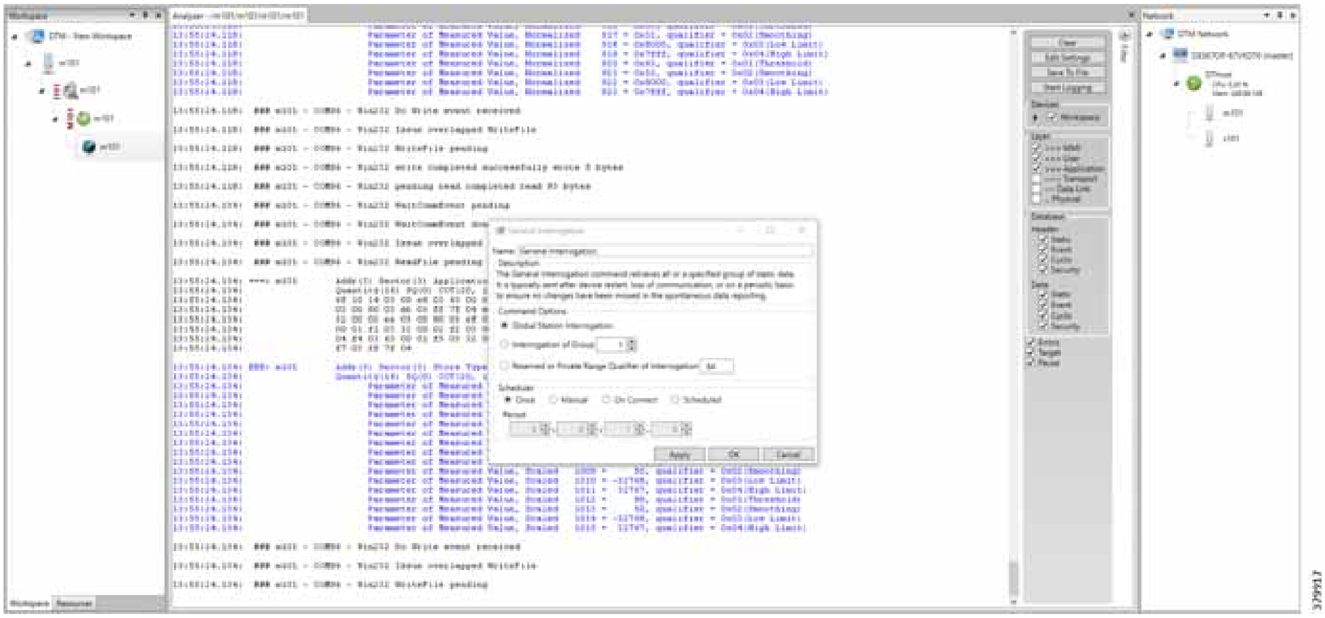
Devices: ☑ Workspace

Layer: ☑ <<-> Info ☑ <<-> User ☑ <<-> Application ☐ ---- Transport ☐ -- Data Link ☐ - Physical

Database — Header: ☑ Static ☑ Event ☑ Cyclic ☑ Security; Data: ☑ Static ☑ Event ☑ Cyclic ☑ Security

☑ Errors ☑ Target ☑ Pause

Figure 88 CC-2 Master Analyzer Logs after Poll Operation



```
13:55:24.118:                  Parameter of Measured Value, Normalized   817 = 0x01, qualifier = 0x02(Smoothing)
13:55:24.118:                  Parameter of Measured Value, Normalized   818 = 0x8000, qualifier = 0x03(Low Limit)
13:55:24.118:                  Parameter of Measured Value, Normalized   819 = 0x7fff, qualifier = 0x04(High Limit)
13:55:24.118:                  Parameter of Measured Value, Normalized   820 = 0x01, qualifier = 0x01(Threshold)
13:55:24.118:                  Parameter of Measured Value, Normalized   821 = 0x01, qualifier = 0x02(Smoothing)
13:55:24.118:                  Parameter of Measured Value, Normalized   822 = 0x8000, qualifier = 0x03(Low Limit)
13:55:24.118:                  Parameter of Measured Value, Normalized   823 = 0x7fff, qualifier = 0x04(High Limit)

13:55:24.118:  ### m101 - COM6 - Win232 Do Write event received

13:55:24.118:  ### m101 - COM6 - Win232 Issue overlapped WriteFile

13:55:24.118:  ### m101 - COM6 - Win232 WriteFile pending

13:55:24.118:  ### m101 - COM6 - Win232 write completed successfully wrote 5 bytes

13:55:24.118:  ### m101 - COM6 - Win232 pending read completed read 83 bytes

13:55:24.134:  ### m101 - COM6 - Win232 WaitCommEvent pending

13:55:24.134:  ### m101 - COM6 - Win232 WaitCommEvent [illegible]

13:55:24.134:  ### m101 - COM6 - Win232 Issue overlapped [illegible]

13:55:24.134:  ### m101 - COM6 - Win232 ReadFile pending

13:55:24.134: <<<: m101        Addr(1) Sector(1) Application [illegible]
13:55:24.134:                  Quantity(16) SQ(0) COT(20, [illegible]
13:55:24.134:                  [illegible]
13:55:24.134:                  [illegible]
13:55:24.134:                  [illegible]
13:55:24.134:                  [illegible]
13:55:24.134:                  [illegible]
13:55:24.134:                  [illegible]

13:55:24.134: <<<: m101        Addr(1) Sector(1) Mtype Type [illegible]
13:55:24.134:                  Quantity(16) SQ(0) COT(20, [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured [illegible]
13:55:24.134:                  Parameter of Measured Value, Scaled   1009 =     50, qualifier = 0x02(Smoothing)
13:55:24.134:                  Parameter of Measured Value, Scaled   1010 = -32768, qualifier = 0x03(Low Limit)
13:55:24.134:                  Parameter of Measured Value, Scaled   1011 =  32767, qualifier = 0x04(High Limit)
13:55:24.134:                  Parameter of Measured Value, Scaled   1012 =     99, qualifier = 0x01(Threshold)
13:55:24.134:                  Parameter of Measured Value, Scaled   1013 =     50, qualifier = 0x02(Smoothing)
13:55:24.134:                  Parameter of Measured Value, Scaled   1014 = -32768, qualifier = 0x03(Low Limit)
13:55:24.134:                  Parameter of Measured Value, Scaled   1015 =  32767, qualifier = 0x04(High Limit)

13:55:24.134:  ### m101 - COM6 - Win232 Do Write event received

13:55:24.134:  ### m101 - COM6 - Win232 Issue overlapped WriteFile

13:55:24.134:  ### m101 - COM6 - Win232 WriteFile pending
```

General Interrogation

Name: General Interrogation

Description

The General Interrogation command retrieves all or a specified group of static data. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure no changes have been missed in the spontaneous data reporting.

Command Options

● Global Station Interrogation

○ Interrogation of Group 1

○ Reserved or Private Range Qualifier of Interrogation 64

Schedule

● Once ○ Manual ○ On Connect ○ Scheduled

Period

Apply OK Cancel

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 Double Point Register (#200) is changed and the same is reported to both Masters. Figure 89, Figure 90, Figure 91, Figure 92, and Figure 93 show the Report by Exception sent to the Master for a particular register:

Figure 89 Slave Register before Control Operation

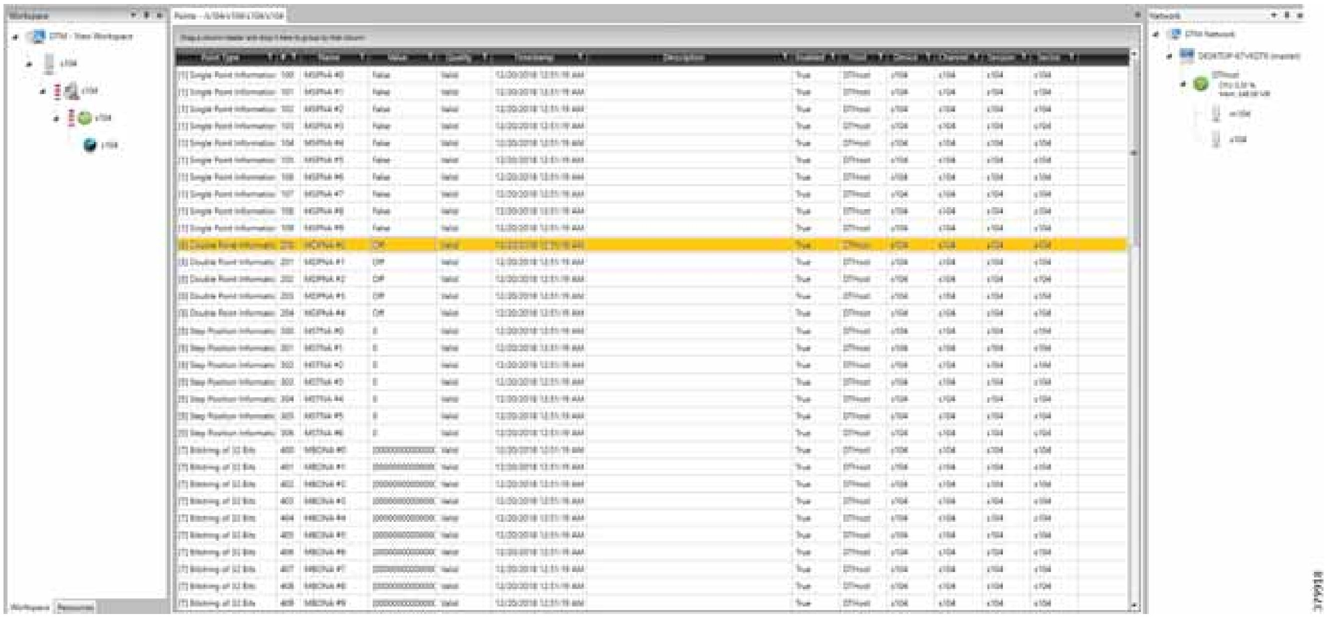


Figure 90 CC-1 Master Control Operation

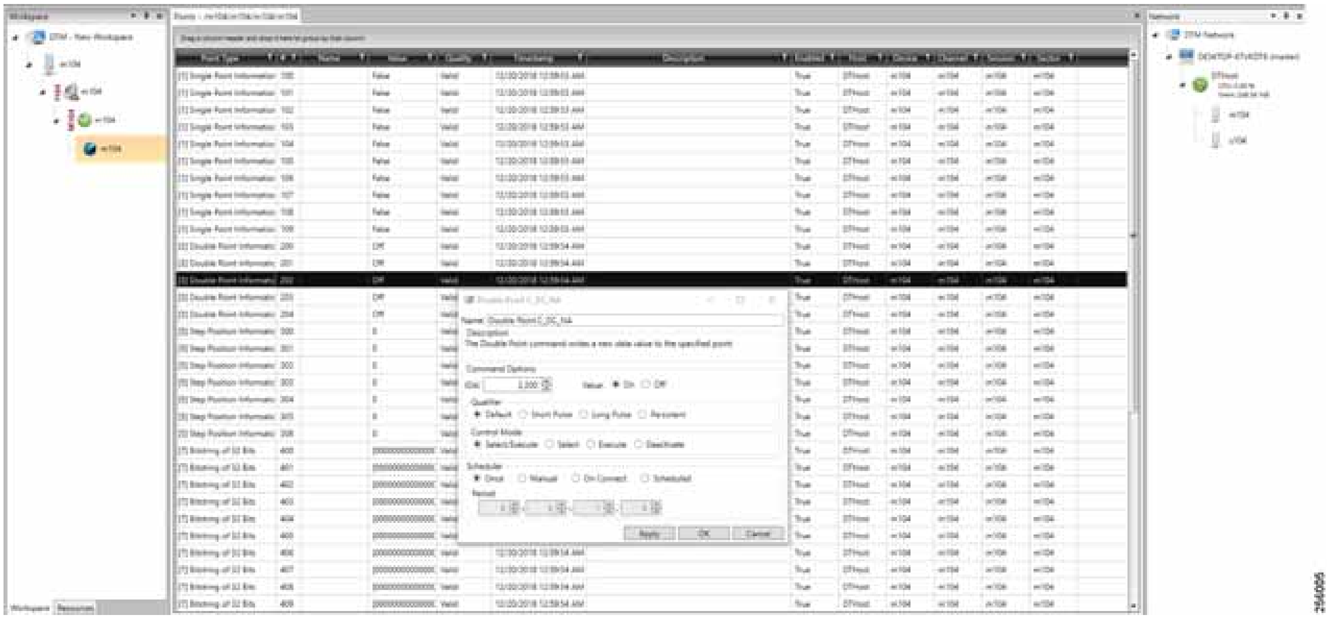
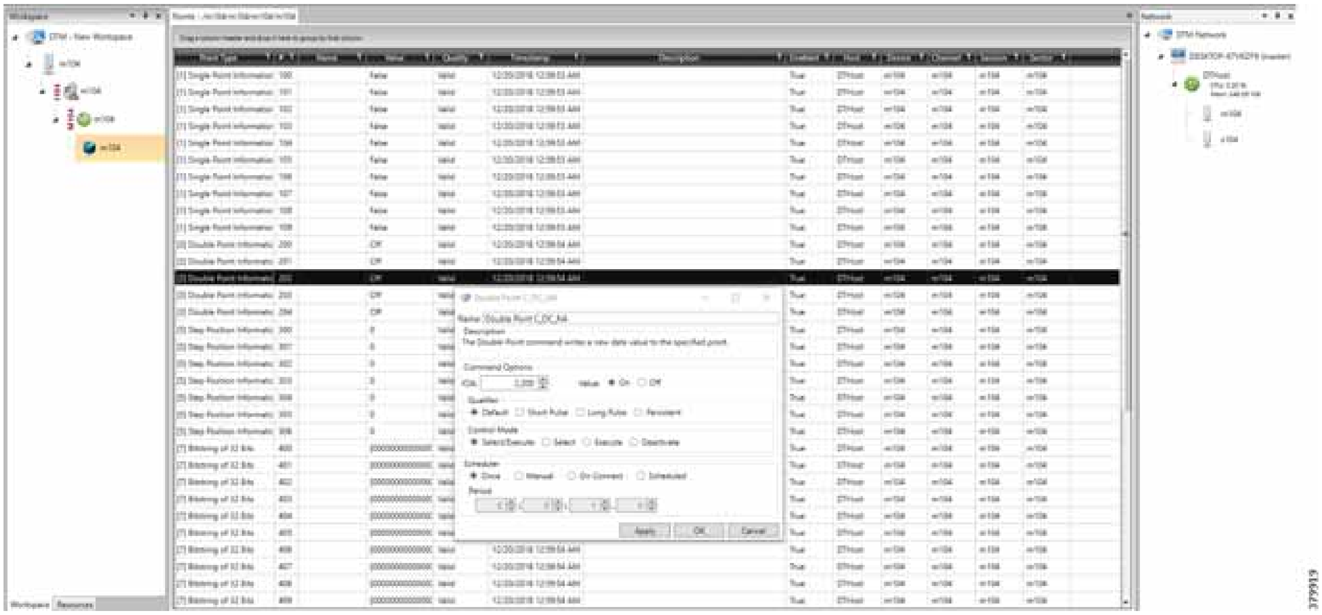


Figure 91 CC-2 Master Control Operation



Name: Double Point C_DC_NA

Description

The Double Point command writes a new data value to the specified point.

Command Options

IOA: 2,202 Value: ● On ○ Off

Qualifier

● Default ○ Short Pulse ○ Long Pulse ○ Persistent

Control Mode

● Select/Execute ○ Select ○ Execute ○ Deactivate

Scheduler

● Once ○ Manual ○ On Connect ○ Scheduled

Period

Figure 92 CC-1 Slave Register after Control Operation

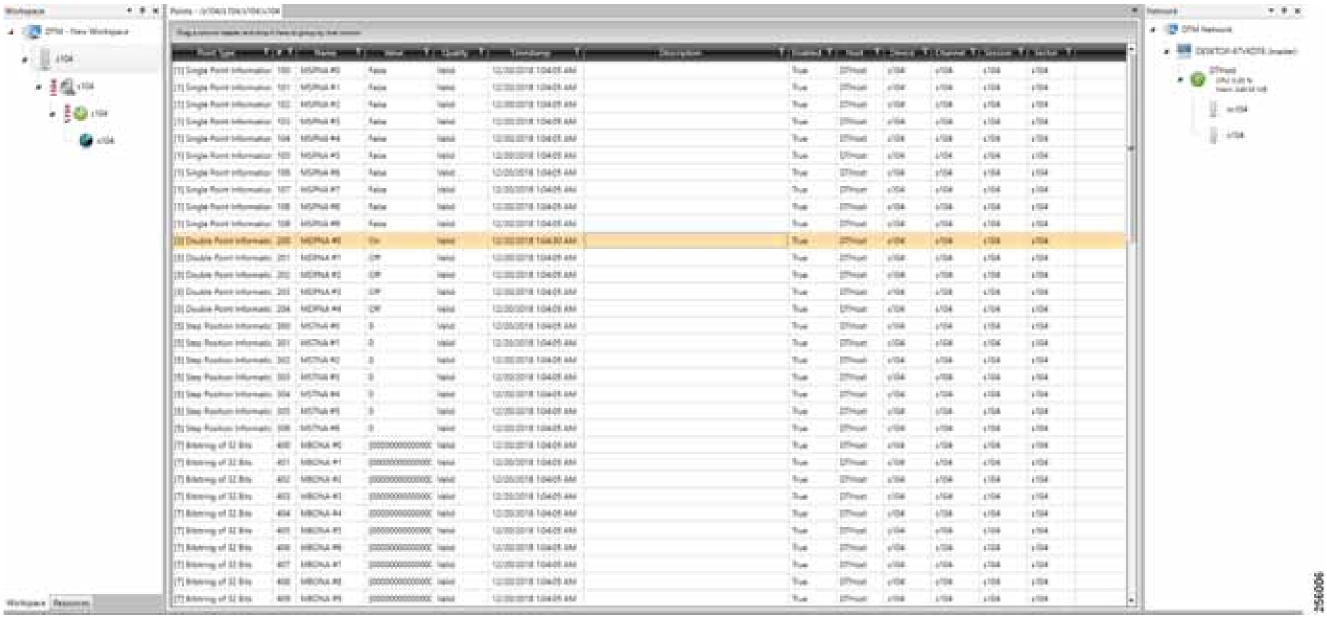
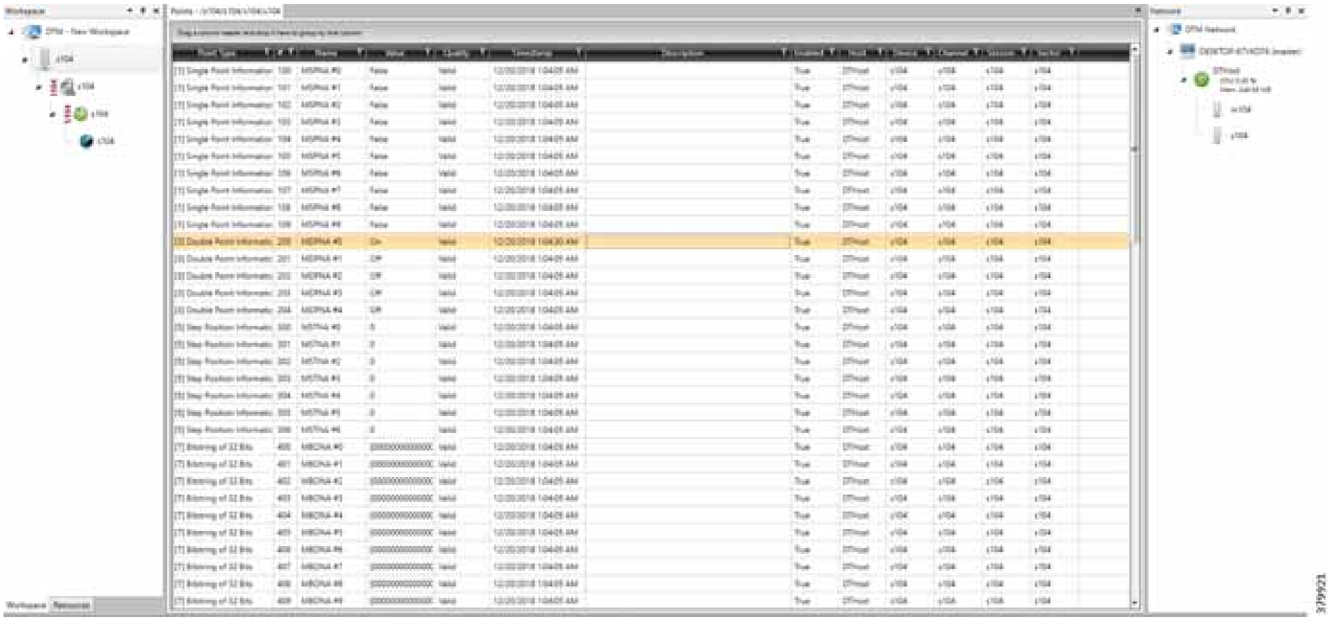


Figure 93 CC-2 Slave Register after Control Operation

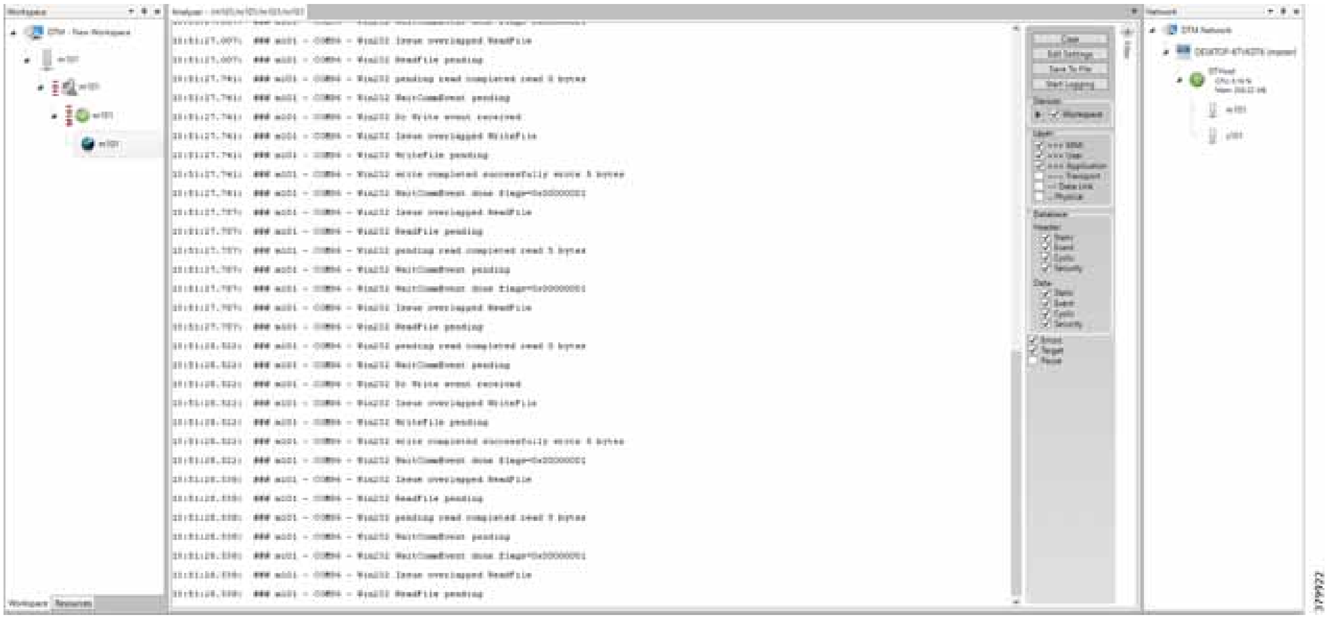

Workspace
DTM - New Workspace
s104
Points - /s104/s104/s104/s104
Drag a column header and drop it here to group by that column
Network
DTM Network
DESKTOP-
DTHost
Workspace
Resources
379921

Point Type	IOA	Name	Value	Quality	TimeStamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	200	MDPNA #0	On	Valid	12/20/2018 1:04:30 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	201	MDPNA #1	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	202	MDPNA #2	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	203	MDPNA #3	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	204	MDPNA #4	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	300	MSTNA #0	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	301	MSTNA #1	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	302	MSTNA #2	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	303	MSTNA #3	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	304	MSTNA #4	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	305	MSTNA #5	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	306	MSTNA #6	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	00000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104

Report by Exception

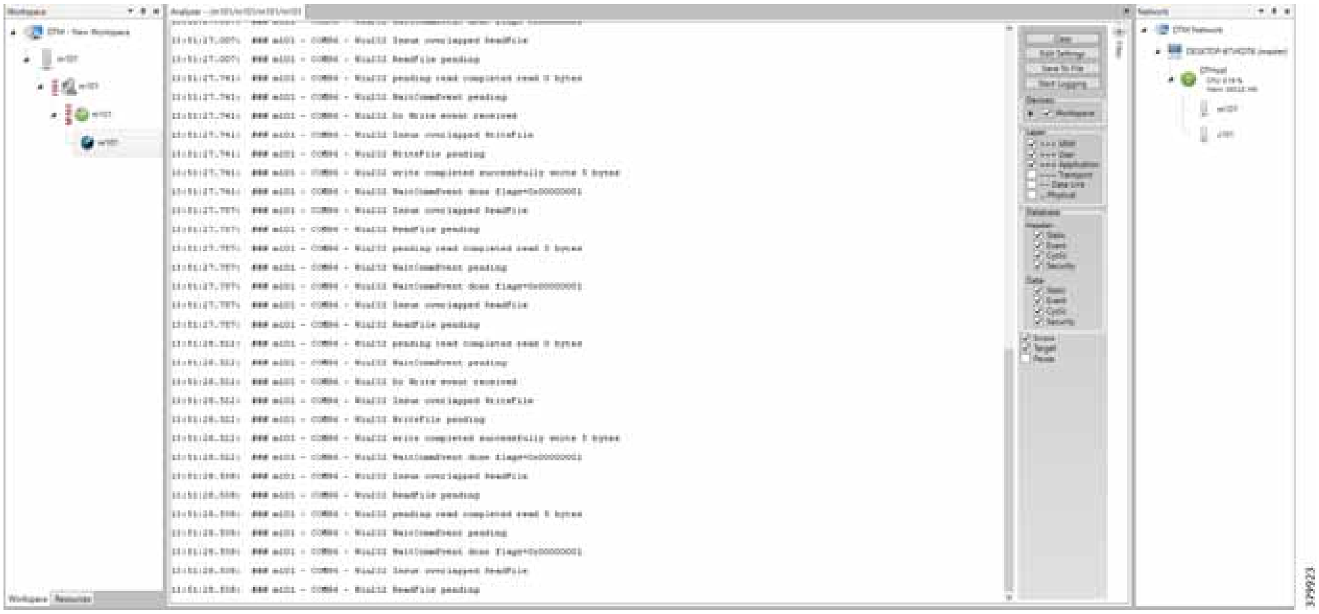
Report by Exception is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register are reported to the SCADA-Master. This notification can be seen on the Master Analyzer of DTM software. Figure 94, Figure 95, Figure 96, Figure 97, Figure 98, and Figure 99 show the Report by Exception on the analyzer. The other operations such as Poll and Control can be executed, and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to both Masters. Figure 94, Figure 95, Figure 96, Figure 97, Figure 98, and Figure 99 show the Report by Exception sent to both Masters for a particular register:

Figure 94 CC-1 Master Analyzer



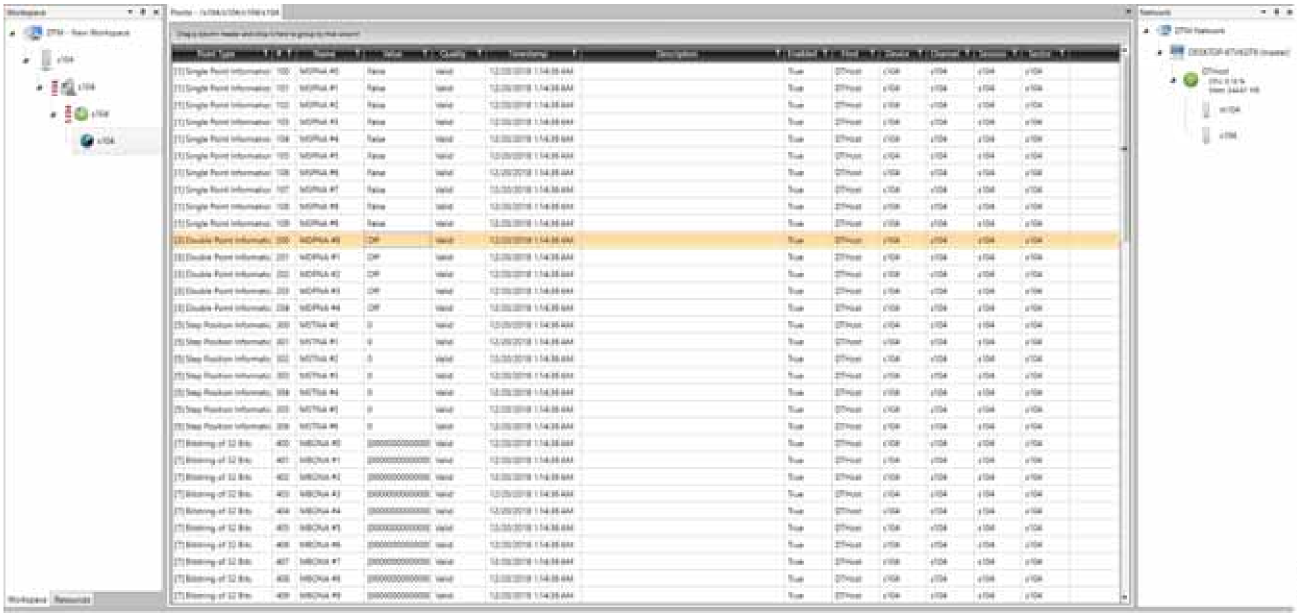
```
15:51:27.007: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:27.007: ### mi01 - COM4 - Win32 ReadFile pending
15:51:27.761: ### mi01 - COM4 - Win32 pending read completed read 8 bytes
15:51:27.761: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:27.761: ### mi01 - COM4 - Win32 Tx Write event received
15:51:27.761: ### mi01 - COM4 - Win32 Issue overlapped WriteFile
15:51:27.761: ### mi01 - COM4 - Win32 WriteFile pending
15:51:27.761: ### mi01 - COM4 - Win32 write completed successfully wrote 5 bytes
15:51:27.761: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:27.787: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:27.787: ### mi01 - COM4 - Win32 ReadFile pending
15:51:27.787: ### mi01 - COM4 - Win32 pending read completed read 5 bytes
15:51:27.787: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:27.787: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:27.787: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:27.787: ### mi01 - COM4 - Win32 ReadFile pending
15:51:28.512: ### mi01 - COM4 - Win32 pending read completed read 8 bytes
15:51:28.512: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:28.512: ### mi01 - COM4 - Win32 Tx Write event received
15:51:28.512: ### mi01 - COM4 - Win32 Issue overlapped WriteFile
15:51:28.512: ### mi01 - COM4 - Win32 WriteFile pending
15:51:28.512: ### mi01 - COM4 - Win32 write completed successfully wrote 5 bytes
15:51:28.512: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:28.538: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:28.538: ### mi01 - COM4 - Win32 ReadFile pending
15:51:28.538: ### mi01 - COM4 - Win32 pending read completed read 5 bytes
15:51:28.538: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:28.538: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:28.538: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:28.538: ### mi01 - COM4 - Win32 ReadFile pending
```

Figure 95 CC-2 Master Analyzer



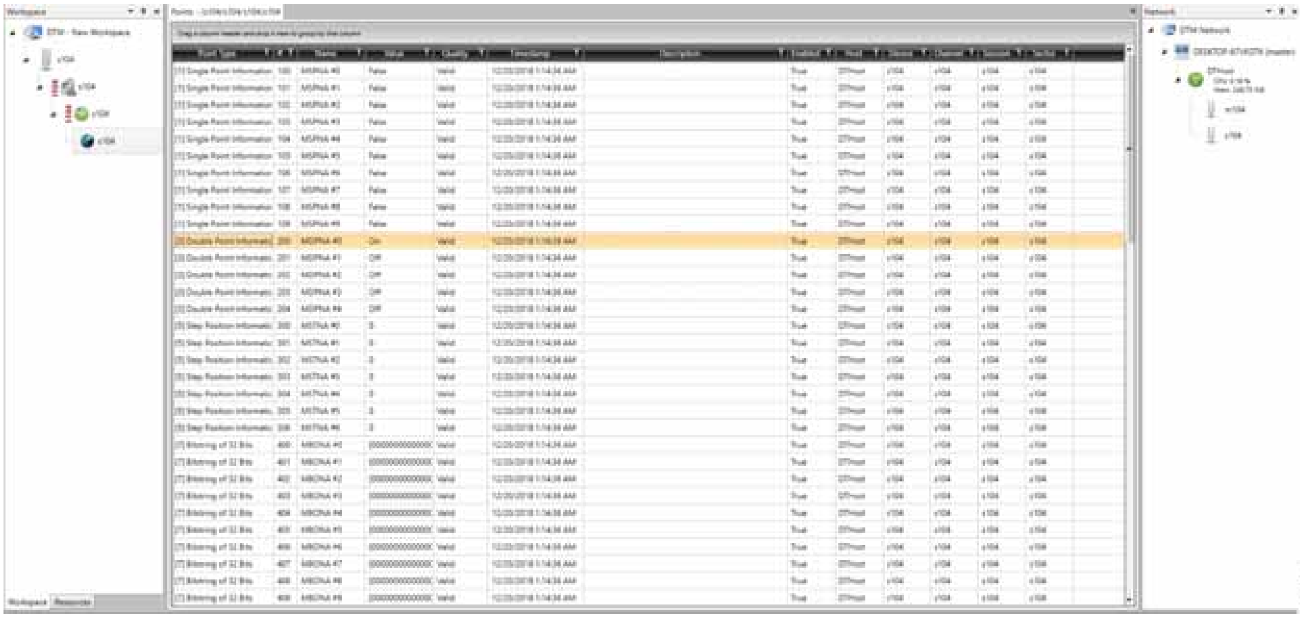
```
15:51:27.007: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:27.007: ### mi01 - COM4 - Win32 ReadFile pending
15:51:27.761: ### mi01 - COM4 - Win32 pending read completed read 8 bytes
15:51:27.761: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:27.761: ### mi01 - COM4 - Win32 Tx Write event received
15:51:27.761: ### mi01 - COM4 - Win32 Issue overlapped WriteFile
15:51:27.761: ### mi01 - COM4 - Win32 WriteFile pending
15:51:27.761: ### mi01 - COM4 - Win32 write completed successfully wrote 5 bytes
15:51:27.761: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:27.787: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:27.787: ### mi01 - COM4 - Win32 ReadFile pending
15:51:27.787: ### mi01 - COM4 - Win32 pending read completed read 5 bytes
15:51:27.787: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:27.787: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:27.787: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:27.787: ### mi01 - COM4 - Win32 ReadFile pending
15:51:28.512: ### mi01 - COM4 - Win32 pending read completed read 8 bytes
15:51:28.512: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:28.512: ### mi01 - COM4 - Win32 Tx Write event received
15:51:28.512: ### mi01 - COM4 - Win32 Issue overlapped WriteFile
15:51:28.512: ### mi01 - COM4 - Win32 WriteFile pending
15:51:28.512: ### mi01 - COM4 - Win32 write completed successfully wrote 5 bytes
15:51:28.512: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:28.538: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:28.538: ### mi01 - COM4 - Win32 ReadFile pending
15:51:28.538: ### mi01 - COM4 - Win32 pending read completed read 5 bytes
15:51:28.538: ### mi01 - COM4 - Win32 WaitCommEvent pending
15:51:28.538: ### mi01 - COM4 - Win32 WaitCommEvent done flags=0x00000001
15:51:28.538: ### mi01 - COM4 - Win32 Issue overlapped ReadFile
15:51:28.538: ### mi01 - COM4 - Win32 ReadFile pending
```

Figure 96 Slave Registers



Point Type	#	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	MSPNA #0	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	101	MSPNA #1	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	102	MSPNA #2	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	103	MSPNA #3	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	104	MSPNA #4	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	105	MSPNA #5	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	106	MSPNA #6	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	107	MSPNA #7	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	108	MSPNA #8	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	109	MSPNA #9	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104

Figure 97 Change in Slave Register Value



Point Type	#	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	MDPNA #0	On	Valid	12/20/2018 1:16:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	MDPNA #1	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	MDPNA #2	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	MDPNA #3	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	MDPNA #4	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	MSTNA #0	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	MSTNA #1	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	MSTNA #2	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	MSTNA #3	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	MSTNA #4	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	MSTNA #5	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	MSTNA #6	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	[00000000000000	Valid	12/20/2018 1:14:36 AM		True	DTHost	s104	s104	s104	s104

Figure 98 CC-1 Master Analyzer after Change in Register Value

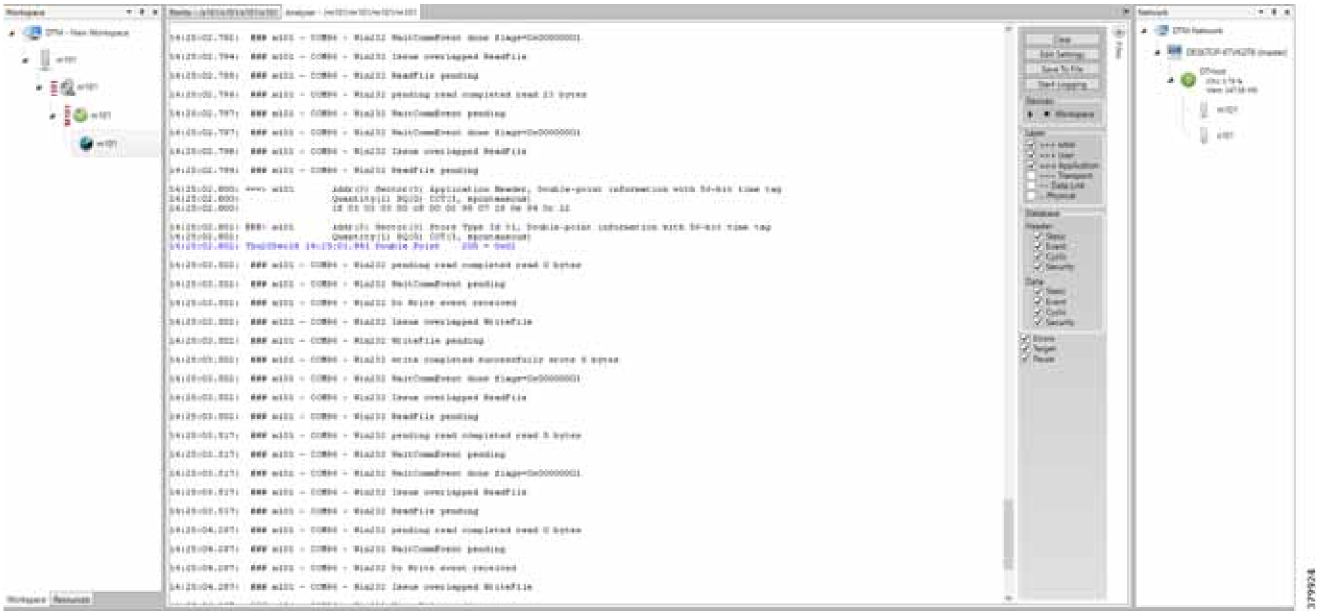
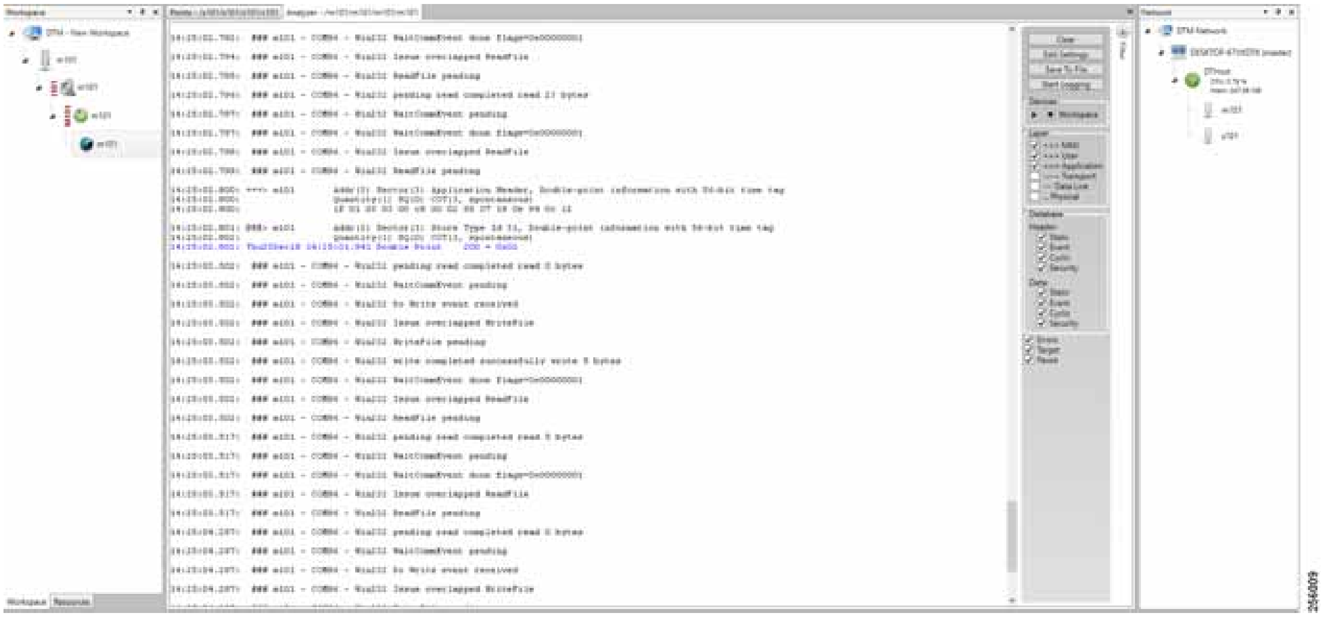


Figure 99 CC-2 Master Analyzer after Change in Register Value

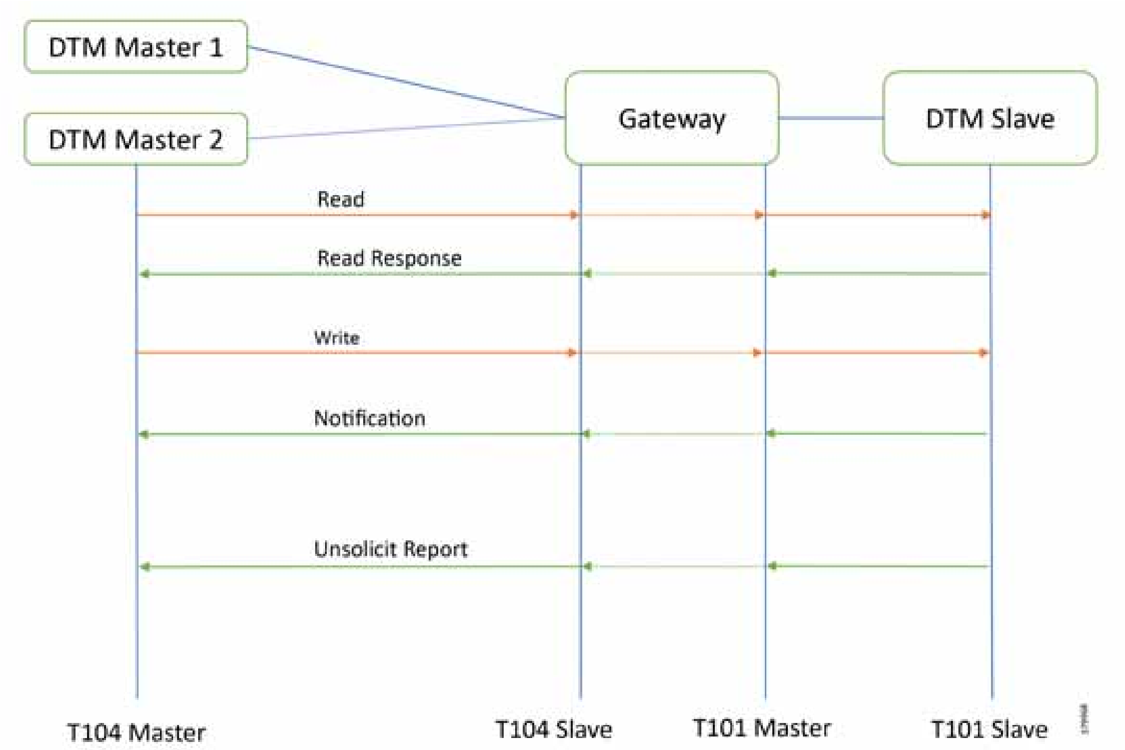


SCADA Gateway

Protocol Validated

The protocol we have validated for this release is IEC 60870-5-101 and IEC 60870-5-104.

Figure 100 T101 to T104 Protocol Translation Control Flow



As shown in Figure 100, both DTM Masters can read and write the Slave via the DA Gateway using protocol translation, and the Slave can send the Report by Exception to both Masters via the DA Gateway using protocol translation.

IR807 SCADA Protocol Translation

```
interface Async1
    no ip address
    encapsulation scada
!

line 4
    databits 8
    stopbits 1
    speed 9600 parity none
!

scada-gw protocol t101
    channel t101_ch1
    link-addr-size two
    bind-to-interface Async1
session t101_session1
    attach-to-channel t101_ch1
sector t101_sector1
    attach-to-session t101_session1
scada-gw protocol t104
```

```
    channel t104_ch1
    t3-timeout 20
    tcp-connection 0 local-port 25000 remote-ip any
    tcp-connection 1 local-port 25001 remote-ip any
session t104_session1
    attach-to-channel t104_ch1 sector t104_sector1
    attach-to-session t104_session1
    map-to-sector t101_sector1
scada-gw enable
```

IR1101 SCADA Protocol Translation

```
interface Async0/2/0
    no ip address
    encapsulation scada
!

line 0/2/0
    databits 8
    stopbits 1
    speed 9600
    parity none
!

scada-gw protocol t101
channel t101_ch1
    link-addr-size two
    bind-to-interface Async0/2/0
session t101_session1
    attach-to-channel t101_ch1
sector t101_sector1
    attach-to-session t101_session1
scada-gw protocol t104
channel t104_ch1
    t3-timeout 20
    tcp-connection 0 local-port 25000 remote-ip any
    tcp-connection 1 local-port 25001 remote-ip any
session t104_session1
    attach-to-channel t104_ch1
sector t104_sector1
    attach-to-session t104_session1
    map-to-sector t101_sector1
scada-gw enable
```

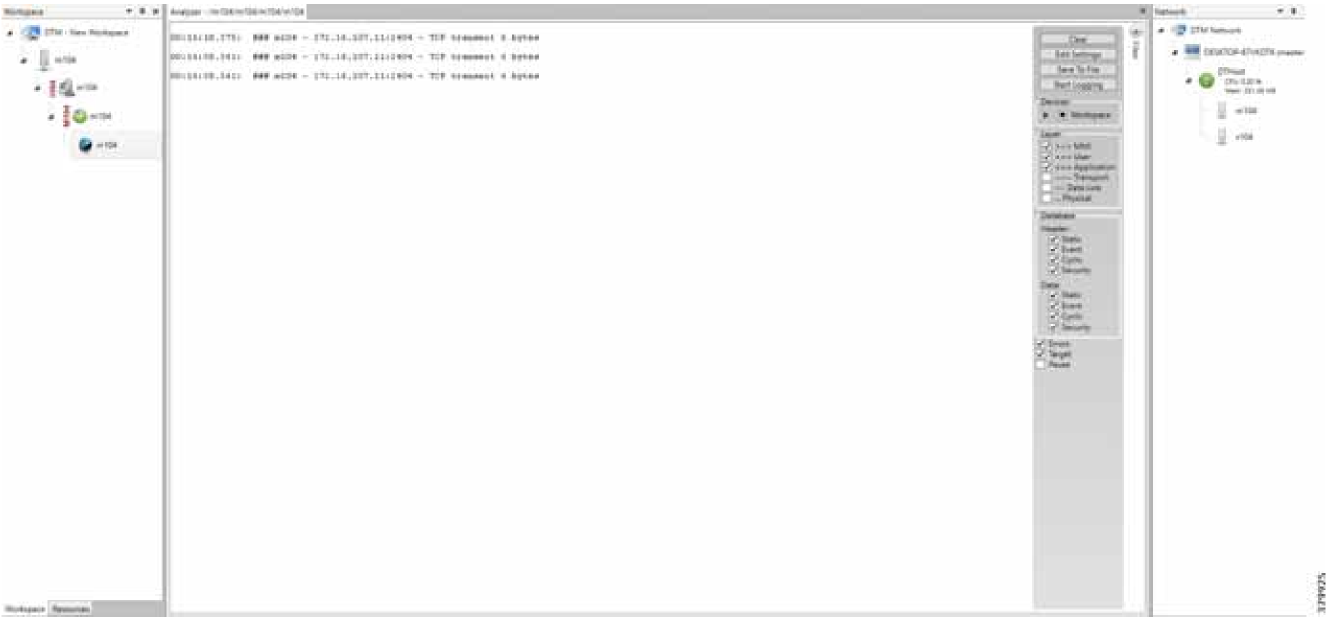
SCADA Operations

The Master and the Slave can communicate via the network. Poll and Control operations are initiated from the Masters. Report by Exception is sent to both Masters from the Slave. Figure 101, Figure 102, Figure 103, and Figure 104 show the Poll operation from Dual SCADA-Masters. Similarly, Control and Report by Exception can also be seen on both 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, a Poll on a set of registers, or a Poll on a single register. In Figure 101, Figure 102, Figure 103, and Figure 104, we see a general Poll executed on the Slave side. Initially the Master Analyzer is empty; however, when the *General Interrogation* command is executed, the values of all the registers are displayed on both Master Analyzer of DTM.

Figure 101 CC-1 Master Analyzer Logs before Poll Operation



```
[illegible] ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
[illegible] ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
[illegible] ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

Figure 102 CC-2 Master Analyzer Logs before Poll Operation

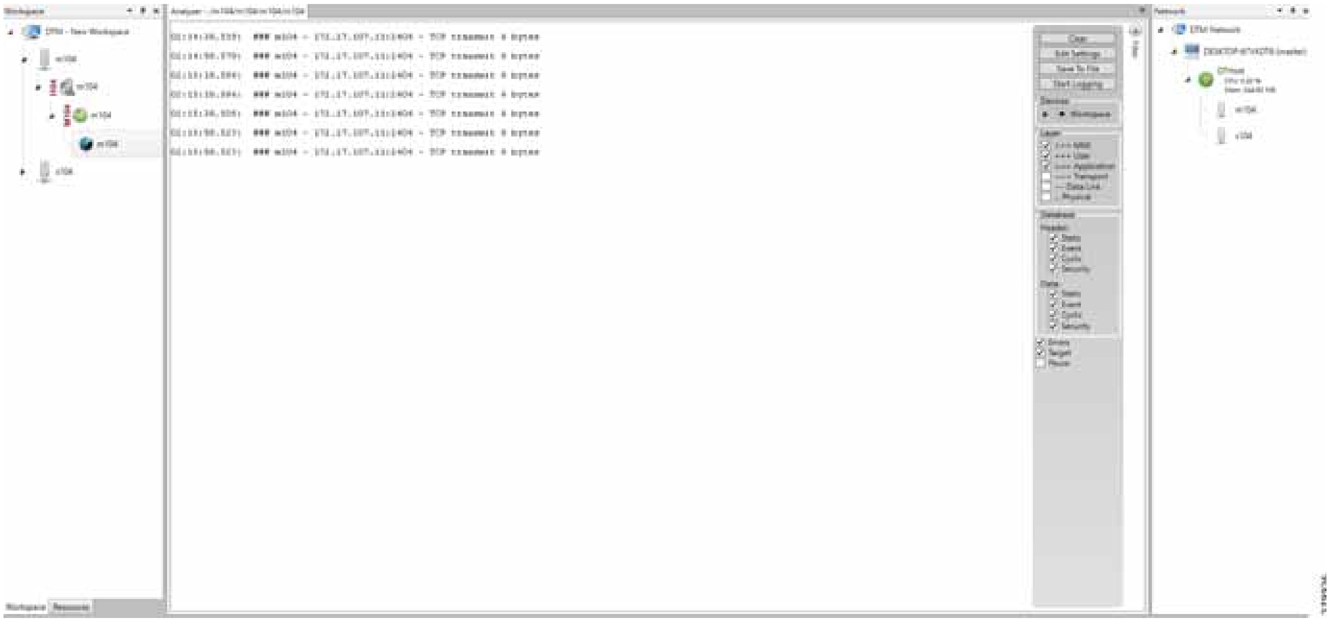


Figure 103 CC-1 Master Analyzer Logs after Poll Operation

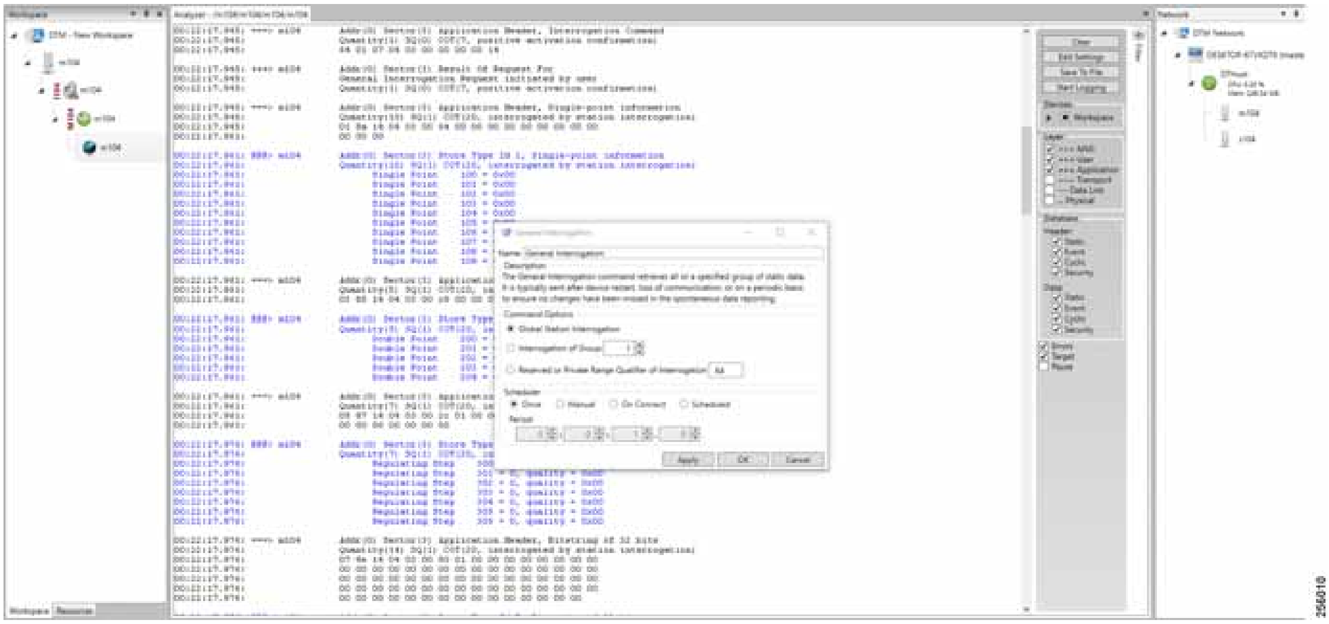
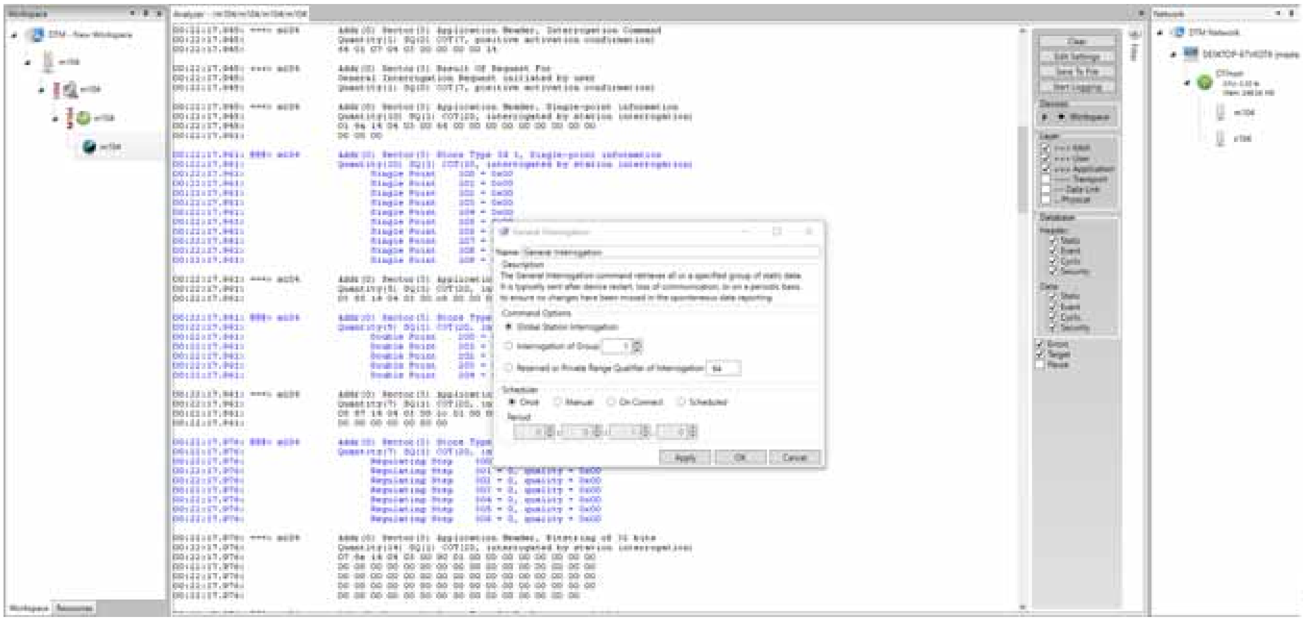


Figure 104 CC-2 Master Analyzer Logs after Poll Operation



```
00:22:17.845: ---> m104     ASDU(0) Sector(3) Application Header, Interrogation Command
00:22:17.845:               Quantity(1) SQ(0) COT(7, positive activation confirmation)
00:22:17.845:               64 01 07 04 03 00 00 00 00 14

00:22:17.845: <--> m104     ASDU(0) Sector(3) Result Of Request For
00:22:17.845:               General Interrogation Request initiated by user
00:22:17.845:               Quantity(1) SQ(0) COT(7, positive activation confirmation)

00:22:17.860: ---> m104     ASDU(0) Sector(3) Application Header, Single-point information
00:22:17.860:               Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.860:               01 8a 14 04 03 00 64 00 00 00 00 00 00 00 00 00
00:22:17.861:               00 00 00

00:22:17.861: ===> m104     ASDU(0) Sector(3) Store Type 01 1, Single-point information
00:22:17.861:               Quantity(10) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.861:                       Single Point     100 = 0x00
00:22:17.861:                       Single Point     101 = 0x00
00:22:17.861:                       Single Point     102 = 0x00
00:22:17.861:                       Single Point     103 = 0x00
00:22:17.861:                       Single Point     104 = 0x00
00:22:17.861:                       Single Point     105 =
00:22:17.861:                       Single Point     106 =
00:22:17.861:                       Single Point     107 =
00:22:17.861:                       Single Point     108 =
00:22:17.861:                       Single Point     109 =

00:22:17.861: ---> m104     ASDU(0) Sector(3) Applicatio
00:22:17.861:               Quantity(5) SQ(1) COT(20, in
00:22:17.861:               03 85 14 04 03 00 c8 00 00 0

00:22:17.861: ===> m104     ASDU(0) Sector(3) Store Type
00:22:17.861:               Quantity(5) SQ(1) COT(20, in
00:22:17.861:                       Double Point     200 =
00:22:17.861:                       Double Point     201 =
00:22:17.861:                       Double Point     202 =
00:22:17.861:                       Double Point     203 =
00:22:17.861:                       Double Point     204 =

00:22:17.861: ---> m104     ASDU(0) Sector(3) Applicatio
00:22:17.861:               Quantity(7) SQ(1) COT(20, in
00:22:17.861:               05 87 14 04 03 00 2c 01 00 0
00:22:17.861:               00 00 00 00 00 00 00

00:22:17.876: ===> m104     ASDU(0) Sector(3) Store Type
00:22:17.876:               Quantity(7) SQ(1) COT(20, in
00:22:17.876:                       Regulating Step     300
00:22:17.876:                       Regulating Step     301 = 0, quality = 0x00
00:22:17.876:                       Regulating Step     302 = 0, quality = 0x00
00:22:17.876:                       Regulating Step     303 = 0, quality = 0x00
00:22:17.876:                       Regulating Step     304 = 0, quality = 0x00
00:22:17.876:                       Regulating Step     305 = 0, quality = 0x00
00:22:17.876:                       Regulating Step     306 = 0, quality = 0x00

00:22:17.876: ---> m104     ASDU(0) Sector(3) Application Header, Bitstring of 32 bits
00:22:17.876:               Quantity(16) SQ(1) COT(20, interrogated by station interrogation)
00:22:17.876:               07 8a 14 04 03 00 90 01 00 00 00 00 00 00 00 00
00:22:17.876:               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.876:               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.876:               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00:22:17.876:               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

General Interrogation

Name: General Interrogation

Description

The General Interrogation command retrieves all or a specified group of static data. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure no changes have been missed in the spontaneous data reporting.

Command Options

● Global Station Interrogation

○ Interrogation of Group 1

○ Reserved or Private Range Qualifier of Interrogation 64

Schedule

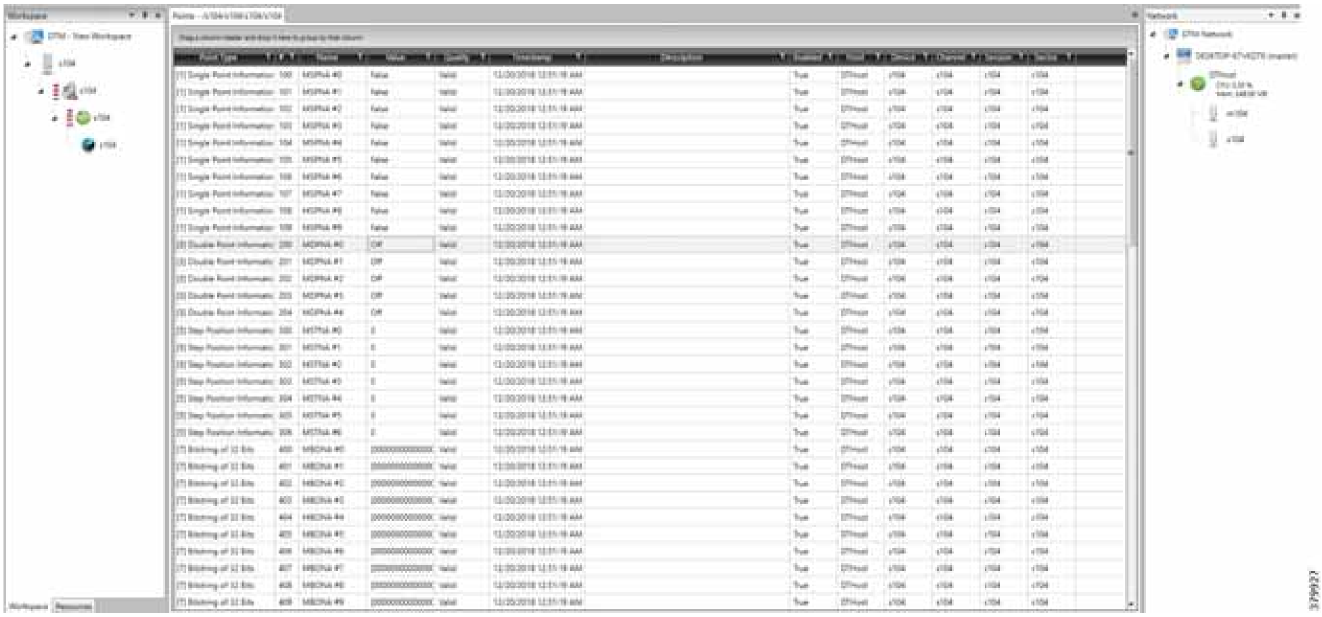
● Once ○ Manual ○ On Connect ○ Scheduled

Period

Control

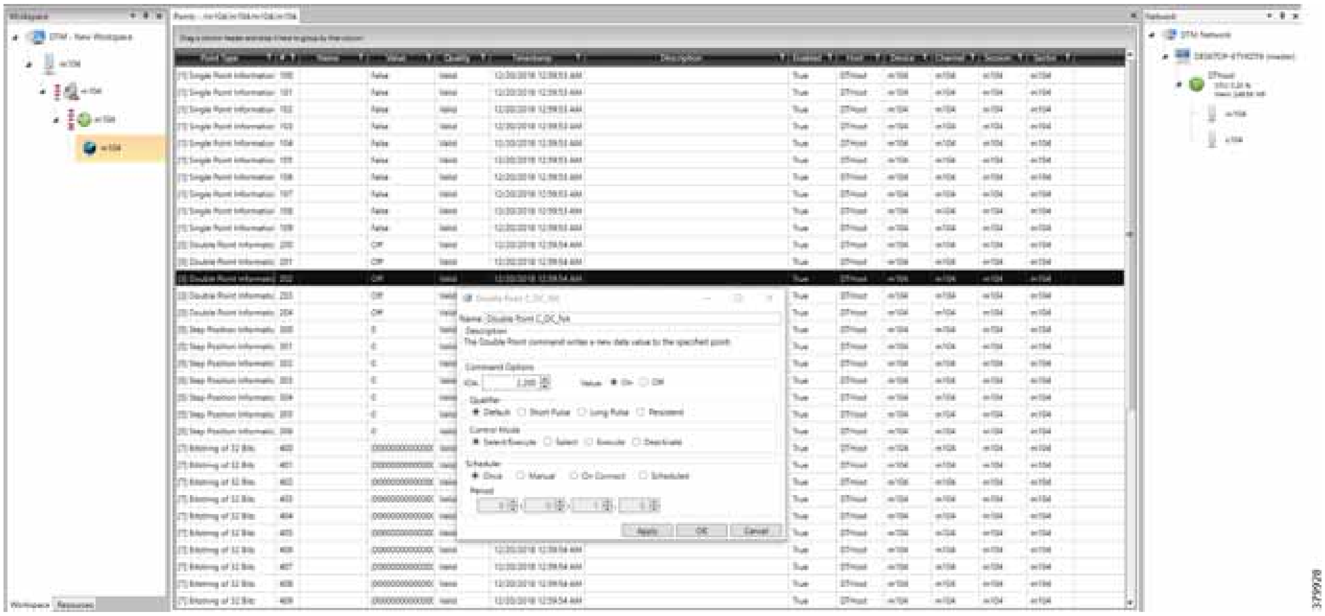
The control operation basically sending the control command from the both SCADA Master to SCADA Slave for the purpose of controlling the operation of end devices. The control command can be executed and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to both Masters. Figure 105, Figure 106, Figure 107, Figure 108, and Figure 109 show the Report by Exception sent to both Masters for a particular register:

Figure 105 Slave Register before Control Operation



Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Informatio	100	M_SP_NA #0	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	101	M_SP_NA #1	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	102	M_SP_NA #2	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	103	M_SP_NA #3	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	104	M_SP_NA #4	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	105	M_SP_NA #5	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	106	M_SP_NA #6	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	107	M_SP_NA #7	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	108	M_SP_NA #8	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Informatio	109	M_SP_NA #9	False	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	200	M_DP_NA #0	Off	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	201	M_DP_NA #1	Off	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	202	M_DP_NA #2	Off	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	203	M_DP_NA #3	Off	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatio	204	M_DP_NA #4	Off	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	300	M_ST_NA #0	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	301	M_ST_NA #1	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	302	M_ST_NA #2	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	303	M_ST_NA #3	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	304	M_ST_NA #4	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	305	M_ST_NA #5	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatio	306	M_ST_NA #6	0	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	M_BO_NA #0	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	M_BO_NA #1	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	M_BO_NA #2	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	M_BO_NA #3	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	M_BO_NA #4	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	M_BO_NA #5	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	M_BO_NA #6	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	M_BO_NA #7	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	M_BO_NA #8	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	M_BO_NA #9	000000000000000(	Valid	12/20/2018 12:11:19 AM		True	DTHost	s104	s104	s104	s104

Figure 106 CC-1 Master Control Operation



Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	101		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	102		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	103		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	104		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	105		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	106		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	107		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	108		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[1] Single Point Information	109		False	Valid	12/20/2018 12:59:53 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatio	200		Off	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatio	201		Off	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatio	202		Off	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[3] Double Point Informatio	203		Off	Valid			True	DTHost	m104	m104	m104	m104
[3] Double Point Informatio	204		Off	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	300		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	301		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	302		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	303		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	304		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	305		0	Valid			True	DTHost	m104	m104	m104	m104
[5] Step Position Informatio	306		0	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	400		000000000000000(	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	401		000000000000000(	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	402		000000000000000(	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	403		000000000000000(	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	404		000000000000000(	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	405		000000000000000(	Valid			True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	406		000000000000000(	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	407		000000000000000(	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	408		000000000000000(	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104
[7] Bitstring of 32 Bits	409		000000000000000(	Valid	12/20/2018 12:59:54 AM		True	DTHost	m104	m104	m104	m104

Name: Double Point C_DC_NA

Description

The Double Point command writes a new data value to the specified point.

Command Options

IOA: 1,200 Value: ● On ○ Off

Qualifier

● Default ○ Short Pulse ○ Long Pulse ○ Persistent

Control Mode

● Select/Execute ○ Select ○ Execute ○ Deactivate

Schedule

● Once ○ Manual ○ On Connect ○ Scheduled

Period

0 0 0 0

Figure 107 CC-2 Master Control Operation

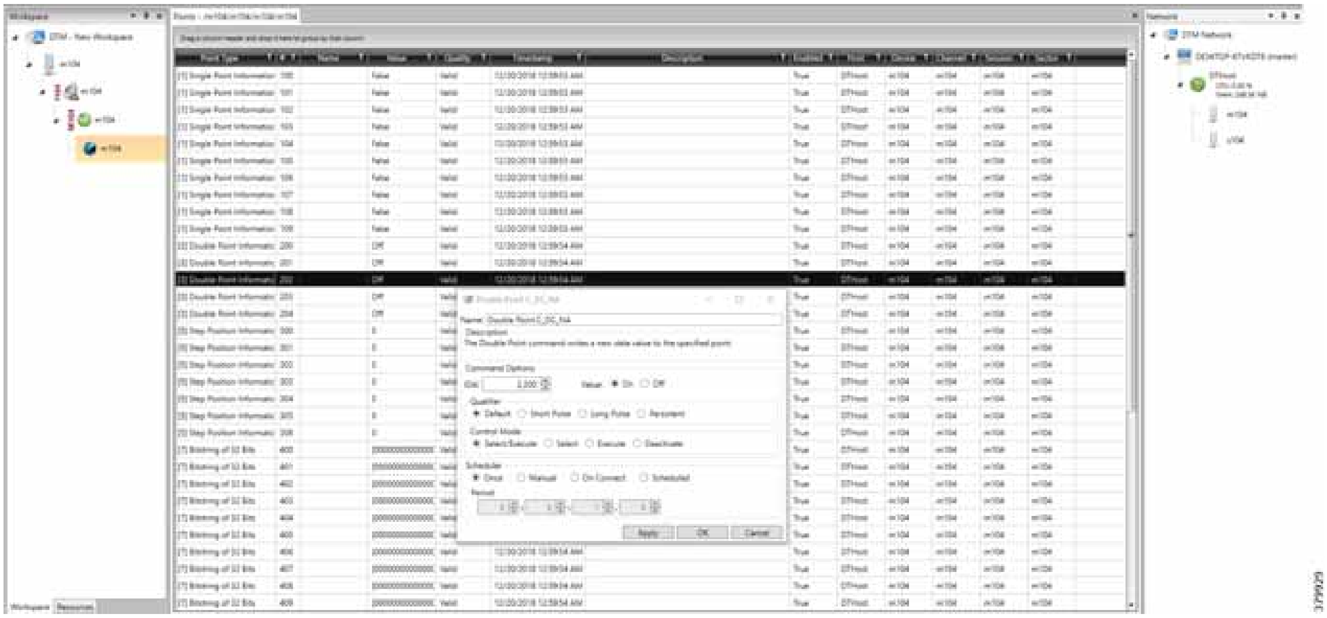


Figure 108 CC-1 Slave Register after Control Operation

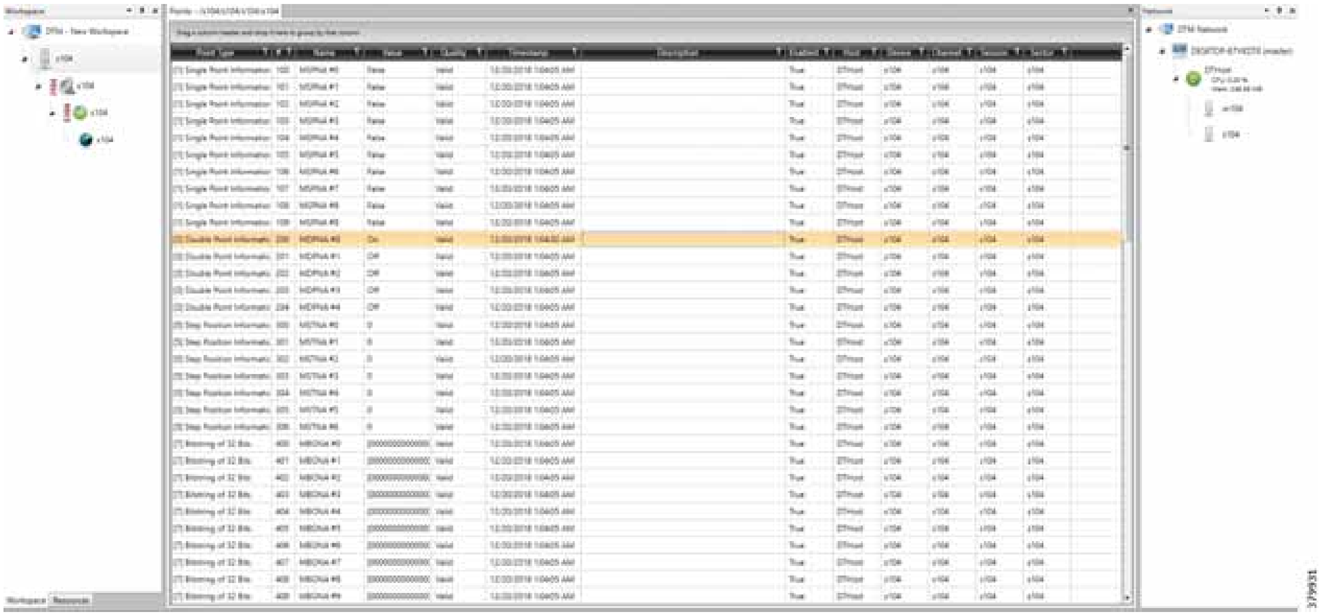
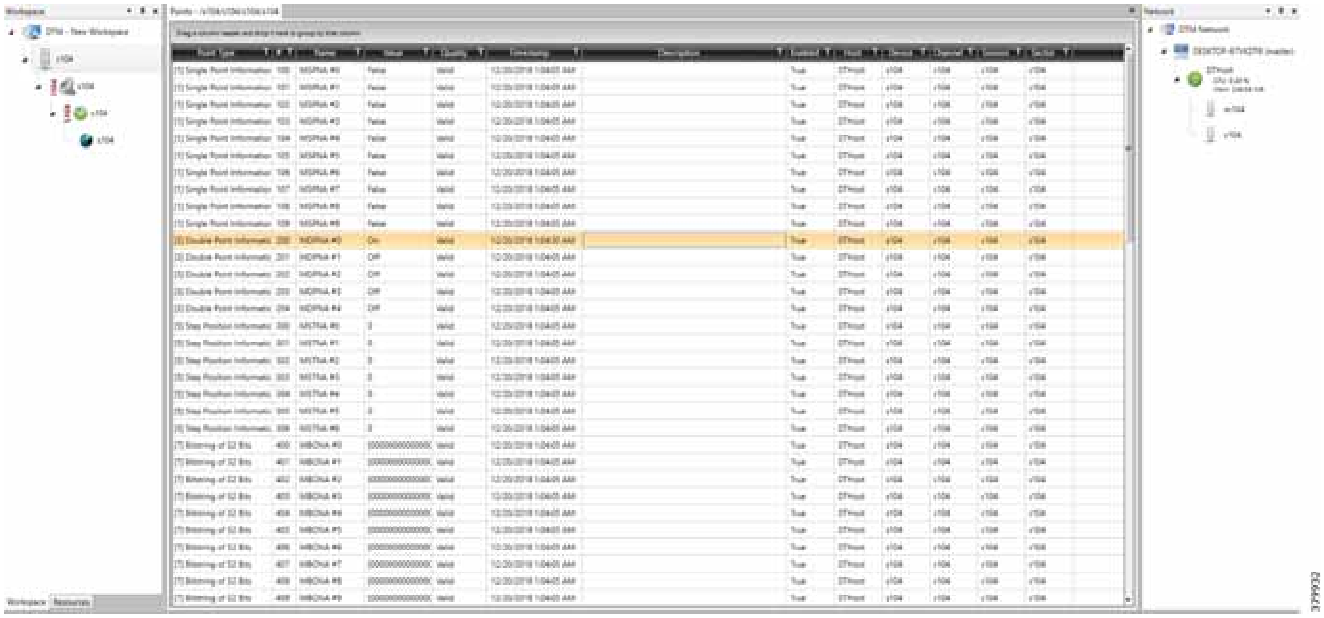


Figure 109 CC-2 Slave Register after Control Operation

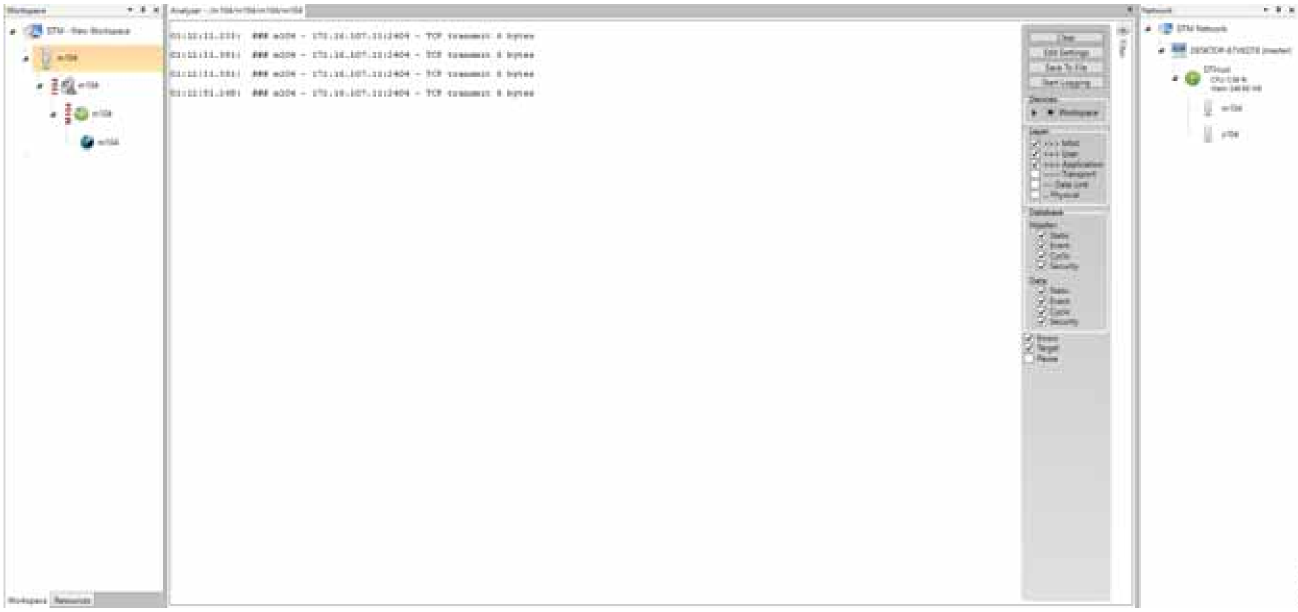


Point Type	[illegible]	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	200	MDPNA #0	On	Valid	12/20/2018 1:04:30 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	201	MDPNA #1	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	202	MDPNA #2	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	203	MDPNA #3	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[3] Double Point Informatic	204	MDPNA #4	Off	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	300	MSTNA #0	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	301	MSTNA #1	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	302	MSTNA #2	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	303	MSTNA #3	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	304	MSTNA #4	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	305	MSTNA #5	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[5] Step Position Informatic	306	MSTNA #6	0	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	400	MBONA #0	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	401	MBONA #1	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	402	MBONA #2	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	403	MBONA #3	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	404	MBONA #4	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	405	MBONA #5	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	406	MBONA #6	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	407	MBONA #7	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	408	MBONA #8	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104
[7] Bitstring of 32 Bits	409	MBONA #9	{000000000000000	Valid	12/20/2018 1:04:05 AM		True	DTHost	s104	s104	s104	s104

Report by Exception

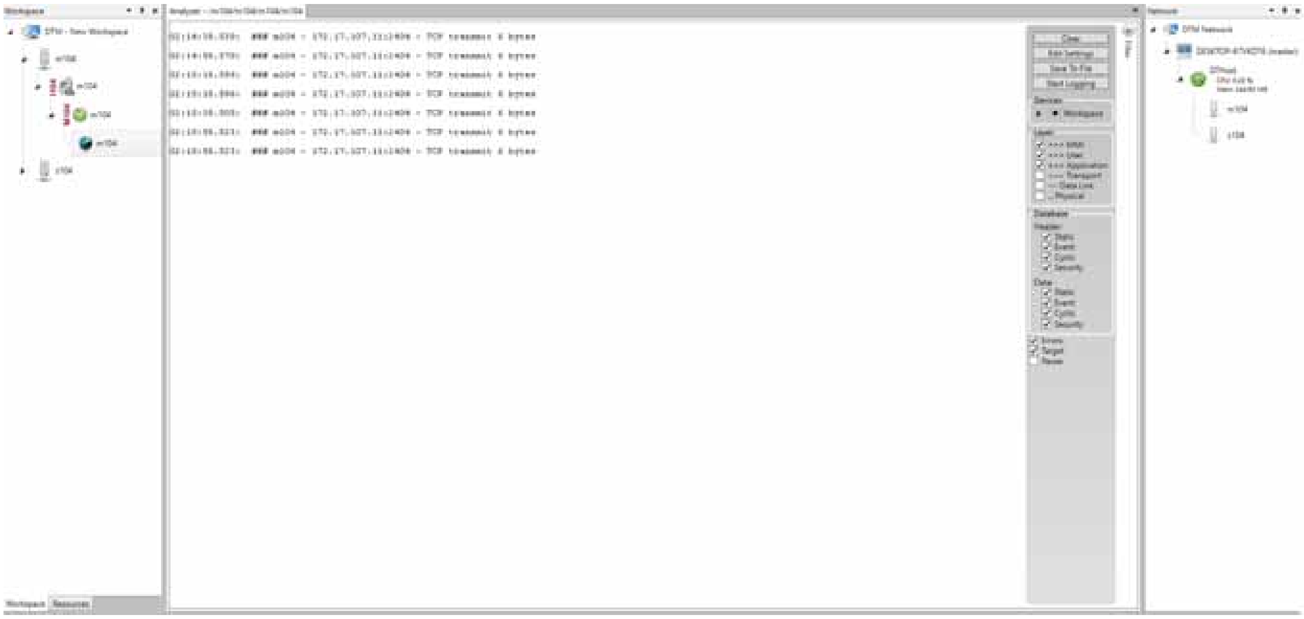
Report by Exception is initiated by the Slave, which is connected to the DA Gateway. Changes to the value of the Slave register changes, are reported to both SCADA-Masters. This notification can be seen on both Master Analyzers of the DTM software. Figure 110, Figure 111, Figure 112, Figure 113, Figure 114, and Figure 115 show the Report by Exception on the analyzer. The other operations, such as Poll and Control, can be executed and the results can be seen on the analyzer. The value of Double Point Register (#200) is changed and the same is reported to both Masters. Figure 110, Figure 111, Figure 112, Figure 113, Figure 114, and Figure 115 show the Report by Exception sent to both Masters for a particular register:

Figure 110 CC-1 Master Analyzer



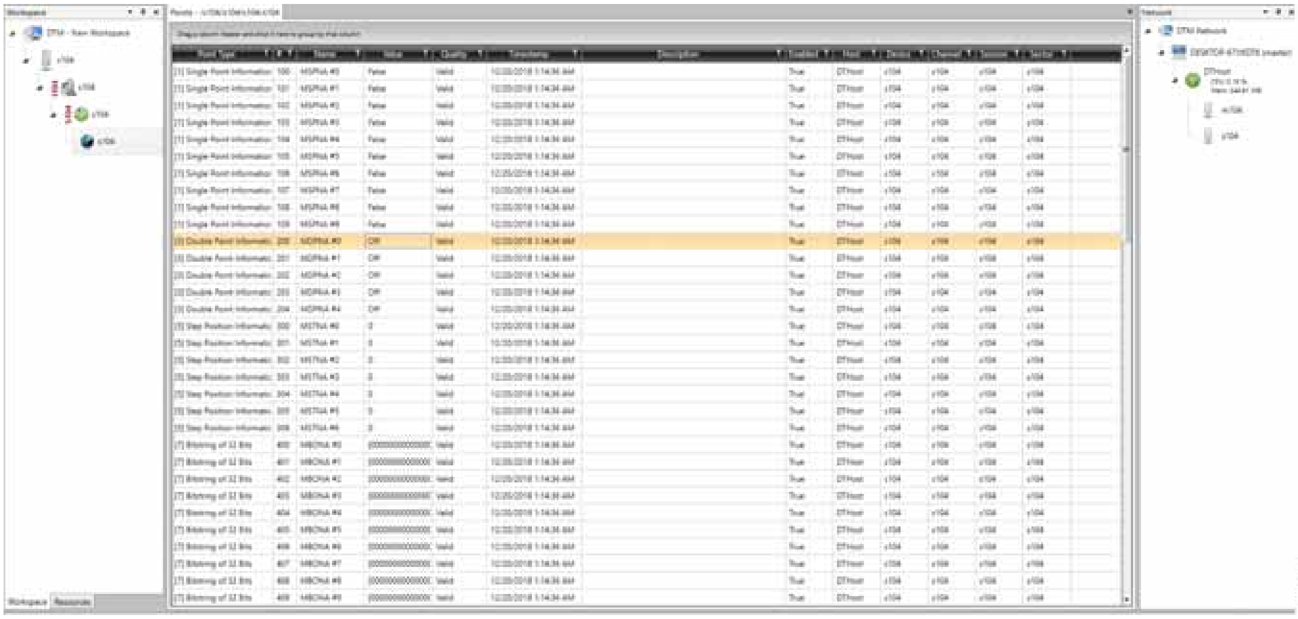
```
[illegible]  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

Figure 111 CC-2 Master Analyzer



```
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
[illegible]  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
```

Figure 112 Slave Registers

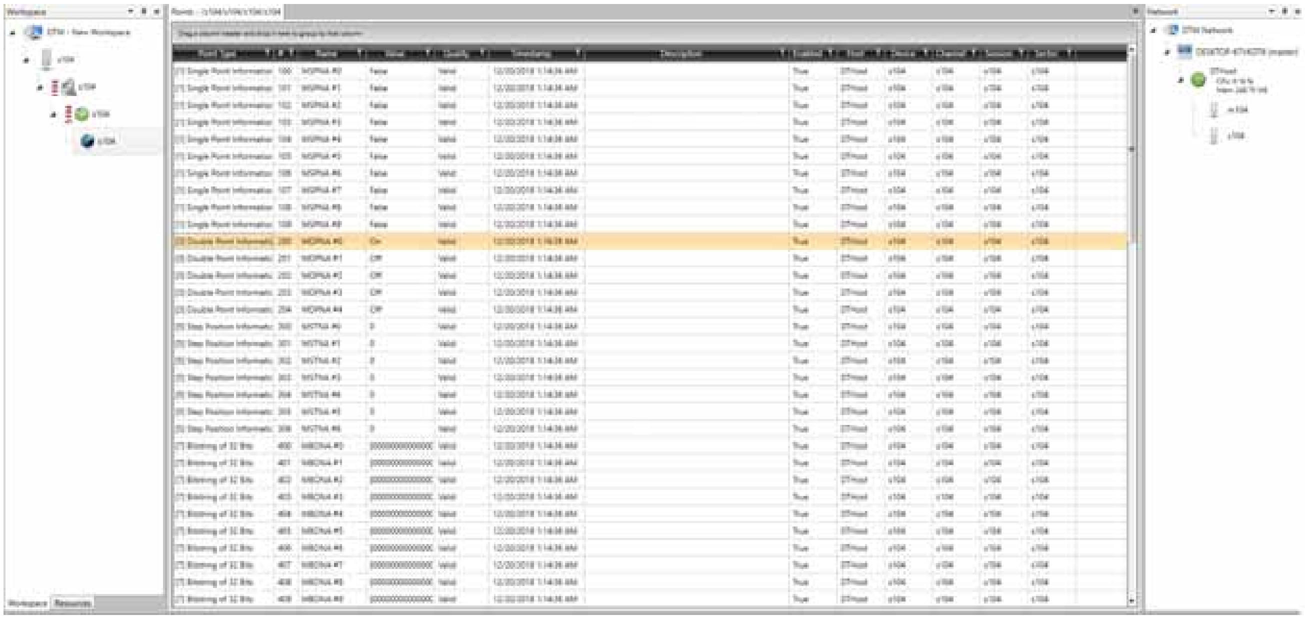


Points - /c104/c104/c104/c104

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

Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	200	MDPNA #0	Off	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	201	MDPNA #1	Off	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	202	MDPNA #2	Off	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	203	MDPNA #3	Off	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	204	MDPNA #4	Off	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	300	MSTNA #0	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	301	MSTNA #1	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	302	MSTNA #2	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	303	MSTNA #3	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	304	MSTNA #4	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	305	MSTNA #5	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	306	MSTNA #6	0	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	400	MBONA #0	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	401	MBONA #1	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	402	MBONA #2	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	403	MBONA #3	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	404	MBONA #4	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	405	MBONA #5	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	406	MBONA #6	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	407	MBONA #7	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	408	MBONA #8	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	409	MBONA #9	{00000000000000(	Valid	12/20/2018 1:14:34 AM		True	DTHost	c104	c104	c104	c104

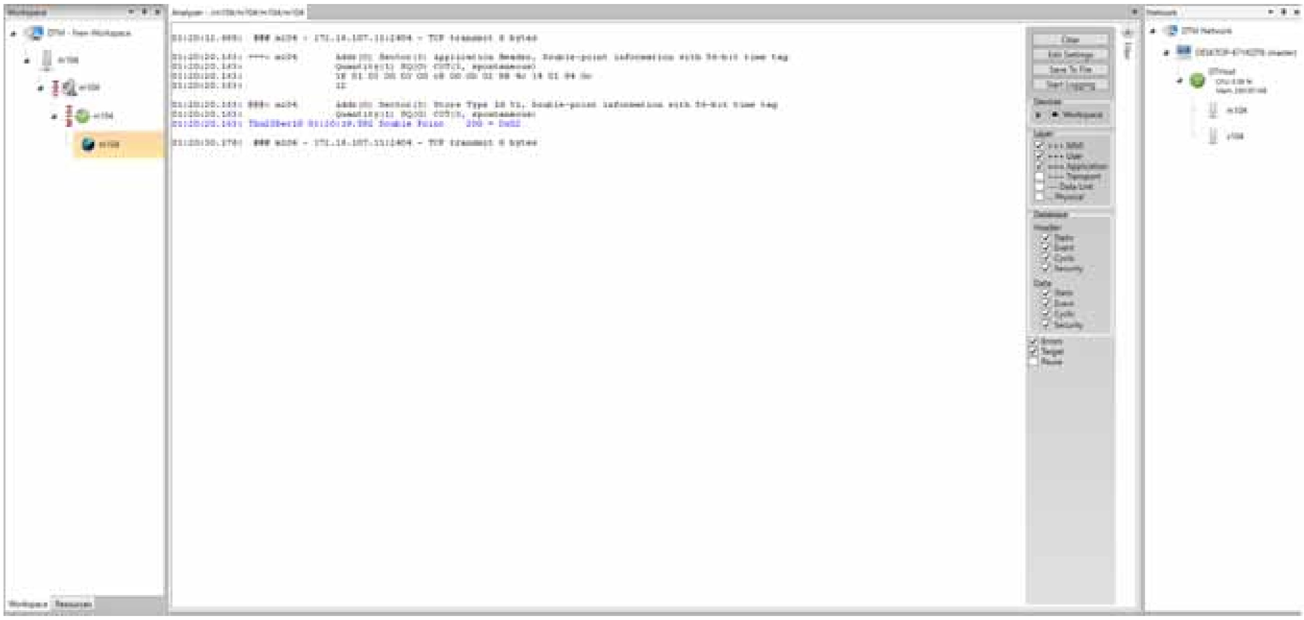
Figure 113 Change in Slave Register Value



Points - /c104/c104/c104/c104

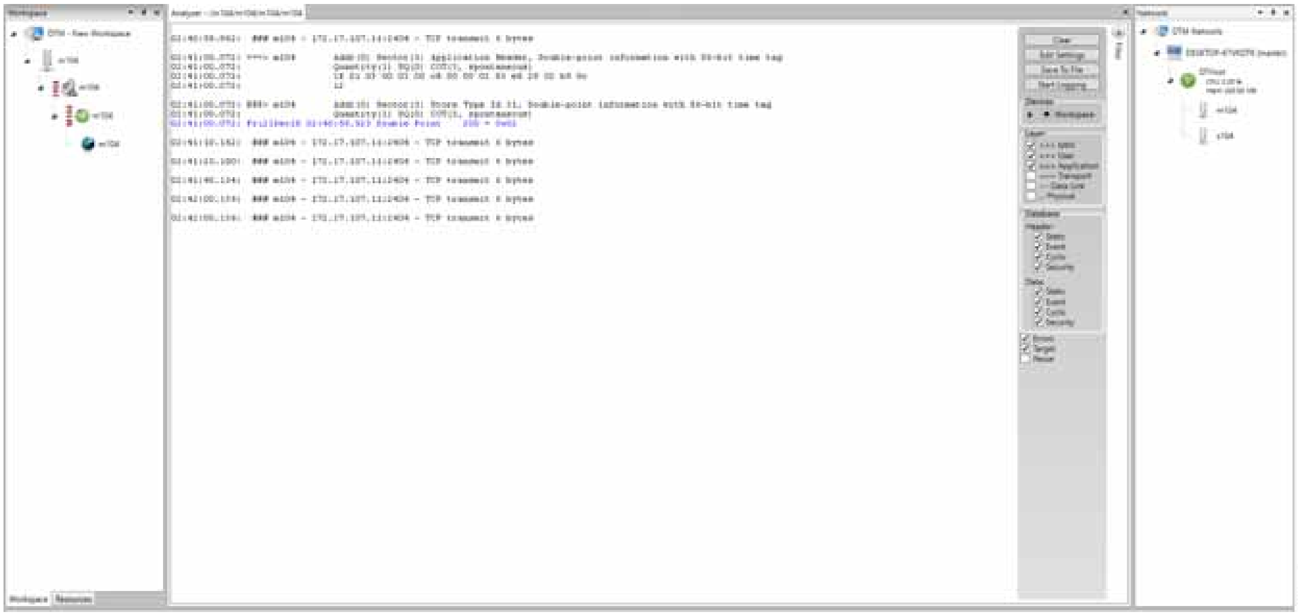
Drag a column header and drop it here to group by that column

Point Type	IOA	Name	Value	Quality	Timestamp	Description	Enabled	Host	Device	Channel	Session	Sector
[1] Single Point Information	100	MSPNA #0	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	101	MSPNA #1	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	102	MSPNA #2	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	103	MSPNA #3	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	104	MSPNA #4	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	105	MSPNA #5	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	106	MSPNA #6	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	107	MSPNA #7	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	108	MSPNA #8	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[1] Single Point Information	109	MSPNA #9	False	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	200	MDPNA #0	On	Valid	12/20/2018 1:18:29 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	201	MDPNA #1	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	202	MDPNA #2	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	203	MDPNA #3	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[3] Double Point Informati	204	MDPNA #4	Off	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	300	MSTNA #0	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	301	MSTNA #1	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	302	MSTNA #2	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	303	MSTNA #3	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	304	MSTNA #4	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	305	MSTNA #5	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[5] Step Position Informati	306	MSTNA #6	0	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	400	MBONA #0	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	401	MBONA #1	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	402	MBONA #2	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	403	MBONA #3	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	404	MBONA #4	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	405	MBONA #5	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	406	MBONA #6	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	407	MBONA #7	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	408	MBONA #8	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104
[7] Bitstring of 32 Bits	409	MBONA #9	{00000000000000(	Valid	12/20/2018 1:14:36 AM		True	DTHost	c104	c104	c104	c104



```
01:20:12.885:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes

01:20:20.143: <--- m104       ASDU[0] Sector[3] Application Header, Double-point information with 56-bit time tag
01:20:20.143:                 Quantity[1] SQ[0] COT[3, spontaneous]
01:20:20.143:                 [illegible]
01:20:20.143:                 12

01:20:20.143: ###> m104       ASDU[0] Sector[3] Store Type 1E 31, Double-point information with 56-bit time tag
01:20:20.143:                 Quantity[1] SQ[0] COT[3, spontaneous]
01:20:20.143: Thu20Dec18 01:20:18.592 Double Point    200 = DoR2

01:20:30.278:  ### m104 - 172.16.107.11:2404 - TCP transmit 6 bytes
```

Figure 114 CC-1 Master Analyzer after Change in Register



```
02:40:58.862:  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes

02:41:00.072: <--- m104       ASDU[0] Sector[3] Application Header, Double-point information with 56-bit time tag
02:41:00.072:                 Quantity[1] SQ[0] COT[3, spontaneous]
02:41:00.072:                 [illegible]
02:41:00.072:                 12

02:41:00.072: ###> m104       ASDU[0] Sector[3] Store Type 1E 31, Double-point information with 56-bit time tag
02:41:00.072:                 Quantity[1] SQ[0] COT[3, spontaneous]
02:41:00.072: Fri21Dec18 02:40:58.527 Double Point    200 = DoR2

02:41:10.162:  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes

02:41:20.180:  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes

02:41:40.134:  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes

02:42:00.173:  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes

02:42:00.136:  ### m104 - 172.17.107.11:2404 - TCP transmit 6 bytes
```

Figure 115 CC-2 Master Analyzer after Change in Register Value

IEC 61850

This section covers the implementation of the solution architecture for MMS and GOOSE. The architecture involves the communication between SCADA to IEDs and IEDs to IEDs.

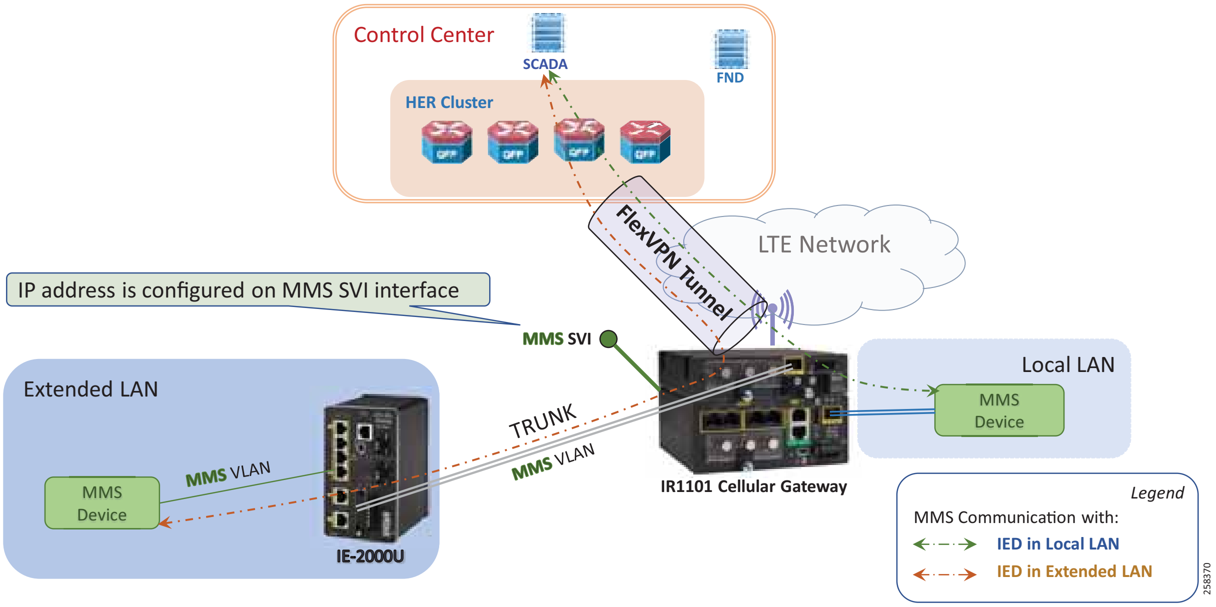
For design and conceptual understanding of this section please refer to the "Distribution Automation Solution Architecture" chapter of the Design Guide. To enable the network to allow MMS and GOOSE traffic, the following additional configurations are needed:

- HER and FAR Configuration for MMS, page 114
- HER and MMS Configuration for GOOSE, page 116

HER and FAR Configuration for MMS

Figure 116 shows the flow of MMS traffic from SCADA to the IEDs. This section covers the configuration required on HER and FAR to enable communication between SCADA and the MMS device.

Figure 116 IEC 61850 MMS Communication Flow with IEDs in Local LAN and Extended LAN



Note: No additional configuration on the HER is needed.

SCADA in the control center connects to the loopback 0 address on the FAR on a particular port number. This connection from the SCADA control center is translated to a local address of the MMS device using NAT. The loopback address is enabled as part of ZTD. For ZTD and the loopback addressing, please refer to IoT Gateway Onboarding and Management, page 14.

The MMS device can reside in the local LAN or in the Extended LAN as shown in the Figure 116 above. These devices are in a private network; therefore, NAT configuration is required. This configuration helps in scaling when a large number of FARs have to be configured. The following details provide the step-by-step configuration:

1. The MMS device can reside either in the local LAN or in the extended LAN. Either of the connections to the FAR are via the gig port. As shown in the above figure, the ports connected to MMS device are VLAN 300 and SVI created for routing packets from SCADA to MMS device and vice versa. The following configurations have to be added in this step:

```
interface Vlan300
 ip address 192.168.0.10 255.255.255.0
```

2. The next step is to add the NAT configuration to the FAR. This configuration enables communication from SCADA to the MMS device. The port connected to the MMS device is configured with “vlan 300" , the corresponding “interface vlan 300" is configured with “ip nat inside” and the connectivity to SCADA through which the tunnel interface is configured with “ip nat outside.” The elucidated configurations are as shown below and the lines in bold are the modifications:

```
!
ip nat inside source static tcp 192.168.0.3 102 interface Loopback0 102
!
interface GigabitEthernet0/0/5
 switchport trunk allowed vlan 300,600
 switchport mode trunk
end
!
interface Tunnel0
 description IPsec tunnel to HER1.ipg.cisco.com
 ip unnumbered Loopback0
 ip nat outside
 ipv6 unnumbered Loopback0
 qos pre-classify
 tunnel source Cellular0/3/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
end
!
interface Vlan300
 ip address 192.168.0.10 255.255.255.0
 ip nat inside

!
```

HER and MMS Configuration for GOOSE

Figure 117 shows a diagram of the IED-IED communication architecture using GOOSE. This communication can be between two locally-connected GOOSE devices or between two IEDs in different extended LANs. In this section, we will cover the configurations that have to be added on HER and FAR for the GOOSE infrastructure to enable communication. Figure 118 shows a logical diagram of the GOOSE flow over the cellular network:

Figure 117 IED-IED GOOSE Architectural Flow

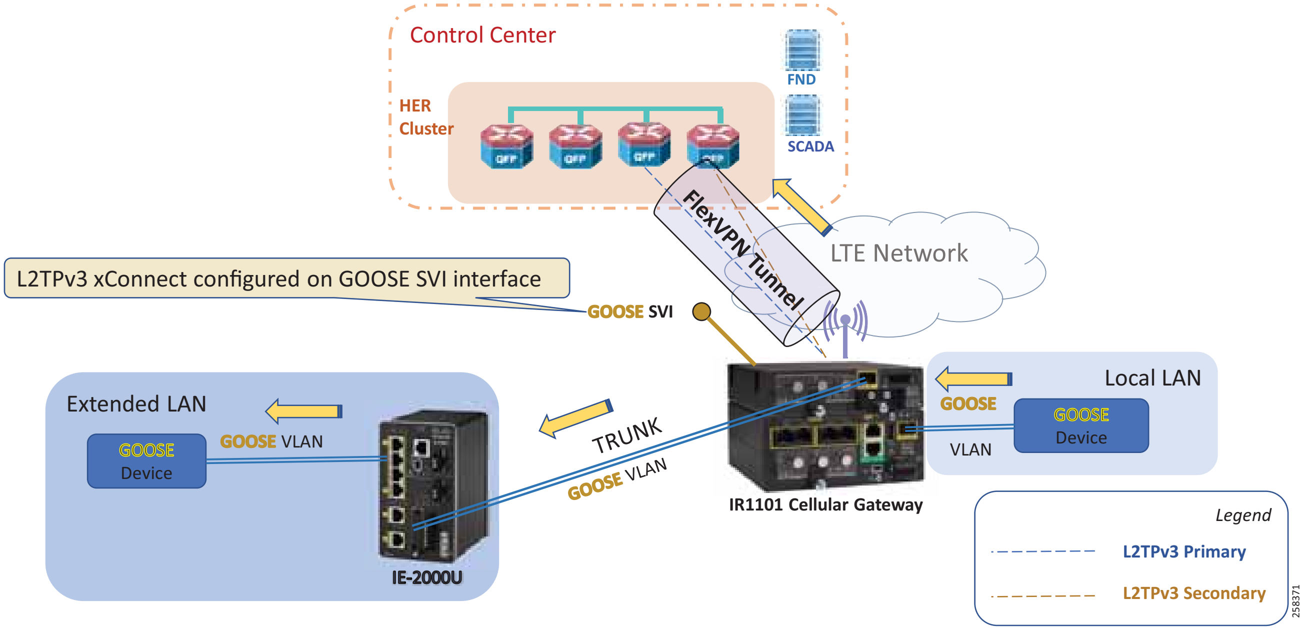
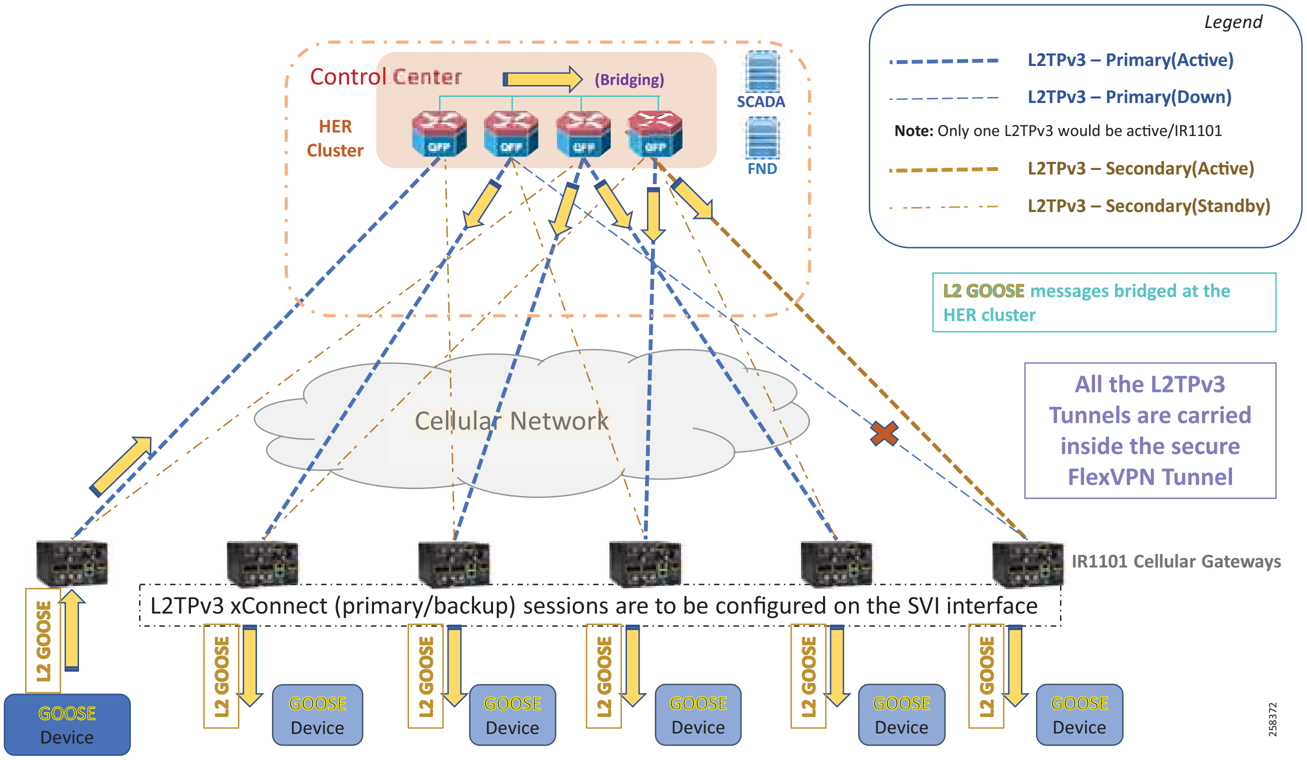
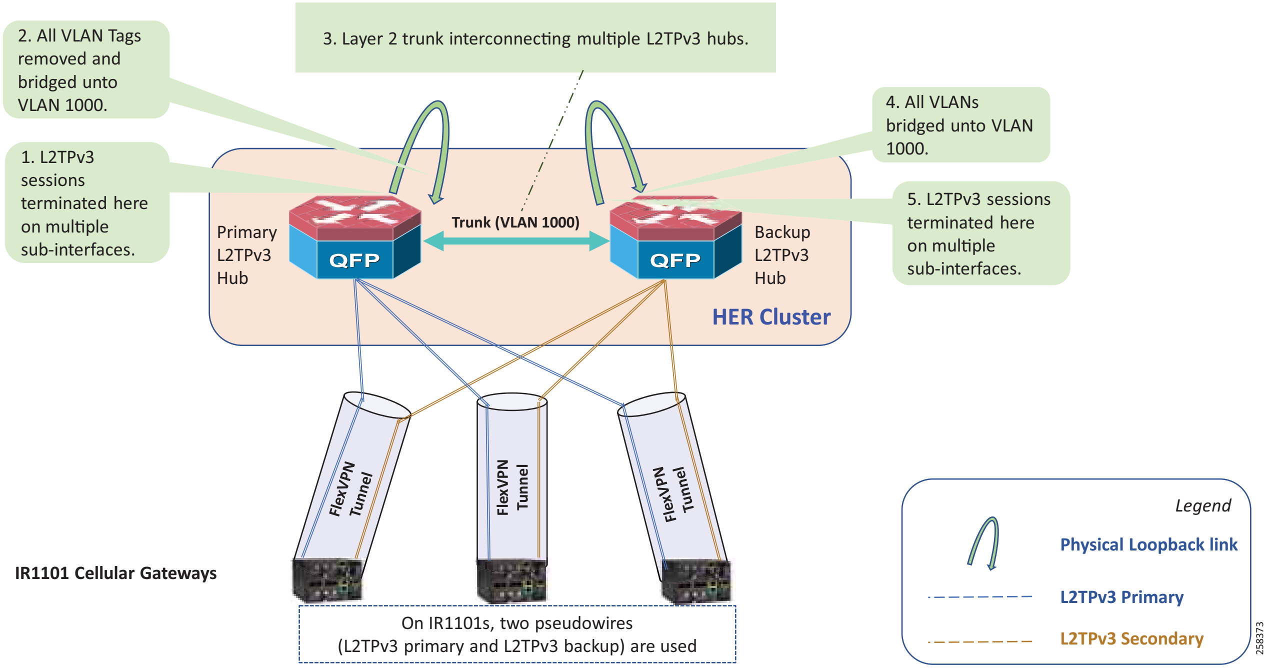


Figure 118 IED-IED Flow Hub-switched DA Design


Control Center
(Bridging)
HER
Cluster
SCADA
FND
Legend
L2TPv3 – Primary(Active)
L2TPv3 – Primary(Down)
Note: Only one L2TPv3 would be active/IR1101
L2TPv3 – Secondary(Active)
L2TPv3 – Secondary(Standby)
L2 GOOSE messages bridged at the HER cluster
All the L2TPv3 Tunnels are carried inside the secure FlexVPN Tunnel
Cellular Network
IR1101 Cellular Gateways
L2TPv3 xConnect (primary/backup) sessions are to be configured on the SVI interface
L2 GOOSE
GOOSE
Device
258372

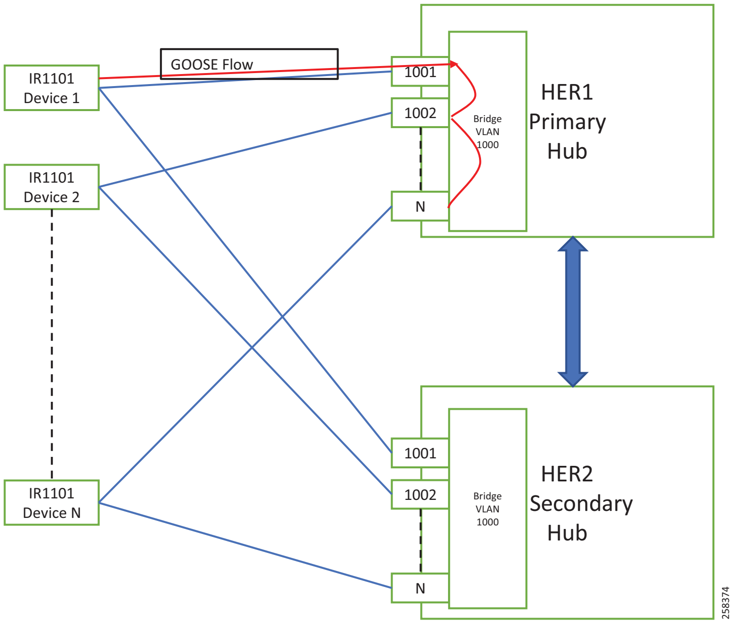
Before FAR can be configured with L2TPV3, HER acts as the L2TPv3 Hub and the necessary configurations have to be added on the HER. Figure 119 shows HER as L2TPv3 Hub for creating Layer 2 Bridge Domain:

Figure 119 HER as L2TPv3 Hub


2. All VLAN Tags removed and bridged unto VLAN 1000.
3. Layer 2 trunk interconnecting multiple L2TPv3 hubs.
4. All VLANs bridged unto VLAN 1000.
1. L2TPv3 sessions terminated here on multiple sub-interfaces.
5. L2TPv3 sessions terminated here on multiple sub-interfaces.
Primary L2TPv3 Hub
QFP
Trunk (VLAN 1000)
QFP
Backup L2TPv3 Hub
HER Cluster
FlexVPN Tunnel
FlexVPN Tunnel
FlexVPN Tunnel
IR1101 Cellular Gateways
On IR1101s, two pseudowires (L2TPv3 primary and L2TPv3 backup) are used
Legend
Physical Loopback link
L2TPv3 Primary
L2TPv3 Secondary
258373

In Figure 119, two HERs are shown. Multiple HERs can be used for redundancy. Here the second HER acts as the backup hub. Figure 120 shows the logical flow of GOOSE traffic from one IED to another IED. The configuration on HER and FAR should be understood using both Figure 119 and Figure 120 as references.

Figure 120 IED-IED GOOSE Logical Flow



The hub configurations are as follows:

1. Multiple IR1101s connect to the primary hub via the L2TPv3 tunnel. The hub connects to each IR1101 with a different VC ID. Pseudowire configurations mentions the local interface at which the L2TPv3 tunnel must end. For a single tunnel from the hub to one IR1101, a subinterface is created and tagged with VC ID which is unique to the connecting IR1101. Similar subinterfaces must be created for different IR1101 to connect to the hub.

```
pseudowire-class L2TPv3_PW
 encapsulation l2tpv3
 ip local interface Loopback0
 ip tos value 136
!
interface GigabitEthernet8.1001
 platform ring rx 256
 encapsulation dot1Q 1001
 xconnect 192.168.150.18 1001 encapsulation l2tpv3 pw-class L2TPv3_PW
```

2. When packets arrive at the hub over the L2TPV3 tunnel from one IR1101, those packets must be untagged and bridged to one VLAN (this guide implements VLAN 1000). After the packets have been bridged to VLAN 1000, they are sent to other IR1101s in the network with their respective VC IDs. Figure 120 clearly shows the flow of packets from one IR1101 to another. The packet from Device 1 is sent to Hub with VC ID 1001. This VC ID 1001 is removed and sent to the bridge interface to which all the other L2TPv3 tunnels are connected. The received packet from Device 1 is tapped by other tunnel interfaces. The packet is sent over the other L2TPv3 after tagging it with the respective VC ID. The following configuration provides the untagging and bridging:

```
interface GigabitEthernet10
 platform ring rx 256
 no ip address
 negotiation auto
 service instance 1001 ethernet
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
  l2protocol forward
  bridge-domain 1000
 !
```

3. In this step, if another HER needs to be connected, then the Layer 2 trunk needs to be established between the ports connecting the HERs and the configurations done in the previous two steps have to be repeated. This is labeled as Step 4 and Step 5 in Figure 119.

At the FAR side, the configurations are simple. Refer to Figure 119 and Figure 120 for the topological diagram and the logical flow of GOOSE traffic to comprehend the following configuration. The FAR configurations are as follows:

1. The pseudowire configurations are similar to the pseudo wire configured on the Hub.

```
         pseudowire-class L2TPv3_PW
 encapsulation l2tpv3
 ip local interface Loopback0
 ip tos value 136
```

2. In this step, the xConnect configurations have to made on VLAN, which is used to connect to the IED. In this guide, we are using VLAN 600 to connect to the IED. The following configuration lines display the necessary configurations required to configure xConnect on FAR:

```
interface Vlan600
 description "GOOSE_INTERCAB"
 no ip address
 xconnect 192.168.150.1 1001 encapsulation l2tpv3 pw-class PW_L2TPV3
  backup peer 192.168.150.2 1001 pw-class PW_L2TPV3
```

Note: Avoid using default routes on FAR to achieve better Layer 2 resiliency timers.

End-to-End Application Use Case Scenarios

This chapter includes the following major topics:

Volt/VAR

The main purpose of Volt/VAR Control (VVC) is to maintain acceptable voltage levels 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 Volt/VAR Optimization (VVO) application will be using two-way communication infrastructure and remote control capability for capacitor banks, and voltage-regulating transformers, to optimize the energy delivery efficiency at the distribution level. In fact, the reactive power flow creates a voltage drop on an inductive element of wires. So, in order to keep the voltage always within certain limits, the reactive power flow and voltage control must be considered together. Therefore, 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 ability of the operator to maintain the voltage on the feeder at an acceptable range by changing the position of a 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 radial feeder setup for simulating the Volt/VAR use case.

Volt/VAR Devices

The devices involved in the Volt/VAR use case are listed in Table 15:

Table 15 Volt/VAR Devices

Device	Location	Description
End of Line Voltage Monitor	At 1.0 in Feeder line	To monitor the end of the line voltage
Cap Bank Controller 1	At 0.25 in Feeder line	To monitor the voltage and On/Off CapBank
Cap Bank Controller 2	At 0.50 in Feeder line	To monitor the voltage and On/Off CapBank
Cap Bank Controller 3	At 0.75 in Feeder line	To monitor the voltage and On/Off CapBank
Load Tap Controller	At Substation	To raise/lower load tap
Substation Meter	At Substation	To monitor substation device status/reading

Data Points

The data points involved in the Volt/VAR use case are listed in Table 16:

Table 16 Volt/VAR Devices Data Points

Device	Register Type	Description
End of Line Voltage Monitor	Measured Value, Short Floating Point	Voltage at End of line
Cap Bank Controller 1	Double Point Information	Cap Bank Controller - Status
	Measured Value, Short Floating Point	Voltage at CapBank Controller

Table 16 Volt/VAR Devices Data Points (continued)

Device	Register Type	Description
Cap Bank Controller 2	Double Point Information	Cap Bank Controller - Status
	Measured Value, Short Floating Point	Voltage at CapBank Controller
Cap Bank Controller 3	Double Point Information	Cap Bank Controller - Status
	Measured Value, Short Floating Point	Voltage at CapBank Controller
Load Tap Controller	Measured Value, Short Floating Point	LTC Position
	Single Point Information	To raise LTC
	Single Point Information	To lower LTC
Substation Meter	Measured Value, Short Floating Point	Power (kW)
	Measured Value, Short Floating Point	Q-Power (kVAR)
	Measured Value, Short Floating Point	Power Factor
	Measured Value, Short Floating Point	Losses (kW)
	Measured Value, Short Floating Point	Substation Meters

Volt/VAR Use Case Simulation Components

The entire event sequence of the Volt/VAR use case is simulated using the Triangle MicroWork's DTM application with the help of the Java script.

Table 17 describes the components involved in Volt/VAR simulation:

Table 17 Volt/VAR Simulation Components

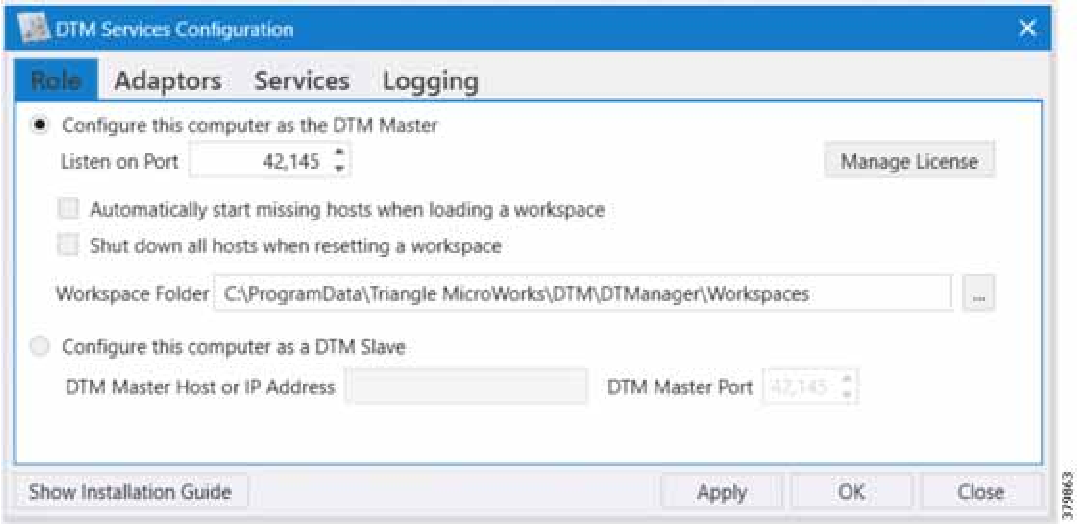
Role	Component / Application	Description	Version
SCADA Control Center	TMW's DTM application	Triangle MicroWork's DTM application is used to simulate the SCADA Control Center functionality.	DTM v1.3.1.4
Outstation Devices/IEDs	TMW's DTM application	Triangle MicroWork's DTM application is used to simulate the Outstation / IEDs devices.	DTM v1.3.1.4
Remote Terminal Unit	Eximprod's Virtual RTU	Eximprod's Virtual RTU application is used to simulate Substation RTU functionality.	ES200 v2.12.6883

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 121 DTM SCADA Control Server Role



DTM Services Configuration

● Configure this computer as the DTM Master

Listen on Port 42,145

□ Automatically start missing hosts when loading a workspace

□ Shut down all hosts when resetting a workspace

Workspace Folder C:\ProgramData\Triangle MicroWorks\DTM\DTManager\Workspaces

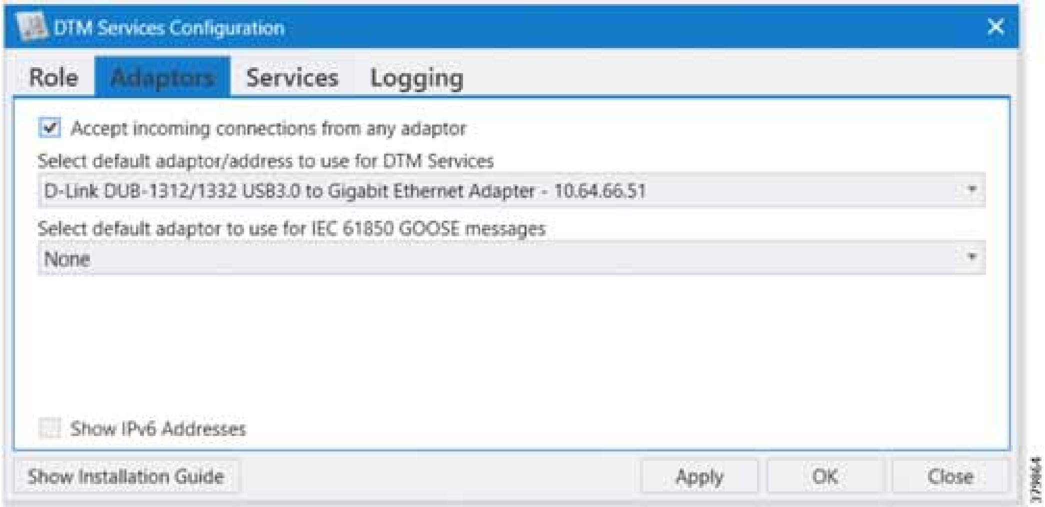
○ Configure this computer as a DTM Slave

DTM Master Host or IP Address

DTM Master Port 42,145

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

Figure 122 DTM SCADA Control Center Adapter Configuration



DTM Services Configuration

☑ Accept incoming connections from any adaptor

Select default adaptor/address to use for DTM Services

D-Link DUB-1312/1332 USB3.0 to Gigabit Ethernet Adapter - 10.64.66.51

Select default adaptor to use for IEC 61850 GOOSE messages

None

□ Show IPv6 Addresses

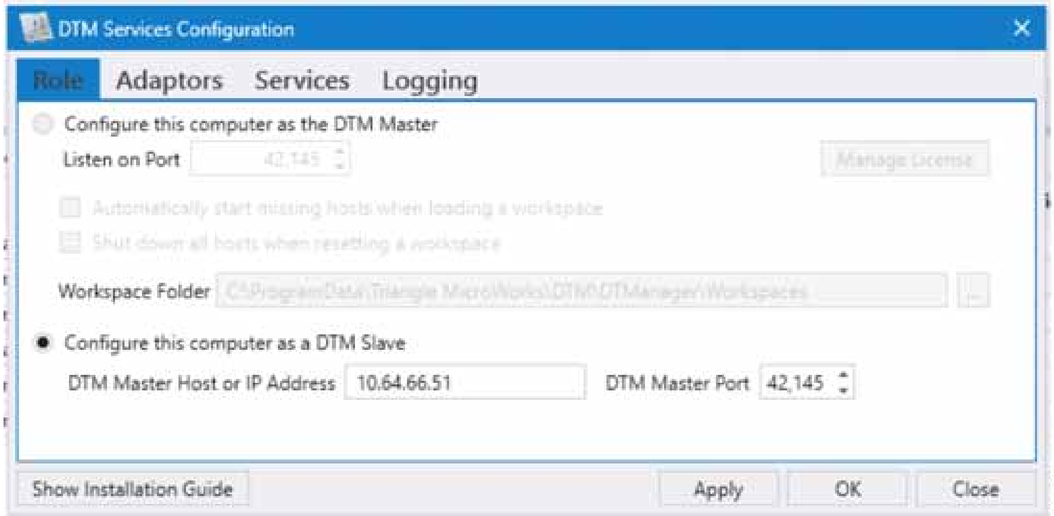
3. The chosen network interface adapter would be used for communication between the DTM Master and the DTM Slave/Client PC.

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 the TMW's DTM application.

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

Figure 123 DTM Outstation Role



DTM Services Configuration

Role | Adaptors | Services | Logging

○ Configure this computer as the DTM Master

Listen on Port 42,145

□ Automatically start missing hosts when loading a workspace

□ Shut down all hosts when resetting a workspace

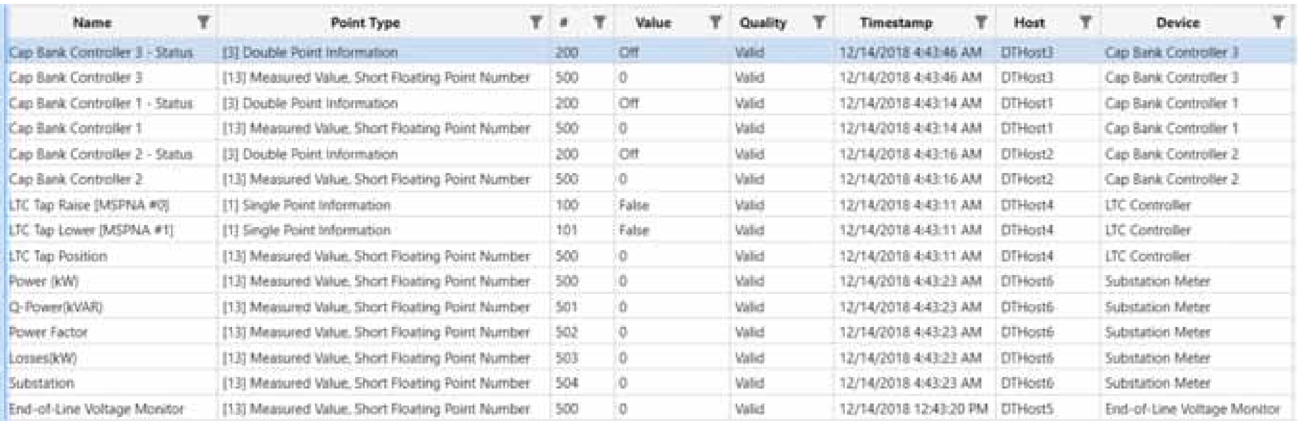
Workspace Folder C:\ProgramData\Triangle MicroWorks\DTM\DTManager\Workspaces

● Configure this computer as a DTM Slave

DTM Master Host or IP Address 10.64.66.51 DTM Master Port 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 entire outstation configuration is automatically loaded into the client machine as well as the outstation or IED data points per the details in Figure 124:

Figure 124 DTM Outstation Data Points



Name	Point Type	#	Value	Quality	Timestamp	Host	Device
Cap Bank Controller 3 - Status	[3] Double Point Information	200	Off	Valid	12/14/2018 4:43:46 AM	DTHost3	Cap Bank Controller 3
Cap Bank Controller 3	[13] Measured Value, Short Floating Point Number	500	0	Valid	12/14/2018 4:43:46 AM	DTHost3	Cap Bank Controller 3
Cap Bank Controller 1 - Status	[3] Double Point Information	200	Off	Valid	12/14/2018 4:43:14 AM	DTHost1	Cap Bank Controller 1
Cap Bank Controller 1	[13] Measured Value, Short Floating Point Number	500	0	Valid	12/14/2018 4:43:14 AM	DTHost1	Cap Bank Controller 1
Cap Bank Controller 2 - Status	[3] Double Point Information	200	Off	Valid	12/14/2018 4:43:16 AM	DTHost2	Cap Bank Controller 2
Cap Bank Controller 2	[13] Measured Value, Short Floating Point Number	500	0	Valid	12/14/2018 4:43:16 AM	DTHost2	Cap Bank Controller 2
LTC Tap Raise [MSPNA #0]	[1] Single Point Information	100	False	Valid	12/14/2018 4:43:11 AM	DTHost4	LTC Controller
LTC Tap Lower [MSPNA #1]	[1] Single Point Information	101	False	Valid	12/14/2018 4:43:11 AM	DTHost4	LTC Controller
LTC Tap Position	[13] Measured Value, Short Floating Point Number	500	0	Valid	12/14/2018 4:43:11 AM	DTHost4	LTC Controller
Power (kW)	[13] Measured Value, Short Floating Point Number	500	0	Valid	12/14/2018 4:43:23 AM	DTHost6	Substation Meter
Q-Power(kVAR)	[13] Measured Value, Short Floating Point Number	501	0	Valid	12/14/2018 4:43:23 AM	DTHost6	Substation Meter
Power Factor	[13] Measured Value, Short Floating Point Number	502	0	Valid	12/14/2018 4:43:23 AM	DTHost6	Substation Meter
Losses(kW)	[13] Measured Value, Short Floating Point Number	503	0	Valid	12/14/2018 4:43:23 AM	DTHost6	Substation Meter
Substation	[13] Measured Value, Short Floating Point Number	504	0	Valid	12/14/2018 4:43:23 AM	DTHost6	Substation Meter
End-of-Line Voltage Monitor	[13] Measured Value, Short Floating Point Number	500	0	Valid	12/14/2018 12:43:20 PM	DTHost5	End-of-Line Voltage Monitor

Eximprod Virtual Remote Terminal Unit

Eximprod's Virtual RTU is installed on the Industrial Router located in the substation. The Control Center and outstation device data points mapping are configured on the Virtual RTU using Eximprod's ES200 Windows application.

- Eximprod's ES200 installation guide is available at the following URL:
  - http://www.epg.ro/wp-content/uploads/2017/09/ES200-Datasheet-public.pdf
- Virtual RTU IOx application life cycle management guide is available at the following URL:
  - https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/FAN/Virtual-RTU/IG/CU-VRTU-IG/CU-VRTU-IG.html

Alternatively, the virtual RTU application can also be installed from the Local Manager GUI. Please refer to the link for installation steps in the IOx Local Manager Guide at the following URL:

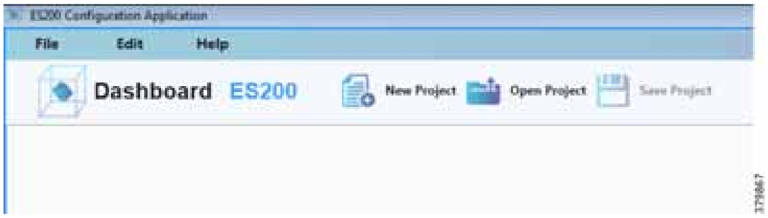
- https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/1-2-0/iox_local_manager_ref_guide.html

Launch the ES200 application and complete the following steps to configure the Control Center data points and the Outstation device points.

Control Center and IED Channel Configuration

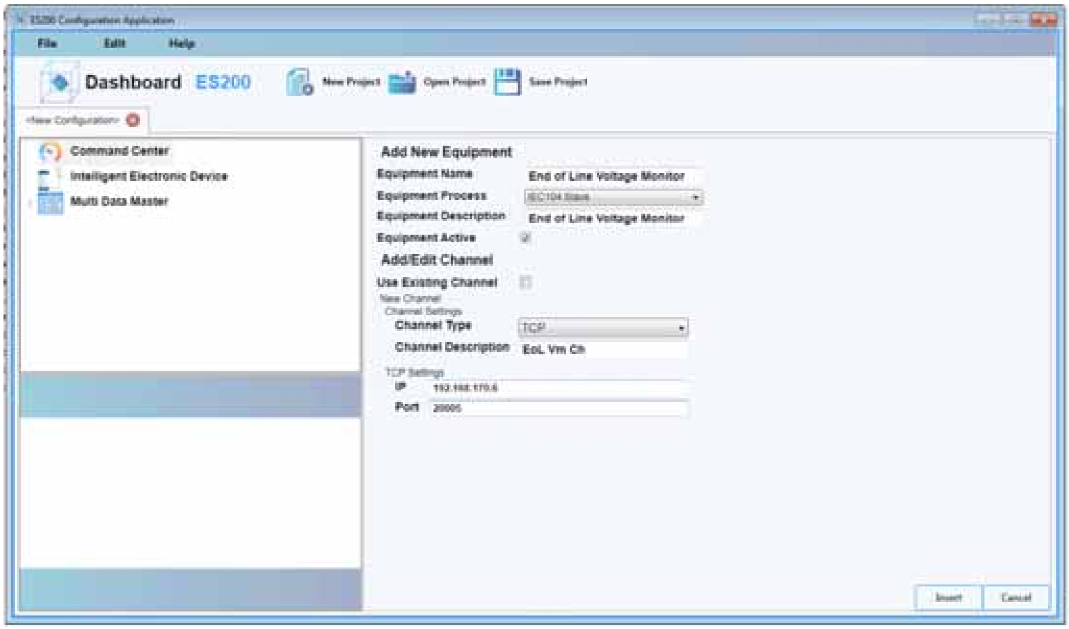
1. Launch the ES200 application and click **New Project**.

Figure 125 Eximprod Create New Project



2. Create a Control Center.

Figure 126 Eximprod Create Control / Command Center



Add New Equipment

Equipment Name: End of Line Voltage Monitor

Equipment Process: IEC104 Slave

Equipment Description: End of Line Voltage Monitor

Equipment Active: ☑

Add/Edit Channel

Use Existing Channel: □

New Channel

Channel Settings

Channel Type: TCP

Channel Description: EoL Vm Ch

TCP Settings

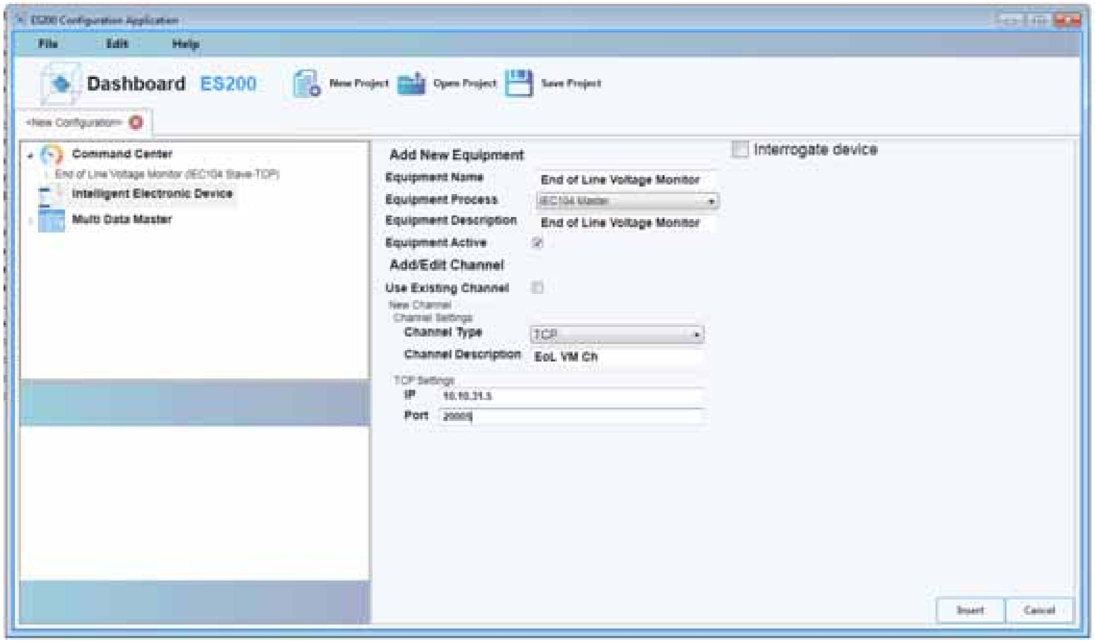
IP: 192.168.170.6

Port: 20005

3. Choose **Equipment Process** as IEC104 Slave and provide the SCADA Control Center IP and Port number. Continue with the default settings in other fields.

4. Create an IED.

Figure 127 Eximprod Create IED / Outstation



Add New Equipment

□ Interrogate device

Equipment Name: End of Line Voltage Monitor

Equipment Process: IEC104 Master

Equipment Description: End of Line Voltage Monitor

Equipment Active: ☑

Add/Edit Channel

Use Existing Channel: □

New Channel

Channel Settings

Channel Type: TCP

Channel Description: EoL VM Ch

TCP Settings

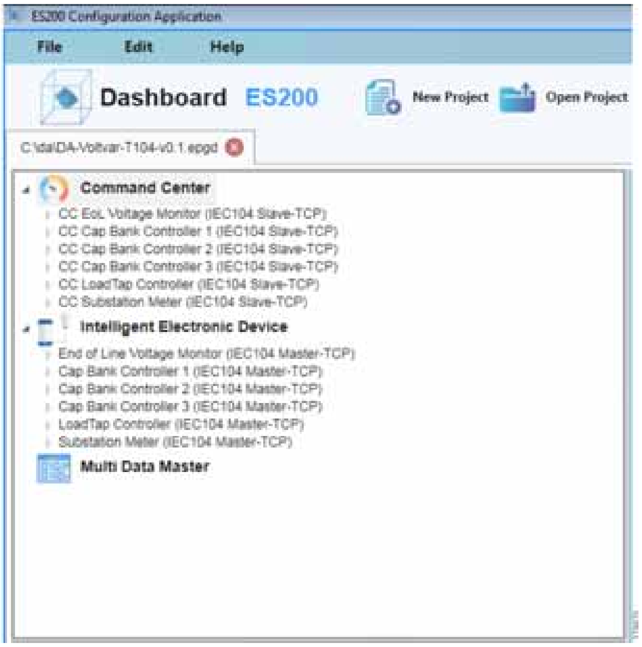
IP: 10.10.31.5

Port: 20005

5. Choose **Equipment Process** as IEC104 Master and provide the IED IP and Port number. Continue with the default settings in other fields.

6. Repeat Steps 2 and 3 to create all Control Center and IEDs.

Figure 128 Eximprod Complete Control Center and IED Created



ES200 Configuration Application

File Edit Help

Dashboard ES200 New Project Open Project

C:\da\DA-Voltvar-T104-v0.1.epgd

Command Center

- CC EoL Voltage Monitor (IEC104 Slave-TCP)
- CC Cap Bank Controller 1 (IEC104 Slave-TCP)
- CC Cap Bank Controller 2 (IEC104 Slave-TCP)
- CC Cap Bank Controller 3 (IEC104 Slave-TCP)
- CC LoadTap Controller (IEC104 Slave-TCP)
- CC Substation Meter (IEC104 Slave-TCP)

Intelligent Electronic Device

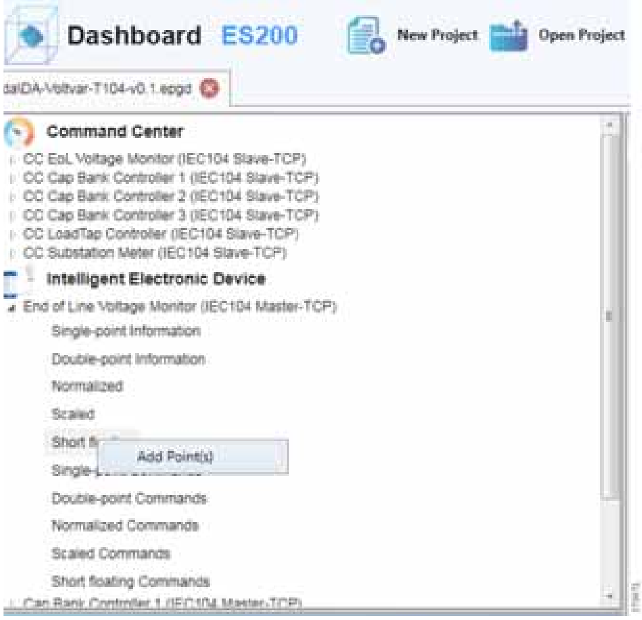
- End of Line Voltage Monitor (IEC104 Master-TCP)
- Cap Bank Controller 1 (IEC104 Master-TCP)
- Cap Bank Controller 2 (IEC104 Master-TCP)
- Cap Bank Controller 3 (IEC104 Master-TCP)
- LoadTap Controller (IEC104 Master-TCP)
- Substation Meter (IEC104 Master-TCP)

Multi Data Master

Outstation Data Points

7. Create IED data points with appropriate register types. Right-click on the IED Register List to add a register.

Figure 129 Eximprod IED Data Point Creation



Dashboard ES200 New Project Open Project

da\DA-Voltvar-T104-v0.1.epgd

Command Center

- CC EoL Voltage Monitor (IEC104 Slave-TCP)
- CC Cap Bank Controller 1 (IEC104 Slave-TCP)
- CC Cap Bank Controller 2 (IEC104 Slave-TCP)
- CC Cap Bank Controller 3 (IEC104 Slave-TCP)
- CC LoadTap Controller (IEC104 Slave-TCP)
- CC Substation Meter (IEC104 Slave-TCP)

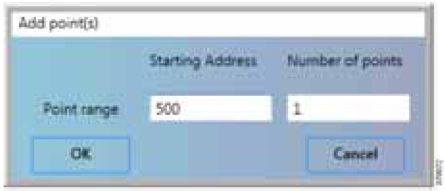
Intelligent Electronic Device

- End of Line Voltage Monitor (IEC104 Master-TCP)
  - Single-point Information
  - Double-point Information
  - Normalized
  - Scaled
  - Short fl
  - Single-
  - Double-point Commands
  - Normalized Commands
  - Scaled Commands
  - Short floating Commands
- Cap Bank Controller 1 (IEC104 Master-TCP)

Add Point(s)

8. Provide the starting address and number of register to create.

Figure 130 Eximprod IED Data Point Register Configuration



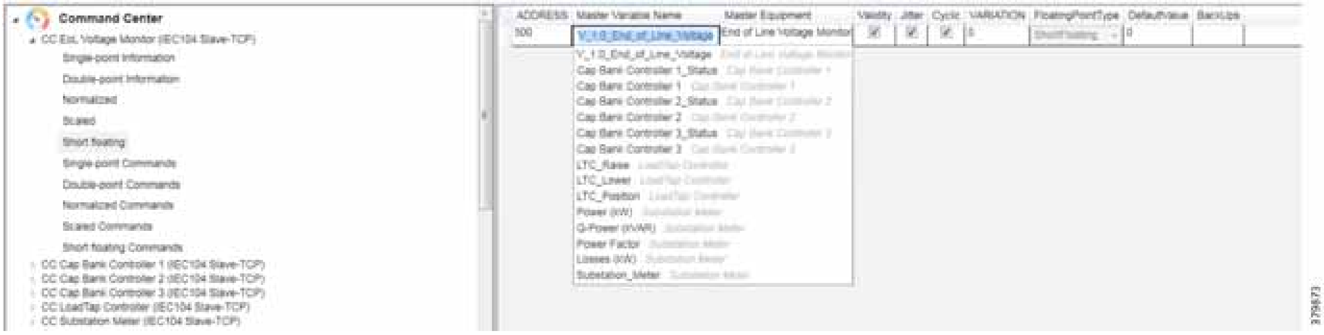
	Starting Address	Number of points
Point range	500	1

Data Points Mapping to Control Center

9. Repeat Steps 5 and 6 to create Control Center data points for all the IED data points.

10. Map the IED data points to Control Center data points.

Figure 131 Eximprod Control Center and IED Data Points Mapping

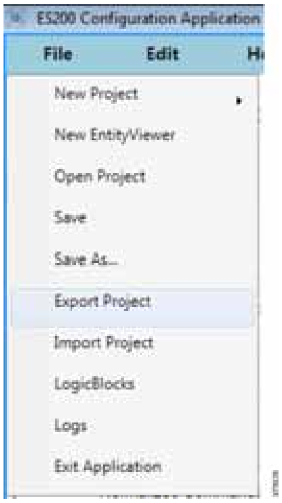

Command Center
CC EoL Voltage Monitor (IEC104 Slave-TCP)
Single-point Information
Double-point Information
Normalized
Scaled
Short floating
Single-point Commands
Double-point Commands
Normalized Commands
Scaled Commands
Short floating Commands
CC Cap Bank Controller 1 (IEC104 Slave-TCP)
CC Cap Bank Controller 2 (IEC104 Slave-TCP)
CC Cap Bank Controller 3 (IEC104 Slave-TCP)
CC LoadTap Controller (IEC104 Slave-TCP)
CC Substation Meter (IEC104 Slave-TCP)
V_1.0_End_of_Line_Voltage End of Line Voltage Monitor
Cap Bank Controller 1_Status Cap Bank Controller 1
Cap Bank Controller 1 Cap Bank Controller 1
Cap Bank Controller 2_Status Cap Bank Controller 2
Cap Bank Controller 2 Cap Bank Controller 2
Cap Bank Controller 3_Status Cap Bank Controller 3
Cap Bank Controller 3 Cap Bank Controller 3
LTC_Raise LoadTap Controller
LTC_Lower LoadTap Controller
LTC_Position LoadTap Controller
Power (kW) Substation Meter
Q-Power (kVAR) Substation Meter
Power Factor Substation Meter
Losses (kW) Substation Meter
Substation_Meter Substation Meter
379673

ADDRESS	Master Variable Name	Master Equipment	Validity	Jitter	Cyclic	VARIATION	FloatingPointType	DefaultValue	BackUps
500	V_1.0_End_of_Line_Voltage	End of Line Voltage Monitor	☑	☑	☑	5	ShortFloating	0	

11. Map all IED data points to Control Center data points and save the database.

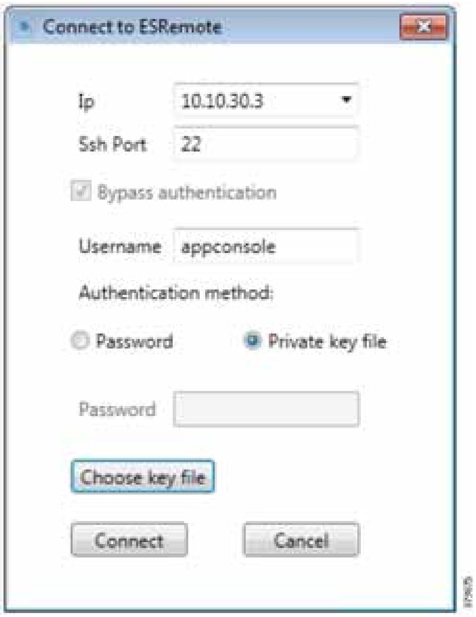
12. To export the Virtual RTU database to Industrial Router, choose **File > Export Project**.

Figure 132 Eximprod Export Project



13. Provide IOx IP, SSH Port, username and PEM file as private key file and then click **Connect**.

Figure 133 Eximprod Export Project - Connect to ESRemote



Connect to ESRemote

Ip: 10.10.30.3

Ssh Port: 22

☑ Bypass authentication

Username: appconsole

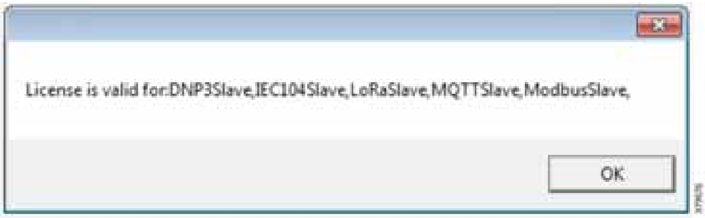
Authentication method:

○ Password ● Private key file

Password:

14. Choose the correct database to export from the **Open** dialogue box. Click **OK** to continue.

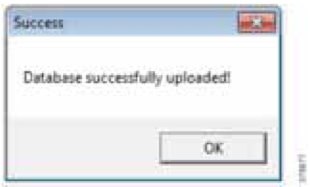
Figure 134 Eximprod License Info



License is valid for:DNP3Slave,IEC104Slave,LoRaSlave,MQTTSlave,ModbusSlave,

15. Click **OK** to continue.

Figure 135 Eximprod DB Upload Status



Success

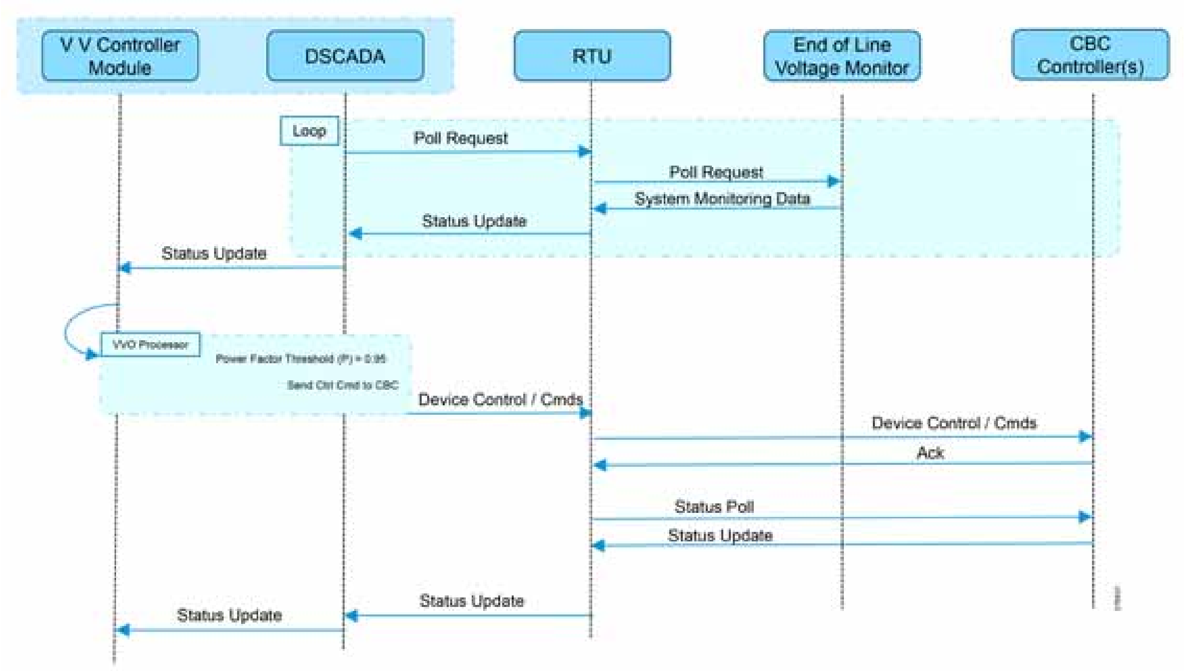
Database successfully uploaded!

VAR Control (Power Factor Regulation)

VAR Control is achieved with the Capacitor Bank Controller On/Off operation.

Event Sequence Diagram

Figure 136 Volt/VAR–VAR Control Sequence Diagram



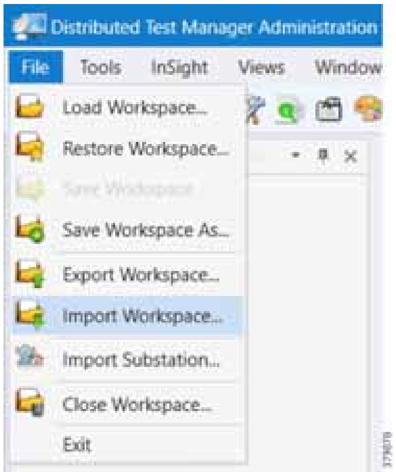
Use Case Steps

1. Event class data poll to the following devices from the RTU:
   - Substation meter, poll Measured Value (Short Floating Point) registers
   - All Capacitor Bank Controller(s), poll Measured Value (Short Floating Point) and Double Point registers
   - End-of-Line voltage monitor, poll Measured Value (Short Floating Point) 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 is sent to the RTU via SCADA to the capacitor banks to close capacitor bank controller N by writing in a Double Point Register of T104.
4. Event class data poll to the following devices from the RTU:
   - Substation meter, poll Measured Value (Short Floating Point) registers
   - All Capacitor Bank Controller(s), poll Measured Value (Short Floating Point) and Double Point registers
   - End-of-Line voltage monitor, poll Measured Value (Short Floating Point) register
5. The above steps are repeated for all the capacitor bank controllers on the feeder line to maintain a power factor value always close to value 1.

VAR Control Use Case Simulation

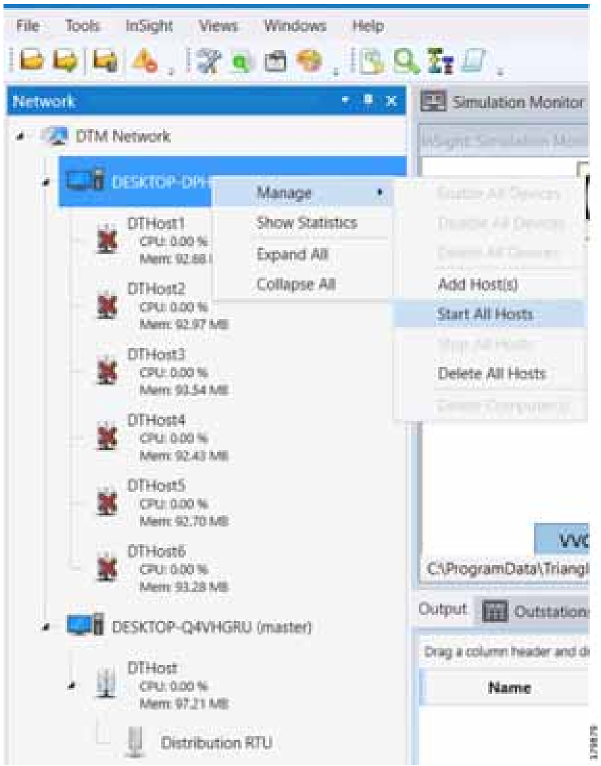
1. Import the Volt/VAR workspace, which is available in Appendix E: End-to-End Application Use Case Scenarios, page 212.

Figure 137 DTM Import Workspace



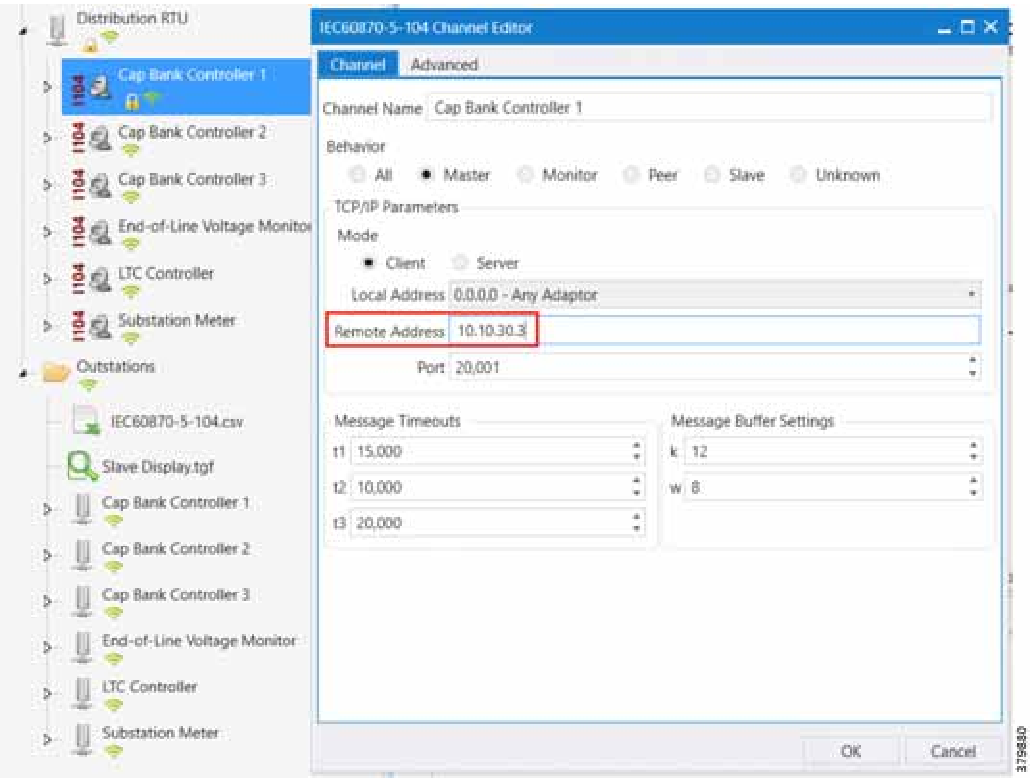
2. Start all the host machines.

Figure 138 DTM VVC Start All Hosts



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

Figure 139 DTM VVC Channel IP Config



Channel Name: Cap Bank Controller 1

Behavior: ○ All ● Master ○ Monitor ○ Peer ○ Slave ○ Unknown

TCP/IP Parameters

Mode: ● Client ○ Server

Local Address: 0.0.0.0 - Any Adaptor

Remote Address: 10.10.30.3

Port: 20,001

Message Timeouts

t1: 15,000

t2: 10,000

t3: 20,000

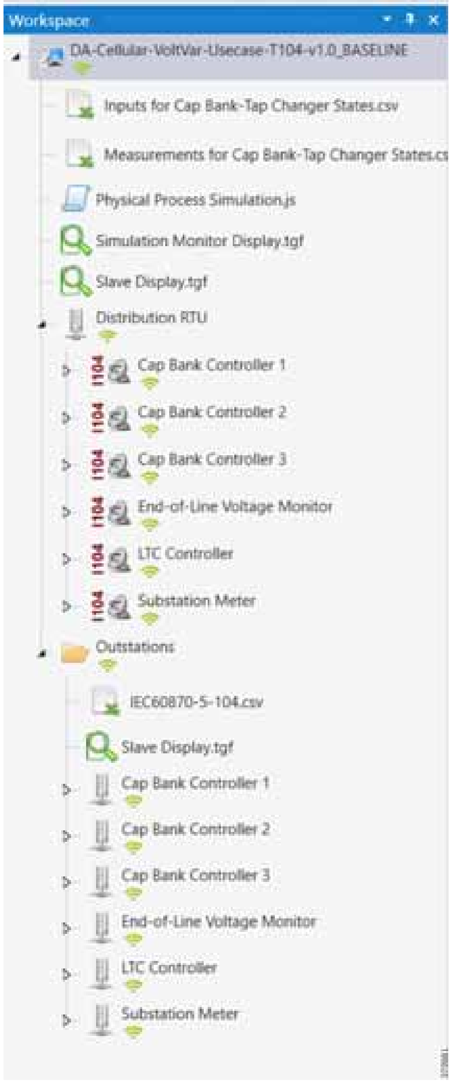
Message Buffer Settings

k: 12

w: 8

4. Make sure all the channels are connected.

Figure 140 DTM VVC Channel Status

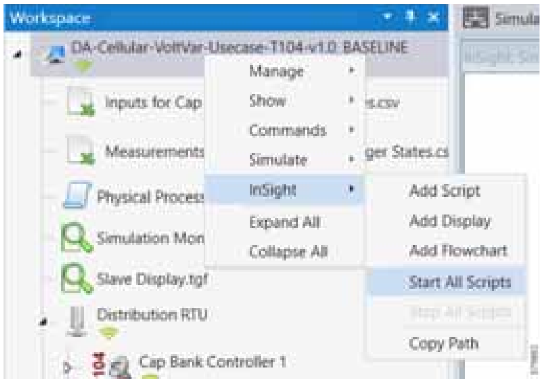


Workspace

- DA-Cellular-VoltVar-Usecase-T104-v1.0_BASELINE
  - Inputs for Cap Bank-Tap Changer States.csv
  - Measurements for Cap Bank-Tap Changer States.cs
  - Physical Process Simulation.js
  - Simulation Monitor Display.tgf
  - Slave Display.tgf
  - Distribution RTU
    - I104 Cap Bank Controller 1
    - I104 Cap Bank Controller 2
    - I104 Cap Bank Controller 3
    - I104 End-of-Line Voltage Monitor
    - I104 LTC Controller
    - I104 Substation Meter
  - Outstations
    - IEC60870-5-104.csv
    - Slave Display.tgf
    - Cap Bank Controller 1
    - Cap Bank Controller 2
    - Cap Bank Controller 3
    - End-of-Line Voltage Monitor
    - LTC Controller
    - Substation Meter

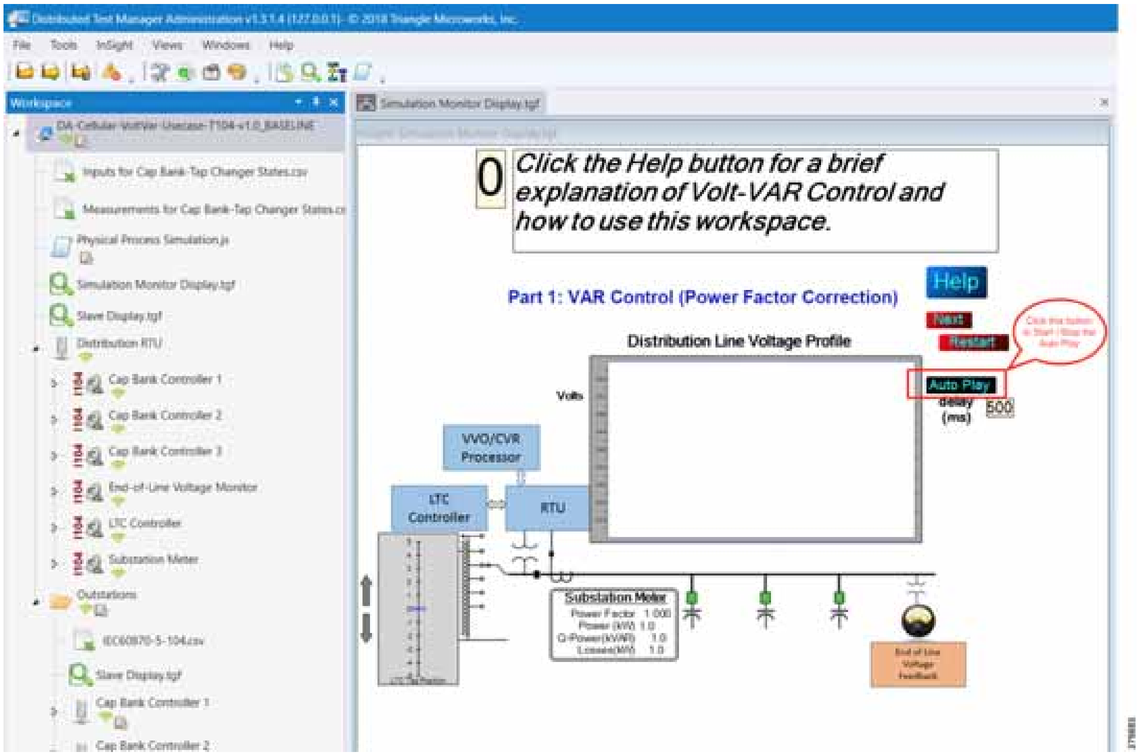
5. Start all the scripts.

Figure 141 DTM VVC Start All Scripts



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

Figure 142 DTM VVC Simulation Auto Play

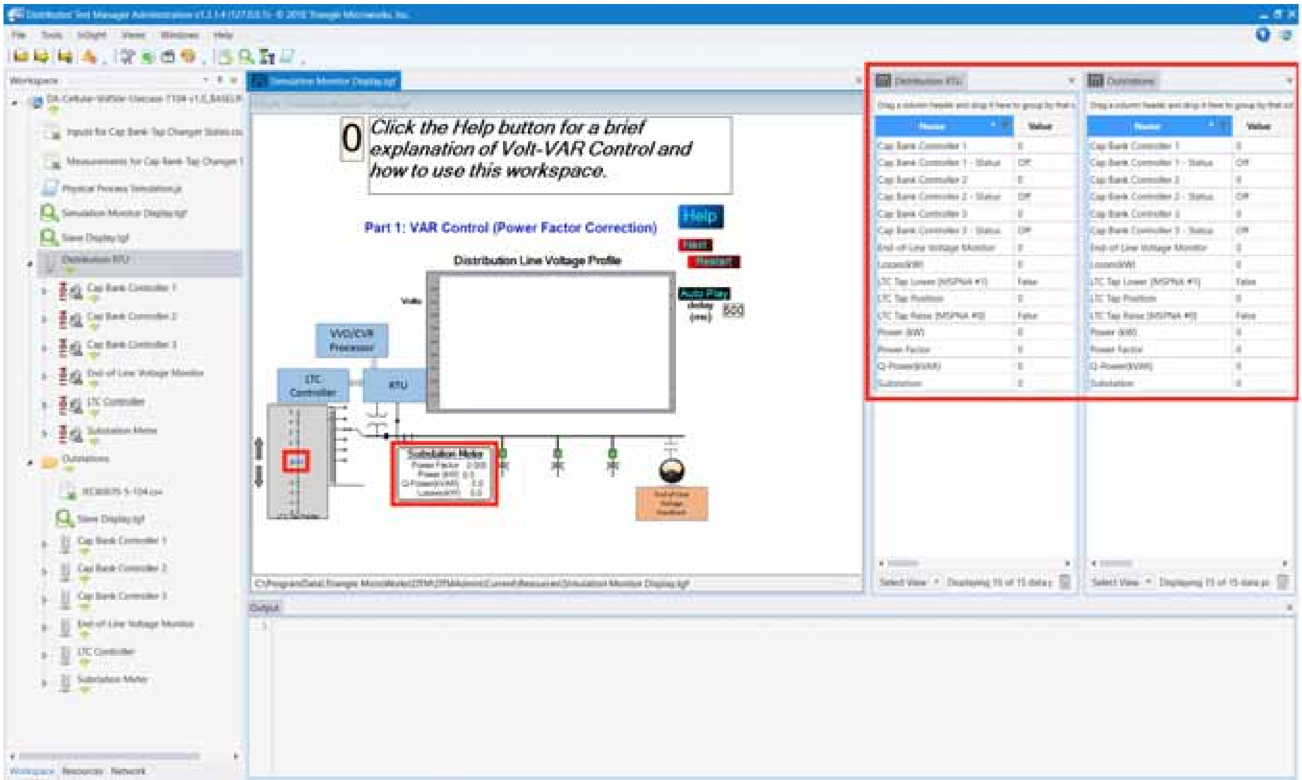

Distributed Test Manager Administration v1.3.1.4 (127.0.0.1) - © 2018 Triangle Microworks, Inc.
File
Tools
InSight
Views
Windows
Help
Workspace
DA-Cellular-VoltVar-Usecase-T104-v1.0_BASELINE
Inputs for Cap Bank-Tap Changer States.csv
Measurements for Cap Bank-Tap Changer States.cs
Physical Process Simulation.js
Simulation Monitor Display.tgf
Slave Display.tgf
Distribution RTU
104
Cap Bank Controller 1
Cap Bank Controller 2
Cap Bank Controller 3
End-of-Line Voltage Monitor
LTC Controller
Substation Meter
Outstations
IEC60870-5-104.csv
Slave Display.tgf
Cap Bank Controller 1
Cap Bank Controller 2
Simulation Monitor Display.tgf
0
Help
Next
Restart
Click this button to Start / Stop the Auto Play
Auto Play
delay (ms)
500
Distribution Line Voltage Profile
Volts
VVO/CVR Processor
LTC Controller
RTU
Substation Meter
Power Factor 1.000
Power (kW) 1.0
Q-Power(kVAR) 1.0
Losses(kW) 1.0
End of Line Voltage Feedback
LTC Tap Position

Click the Help button for a brief explanation of Volt-VAR Control and how to use this workspace.

Part 1: VAR Control (Power Factor Correction)

7. The script, initialize the Outstation data points to default values.

Figure 143 DTM VVC Data Points Initialization


Simulation Monitor Display.tgf
0
Click the Help button for a brief explanation of Volt-VAR Control and how to use this workspace.
Part 1: VAR Control (Power Factor Correction)
Help
Next
Restart
Distribution Line Voltage Profile
Volts
Auto Play
delay (ms)
500
VVO/CVR Processor
LTC Controller
RTU
Substation Meter
Distribution RTU
Outstations
Workspace
Output
379884

Distribution RTU

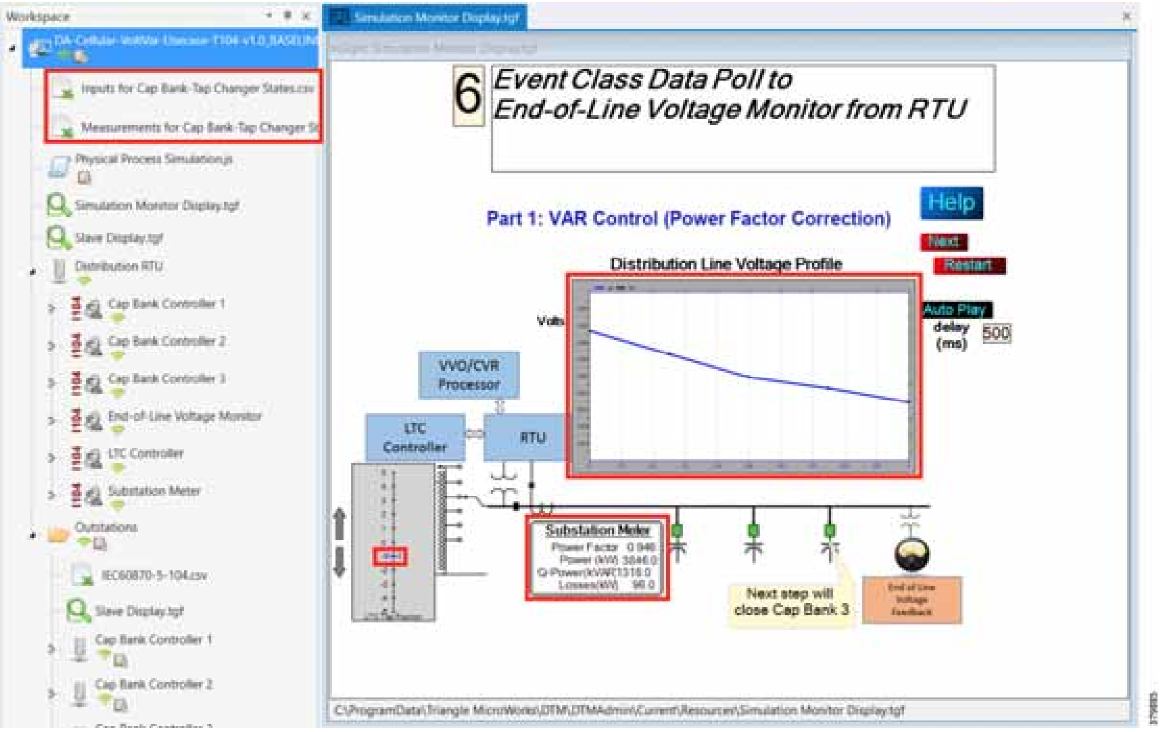
Name	Value
Cap Bank Controller 1	0
Cap Bank Controller 1 - Status	Off
Cap Bank Controller 2	0
Cap Bank Controller 2 - Status	Off
Cap Bank Controller 3	0
Cap Bank Controller 3 - Status	Off
End-of-Line Voltage Monitor	0
Losses(kW)	0
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	0
LTC Tap Raise (MSPNA #0)	False
Power (kW)	0
Power Factor	0
Q-Power(kVAR)	0
Substation	0

Outstations

Name	Value
Cap Bank Controller 1	0
Cap Bank Controller 1 - Status	Off
Cap Bank Controller 2	0
Cap Bank Controller 2 - Status	Off
Cap Bank Controller 3	0
Cap Bank Controller 3 - Status	Off
End-of-Line Voltage Monitor	0
Losses(kW)	0
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	0
LTC Tap Raise (MSPNA #0)	False
Power (kW)	0
Power Factor	0
Q-Power(kVAR)	0
Substation	0

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 144 DTM VVC Event Class Polling



6 *Event Class Data Poll to End-of-Line Voltage Monitor from RTU*

Substation Meter
Power Factor 0.946
Power (kW) 3846.0
Q-Power(kVAR)1318.0
Losses(kW) 96.0

Next step will close Cap Bank 3

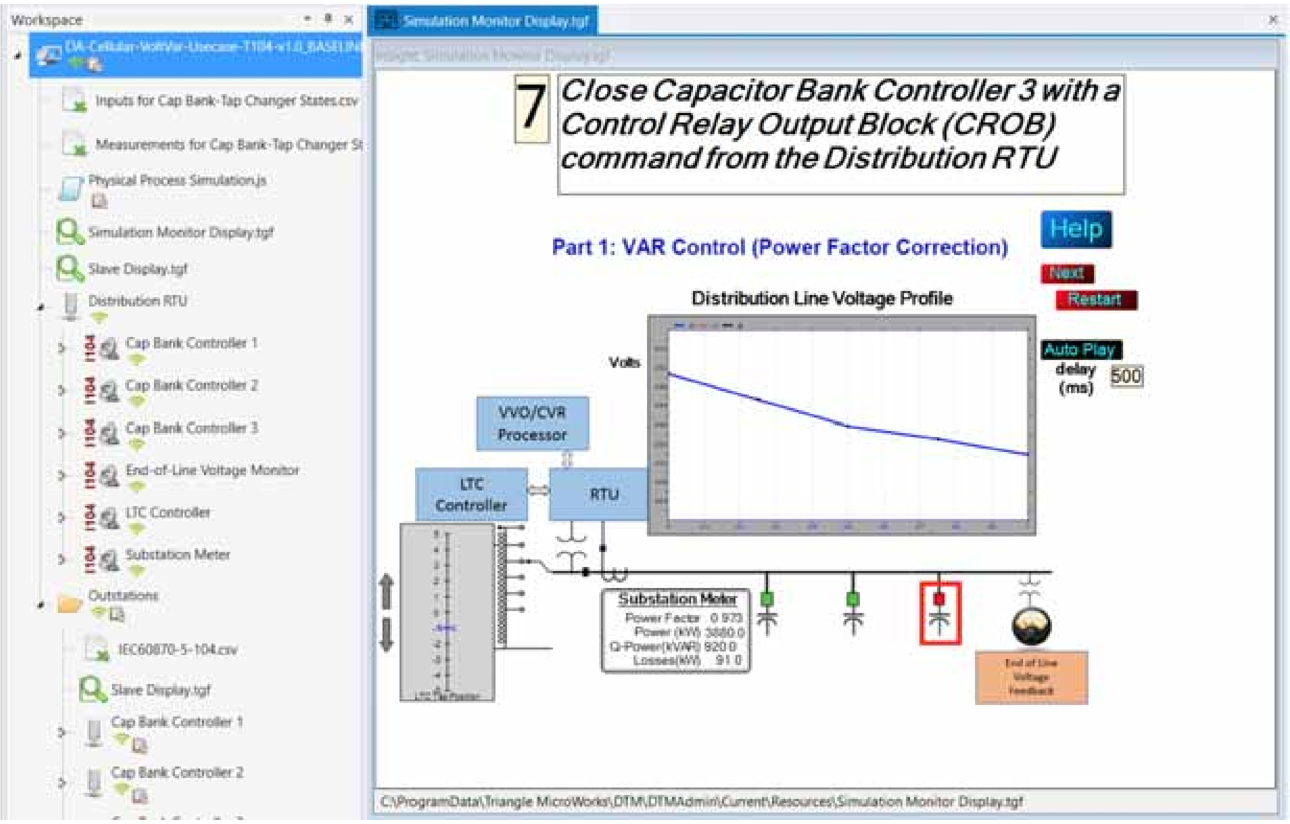
C:\ProgramData\Triangle MicroWorks\DTM\DTMAdmin\Current\Resources\Simulation Monitor Display.tgf

Workspace
DA-Cellular-VoltVar-Usecase-T104-v1.0_BASELINE
Inputs for Cap Bank-Tap Changer States.csv
Measurements for Cap Bank-Tap Changer St
Physical Process Simulation.js
Simulation Monitor Display.tgf
Slave Display.tgf
Distribution RTU
Cap Bank Controller 1
Cap Bank Controller 2
Cap Bank Controller 3
End-of-Line Voltage Monitor
LTC Controller
Substation Meter
Outstations
IEC60870-5-104.csv
Slave Display.tgf
Cap Bank Controller 1
Cap Bank Controller 2
Simulation Monitor Display.tgf
Part 1: VAR Control (Power Factor Correction)
Help
Next
Restart
Distribution Line Voltage Profile
Volts
Auto Play
delay (ms)
500
VVO/CVR Processor
LTC Controller
RTU
End-of-Line Voltage Feedback
379885

9. The Volt/VAR Optimization processor processes the data received from the devices and makes a control command decision based on the power factor calculation.

10. The control command is sent to the RTU via SCADA to the capacitor banks to close the Capacitor Bank Controller 3.

Figure 145 DTM VVC Cap Bank Controller Closing



7 Close Capacitor Bank Controller 3 with a Control Relay Output Block (CROB) command from the Distribution RTU

Substation Meter
Power Factor 0.973
Power (kW) 3880.0
Q-Power(kVAR) 920.0
Losses(kW) 91.0

C:\ProgramData\Triangle MicroWorks\DTM\DTMAdmin\Current\Resources\Simulation Monitor Display.tgf

Workspace
DA-Cellular-VoltVar-Usecase-T104-v1.0_BASELIN
Inputs for Cap Bank-Tap Changer States.csv
Measurements for Cap Bank-Tap Changer St
Physical Process Simulation.js
Simulation Monitor Display.tgf
Slave Display.tgf
Distribution RTU
I104 Cap Bank Controller 1
I104 Cap Bank Controller 2
I104 Cap Bank Controller 3
I104 End-of-Line Voltage Monitor
I104 LTC Controller
I104 Substation Meter
Outstations
IEC60870-5-104.csv
Slave Display.tgf
Cap Bank Controller 1
Cap Bank Controller 2
Simulation Monitor Display.tgf
Part 1: VAR Control (Power Factor Correction)
Help
Next
Restart
Auto Play
delay (ms)
500
Distribution Line Voltage Profile
Volts
VVO/CVR Processor
LTC Controller
RTU
LTC Tap Position
End of Line Voltage Feedback
379886

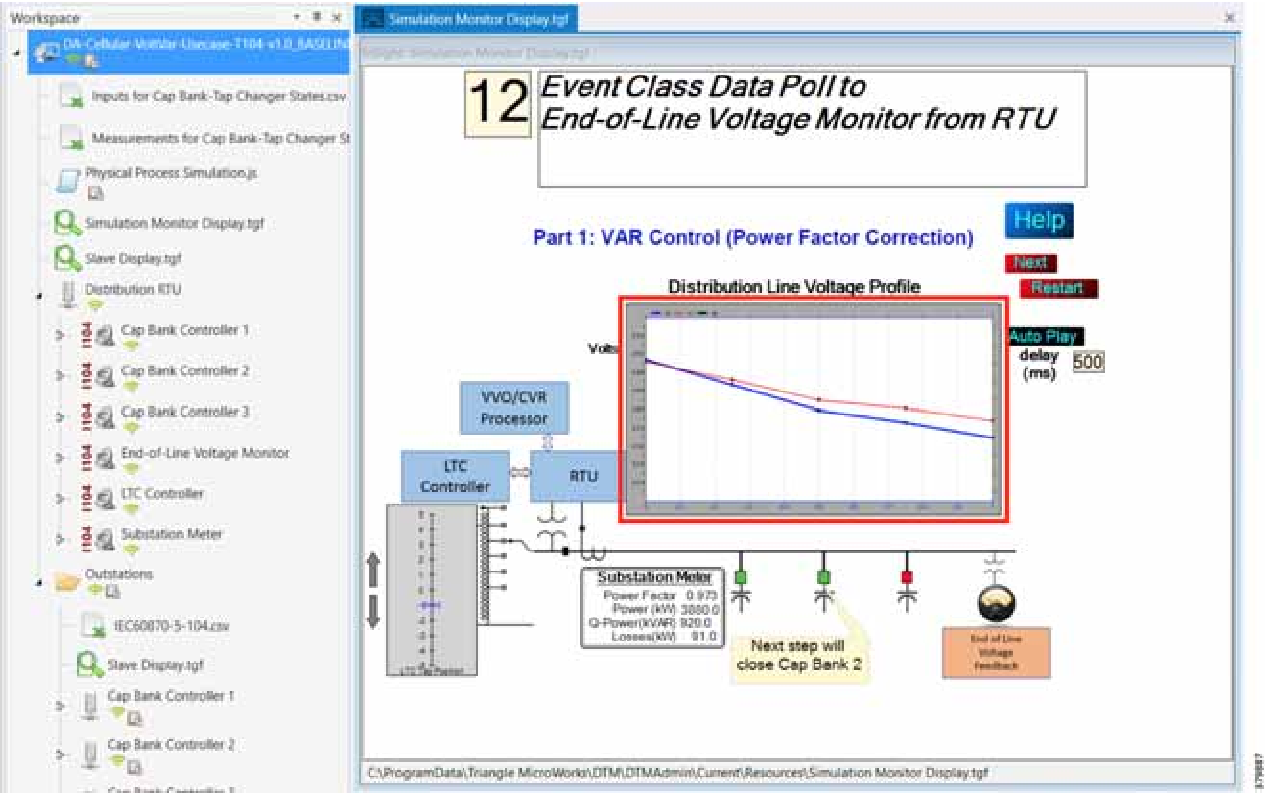
11. Event class data poll to the following devices from the RTU:

   – Substation meter, poll Measured Value (Short Floating Point) registers

   – All Capacitor Bank Controller(s), poll Measured Value (Short Floating Point) and Double Point registers

   – End-of-Line voltage monitor, poll Measured Value (Short Floating Point) register

Figure 146 DTM VVC Event Class Polling with CBC3 Closed



12 Event Class Data Poll to End-of-Line Voltage Monitor from RTU

Part 1: VAR Control (Power Factor Correction)

Substation Meter
Power Factor 0.973
Power (kW) 3880.0
Q-Power(kVAR) 920.0
Losses(kW) 91.0

Next step will close Cap Bank 2

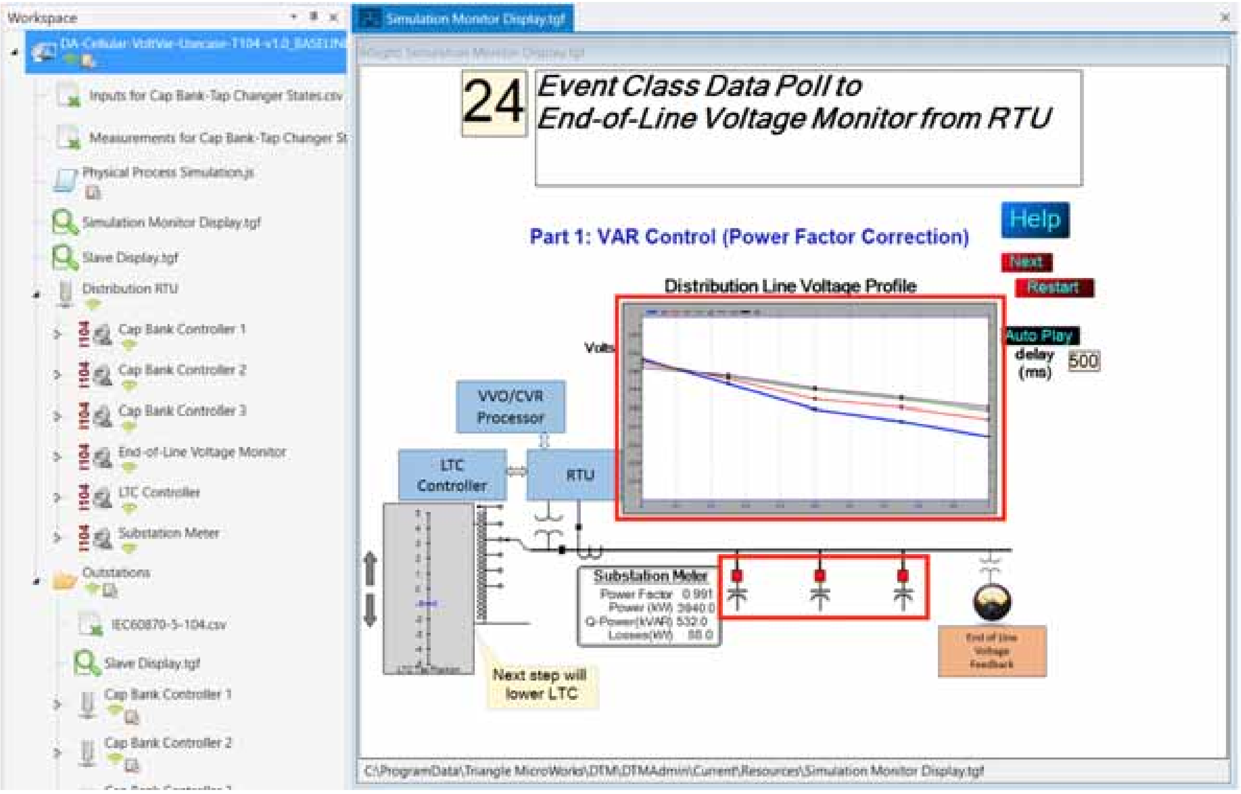
Auto Play delay (ms) 500

C:\ProgramData\Triangle MicroWorks\DTM\DTMAdmin\Current\Resources\Simulation Monitor Display.tgf

Workspace
DA-Cellular-VoltVar-Usecase-T104-v1.0_BASELIN
Inputs for Cap Bank-Tap Changer States.csv
Measurements for Cap Bank-Tap Changer St
Physical Process Simulation.js
Simulation Monitor Display.tgf
Slave Display.tgf
Distribution RTU
I104 Cap Bank Controller 1
I104 Cap Bank Controller 2
I104 Cap Bank Controller 3
I104 End-of-Line Voltage Monitor
I104 LTC Controller
I104 Substation Meter
Outstations
IEC60870-5-104.csv
Slave Display.tgf
Cap Bank Controller 1
Cap Bank Controller 2
Simulation Monitor Display.tgf
Help
Next
Restart
Distribution Line Voltage Profile
Volts
VVO/CVR Processor
LTC Controller
RTU
End of Line Voltage Feedback
379887

12. All the above steps are repeated for all capacitor bank controllers on the feeder line to maintain a power factor value always close to 1 at all the points in the feeder line.

Figure 147 DTM VVC All 3 Cap Bank Controller Closed


Workspace
DA-Cellular-VoltVar-Usecase-T104-v1.0_BASELINE
Inputs for Cap Bank-Tap Changer States.csv
Measurements for Cap Bank-Tap Changer St
Physical Process Simulation.js
Simulation Monitor Display.tgf
Slave Display.tgf
Distribution RTU
I104 Cap Bank Controller 1
I104 Cap Bank Controller 2
I104 Cap Bank Controller 3
I104 End-of-Line Voltage Monitor
I104 LTC Controller
I104 Substation Meter
Outstations
IEC60870-5-104.csv
Slave Display.tgf
Cap Bank Controller 1
Cap Bank Controller 2
Simulation Monitor Display.tgf
24
Event Class Data Poll to End-of-Line Voltage Monitor from RTU
Help
Part 1: VAR Control (Power Factor Correction)
Next
Restart
Distribution Line Voltage Profile
Volts
Auto Play
delay (ms)
500
VVO/CVR Processor
LTC Controller
RTU
Substation Meter
End of Line Voltage Feedback
Next step will lower LTC
LTC Tap Position

Substation Meter
Power Factor 0.991
Power (KW) 3940.0
Q-Power(kVAR) 532.0
Losses(KW) 58.0

C:\ProgramData\Triangle MicroWorks\DTM\DTMAdmin\Current\Resources\Simulation Monitor Display.tgf

13. To stop the simulation, click **Auto Play** again.

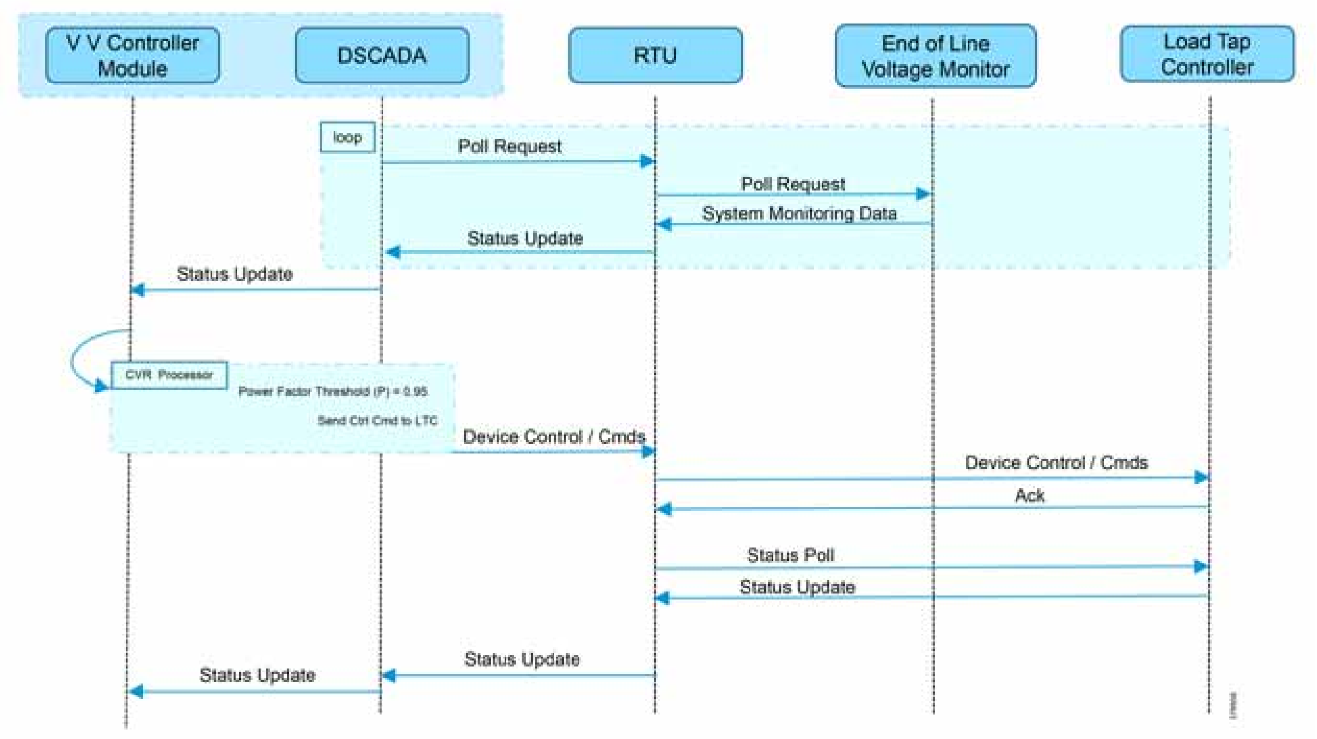
14. To re-start the simulation, click **Restart**.

Voltage Control (Conservation Voltage Reduction)

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

Event Sequence Diagram

Figure 148 Volt/VAR–CVR Sequence Diagram



Use Case Steps

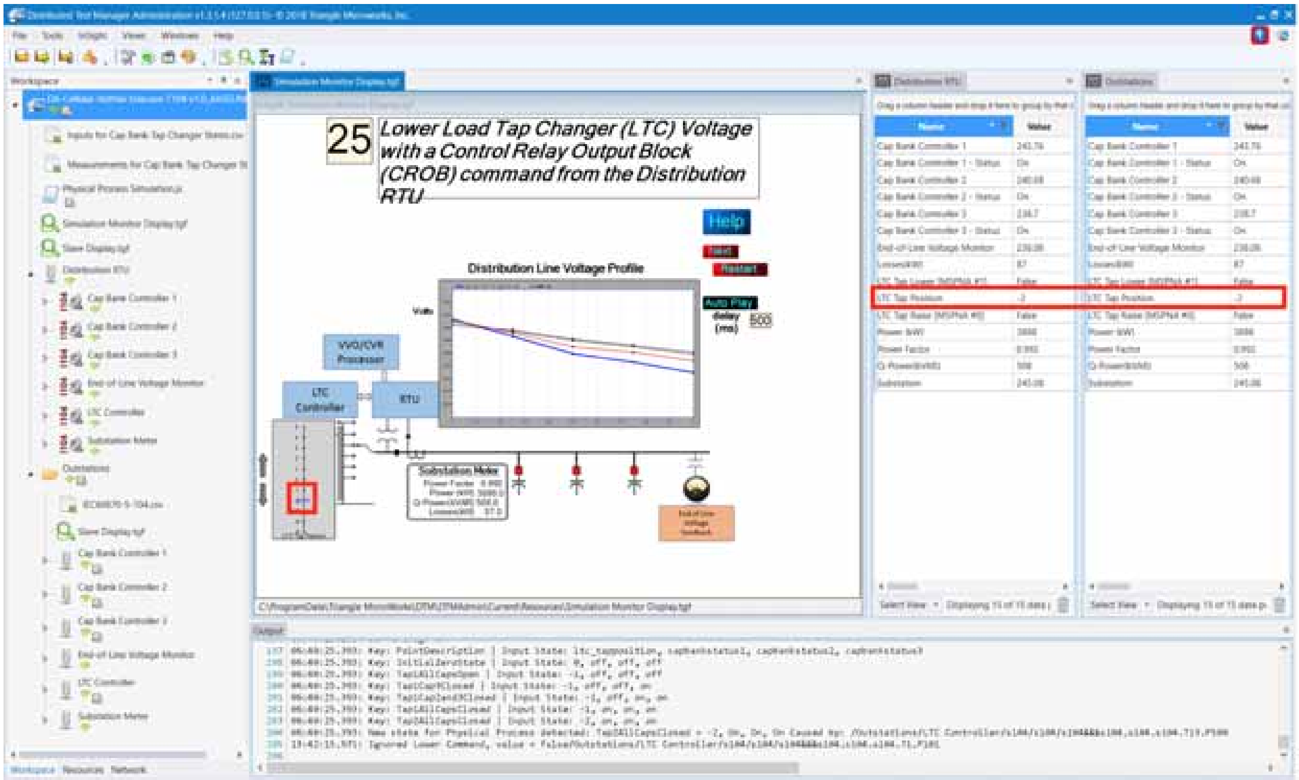
1. Event class data poll to the following devices from the RTU:
   - Substation meter, poll Measured Value (Short Floating Point) registers
   - All Capacitor Bank Controller(s), poll Measured Value (Short Floating Point) and Double Point registers
   - End-of-Line voltage monitor, poll Measured Value (Short Floating Point) 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 is sent to the RTU via SCADA to the LTC to Lower/Raise LTC.
4. Event class data poll to the following devices from the RTU:
   - Substation meter, poll Measured Value (Short Floating Point) registers
   - All Capacitor Bank Controller(s), poll Measured Value (Short Floating Point) and Double Point registers
   - End-of-Line voltage monitor, poll Measured Value (Short Floating Point) register
5. All the above steps are repeated to maintain Power Factor value always close to value 1.

CVR Use Case Simulation

Follow the steps 1 to 8, in VAR Control Use Case Simulation, page 131.

1. After following the steps above, this is the ninth step.
2. Control command is sent to the RTU via SCADA to the LTC to Lower/Raise LTC by writing in a command register. LTC is lowered to -2, by the script.

Figure 149 DTM CVR LTC Lowering



25 Lower Load Tap Changer (LTC) Voltage with a Control Relay Output Block (CROB) command from the Distribution RTU

Distribution RTU

Name	Value
Cap Bank Controller 1	241.76
Cap Bank Controller 1 - Status	On
Cap Bank Controller 2	240.48
Cap Bank Controller 2 - Status	On
Cap Bank Controller 3	238.7
Cap Bank Controller 3 - Status	On
End-of-Line Voltage Monitor	236.06
Losses(kW)	87
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	-2
LTC Tap Raise (MSPNA #0)	False
Power (kW)	3886
Power Factor	0.990
Q-Power(kVAR)	508
Substation	245.06

Outstations

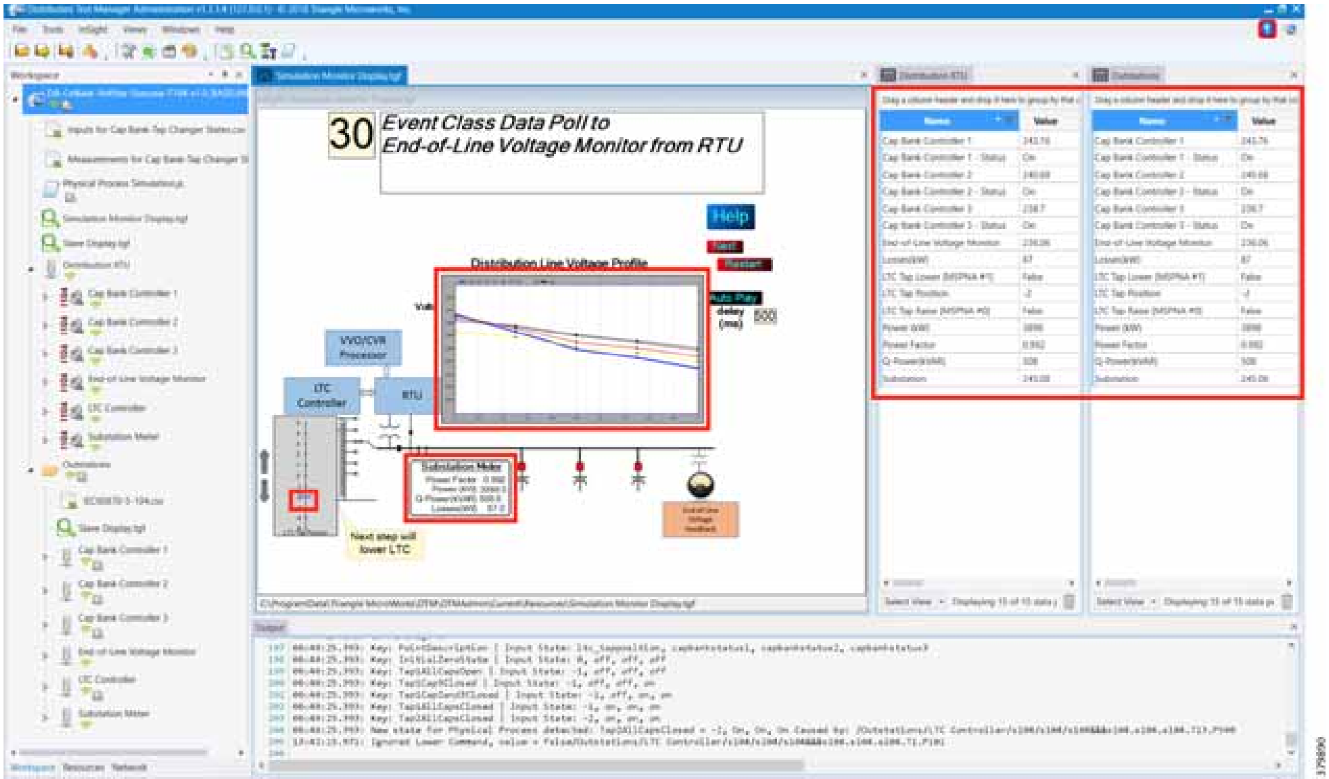
Name	Value
Cap Bank Controller 1	241.76
Cap Bank Controller 1 - Status	On
Cap Bank Controller 2	240.48
Cap Bank Controller 2 - Status	On
Cap Bank Controller 3	238.7
Cap Bank Controller 3 - Status	On
End-of-Line Voltage Monitor	236.06
Losses(kW)	87
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	-2
LTC Tap Raise (MSPNA #0)	False
Power (kW)	3886
Power Factor	0.990
Q-Power(kVAR)	508
Substation	245.06

C:\ProgramData\Triangle MicroWorks\DTM\DTMAdmin\Current\Resources\Simulation Monitor Display.tgf

```
06:40:25.393: Key: PointDescription | Input State: ltc_tapposition, capbankstatus1, capbankstatus2, capbankstatus3
06:40:25.393: Key: InitialZeroState | Input State: 0, off, off, off
06:40:25.393: Key: Tap1AllCapsOpen | Input State: -1, off, off, off
06:40:25.393: Key: Tap1Cap3Closed | Input State: -1, off, off, on
06:40:25.393: Key: Tap1Cap2and3Closed | Input State: -1, off, on, on
06:40:25.393: Key: Tap1AllCapsClosed | Input State: -1, on, on, on
06:40:25.393: Key: Tap2AllCapsClosed | Input State: -2, on, on, on
06:40:25.393: New state for Physical Process detected: Tap2AllCapsClosed = -2, On, On, On Caused by: /Outstations/LTC Controller/s104/s104/s104&&&s104.s104.s104.T1?.P100
13:42:15.571: Ignored Lower Command, value = False/Outstations/LTC Controller/s104/s104/s104&&&s104.s104.s104.T1.P101
```

3. Event class data poll to the following devices from the RTU:
   - Substation meter, poll Measured Value (Short Floating Point) registers
   - All Capacitor Bank Controller(s), poll Measured Value (Short Floating Point) and Double Point registers
   - End-of-Line voltage monitor, poll Measured Value (Short Floating Point) register

Figure 150 DTM CVR Event Class Polling



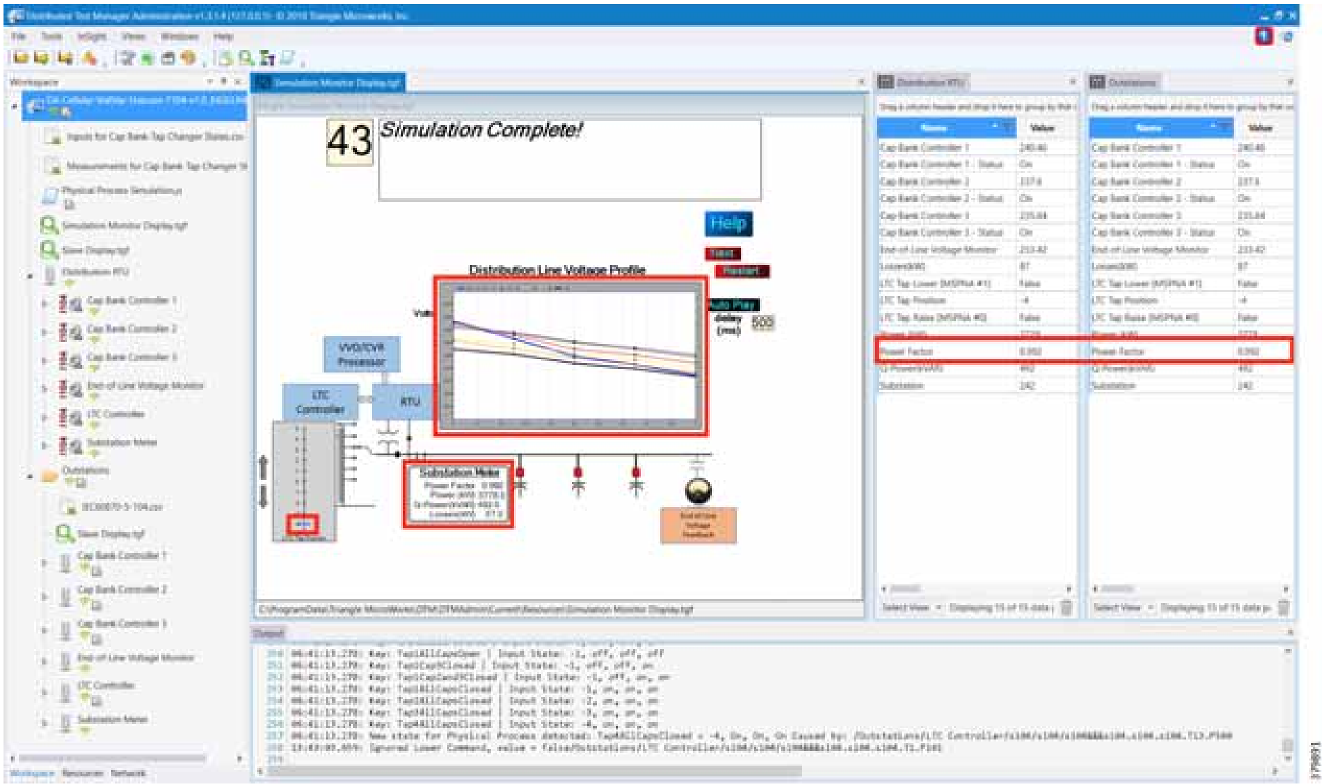
Name	Value
Cap Bank Controller 1	243.76
Cap Bank Controller 1 - Status	On
Cap Bank Controller 2	240.69
Cap Bank Controller 2 - Status	On
Cap Bank Controller 3	238.7
Cap Bank Controller 3 - Status	On
End-of-Line Voltage Monitor	236.06
Losses(kW)	87
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	-2
LTC Tap Raise (MSPNA #0)	False
Power (kW)	3898
Power Factor	0.992
Q-Power(kVAR)	508
Substation	245.08

Name	Value
Cap Bank Controller 1	243.76
Cap Bank Controller 1 - Status	On
Cap Bank Controller 2	240.69
Cap Bank Controller 2 - Status	On
Cap Bank Controller 3	238.7
Cap Bank Controller 3 - Status	On
End-of-Line Voltage Monitor	236.06
Losses(kW)	87
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	-2
LTC Tap Raise (MSPNA #0)	False
Power (kW)	3898
Power Factor	0.992
Q-Power(kVAR)	508
Substation	245.08

```
00:40:25.993: Key: PointDescription | Input State: ltc_tapposition, capbankstatus1, capbankstatus2, capbankstatus3
00:40:25.993: Key: InitialZeroState | Input State: 0, off, off, off
00:40:25.993: Key: Tap1AllCapsOpen | Input State: -1, off, off, off
00:40:25.993: Key: Tap1Cap3Closed | Input State: -1, off, off, on
00:40:25.993: Key: Tap1Cap2and3Closed | Input State: -1, off, on, on
00:40:25.993: Key: Tap1AllCapsClosed | Input State: -1, on, on, on
00:40:25.993: Key: Tap2AllCapsClosed | Input State: -2, on, on, on
00:40:25.993: New state for Physical Process detected: Tap2AllCapsClosed = -2, On, On, On Caused by: /Outstations/LTC Controller/[illegible]
12:41:15.971: Ignored Lower Command, value = False/Outstations/LTC Controller/[illegible]
```

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

Figure 151 DTM CVR End of Simulation



Substation Meter
Power Factor 0.992
Power (kW) 3778.3
Q-Power(kVAR) 492.5
Losses(kW) 87.3

Distribution RTU

Name	Value
Cap Bank Controller 1	240.46
Cap Bank Controller 1 - Status	On
Cap Bank Controller 2	237.6
Cap Bank Controller 2 - Status	On
Cap Bank Controller 3	235.84
Cap Bank Controller 3 - Status	On
End-of-Line Voltage Monitor	233.42
Losses(kW)	87
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	-4
LTC Tap Raise (MSPNA #0)	False
Power (kW)	3778
Power Factor	0.992
Q-Power(kVAR)	492
Substation	242

Outstations

Name	Value
Cap Bank Controller 1	240.46
Cap Bank Controller 1 - Status	On
Cap Bank Controller 2	237.6
Cap Bank Controller 2 - Status	On
Cap Bank Controller 3	235.84
Cap Bank Controller 3 - Status	On
End-of-Line Voltage Monitor	233.42
Losses(kW)	87
LTC Tap Lower (MSPNA #1)	False
LTC Tap Position	-4
LTC Tap Raise (MSPNA #0)	False
Power (kW)	3778
Power Factor	0.992
Q-Power(kVAR)	492
Substation	242

Select View Displaying 15 of 15 data

C:\ProgramData\Triangle MicroWorks\DTM\DTMAdmin\Current\Resources\Simulation Monitor Display.tgf

```
06:41:13.278: Key: Tap1AllCapsOpen | Input State: -1, off, off, off
06:41:13.278: Key: Tap1Cap3Closed | Input State: -1, off, off, on
06:41:13.278: Key: Tap1Cap2and3Closed | Input State: -1, off, on, on
06:41:13.278: Key: Tap1AllCapsClosed | Input State: -1, on, on, on
06:41:13.278: Key: Tap2AllCapsClosed | Input State: -2, on, on, on
06:41:13.278: Key: Tap3AllCapsClosed | Input State: -3, on, on, on
06:41:13.278: Key: Tap4AllCapsClosed | Input State: -4, on, on, on
06:41:13.278: New state for Physical Process detected: Tap4AllCapsClosed = -4, On, On, On Caused by: /Outstations/LTC Controller/s104/s104/s104&&&&s104.s104.s104.T13.P500
13:43:09.459: Ignored Lower Command, value = false/Outstations/LTC Controller/s104/s104/s104&&&&s104.s104.s104.T1.P101
```

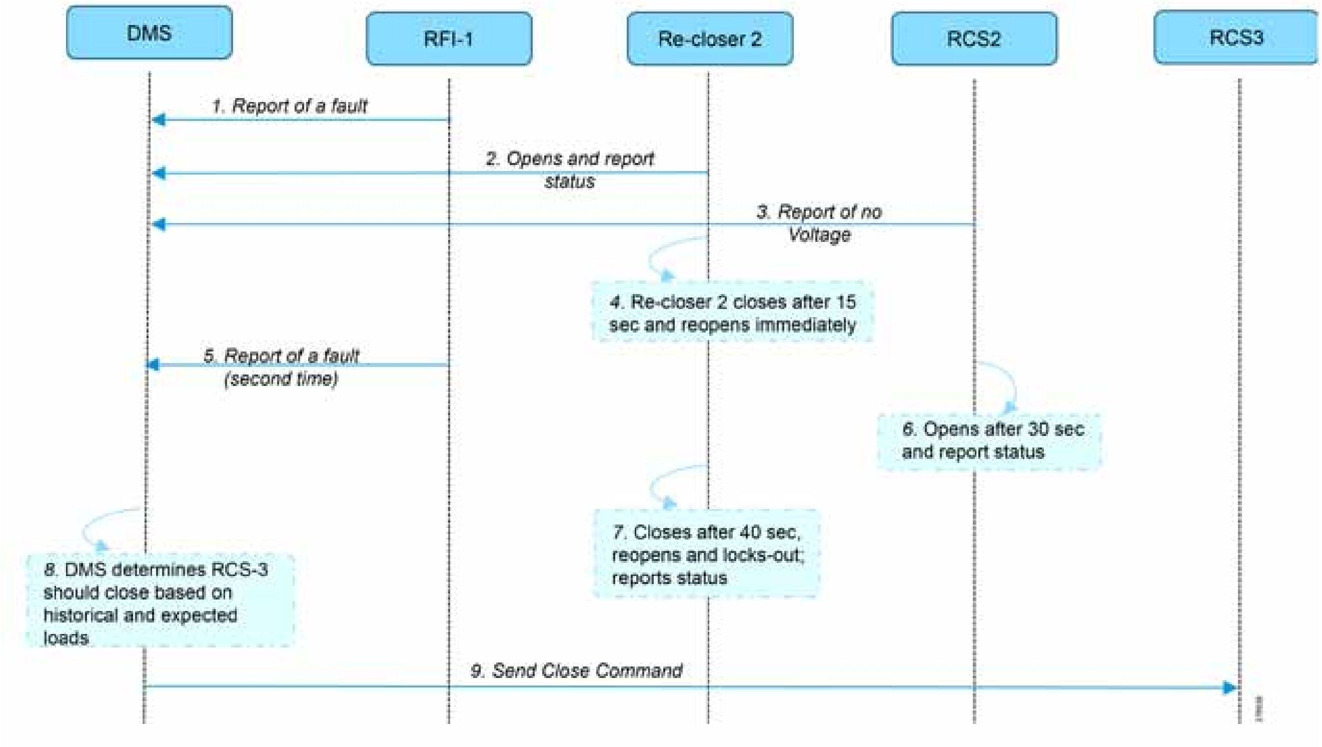
Fault Location, Isolation, and Service Restoration

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 the fault location and isolate the smallest possible section affected by the fault. Then restore the power to the larger possible section of the grid.

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

Event Sequence Diagram

Figure 152 FLISR–Semi-Automatic Sequence Diagram


DMS
RFI-1
Re-closer 2
RCS2
RCS3
1. Report of a fault
2. Opens and report status
3. Report of no Voltage
4. Re-closer 2 closes after 15 sec and reopens immediately
5. Report of a fault (second time)
6. Opens after 30 sec and report status
7. Closes after 40 sec, reopens and locks-out; reports status
8. DMS determines RCS-3 should close based on historical and expected loads
9. Send Close Command

Use Case Steps

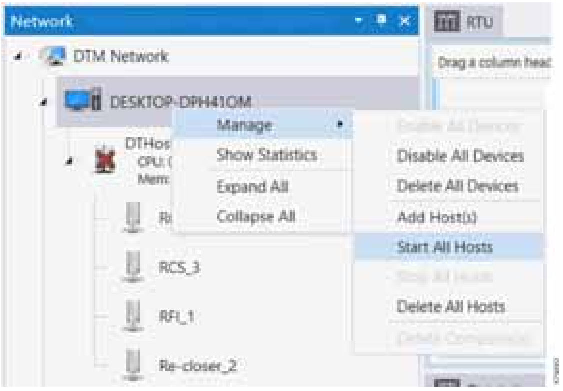
1. Remote Fault Indicator (RFI) 1 reports to Distribution Management System (DMS) whenever it encounters a fault.
2. Re-closer 2 opens and send a report to DMS when it encounters a temporary fault.
3. Remote Control Switch (RCS) 2 reports no voltage status to DMS.
4. RCS 2 closes after 15 seconds and 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 reports status to DMS.
8. DMS determines to issue a close command to RCS 3.
9. 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: End-to-End Application Use Case Scenarios, page 212.

2. Start all the host machines.

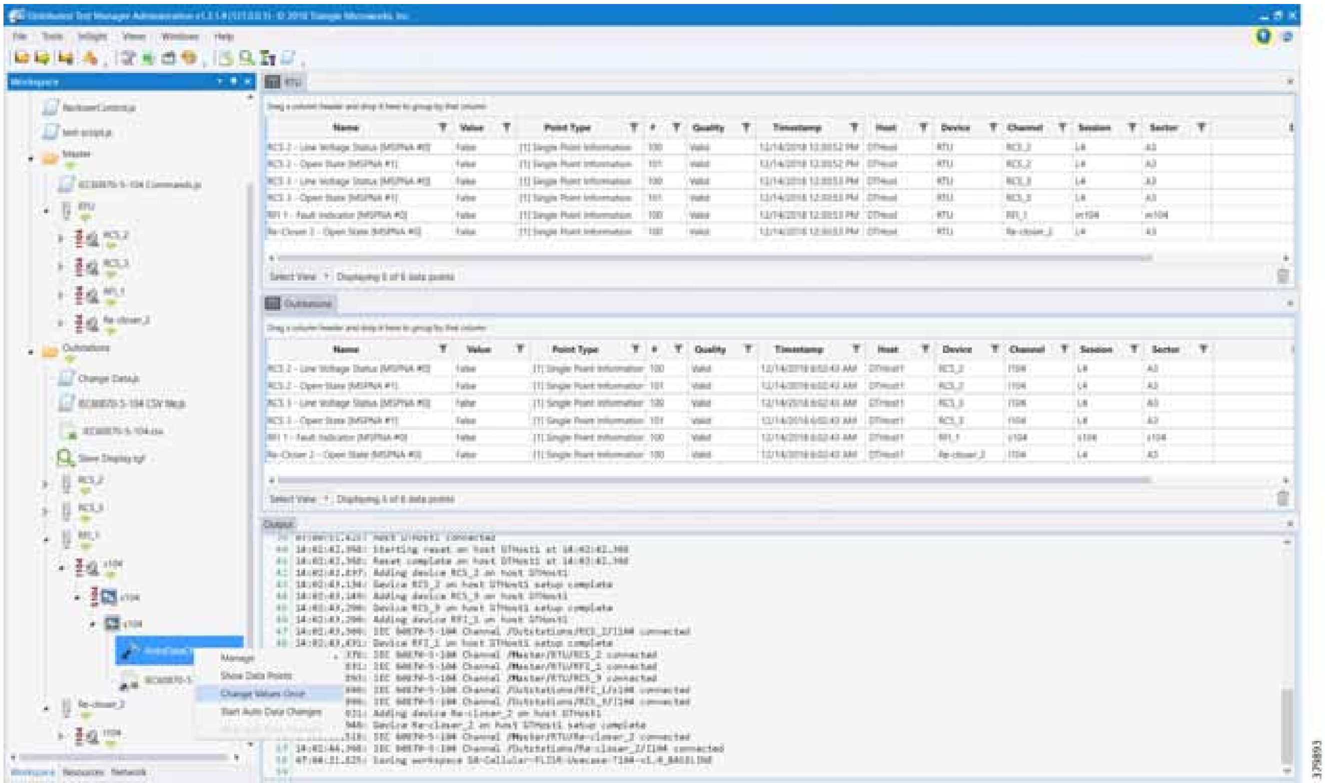
Figure 153 DTM FLISR Start All Hosts



3. Start the FLISR DTM Simulation script.

4. Simulate the fault by changing the RFI1 data once.

Figure 154 DTM FLISR Execute the RFI Script Once



RTU

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

Name	Value	Point Type	#	Quality	Timestamp	Host	Device	Channel	Session	Sector
RCS 2 - Line Voltage Status [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 12:00:52 PM	DTHost	RTU	RCS_2	L4	A3
RCS 2 - Open State [MSPNA #1]	False	[1] Single Point Information	101	Valid	12/14/2018 12:00:52 PM	DTHost	RTU	RCS_2	L4	A3
RCS 3 - Line Voltage Status [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 12:00:53 PM	DTHost	RTU	RCS_3	L4	A3
RCS 3 - Open State [MSPNA #1]	False	[1] Single Point Information	101	Valid	12/14/2018 12:00:53 PM	DTHost	RTU	RCS_3	L4	A3
RFI 1 - Fault Indicator [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 12:00:53 PM	DTHost	RTU	RFI_1	m104	m104
Re-Closer 2 - Open State [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 12:00:53 PM	DTHost	RTU	Re-closer_2	L4	A3

Select View · Displaying 6 of 6 data points

Outstations

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

Name	Value	Point Type	#	Quality	Timestamp	Host	Device	Channel	Session	Sector
RCS 2 - Line Voltage Status [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 6:02:43 AM	DTHost1	RCS_2	I104	L4	A3
RCS 2 - Open State [MSPNA #1]	False	[1] Single Point Information	101	Valid	12/14/2018 6:02:43 AM	DTHost1	RCS_2	I104	L4	A3
RCS 3 - Line Voltage Status [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 6:02:43 AM	DTHost1	RCS_3	I104	L4	A3
RCS 3 - Open State [MSPNA #1]	False	[1] Single Point Information	101	Valid	12/14/2018 6:02:43 AM	DTHost1	RCS_3	I104	L4	A3
RFI 1 - Fault Indicator [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 6:02:43 AM	DTHost1	RFI_1	i104	i104	i104
Re-Closer 2 - Open State [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 6:02:43 AM	DTHost1	Re-closer_2	I104	L4	A3

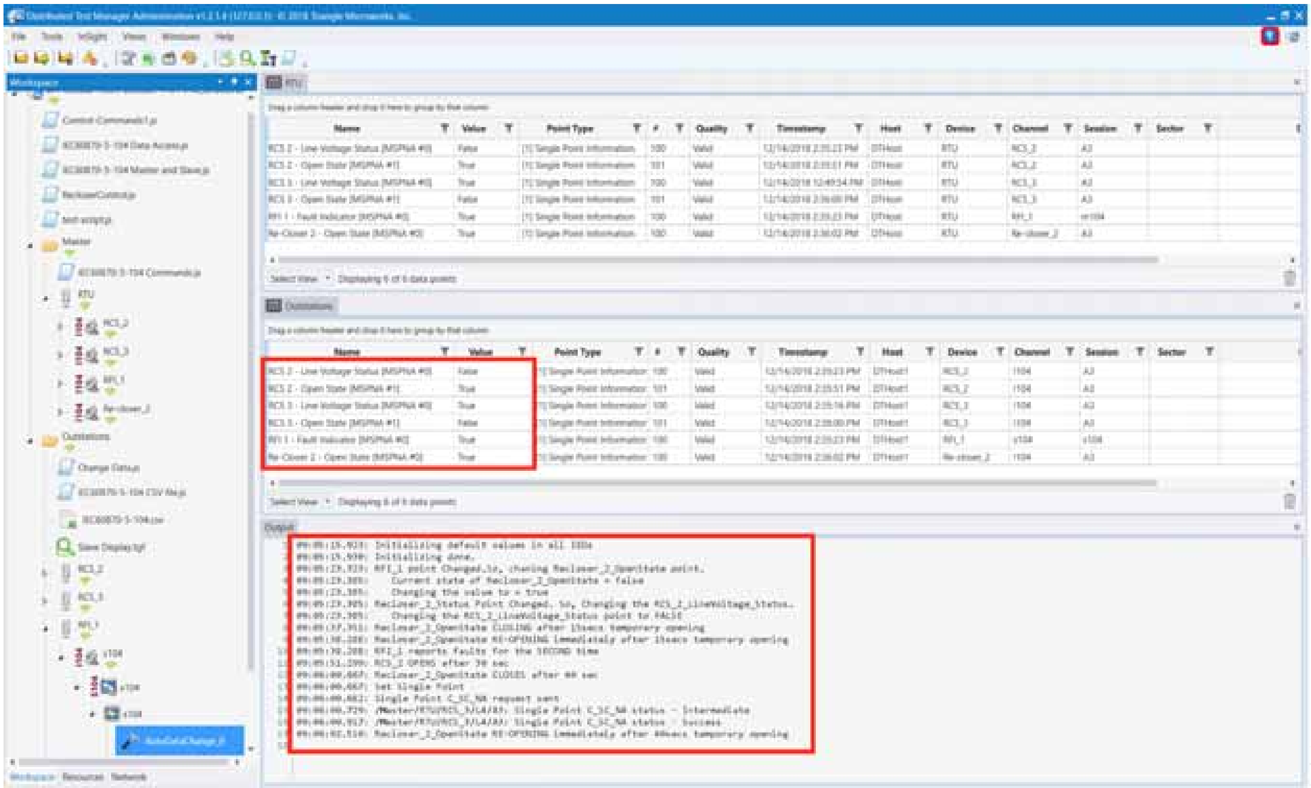
Select View · Displaying 6 of 6 data points

Output

```
07:00:11.423: Host DTHost1 connected
14:02:42.398: Starting reset on host DTHost1 at 14:02:42.368
14:02:42.368: Reset complete on host DTHost1 at 14:02:42.368
14:02:42.897: Adding device RCS_2 on host DTHost1
14:02:43.134: Device RCS_2 on host DTHost1 setup complete
14:02:43.149: Adding device RCS_3 on host DTHost1
14:02:43.290: Device RCS_3 on host DTHost1 setup complete
14:02:43.290: Adding device RFI_1 on host DTHost1
14:02:43.300: IEC 60870-5-104 Channel /Outstations/RCS_2/I104 connected
14:02:43.431: Device RFI_1 on host DTHost1 setup complete
              370: IEC 60870-5-104 Channel /Master/RTU/RCS_2 connected
              831: IEC 60870-5-104 Channel /Master/RTU/RFI_1 connected
              893: IEC 60870-5-104 Channel /Master/RTU/RCS_3 connected
              898: IEC 60870-5-104 Channel /Outstations/RFI_1/i104 connected
              898: IEC 60870-5-104 Channel /Outstations/RCS_3/I104 connected
              831: Adding device Re-closer_2 on host DTHost1
              948: Device Re-closer_2 on host DTHost1 setup complete
              518: IEC 60870-5-104 Channel /Master/RTU/Re-closer_2 connected
14:02:44.368: IEC 60870-5-104 Channel /Outstations/Re-closer_2/I104 connected
07:00:21.825: Saving workspace SA-Cellular-FLISR-Usecase-T104-v1.0_BASELINE
```

Note: The FLISR use case steps 1 to 9 are fully automated by the scripts

Figure 155 DTM FLISR Simulation Completed



RTU

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

Name	Value	Point Type	#	Quality	Timestamp	Host	Device	Channel	Session	Sector
RCS 2 - Line Voltage Status [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 2:35:23 PM	DTHost	RTU	RCS_2	A3	
RCS 2 - Open State [MSPNA #1]	True	[1] Single Point Information	101	Valid	12/14/2018 2:35:51 PM	DTHost	RTU	RCS_2	A3	
RCS 3 - Line Voltage Status [MSPNA #0]	True	[1] Single Point Information	100	Valid	12/14/2018 12:49:34 PM	DTHost	RTU	RCS_3	A3	
RCS 3 - Open State [MSPNA #1]	False	[1] Single Point Information	101	Valid	12/14/2018 2:36:00 PM	DTHost	RTU	RCS_3	A3	
RFI 1 - Fault Indicator [MSPNA #0]	True	[1] Single Point Information	100	Valid	12/14/2018 2:35:23 PM	DTHost	RTU	RFI_1	m104	
Re-Closer 2 - Open State [MSPNA #0]	True	[1] Single Point Information	100	Valid	12/14/2018 2:36:02 PM	DTHost	RTU	Re-closer_2	A3	

Select View ▾ Displaying 6 of 6 data points

Outstations

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

Name	Value	Point Type	#	Quality	Timestamp	Host	Device	Channel	Session	Sector
RCS 2 - Line Voltage Status [MSPNA #0]	False	[1] Single Point Information	100	Valid	12/14/2018 2:35:23 PM	DTHost1	RCS_2	I104	A3	
RCS 2 - Open State [MSPNA #1]	True	[1] Single Point Information	101	Valid	12/14/2018 2:35:51 PM	DTHost1	RCS_2	I104	A3	
RCS 3 - Line Voltage Status [MSPNA #0]	True	[1] Single Point Information	100	Valid	12/14/2018 2:35:16 PM	DTHost1	RCS_3	I104	A3	
RCS 3 - Open State [MSPNA #1]	False	[1] Single Point Information	101	Valid	12/14/2018 2:36:00 PM	DTHost1	RCS_3	I104	A3	
RFI 1 - Fault Indicator [MSPNA #0]	True	[1] Single Point Information	100	Valid	12/14/2018 2:35:23 PM	DTHost1	RFI_1	s104	s104	
Re-Closer 2 - Open State [MSPNA #0]	True	[1] Single Point Information	100	Valid	12/14/2018 2:36:02 PM	DTHost1	Re-closer_2	I104	A3	

Select View ▾ Displaying 6 of 6 data points

Output

```
09:05:15.923: Initializing default values in all IEDs
09:05:15.930: Initializing done.
09:05:23.323: RFI_1 point Changed.1s, chaning Recloser_2_OpenState point.
09:05:23.385:     Current state of Recloser_2_OpenState = false
09:05:23.385:     Changing the value to = true
09:05:23.385: Recloser_2_Status Point Changed. 1s, Changing the RCS_2_LineVoltage_Status.
09:05:23.385:     Changing the RCS_2_LineVoltage_Status point to FALSE
09:05:37.351: Recloser_2_OpenState CLOSING after 15secs temporary opening
09:05:38.288: Recloser_2_OpenState RE-OPENING immediately after 15secs temporary opening
09:05:38.288: RFI_1 reports faults for the SECOND time
09:05:51.299: RCS_2 OPENS after 30 sec
09:06:00.667: Recloser_2_OpenState CLOSES after 40 sec
09:06:00.667: Set Single Point
09:06:00.682: Single Point C_SC_NA request sent
09:06:00.729: /Master/RTU/RCS_3/L4/A3: Single Point C_SC_NA status - Intermediate
09:06:00.917: /Master/RTU/RCS_3/L4/A3: Single Point C_SC_NA status - Success
09:06:02.510: Recloser_2_OpenState RE-OPENING immediately after 40secs temporary opening
```

High Availability at Various Layers

High Availability has been implemented at the following layers:

- Headend Router Level Redundancy, page 147
- Dual Control Center, page 149
- IPv6 Backhaul, page 150
- IoT Gateway WAN Backhaul Redundancy over Cellular/Ethernet, page 152
- IoT Gateway WAN Backhaul Redundancy over Cellular/Cellular, page 156

Note: Throughout this chapter, configurations captured for IoT Gateway (also referred to as FAR) are for reference purposes only. They need not be configured manually. When the Bootstrapped IoT Gateway is deployed at the desired deployment location, configurations are pushed by FND as part of Zero Touch. Please refer to Appendix B: FND Zero Touch Deployment Profiles, page 188.

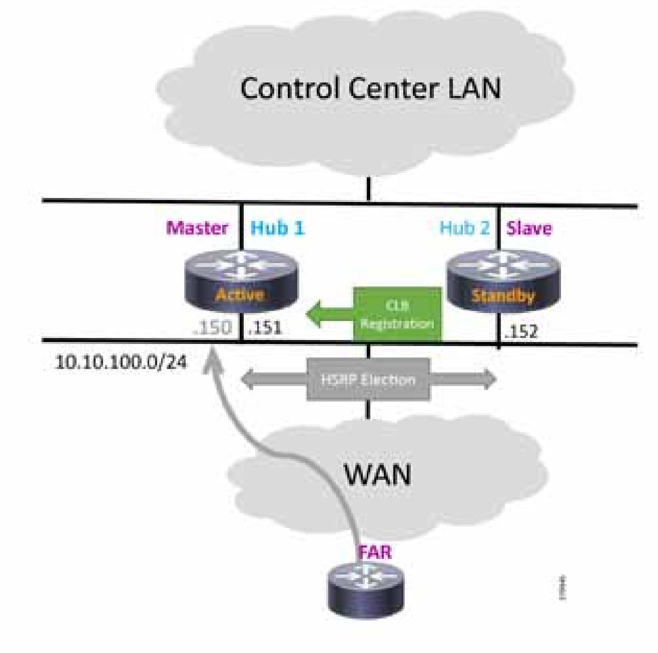
Headend Router Level Redundancy

As covered in the Design Guide, the IKEv2 Load Balancer feature is used to simulate HER redundancy within a single control center. The IKEv2 connection requests coming in from the remote FARs (acting as FlexVPN clients) are distributed among the HER present within a control center (acting as FlexVPN gateways).

HSRP and IKEv2 CLB mechanism is configured specifically on the FlexVPN server side, whereas IKEv2 redirect mechanism is configured on both the server and the client.

This section covers the configuration details used to implement the IKEv2 Load balancer feature using IPv4 backhaul in this solution.

Figure 156 HER Redundancy within a Control Center



Headend Router

On the server side, a single HSRP group is configured comprising the cluster elements (aka Headend Routers or HERs) for load balancing. The HSRP master that is the active router also plays the role of the CLB master to receive the connection requests from remote clients (aka FARs) and redirects those requests to the least loaded CLB slave.

1. Log in to each HER in the cluster and configure the following commands on the WAN interface to configure an HSRP group. Ensure that the priority is set differently for each cluster member since the active router with higher priority will become the CLB master.

```
!
interface GigabitEthernet0/0/0
ip address 10.10.100.151 255.255.255.0
standby version 2
standby 1 ip 10.10.100.150
standby 1 priority 110
standby 1 name cluster1
exit
!
```

2. Configure the load management mechanism on each cluster element as shown below:

```
!
crypto ikev2 cluster
standby-group cluster1
slave priority 90
slave max-session 100
no shutdown
exit
!
```

3. Activate the IKEv2 redirect mechanism on each cluster member using the following command globally:

```
!
crypto ikev2 redirect gateway init
!
```

Field Area Router

On the client side, configuration is minimal since FlexVPN clients only need to know the Virtual IP (VIP) address of the HSRP cluster.

1. Activate the IKEv2 redirect mechanism on each remote FlexVPN client using the following command:

```
!
crypto ikev2 redirect client
!
```

2. Point each client to the cluster VIP to connect to under the FlexVPN client configuration section as shown below:

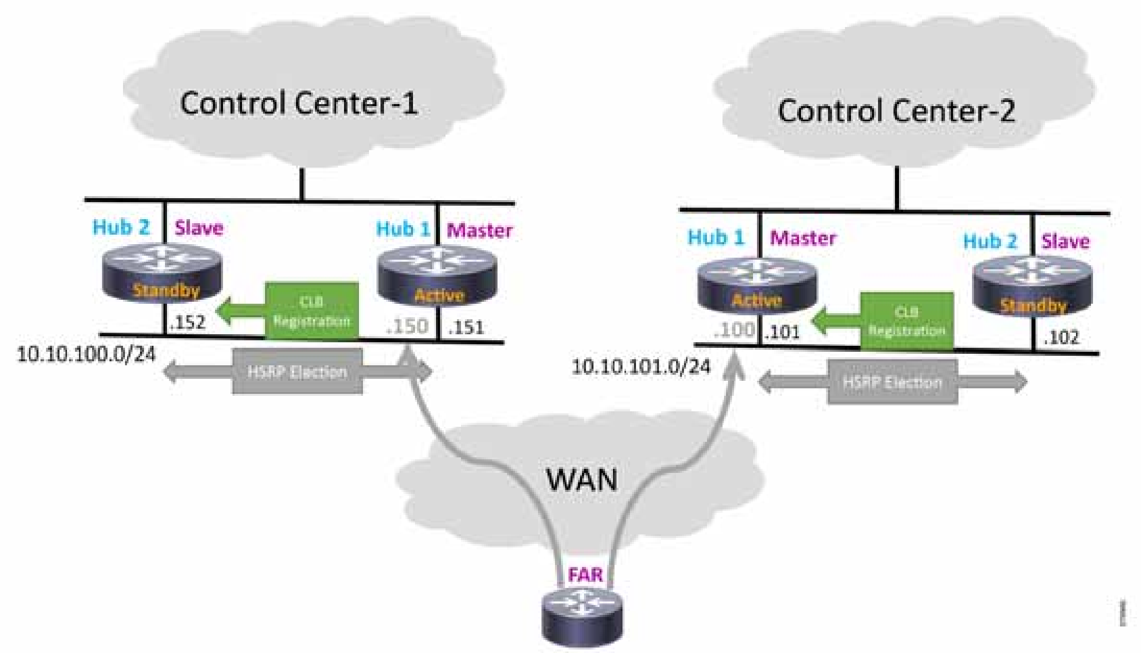
```
!
crypto ikev2 client flexvpn FlexVPN_Client
peer 1 10.10.100.150
client connect Tunnel1
!
```

Note: For the complete set of working configurations on HER and FAR, please refer to Appendix C: FlexVPN Configurations, page 196.

Dual Control Center

As covered in the Design Guide, to simulate control center redundancy from the FAR perspective, two independent clusters of FlexVPN gateways are enabled where each HER cluster represents one control center thereby providing a dual control center topology as shown below.

Figure 157 Dual Control Center Topology



The remote FAR will form two active VPN tunnels, one with each control center. Within each control center though, IKEv2 CLB over IPv4 backhaul will still be used to simulate HER redundancy.

The following configuration shows the specific steps needed on the FAR to achieve this:

```
!
interface Tunnel1
description IPSec tunnel-1 to HER Cluster1
ip unnumbered Loopback0
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet2/1
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
end
!

interface Tunnel2
description IPSec tunnel-2 to HER Cluster2
ip unnumbered Loopback0
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet2/1
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
end
!

crypto ikev2 client flexvpn FlexVPNClient_1
peer 1 10.10.100.150
```

```
client connect Tunnel1
!

crypto ikev2 client flexvpn FlexVPNClient_2
peer 1 10.10.101.100
client connect Tunnel2
!
```

IPv6 Backhaul

This section provides the sample FlexVPN config needed on the CGR and HER to bring up the tunnel over the IPv6 backhaul. It includes a virtual template configuration on the hub that allows multiple spoke sessions to be established.

The configuration contains all of the standard building blocks commonly seen within IPv4 backhaul-based FlexVPN with a notable difference being the tunnel mode that uses GRE IPv6 for IPv6 transport address. The tunnel source contains the interface name that has the IPv6 address configured while the tunnel destination directly references the peer IPv6 address on the spoke. For the communication between the hub and the spoke to be successful, the encryption algorithm, hashing algorithm, and Diffie-Hellman group should match between the hub and the spoke. This guide uses X.509 certificate-based authentication.

Note: The IKEv2 Load Balancer feature is currently supported only with IPv4 addressing. An enhancement DDTS filed CSCvc92001 exists to add support to this feature for IPv6 addressing.

Field Area Router

Note: The listed configuration is for reference purposes only because they are pushed by FND as part of PnP bootstrapping, followed by ZTD.

```
ipv6 unicast-routing
ipv6 cef
!
aaa new-model
aaa authorization network FlexVPN_Author_v6 local
!
crypto ikev2 authorization policy FlexVPN_v6_Author_Policy
route set interface
!
crypto ikev2 proposal FlexVPN_v6_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FLexVPN_v6_IKEv2_Policy
proposal FlexVPN_v6_IKEv2_Proposal
!

crypto ikev2 profile FlexVPN_v6_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_v6 FlexVPN_v6_Author_Policy
virtual-template 1
!
crypto IPSec transform-set FlexVPN_v6_IPSec_Transform_Set esp-aes esp-sha-hmac
mode transport
!
crypto IPSec profile FlexVPN_v6_IPSec_Profile
set transform-set FlexVPN_v6_IPSec_Transform_Set
set pfs group14
set ikev2-profile FlexVPN_v6_IKEv2_Profile
!
interface Loopback0
ip address 192.168.150.6 255.255.255.255
ipv6 address 2001:DB8:BABA:FACE:6C1C:D5F4:B98E:11B3/128
ipv6 enable
!
interface GigabitEthernet2/2
no switchport
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:10:62::1000/64
!
ipv6 route ::/0 2001:DB8:10:62::1
!
interface Tunnel1
description ipv6 tunnel to FAN-PHE-HER2
no ip address
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet2/2
tunnel mode gre ipv6
tunnel destination 2001:DB8:1010:903::5
tunnel protection IPSec profile FlexVPN_v6_IPSec_Profile
!
interface Virtual-Template1 type tunnel
no ip address
ip nhrp network-id 1
ip nhrp shortcut virtual-template 1
ip nhrp redirect ipv6 unnumbered Loopback0
tunnel mode gre ipv6
tunnel protection IPSec profile FlexVPN_v6_IPSec_Profile
end
!
```

Headend Router

Note: HER configuration is a one-time manual configuration.

```
ipv6 unicast-routing
!
aaa new-model
aaa authorization network FlexVPN_Author_v6 local
!
crypto ikev2 authorization policy FlexVPN_v6_Author_Policy
route set interface
!
crypto ikev2 proposal FlexVPN_v6_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FlexVPN_v6_IKEv2_Policy
proposal FlexVPN_v6_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_v6_IKEv2_Profile
match certificate FlexVPN_Cert_Map
identity local dn
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint LDevID
```

```
dpd 30 3 periodic
aaa authorization group cert list FlexVPN_Author_v6 FlexVPN_v6_Author_Policy
virtual-template 1
!
crypto IPSec transform-set FlexVPN_v6_IPSec_Transform_Set esp-aes esp-sha-hmac
mode transport
!
crypto IPSec profile FlexVPN_v6_IPSec_Profile
set transform-set FlexVPN_v6_IPSec_Transform_Set
set pfs group14
set ikev2-profile FlexVPN_v6_IKEv2_Profile
responder-only
!
interface Loopback0
no ip address
ipv6 address 2001:DB8:BABA:FACE::2/64
ipv6 enable
!
interface GigabitEthernet0/0/7
description connected to port8 on fan-phe-dmz-switch (ie5k_rr07)
no ip address
negotiation auto
cdp enable
ipv6 address 2001:DB8:1010:903::5/64
ipv6 enable
!
ipv6 route ::/0 2001:DB8:1010:903::22
!
interface Virtual-Template1 type tunnel
no ip address
ipv6 unnumbered Loopback0
ipv6 enable
tunnel mode gre ipv6
tunnel path-mtu-discovery
tunnel protection IPSec profile FlexVPN_v6_IPSec_Profile
!
```

IoT Gateway WAN Backhaul Redundancy over Cellular/Ethernet

The Secondary Substation Router or DA Gateways can also be commonly referred to as the IoT Gateway or as FAR.

Secure tunnels are established between the IoT Gateway and the HERs. On the IoT Gateway, the tunnel could be established over a cellular or Ethernet interface, with the tunnel terminating on the same HER. The primary tunnel is established over a cellular interface. The secondary (or backup) tunnel is established over an Ethernet interface. The primary/backup tunnels would operate in active/standby, which means:

- Failover—If the primary tunnel fails, the secondary tunnel would be activated.
- Recovery—If the primary tunnel is up, the secondary tunnel would be de-activated.
- This automatic failover/recovery is handled with the help of EEM script.

The following sections are enumerated in detail:

- Head End Router Configuration, page 153
- IoT Gateway Configuration, page 154
- EEM Script—Automatic Failover/Recovery, page 156

Head End Router Configuration

The following lines are the necessary configurations required on the HER to establish a tunnel with the FAR.

Note: HER configuration is a one-time manual configuration.

```
!
!
aaa authorization network FlexVPN_Author local
!
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 policy FlexVPN_IKEv2_Policy
proposal FlexVPN_IKEv2_Proposal
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
match certificate FlexVPN_Cert_Map
identity local dn
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint LDevID
dpd 30 3 periodic
aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
virtual-template 1
!
crypto ikev2 fragmentation
!
crypto ikev2 cluster
standby-group DMZ_NW
slave priority 90
slave max-session 100
no shutdown
!
crypto isakmp invalid-spi-recovery
!
crypto IPSec security-association replay disable
crypto IPSec security-association replay window-size 512
!
crypto IPSec transform-set FlexVPN_IPSec_Transform_Set 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
!
interface GigabitEthernet2
description DMZ Interface
ip address <Public DMZ IP>
standby use-bia
standby version 2
standby 72 ip <Public DMZ Virtual IP>
standby 72 priority 200
standby 72 preempt
standby 72 name DMZ_NW
negotiation auto
!
interface Virtual-Template1 type tunnel
description to establish tunnels from the multiple IoT Gateways.
ip unnumbered Loopback0
tunnel protection IPSec profile FlexVPN_IPSec_Profile

!
ip access-list standard FlexVPN_Client_Default_ipv4_Route
permit 192.168.103.100 ## Advertising FND's IP
permit 192.168.150.1 ## Advertising HER's Loopback IP
!
ipv6 access-list FlexVPN_Client_Default_ipv6_Route
permit ipv6 any any
! It's recommended to advertise specific host routes
!
```

IoT Gateway Configuration

The configuration on the FAR is pushed from the FND:

- Tunnel 0 is the primary tunnel and it is established over cellular.
- Tunnel 1 is the secondary tunnel and it is established over Ethernet.

Both tunnels use the same IPSec tunnel protection mode, with both the tunnels connecting to the same public IP address configured on HER. The configurations that follow are the configurations required to establish the FlexVPN tunnels, the tunnel configurations, and the interface configurations.

The following configuration, which uses the interface names that are applicable to IR1101, is applicable to other platforms using the appropriate interface naming convention applicable to the platform on which the configuration is applied.

Note: The listed configuration is for reference purpose only since FND pushes it as part of ZTD.

```
!
!
aaa authorization network FlexVPN_Author local
crypto pki certificate map FlexVPN_Cert_Map 1
issuer-name co cn = ipg-rsa-root-ca ## CN of the Utility PKI CA server.
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface ## Advertising Routes from IoT Gateway to HER
route set access-list FlexVPN_Client_ipv4_LAN
route set access-list ipv6 FlexVPN_Client_ipv6_LAN
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy
proposal FlexVPN_IKEv2_Proposal
!
crypto ikev2 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 IPSec transform-set FlexVPN_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
!
ip access-list standard FlexVPN_Client_ipv4_LAN
permit 192.168.150.42 ## Loopback IP of IoT Gateway.
permit 192.168.0.0 0.0.0.255
!
ipv6 access-list FlexVPN_Client_ipv6_LAN
sequence 20 permit ipv6 host 2001:DB8:BABA:FACE:3D13:2C3E:3B2:C1D1 any
!
interface Tunnel0
description Primary IPSec tunnel to HER1.ipg.cisco.com
ip unnumbered Loopback0
tunnel source Cellular0/1/0
tunnel destination <HER_Public_IP_address>
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
interface Tunnel1
description IPSec tunnel to HER1.ipg.cisco.com
ip unnumbered Loopback0
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet0/0/0
tunnel destination <HER_Public_IP_address>
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
interface Cellular0/1/0
mtu 1430
ip address negotiated
dialer in-band
dialer idle-timeout 0
dialer-group 1
ipv6 enable
pulse-time 1
!
interface GigabitEthernet0/0/0
ip address dhcp
!
!
```

In the above configuration:

- Tunnel0 is established over cellular interface
- Tunnel1 is established over Ethernet interface
- Both the tunnels are protected with the same IPSec Profile

Note: The listed configuration is for reference purpose only since the FND pushes it as part of ZTD. The cellular interface is tracked for line-protocol status. If the cellular interface goes down, then tunnel 1 comes up over Ethernet. This redundancy configuration on the IoT Gateway helps minimize the traffic loss and maintain connectivity to the control center.

EEM Script–Automatic Failover/Recovery

In a normal operational mode, FAR connects to HER securely over Tunnel0. Therefore, Tunnel 0 becomes the primary mode of communication between the FAR and the HER. When connectivity over cellular interface fails, the communication between the FAR and the HER must be restored and secured. This restoration of connectivity between the FAR and the HER over a different medium (Ethernet) must be operational and this failover operation of the network helps minimize packet loss and enables secure connectivity over Tunnel 1. This activation of Tunnel1 to carry the load in the event of Tunnel0 failure is referred as Failover.

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

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

Note: The listed configuration is for reference purpose only since the FND pushes it as part of ZTD.

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

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

IoT Gateway WAN Backhaul Redundancy over Cellular/Cellular

The Secondary Substation Router or DA Gateways can also be commonly referred to as the IoT Gateway or the FAR.

Secure tunnels are established between the IoT Gateway and the HERs. On the IoT Gateway, the tunnel is established over a cellular interface with the tunnel terminating on the same HER. The tunnel is established over the primary cellular interface. A secondary cellular interface provides a redundant feature for the tunnel terminating on the same HER. The tunnel terminating on the HER can be established over the primary or the secondary cellular interface. The primary/backup cellular interfaces would operate in active/standby, which means:

- Failover-If the tunnel over primary cellular interface fails, the tunnel would be activated on the secondary cellular interface.
- Recovery-If the tunnel over primary cellular interface is up, the secondary cellular interface would be de-activated.
- This automatic failover/recovery is handled with the help of EEM script.

Please refer to the Design Guide, which articulates the various scenarios discussed in this guide, for more information.

The following sections are enumerated in detail:

- Head End Router Configuration, page 157
- IoT Gateway Configuration, page 157
- Active/Standby-Shut Scenario, page 159
- Active/Standby-UP Scenario, page 163
- Active/Active Load Sharing, page 167
- WAN Monitoring, page 168

Head End Router Configuration

The following lines are the necessary configurations required on the HER to establish a tunnel with the FAR.

Note: The HER configuration is a one-time manual configuration.

The HER configurations are the same as listed in Head End Router Configuration, page 153. The following lines needed to be added in order to enable inter HER routing.

```
!
router ospf 1
 redistribute static subnets
 network 192.168.10.0 0.0.0.255 area 0
!
```

IoT Gateway Configuration

This section discusses the implementation of the redundant scenarios covered in the Design Guide.

For Active/Standby, the configuration on the FAR is pushed from the FND:

- Tunnel 0 is the FlexVPN tunnel and it is established over the primary cellular interface.
- If there is a failure to connect over primary cellular interface, connectivity is established over the secondary cellular interface.

The tunnel connects to the same public IP address configured on HER. The configurations that follow are the configurations required to establish the FlexVPN tunnels, the tunnel configurations, and the interface configurations.

The following configuration, which uses the interface names that are applicable to IR1101, is applicable to other platforms using the appropriate interface naming convention applicable to the platform on which the configuration is applied. The below configuration is applicable to both Active/Standby and Active/Active scenarios as illustrated in the Design Guide.

Note: The listed configuration is for reference purpose only since FND pushes it as part of ZTD.

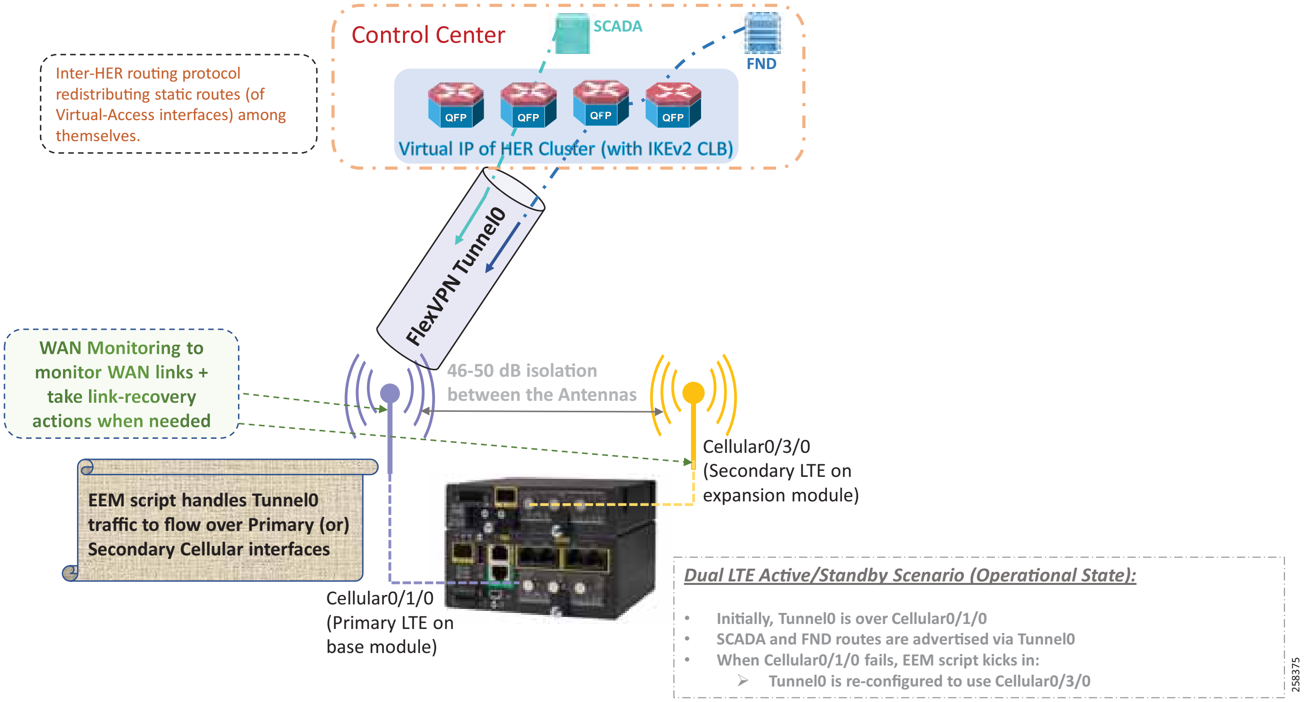
```
!
!
aaa authorization network FlexVPN_Author local crypto pki certificate map FlexVPN_Cert_Map 1
issuer-name co cn = ipg-rsa-root-ca ## CN of the Utility PKI CA server.
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface ## Advertising Routes from IoT Gateway to HER route set access-list
FlexVPN_Client_ipv4_LAN
route set access-list ipv6 FlexVPN_Client_ipv6_LAN
```

```
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal encryption aes-cbc-256
integrity sha256 group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy proposal FlexVPN_IKEv2_Proposal
!
crypto ikev2 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 IPSec transform-set FlexVPN_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
!
ip access-list standard FlexVPN_Client_ipv4_LAN permit 192.168.150.42 ## Loopback IP of IoT
Gateway. permit 192.168.0.0 0.0.0.255
!
ipv6 access-list FlexVPN_Client_ipv6_LAN
sequence 20 permit ipv6 host 2001:DB8:BABA:FACE:3D13:2C3E:3B2:C1D1 any
!
interface Tunnel0
description Primary IPSec tunnel to HER1.ipg.cisco.com ip unnumbered Loopback0
tunnel source <on Availability>
tunnel destination <HER1_Public_IP_address>
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
!
interface Tunnel1
description IPSec tunnel to HER1.ipg.cisco.com ip unnumbered Loopback0
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet0/0/0
tunnel destination <HER 2_Public_IP_address>
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
interface Cellular0/1/0 mtu 1430
ip address negotiated dialer in-band
dialer idle-timeout 0
dialer-group 1 ipv6 enable pulse-time 1

interface Cellular0/3/0 mtu 1430
ip address negotiated dialer in-band
dialer idle-timeout 0
dialer-group 1 ipv6 enable pulse-time 1

!
interface GigabitEthernet0/0/0 ip address dhcp
```

Active/Standby-Shut Scenario

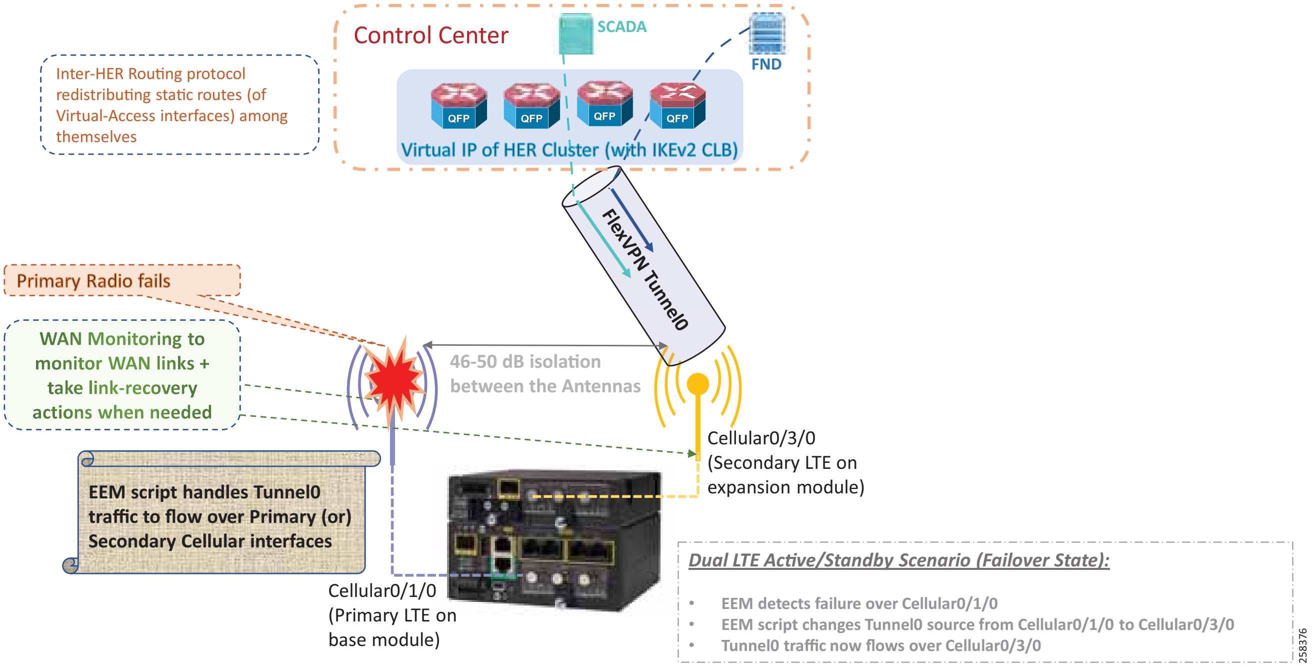
In this case, the secondary cellular interface is in down state. In a normal operational mode, FAR connects to HER securely over Tunnel0 over the primary cellular interface (Cellular 0/1/0). This is shown in Figure 158:

Figure 158 Dual-LTE (Active/Standby): Operational State–Traffic over Primary Radio


Control Center
SCADA
FND
Inter-HER routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves.
QFP
QFP
QFP
QFP
Virtual IP of HER Cluster (with IKEv2 CLB)
FlexVPN Tunnel0
WAN Monitoring to monitor WAN links + take link-recovery actions when needed
46-50 dB isolation between the Antennas
Cellular0/3/0 (Secondary LTE on expansion module)
EEM script handles Tunnel0 traffic to flow over Primary (or) Secondary Cellular interfaces
Cellular0/1/0 (Primary LTE on base module)
Dual LTE Active/Standby Scenario (Operational State):
• Initially, Tunnel0 is over Cellular0/1/0
• SCADA and FND routes are advertised via Tunnel0
• When Cellular0/1/0 fails, EEM script kicks in:
➢ Tunnel0 is re-configured to use Cellular0/3/0
258375

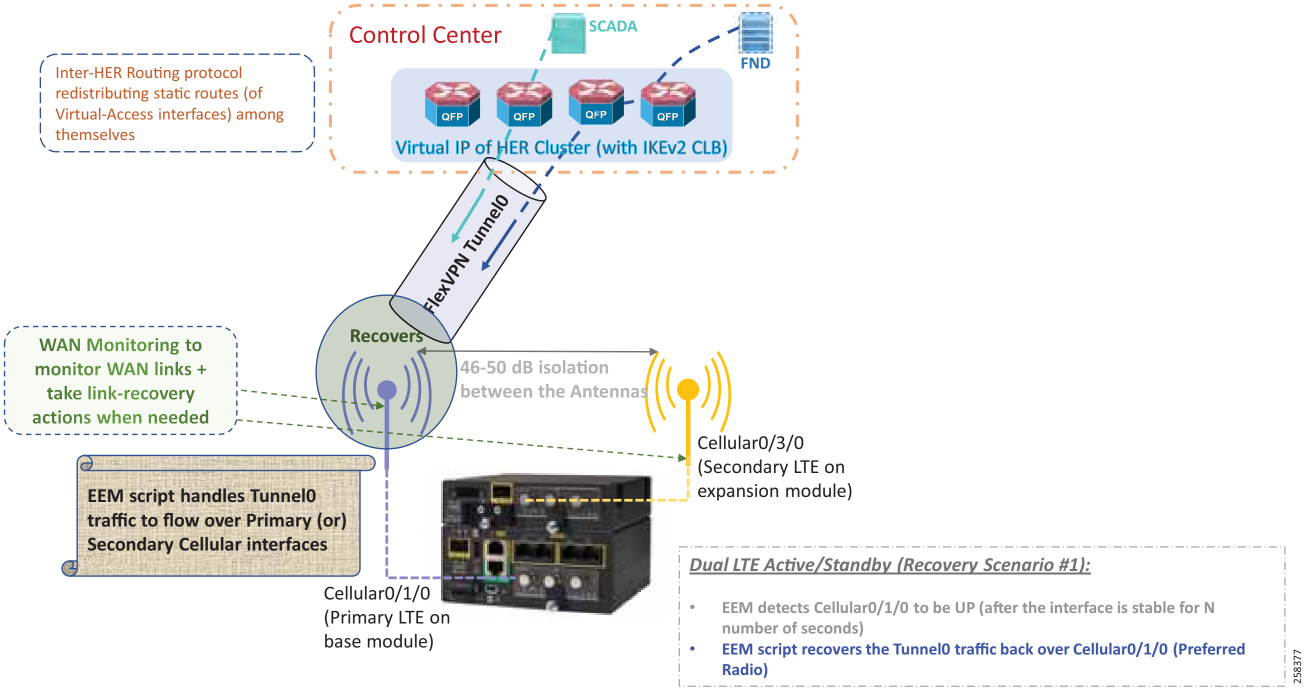
Therefore, Tunnel 0 over Cellular0/1/0 becomes the primary mode of communication between the FAR and the HER. When connectivity over the primary cellular interface fails, the communication between the FAR and the HER must be restored and secured. This restoration of connectivity between the FAR and the HER over the secondary cellular interface (Cellular 0/3/0) must be operational and this failover operation of the network helps minimize packet loss. This activation of Cellular 0/3/0 to carry the load in the event of Cellular 0/1/0 failure is referred as Failover. The switching of traffic from Primary to Secondary is shown in Figure 159:

Figure 159 Dual-LTE (Active/Standby): Failover State–Traffic over Secondary Radio


Control Center
SCADA
FND
Inter-HER Routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves
QFP
QFP
QFP
QFP
Virtual IP of HER Cluster (with IKEv2 CLB)
FlexVPN Tunnel0
Primary Radio fails
WAN Monitoring to monitor WAN links + take link-recovery actions when needed
46-50 dB isolation between the Antennas
Cellular0/3/0 (Secondary LTE on expansion module)
EEM script handles Tunnel0 traffic to flow over Primary (or) Secondary Cellular interfaces
Cellular0/1/0 (Primary LTE on base module)
Dual LTE Active/Standby Scenario (Failover State):
• EEM detects failure over Cellular0/1/0
• EEM script changes Tunnel0 source from Cellular0/1/0 to Cellular0/3/0
• Tunnel0 traffic now flows over Cellular0/3/0
258376

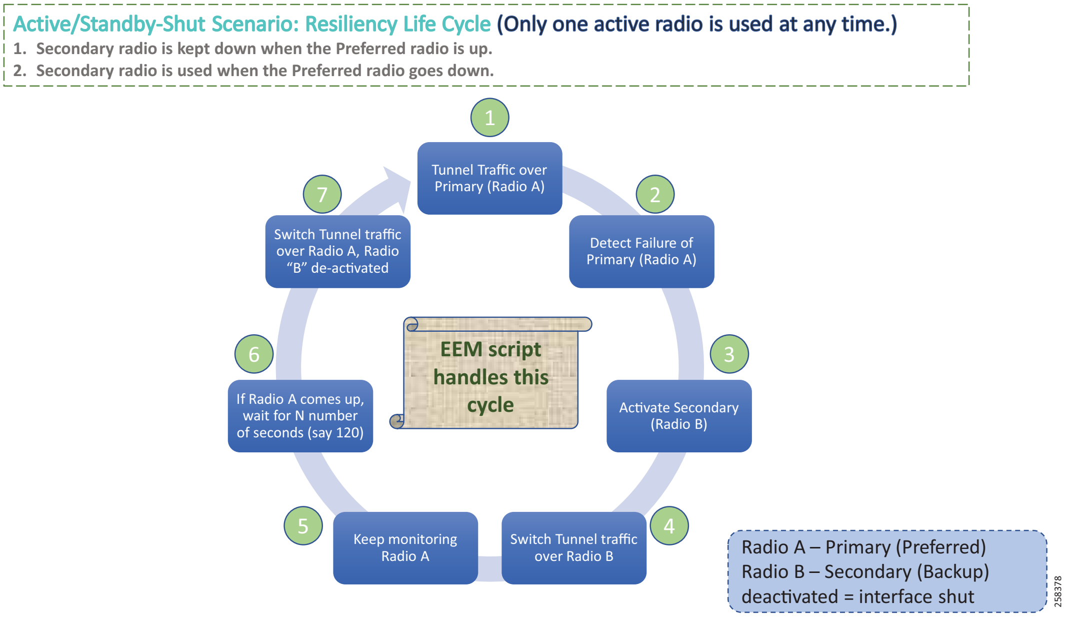
When connectivity over Cellular 0/1/0 is restored, the FAR and the HER can communicate securely using Tunnel 0 over Cellular 0/1/0. This switchover of tunnel source from Cellular 0/3/0 to Cellular 0/1/0 is known as Recovery. This is shown in Figure 160:

Figure 160 Dual-LTE (Active/Standby): Recovery State—Switching back to Primary Radio


Control Center
SCADA
FND
Inter-HER Routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves
QFP
Virtual IP of HER Cluster (with IKEv2 CLB)
FlexVPN Tunnel0
Recovers
WAN Monitoring to monitor WAN links + take link-recovery actions when needed
46-50 dB isolation between the Antennas
Cellular0/3/0 (Secondary LTE on expansion module)
EEM script handles Tunnel0 traffic to flow over Primary (or) Secondary Cellular interfaces
Cellular0/1/0 (Primary LTE on base module)
Dual LTE Active/Standby (Recovery Scenario #1):
EEM detects Cellular0/1/0 to be UP (after the interface is stable for N number of seconds)
EEM script recovers the Tunnel0 traffic back over Cellular0/1/0 (Preferred Radio)
258377

For the switchover to be automatic, EEM script is configured on the FAR. The sequence of states from Failover to Recovery is shown in the state diagram in Figure 161. The configuration below the diagram implements the state transitions.

Figure 161 Active/Standby-Shut Scenario: Resiliency Life Cycle (EEM Script State Diagram)


Active/Standby-Shut Scenario: Resiliency Life Cycle (Only one active radio is used at any time.)
1. Secondary radio is kept down when the Preferred radio is up.
2. Secondary radio is used when the Preferred radio goes down.
1
Tunnel Traffic over Primary (Radio A)
2
Detect Failure of Primary (Radio A)
3
Activate Secondary (Radio B)
4
Switch Tunnel traffic over Radio B
5
Keep monitoring Radio A
6
If Radio A comes up, wait for N number of seconds (say 120)
7
Switch Tunnel traffic over Radio A, Radio "B" de-activated
EEM script handles this cycle
Radio A – Primary (Preferred)
Radio B – Secondary (Backup)
deactivated = interface shut
258378

Note: The listed configuration is for reference purpose only since the FND pushes it as part of ZTD.

1. The tunnel traffic is over Primary Radio.

2. Failure of the primary cellular interface is detected from the following configuration:

```
track 3 interface Cellular0/1/0 line-protocol
 delay up 120
track 6 interface Cellular0/3/0 line-protocol
!
!
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0 track 3
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 track 6
!
```

3. As soon as a failure is detected on the primary radio, the following lines are executed to activate the Secondary Radio:

```
event manager applet Failover
 event track 3 state down
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface cellular 0/3/0"
 action 4  cli command "no shutdown"
 action 5  cli command "interface tunnel0"
 action 6  cli command "tunnel source Cellular0/3/0"
 action 7  cli command "end"
 action 99 syslog msg "NOTE: Cellular 0/1/0 down, switching to Cellular 0/3/0 "
```

4. Once the secondary LTE is activated, the tunnel traffic now flows through Secondary Radio.

5. Radio A is continuously monitored using the same commands configured in Step 2 above. The WAN monitoring feature can also used to bring up Radio A from any glitch.

6. If Radio A comes up, we wait for 120s until the tunnel traffic can be switched to Radio A. This is to ensure that the primary radio (Radio A) is stable. This configuration is also covered in Step 2 above by the command “delay up 120.”

7. Once the stability of Radio A is ensured, the following lines are executed to switch the tunnel traffic back to Radio A and the secondary radio (Radio B) is shut.

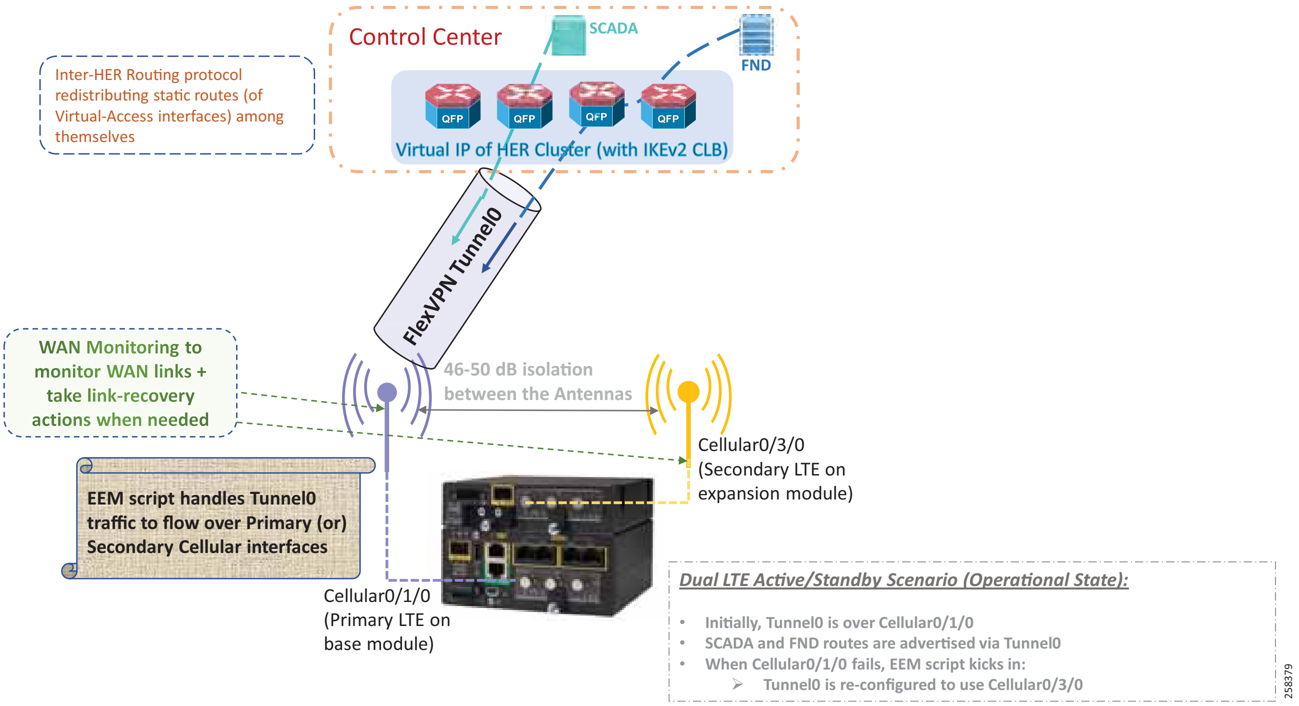
```
event manager applet Recovery
 event track 3 state up
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface tunnel0"
 action 4  cli command "tunnel source Cellular0/1/0"
 action 5  cli command "interface cellular 0/3/0"
 action 6  cli command "shutdown"
 action 7  cli command "end"
 action 99 syslog msg "NOTE: Connectivity Restored on Cellular 0/1/0"
```

Active/Standby-UP Scenario

In this case, the secondary cellular interface is in UP state.

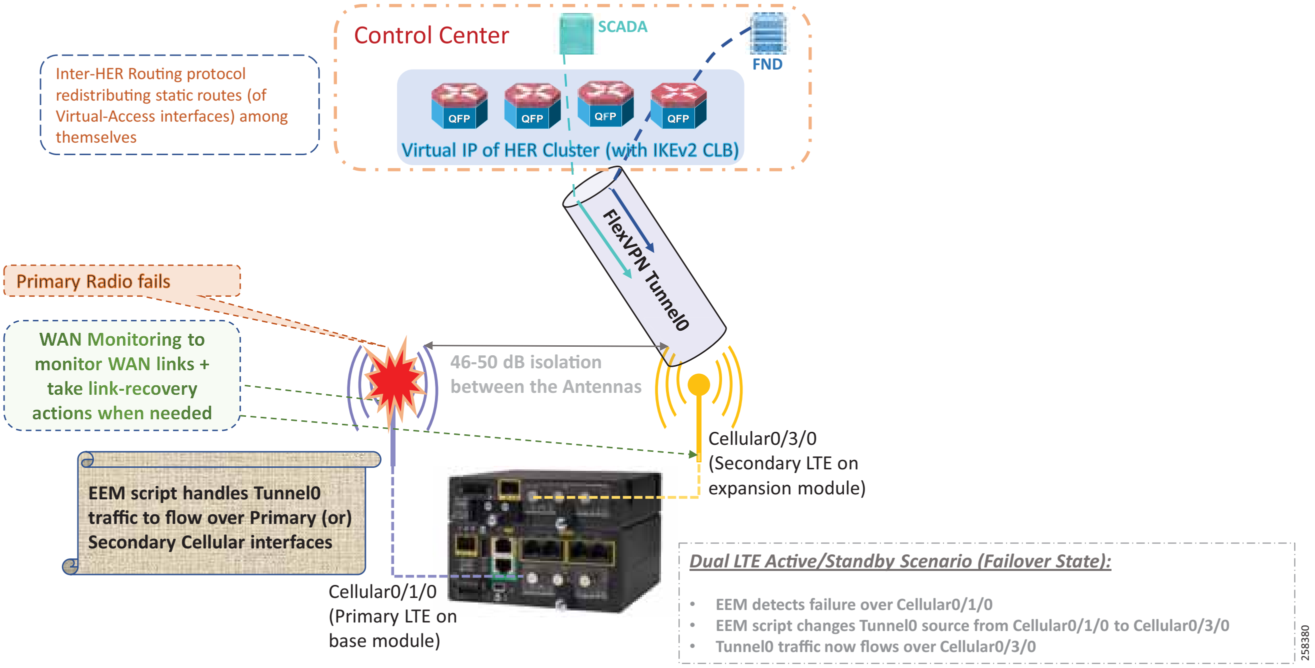
In a normal operational mode, FAR connects to HER securely over Tunnel0 over the primary cellular interface (Cellular 0/1/0). Therefore, the Tunnel 0 over Cellular0/1/0 becomes the primary mode of communication between the FAR and the HER. As shown in Figure 162, Tunnel traffic flows through the primary radio.

Figure 162 Dual-LTE (Active/Standby): Operational State–Traffic over Primary Radio


Control Center
SCADA
FND
Inter-HER Routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves
QFP
QFP
QFP
QFP
Virtual IP of HER Cluster (with IKEv2 CLB)
FlexVPN Tunnel0
WAN Monitoring to monitor WAN links + take link-recovery actions when needed
46-50 dB isolation between the Antennas
Cellular0/3/0 (Secondary LTE on expansion module)
EEM script handles Tunnel0 traffic to flow over Primary (or) Secondary Cellular interfaces
Cellular0/1/0 (Primary LTE on base module)
Dual LTE Active/Standby Scenario (Operational State):
• Initially, Tunnel0 is over Cellular0/1/0
• SCADA and FND routes are advertised via Tunnel0
• When Cellular0/1/0 fails, EEM script kicks in:
➢ Tunnel0 is re-configured to use Cellular0/3/0
258379

When connectivity over the primary cellular interface fails, the communication between the FAR and the HER must be restored and secured. This restoration of connectivity between the FAR and the HER over the secondary cellular interface (Cellular 0/3/0) must be operational and this failover operation of the network helps minimize packet loss. The change in tunnel source to Cellular 0/3/0 to carry the load in the event of Cellular 0/1/0 failure is referred as Failover. This is shown in Figure 163:

Figure 163 Dual-LTE (Active/Standby): Failover State–Traffic over Secondary Radio

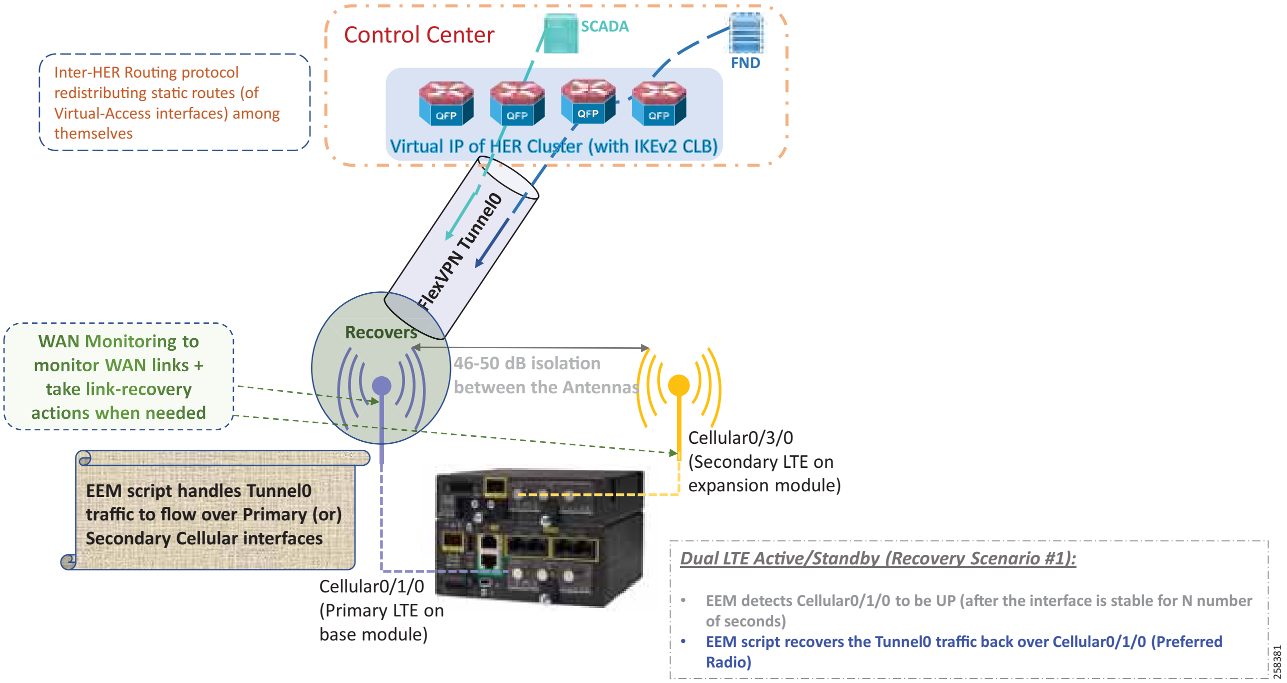

Control Center
SCADA
FND
Inter-HER Routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves
QFP
QFP
QFP
QFP
Virtual IP of HER Cluster (with IKEv2 CLB)
FlexVPN Tunnel0
Primary Radio fails
WAN Monitoring to monitor WAN links + take link-recovery actions when needed
46-50 dB isolation between the Antennas
Cellular0/3/0 (Secondary LTE on expansion module)
EEM script handles Tunnel0 traffic to flow over Primary (or) Secondary Cellular interfaces
Cellular0/1/0 (Primary LTE on base module)
258380

Dual LTE Active/Standby Scenario (Failover State):

- EEM detects failure over Cellular0/1/0
- EEM script changes Tunnel0 source from Cellular0/1/0 to Cellular0/3/0
- Tunnel0 traffic now flows over Cellular0/3/0

When connectivity over Cellular 0/1/0 is restored, the FAR and the HER can communicate securely using Tunnel 0 over Cellular 0/1/0. This switchover of tunnel source from Cellular 0/3/0 to Cellular 0/1/0 is known as Recovery.

Figure 164 Dual-LTE (Active/Standby): Recovery State–Switching back to Primary Radio

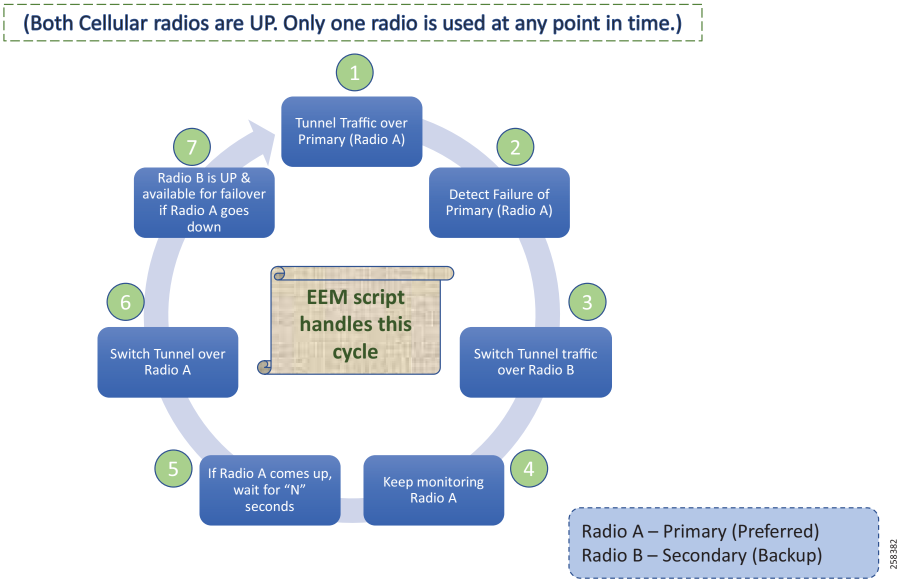

Control Center
SCADA
FND
Inter-HER Routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves
QFP
QFP
QFP
QFP
Virtual IP of HER Cluster (with IKEv2 CLB)
FlexVPN Tunnel0
Recovers
WAN Monitoring to monitor WAN links + take link-recovery actions when needed
46-50 dB isolation between the Antennas
Cellular0/3/0 (Secondary LTE on expansion module)
EEM script handles Tunnel0 traffic to flow over Primary (or) Secondary Cellular interfaces
Cellular0/1/0 (Primary LTE on base module)
258381

Dual LTE Active/Standby (Recovery Scenario #1):

- EEM detects Cellular0/1/0 to be UP (after the interface is stable for N number of seconds)
- EEM script recovers the Tunnel0 traffic back over Cellular0/1/0 (Preferred Radio)

For the switchover to be automatic, EEM script is configured on the FAR. The sequence of states from Failover to Recovery is shown in the state diagram in Figure 165. The configuration following the diagram implements the state transitions.

Figure 165 Active/Standby-UP Scenario: Recovering back to Preferred Radio Case


(Both Cellular radios are UP. Only one radio is used at any point in time.)
1
Tunnel Traffic over Primary (Radio A)
2
Detect Failure of Primary (Radio A)
3
Switch Tunnel traffic over Radio B
4
Keep monitoring Radio A
5
If Radio A comes up, wait for "N" seconds
6
Switch Tunnel over Radio A
7
Radio B is UP & available for failover if Radio A goes down
EEM script handles this cycle
Radio A – Primary (Preferred)
Radio B – Secondary (Backup)
258382

Note: The listed configuration is for reference purpose only since the FND pushes it as part of ZTD.

1. The tunnel traffic is over the Primary Radio.
2. Failure of the primary cellular interface is detected from the following configuration:

```
track 3 interface Cellular0/1/0 line-protocol
 delay up 120
track 6 interface Cellular0/3/0 line-protocol
!
!
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0 track 3
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 track 6
!
```

3. As soon as a failure is detected on the Primary Radio, the following lines are executed to switch the tunnel traffic to utilize Secondary Radio (Radio B):

```
event manager applet Failover
 event track 3 state down
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface tunnel0"
 action 4  cli command "tunnel source Cellular0/3/0"
 action 5  cli command "end"
 action 99 syslog msg "NOTE: Cellular 0/1/0 down, switching to Cellular 0/3/0 "
```

4. Once the tunnel source is switched, the tunnel traffic now flows through the Secondary Radio.
5. Radio A is continuously monitored using the same commands configured in Step 2. WAN monitoring feature can also used to bring up Radio A from any glitch.
6. If Radio A comes up, we wait for 120s until the tunnel traffic can be switched to Radio A. This is to ensure that the Primary Radio (Radio A) is stable. This configuration is also covered in Step 2 above by the command "delay up 120."

7. Once the stability of Radio A is ensured, the following lines are executed to switch the tunnel traffic back to Radio A:

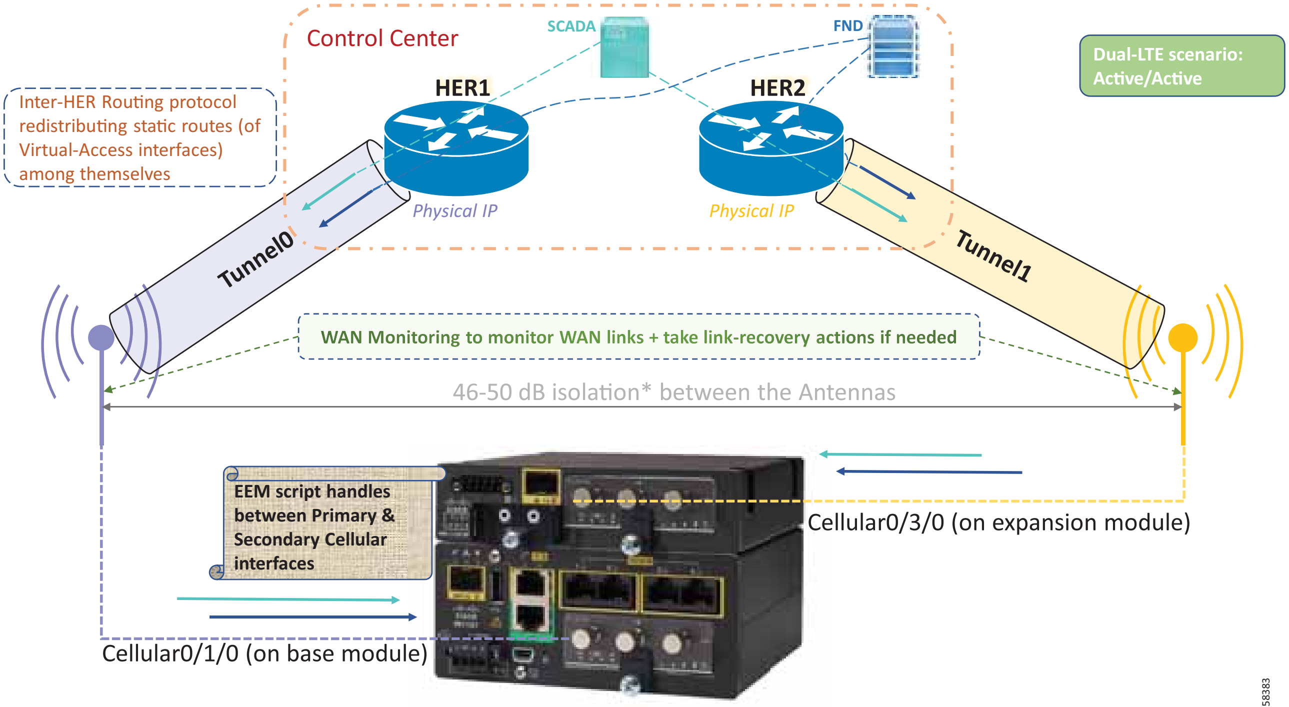
```
event manager applet Recovery
 event track 3 state up
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface tunnel0"
 action 4  cli command "tunnel source Cellular0/1/0"
 action 5  cli command "end"
 action 99 syslog msg "NOTE: Connectivity Restored on Cellular 0/1/0"
```

Active/Active Load Sharing

The FAR configuration is pushed from FND and a sample has been provided on page 164.

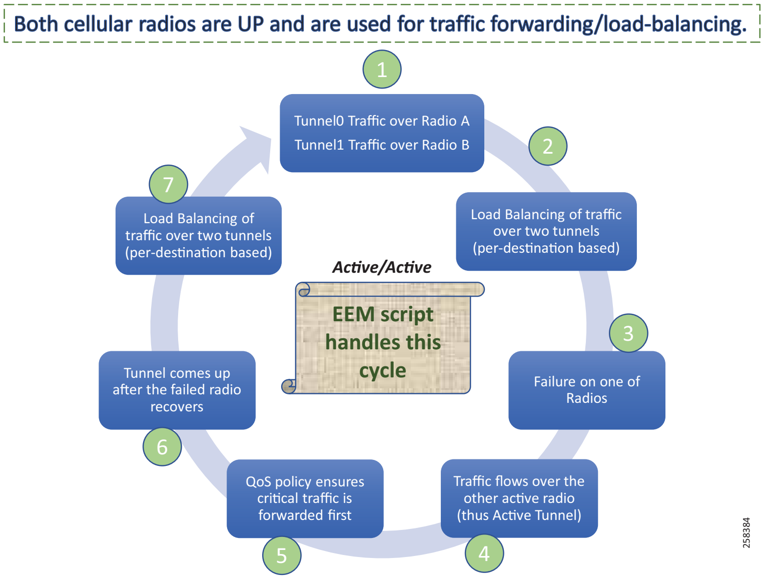
In this operational mode, FAR connects to HER1 securely over Tunnel0 over the primary cellular interface (Cellular 0/1/0) and FAR connects to HER2 securely over Tunnel1 over the secondary cellular interface (Cellular 0/3/0). This is shown in Figure 166:

Figure 166 Active/Active Scenario


Control Center
SCADA
FND
HER1
HER2
Dual-LTE scenario: Active/Active
Inter-HER Routing protocol redistributing static routes (of Virtual-Access interfaces) among themselves
Physical IP
Physical IP
Tunnel0
Tunnel1
WAN Monitoring to monitor WAN links + take link-recovery actions if needed
46-50 dB isolation* between the Antennas
EEM script handles between Primary & Secondary Cellular interfaces
Cellular0/3/0 (on expansion module)
Cellular0/1/0 (on base module)
258383

When connectivity over tunnel0 fails, tunnel1 would be up, which allows the traffic to be routed through the second tunnel. If Active/Standby is implemented, then tunnel 1 has to be shutdown. If Active/Active is implemented, both tunnel 0 and tunnel 1 should be in the up state. The traffic flow, recovery, and failover is shown as a state diagram in Figure 167:

Figure 167 Dual-LTE (Active/Active): Traffic Flow Resiliency Cycle


Both cellular radios are UP and are used for traffic forwarding/load-balancing.
1
Tunnel0 Traffic over Radio A
Tunnel1 Traffic over Radio B
2
Load Balancing of traffic over two tunnels (per-destination based)
3
Failure on one of Radios
4
Traffic flows over the other active radio (thus Active Tunnel)
5
QoS policy ensures critical traffic is forwarded first
6
Tunnel comes up after the failed radio recovers
7
Load Balancing of traffic over two tunnels (per-destination based)
Active/Active
EEM script handles this cycle
258384

Both the LTEs and the respective tunnel interfaces are up. The traffic can take any path to the control center. This approach provides more redundancy and bandwidth and ensures that the data loss is minimized to the maximum extent.

1. The Tunnel0 traffic flows through Radio A and the Tunnel1 traffic flows through Radio B.
2. Load Balancing of traffic happens as there exists two paths to the destination.
3. Failure of one Radio does not affect the flow traffic, as the traffic flows over the other active tunnel.
4. QoS policies are configured to ensure that critical traffic is given priority. This is discussed in the subsequent sections.
5. WAN monitoring can be used to recover the radio.
6. If the failed Radio is recovered, load balancing of the traffic continues and the process repeats.

WAN Monitoring

In the previous sections, we talked about EEM scripts that have been used to switch from one radio to another. Sometimes due to a glitch in the hardware, the possibility exists that one of the radio may fail. In such cases, a simple manual 'shut'/'no shut' CLI execution on the device may trigger the radio to come up. However, if the FARs are located in a remote place where a console connection is unlikely, then a manual 'shut'/'no shut' operation is not possible. However, a substitute to this manual operation is the WAN monitoring feature available in the latest software for the FAR. Using this feature, the glitch in the hardware can be overcome to recover the failed radio. This feature can be implemented in both Active/Standby and Active/Active scenarios. Following is an example configuration, which can be extended to recover both interfaces.

```
track 10 ip sla 10
ip sla 10
 icmp-echo <DMZ IP>
 timeout 6000
 frequency 300
ip sla schedule 10 life forever start-time now
event manager environment wanmon_if_list {cellular0/1/0 {ipsla 10}}
event manager policy tm_wanmon.tcl authorization bypass
```

For design and conceptual understanding, please refer to the “WAN Backhaul Redundancy” section in the Design Guide.

IP Services

This chapter includes the following major topics:

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.

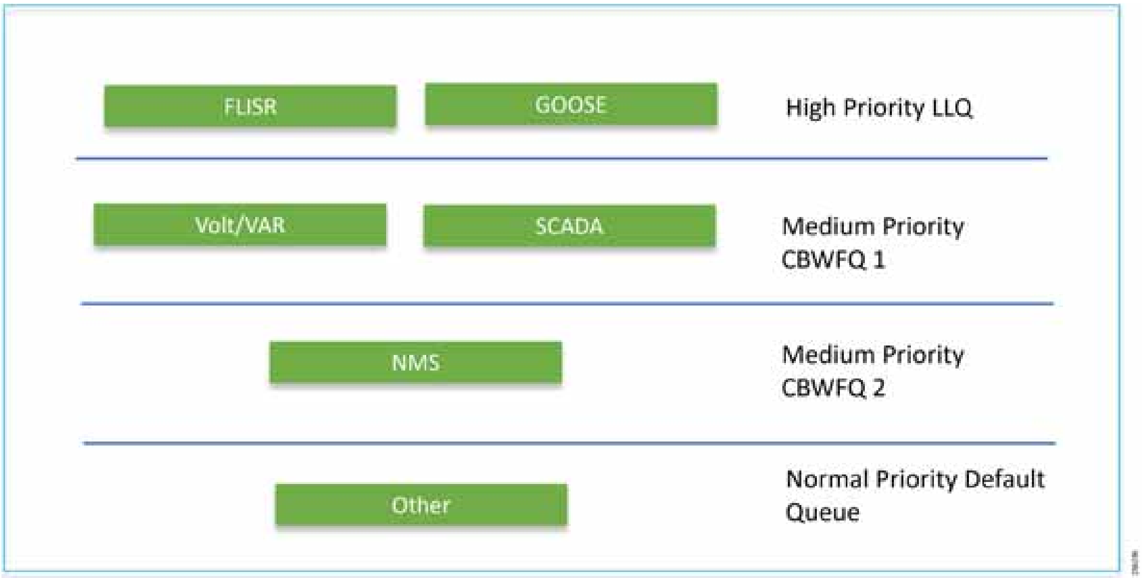
In the case of dual-WAN interfaces with different bandwidth capabilities (that is, cellular), QoS policies must be applied to prioritize the traffic allowed to flow over these limited bandwidth links, to determine which traffic can be dropped, etc.

On a multi-services DA solution, QoS DiffServ and CoS (IEEE 802.1p) 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
- **Layer 2 Traffic**–Distribution Automation such as IEC 61850 GOOSE/SV traffic switches between Ethernet interfaces and IEC 61850 traffic bridged over WAN links between substations

Figure 168 lists the different priorities among Distribution Automation traffic:

Figure 168 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 Precedence 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.

The SSR or DA Gateway performs QoS actions on Layer 3 (cellular, Ethernet) interfaces. The sequencing of QoS actions on egress traffic is as follows:

- Classification
- Marking
- Queuing

Upstream QoS—From DA IED to SCADA

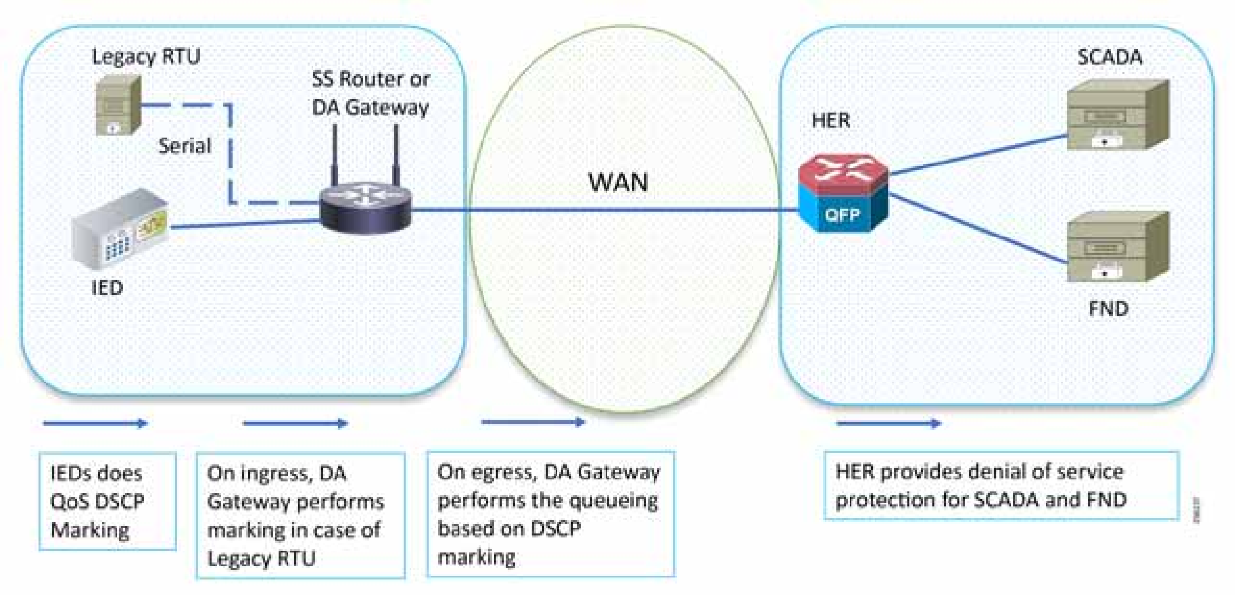
The DA IEDs perform the marking functionality. If the IED does not have capability to mark the IP packets, the DA Gateway or SSR can perform the marking functionality. On egress WAN interface, queuing will be performed. High priority FLISR and GOOSE traffic will be assigned in Low Latency Queue. Medium 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 Queue2. 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 values so that the same policy can be applied across Cellular or Ethernet backhaul interfaces

Headend Router: ASR 1000, which supports a rich QoS feature set from Cisco IOS, provides DoS protection for applications like the FND and SCADA. For complete details, refer to the latest documentation link:

- https://www.cisco.com/c/en/us/products/collateral/routers/asr-1002-router/solution_overview_c22-449961.html

Figure 169 Upstream QoS IED to SCADA



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 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 percent 10
class volt-var
bandwidth remaining-percent 20
class NMS
bandwidth percent remaining-percent 30
class class-default
```

Network Address Translation

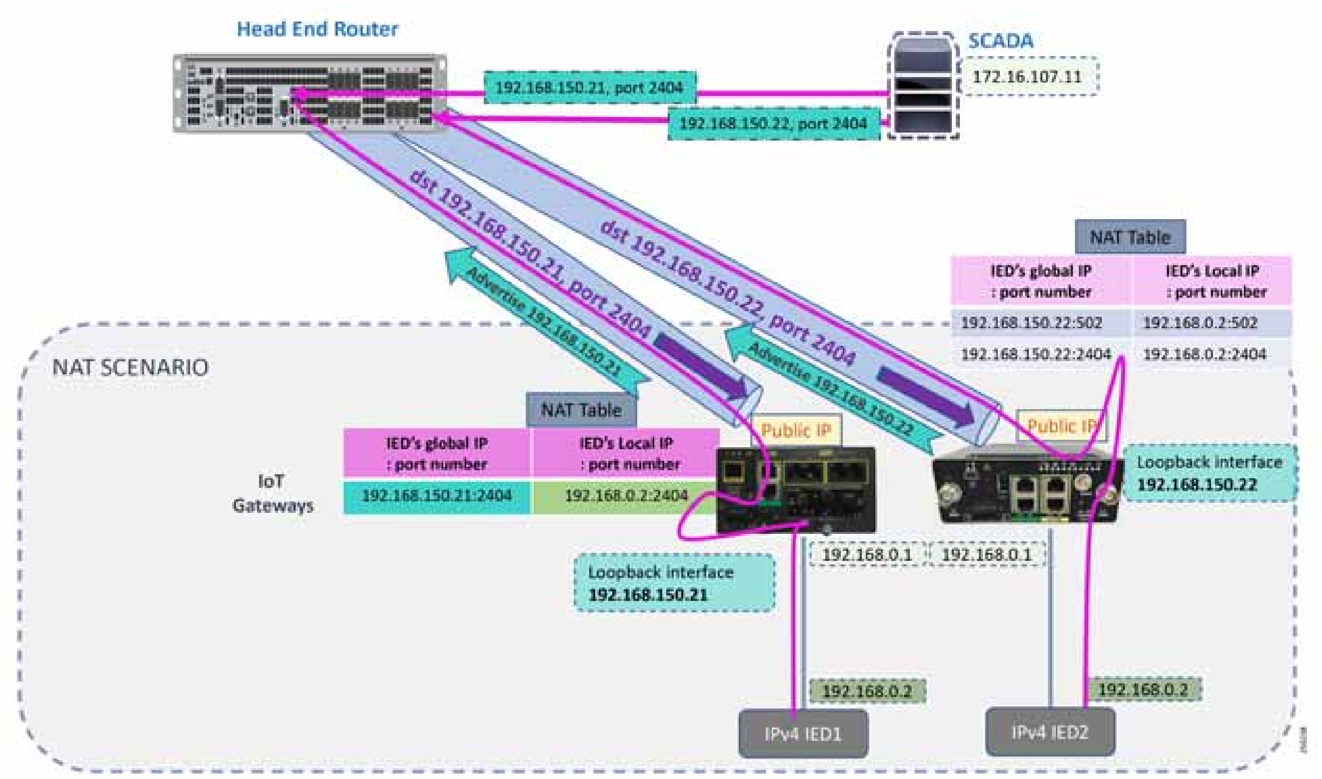
This section corresponds to the “Network Address Translation” section of the Design Guide, which can be referred to for more details. The IoT Gateway is capable of supporting both NAT and non-NAT scenarios described in the Design Guide. The NAT scenario has been implemented in this Implementation Guide.

Note: This configuration is pushed as part of ZTD (during device registration phase). The FND leverages the SCADA ICT Enablement profiles discussed in Appendix D: SCADA ICT Enablement Profiles, page 200.

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.

In Figure 170, 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 2404.

Figure 170 Network Address Translation



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 2404, 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 2404. In summary:

- The SCADA communication on 192.168.150.21 on port 2404 is sent to IED1:2404
- The SCADA communication on 192.168.150.22 on port 2404 is sent to IED2:2404

NAT on IR1101

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 Tunnel0
ip nat outside
!
! /* NAT the traffic on Loopback_IP:2404 to 192.168.0.2(IED_IP):2404 */
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
```

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 Tunnel0 ip nat outside
!
! /* NAT the traffic on Loopback_IP:2404 to 192.168.0.2(IED_IP):2404 */
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
```

NAT configurations on other IoT Gateway platforms (like CGR1000 and IR8xx platforms) would be similar to the ones captured above.

Appendix A: PnP Profiles

This appendix includes the following major topics:

Bootstrapping Template for IPv4 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: IPv4-BOOTSTRAP

```
<#if far.isRunningIos()>
<#-- New section to support Day 0 operation -->
<#if isBootstrapping??>
<#assign sublist=far.eid?split("+")[0..1]>
<#assign pid=sublist[0]>
<#assign sn=sublist[1]>
!
file prompt quiet
<#if far.bootimage??>
boot-start-marker
<#if pid?starts_with("IR1101")>
boot system bootflash:${far.bootimage}
<#else>
boot system flash:${far.bootimage}
</#if>
boot-end-marker
</#if>
!
!! ip host configurations
ip host ra.ipg.cisco.com 172.16.241.2
ip host tps.ipg.cisco.com 172.16.242.242
ip host ntp.ipg.cisco.com 10.10.100.100
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
!
<#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>
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
!
!username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
!
crypto pki profile enrollment LDevID
enrollment url http://ra.ipg.cisco.com
enrollment credential CISCO_IDEVID_SUDI
!
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
!
cgna gzip
!
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
gzip
!
do delete /force /recursive 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 configsÖ
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>
!
!
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
!
!ip http client connection timeout 5
!ip http client connection retry 5
!
! Disabling http server
no ip http server
!
! Enabling http secure server.
ip http secure-server
!
!
!
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
!
!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
!
!
!! 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
!
!
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_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
!
do copy running-config flash:express-setup-config2
no file prompt quiet
do term len 30
!
!
!
exit
</#if>
!
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

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 far.isRunningIos()>
<#-- New section to support Day 0 operation -->
<#if isBootstrapping??>
<#assign sublist=far.eid?split("+")[0..1]>
<#assign pid=sublist[0]>
<#assign sn=sublist[1]>
!
file prompt quiet
<#if far.bootimage??>
boot-start-marker
<#if pid?starts_with("IR1101")>
boot system bootflash:${far.bootimage}
<#else>
boot system flash:${far.bootimage}
</#if>
boot-end-marker
</#if>
!
!! 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>
!
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
!
<#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>
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
!
!username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
!
crypto pki profile enrollment LDevID
enrollment url http://ra.ipg.cisco.com
enrollment credential CISCO_IDEVID_SUDI
!
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
!
cgna gzip
!
!
interface loopback999
description workaround for CSCvb49055
ip address 169.254.1.1 255.255.255.255
!
cgna initiator-profile cg-nms-tunnel
callhome-url https://tps.ipg.cisco.com:9120/cgna/ios/config
execution-url https://169.254.1.1:8443/wsma/config
post-commands
active
!
!
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
gzip
interval 10
!
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
!
!
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>
!
!
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
!
!ip http client connection timeout 5
!ip http client connection retry 5
!
! Disabling http server
no ip http server
!
! Enabling http secure server.
ip http secure-server
!
!
!
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
!
!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
```

```
!
!
!! 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
!
!
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_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
!
do copy running-config flash:express-setup-config2
no file prompt quiet
do term len 30
!
!
!
exit
</#if>
!
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

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

```
<#if far.isRunningIos()>
<#-- New section to support Day 0 operation -->
<#if isBootstrapping??>
<#assign sublist=far.eid?split("+")[0..1]>
<#assign pid=sublist[0]>
<#assign sn=sublist[1]>
!
```

```
file prompt quiet
!
<#if far.bootimage??>
boot-start-marker
<#if pid?starts_with("IR1101")>
boot system bootflash:${far.bootimage}
<#else>
boot system flash:${far.bootimage}
</#if>
boot-end-marker
</#if>
!
!! ip host configurations
ip host ra.ipg.cisco.com 2001:db8:10:241::5921
ip host tps.ipg.cisco.com 2001:db8:10:242::242
ip host ntp.ipg.cisco.com 2001:db8:1010:903::2
!
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
!
<#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>
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
!
username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
!
crypto pki profile enrollment LDevID
enrollment url http://ra.ipg.cisco.com
enrollment credential CISCO_IDEVID_SUDI
!
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
!
cgna gzip
!
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
gzip
!
!
!
do delete /force /recursive flash:archive
do mkdir flash:archive
archive
path flash:/archive
maximum 8
!
!
!
!
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
!
!
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>
!
!
!
!
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
!
!ip http client connection timeout 5
!ip http client connection retry 5
```

```
!
! Disabling http server
no ip http server
!
! Enabling http secure server.
ip http secure-server
!
!
!
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
!
!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
!
!
!! 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
!
!
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_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
!
no file prompt quiet
exit
</#if>
!
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

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.

```
<#if far.isRunningIos()>
  <#-- New section to support Day 0 operation -->
  <#if isBootstrapping??>
    <#assign sublist=far.eid?split("+")[0..1]>
    <#assign pid=sublist[0]>
    <#assign sn=sublist[1]>
    !
    file prompt quiet
!
    <#if far.bootimage??>
      boot-start-marker
      <#if pid?starts_with("IR1101")>
      boot system bootflash:${far.bootimage}
      <#else>
      boot system flash:${far.bootimage}
      </#if>
      boot-end-marker
    </#if>
!
    !
    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
    !
    <#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>
    !
    aaa new-model
    aaa authentication login default local
    aaa authorization exec default local
    !
    !
    username ${far.adminUsername} privilege 15 algorithm-type sha256 secret ${far.adminPassword}
    username cisco privilege 15 algorithm-type sha256 secret Cisco@123
    !
    crypto pki profile enrollment LDevID
    enrollment url  http://ra.ipg.cisco.com
    enrollment credential  CISCO_IDEVID_SUDI
    !
    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
    !
    cgna gzip
    !
    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
    !
    !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
    !
    !
    !
    interface loopback999
    description workaround for CSCvb49055
    ip address 169.254.1.1 255.255.255.255
    !
    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
   !
   !
   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
    !
    !
    !
    !
    do delete /force /recursive flash:archive
    do mkdir flash:archive
    archive
    path flash:/archive
    maximum 8
    !
    !
    !
    !
    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
    !
    !
    !
    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>
    !
    !
    !
    !
    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
    !
    !ip http client connection timeout 5
    !ip http client connection retry 5
    !
! Disabling http server
no ip http server
!
! Enabling http secure server.
ip http secure-server
!
!
    !
    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
    !
    !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
    !
    !
    !! 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
    !
    !
    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 = $_cli_result"
     action 2.1 cli command "do cgna exec profile cg-nms-tunnel"
     action 2.2  puts "EEM:: Removing the applet manager REMOVE_IDEVID_AS_TP as the CLI change is 
done"
     action 2.3  cli command "no event manager applet REMOVE_IDEVID_AS_TP"
     action 2.4  cli command "exit"
     action 2.5 else
     action 2.6 puts "EEM:: LDevID not Granted yet. Will check after 30 seconds"
     action 3.0 end
!
  ! track 1 interface Cellular0/1/0 line-protocol
  !   delay down 5 up 10
!
  ! event manager applet Default_route_via_Cellular
       !event track 1 state up
!trigger delay 600
!action 1.0 cli command "enable"
!action 1.1 cli command "show run | sec ZTD_SCEP_Enabled"
!action 1.2 string match "*TRUE" "$_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
!
no file prompt quiet
exit
  </#if>
  !
<#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

The Tunnel Provisioning Profile could also be referred 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.

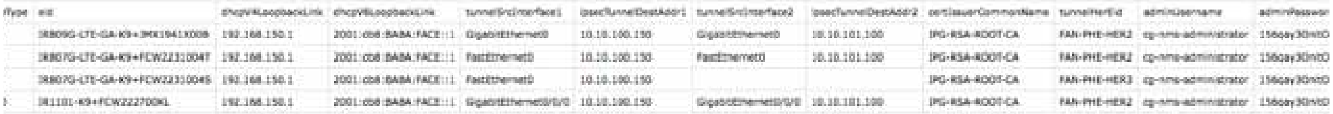
Once the Tunnel group is created, move the IoT Gateways under the appropriate "Tunnel Group." For steps, please refer to the "Moving FARs to Another Group" section of the Cisco IoT FND Guide.

Tunnel Group for IPv4 Network

Tunnel Group Name: IPv4_primary_tunnel_provision Sample csv file to import in FND

IoT Gateways need to be added into FND for the purpose of management. They could be added to FND by importing a csv file. A sample csv file is shown in Figure 171:

Figure 171 IoT-Gateway-deployment-over-IPv4-Backhaul-csvfile



Type	eid	dhcpV4LoopbackLink	dhcpV6LoopbackLink	tunnelSrcInterface1	ipsecTunnelDestAddr1	tunnelSrcInterface2	ipsecTunnelDestAddr2	certIssuerCommonName	tunnelHerEid	adminUsername	adminPasswor
	IR809G-LTE-GA-K9+JMX1941X008	192.168.150.1	2001:db8:BABA:FACE::1	GigabitEthernet0	10.10.100.150	GigabitEthernet0	10.10.101.100	IPG-RSA-ROOT-CA	FAN-PHE-HER2	cg-nms-administrator	156say30ntO
	IR807G-LTE-GA-K9+FCW2231004T	192.168.150.1	2001:db8:BABA:FACE::1	FastEthernet0	10.10.100.150	FastEthernet0	10.10.101.100	IPG-RSA-ROOT-CA	FAN-PHE-HER2	cg-nms-administrator	156say30ntO
	IR807G-LTE-GA-K9+FCW22310045	192.168.150.1	2001:db8:BABA:FACE::1	FastEthernet0	10.10.100.150			IPG-RSA-ROOT-CA	FAN-PHE-HER3	cg-nms-administrator	156say30ntO
0	IR1101-K9+FCW22270OKL	192.168.150.1	2001:db8:BABA:FACE::1	GigabitEthernet0/0/0	10.10.100.150	GigabitEthernet0/0/0	10.10.101.100	IPG-RSA-ROOT-CA	FAN-PHE-HER2	cg-nms-administrator	156say30ntO

For more details about various other csv parameters to be used during csv import at FND, please refer to *Prepare .csv (Comma-Separated Value) Files to Import New Devices on FND* at the following URL:

- https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/iot-field-network-director/210446-Prepare-csv-Comma-Separated-Value-fil.html

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 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.

The API also provides the method “dhcpClientId,” 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
<#--
```

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 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

<#--
```

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
FlexVPN_Client_ipv4_LAN

route set access-list ipv6 FlexVPN_Client_ipv6_LAN route set interface
exit


crypto ikev2 proposal FlexVPN_IKEv2_Proposal encryption aes-cbc-256
group 14 integrity sha256 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 remote
rsa-sig
authentication local rsa-sig dpd 120 3 periodic identity local dn
match certificate FlexVPN_Cert_Map pki trustpoint LDevID
exit

<#--
```

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 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>
```

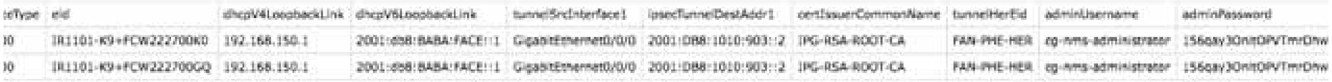
```
crypto IPSec profile FlexVPN_IPSec_Profile set ikev2-profile FlexVPN_IKEv2_Profile set pfs group14
set transform-set FlexVPN_IPSec_Transform_Set exit

<#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}
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

</#if>

!
no event manager environment ZTD_SCEP_Debug
!
ip host fnd.ipg.cisco.com 172.16.103.100
!
!
</#if>
```

Tunnel Group for IPv6 Network

Tunnel Group Name: IPv6_primary_tunnel_provision Sample csv file to import in FND

IoT Gateways need to be added into FND for the purpose of management. They could be added to FND by importing a csv file. A sample csv file is shown in Figure 172:

Figure 172 IoT-Gateway-deployment-over-IPv6-backhaul-csvfile



ceType	eid	dhcpV4LoopbackLink	dhcpV6LoopbackLink	tunnelSrcInterface1	ipsecTunnelDestAddr1	certIssuerCommonName	tunnelHerEid	adminUsername	adminPassword
10	IR1101-K9+FCW222700K0	192.168.150.1	2001:db8:BABA:FACE::1	GigabitEthernet0/0/0	2001:DB8:1010:903::2	IPG-RSA-ROOT-CA	FAN-PHE-HER	cg-nms-administrator	156qay3OnftOPVTmrDhw
10	IR1101-K9+FCW222700GQ	192.168.150.1	2001:db8:BABA:FACE::1	GigabitEthernet0/0/0	2001:DB8:1010:903::2	IPG-RSA-ROOT-CA	FAN-PHE-HER	cg-nms-administrator	156qay3OnftOPVTmrDhw

For more details about csv file parameters, please refer to *Prepare .csv (Comma-Separated Value) Files to Import New Devices on FND* at the following URL:

- https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/iot-field-network-director/210446-Prepare-csv-Comma-Separated-Value-fil.html

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.

The API also provides the method “dhcpClientId.” 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
<#--
```

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

<#--
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’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 FlexVPN_Cert_Map 1 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

<#--
```

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
exit

crypto ikev2 proposal FlexVPN_IKEv2_Proposal encryption aes-cbc-256
group 14 integrity sha256 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 remote
rsa-sig
authentication local rsa-sig dpd 120 3 periodic identity local dn
match certificate FlexVPN_Cert_Map pki trustpoint LDevID

exit

<#--
```

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 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 mode transport
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 tunnel path-mtu-discovery 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
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 integrity sha256 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
<#--
```

If the headend router 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 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 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
!
ip host fnd.ipg.cisco.com 172.16.103.100
!
!
</#if>
```

Device Configuration Profiles

The device configuration profile could also be referred to as the “Configuration Group.” For steps to create a new configuration group and move necessary IoT Gateways under it, please refer to the “Configuring Device Group Settings” section of the Cisco IoT FND Guide at the following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_2/iot_fnd_ug4_2/device_mgmt.html#16666

To enable “Ready to Go” SCADA traffic post ZTD, configuration profiles mentioned in Appendix D: SCADA ICT Enablement Profiles, page 200 could be used.

Appendix C: FlexVPN Configurations

This appendix provides the complete running configuration taken from the CGR and the HER, which includes the IKEv2 CLB bringing up the FlexVPN tunnel over IPv4 backhaul. It includes the following major topics:

- IoT Gateway Configuration, page 196
- Headend Router Configuration, page 198

IoT Gateway Configuration

Note: The IoT Gateway configuration is for reference only since it is configured by ZTD.

```
!
!
aaa new-model
aaa authorization network FlexVPN_Author local
!
ip host ra.ipg.cisco.com 172.16.241.2
ip host tps.ipg.cisco.com 172.16.242.242
ip host ntp.ipg.cisco.com 10.10.100.100 ip cef
!
!
crypto pki trustpoint LDevID
enrollment retry count 4
enrollment retry period 2
enrollment mode ra
enrollment profile LDevID
serial-number none
fqdn none
ip-address none
password
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
subject-name serialNumber=PID:CGR1120/K9
SN:JAD191601KT,CN=CGR1000_JAD191601KT
revocation-check none
rsakeypair LDevID 2048

!
crypto pki profile enrollment LDevID
enrollment url http://ra.ipg.cisco.com
!
crypto pki certificate map FlexVPN_Cert_Map 1
issuer-name co cn = ipg-rsa-root-ca
!
crypto pki certificate chain LDevID
< Hex code removed for clarity >
!
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
!
crypto ikev2 redirect client
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
proposal FlexVPN_IKEv2_Proposal
!
```

```
!
crypto ikev2 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 10.10.100.150
client connect Tunnel0

!
crypto IPSec transform-set FlexVPN_IPSec_Transform_Set esp-aes esp-sha-hmac
mode tunnel
!
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 192.168.150.6 255.255.255.255
ipv6 address 2001:DB8:BABA:FACE:6C1C:D5F4:B98E:11B3/128
!
interface Tunnel0
description IPSec tunnel to FAN-PHE-HER
ip unnumbered Loopback0
ip nhrp network-id 1
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ipv6 unnumbered Loopback0
tunnel source GigabitEthernet2/1
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
interface GigabitEthernet2/1
no switchport
ip address
dhcp duplex auto
speed auto
!
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip nhrp network-id 1
ip nhrp shortcut virtual-template 1 ip
nhrp redirect
tunnel protection IPSec profile FlexVPN_IPSec_Profile

!
ip access-list standard FlexVPN_Client_ipv4_LAN
permit 192.168.150.6
!
ipv6 access-list FlexVPN_Client_ipv6_LAN
sequence 20 permit ipv6 host 2001:DB8:BABA:FACE:6C1C:D5F4:B98E:11B3 any
!
ip route <HER1 DMZ ip> 255.255.255.255 Cellular 0/1/0
ip route <HER1 DMZ ip> 255.255.255.255 Cellular 0/3/0
```

Headend Router Configuration

```
!
aaa new-model
aaa authorization network FlexVPN_Author local
!
ip host rsaca.ipg.cisco.com 172.16.102.2
ip host rsaca.ipg.cisco.comB 172.16.102.2
ip domain name ipg.cisco.com
!
!
crypto pki trustpoint LDevID
enrollment retry count 10
enrollment retry period 2
enrollment mode ra e
nrollment profile LDevID
serial-number
ip-address none
password
fingerprint CFA2613029B11E461430A2DC5F624147CCEE6469
revocation-check none
rsakeypair LDevID
!
crypto pki profile enrollment LDevID
enrollment url http://rsaca.ipg.cisco.com/certsrv/mscep/mscep.dll
!
crypto pki certificate map FlexVPN_Cert_Map 1
issuer-name co cn = ipg-rsa-root-ca
!
crypto pki certificate chain LDevID
< Hex code removed for clarity >
!
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 policy FlexVPN_IKEv2_Policy
proposal FlexVPN_IKEv2_Proposal
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
match certificate FlexVPN_Cert_Map
identity local dn
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint LDevID
dpd 30 3 periodic
aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
virtual-template 1
!
crypto ikev2 cluster
standby-group cluster1
slave priority 90
slave max-session 100
no shutdown
!
!
```

```
crypto IPSec transform-set FlexVPN_IPSec_Transform_Set esp-aes esp-sha-hmac
mode tunnel
!

crypto IPSec profile FlexVPN_IPSec_Profile
set transform-set FlexVPN_IPSec_Transform_Set
set pfs group14
set ikev2-profile FlexVPN_IKEv2_Profile
responder-only
!
!
interface Loopback0
ip address 192.168.150.2 255.255.255.255
ipv6 address 2001:DB8:BABA:FACE::2/64
!
interface GigabitEthernet0/0/0
description connected to Gi1/1 of SWITCH_DMZ
ip address 10.10.100.151 255.255.255.0
standby version 2
standby 1 ip 10.10.100.150
standby 1 priority 110
standby 1 name cluster1
negotiation auto
cdp enable
!
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ipv6 unnumbered Loopback0 ipv6 enable
tunnel protection IPSec profile FlexVPN_IPSec_Profile
!
ip access-list standard FlexVPN_Client_Default_ipv4_Route
permit 172.16.103.100/* IP Address of FND */
permit 192.168.150.0 0.0.0.255 /* Loopback Address subnet for FAR & HER */
!
ipv6 access-list FlexVPN_Client_Default_ipv6_Route
sequence 5 permit ipv6 any host 2001:DB8:16:103::100
sequence 20 permit ipv6 any any
!
```

Appendix D: SCADA ICT Enablement Profiles

This appendix includes the following major topics:

IR1101 Platform: Single Control Center Profiles

ICT Enablement for IP-based IED using IR1101

The following scenarios were validated using this profile:

- IP-based IED is configured with 192.168.0.2.
- Default gateway for IED is 192.168.0.1, which is the IP address of IR1101.
- IED is connected to FastEthernet0/0/1 and listening on port 2404.
- SCADA Master IP address is 172.16.107.11.
- SCADA Master reaches the IP IED on the IoT Gateway IP on port 2404.

Configuration Group Name: IR1101_SINGLE_CC_IP_Only

```
<#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
!
interface Tunnel0
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
!
<#-- End of custom addition of configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

ICT Enablement for Serial and/or IP-based IED using IR1101

The following scenarios were validated using this profile:

- IP-based IED is configured with 192.168.0.2.
- Default gateway for IED is 192.168.0.1, which is the IP address of IR1101.
- IED is connected to FastEthernet0/0/1, and listening on port 2404.
- SCADA Master IP address is 172.16.107.11.
- Configuration of the serial interface validated is 9600-8N1.
- Serial interface validated is Async0/2/0 (corresponds to line 0/2/0).
- SCADA Master reaches the IP IED on IoT Gateway IP on port 2404.
- SCADA Master reaches the Serial IED on IoT Gateway IP on port 25000.

Configuration Group Name: IR1101_SINGLE_CC_IP_and_RawSocket

```
<#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
!
interface Tunnel0 ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
interface Async0/2/0
no ip address
encapsulation raw-tcp
!
line 0/2/0
raw-socket tcp client 172.16.107.11 25000
databits 8
stopbits 1
speed 9600
parity none
!
<#-- End of custom addition of configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

Configuration Group Name: IR1101_SINGLE_CC_IP_and_ProtocolTranslation

```
<#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
!
interface Tunnel0
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
interface Async0/2/0
no ip address
encapsulation scada
!
line 0/2/0
databits 8
stopbits 1
speed 9600
parity none
!
scada-gw protocol t101
channel t101_ch1
link-addr-size two
bind-to-interface Async 0/2/0
session t101_session1
attach-to-channel t101_ch1
sector t101_sector1
attach-to-session t101_session1
scada-gw protocol t104
channel t104_ch1
t3-timeout 20
tcp-connection 0 local-port 25000 remote-ip any
session t104_session1
attach-to-channel t104_ch1
sector t104_sector1
attach-to-session t104_session1
map-to-sector t101_sector1
scada-gw enable
<#-- End of custom addition of configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

IR1101 Platform: Dual Control Center Profiles

ICT Enablement for Serial and/or IP-based IED using IR1101

The following scenarios were validated using this profile:

- IP-based IED is configured with 192.168.0.2.
- Default gateway for IED is 192.168.0.1, which is the IP address of IR1101.
- IED is connected to FastEthernet0/0/1, and listening on port 2404.
- SCADA Master1 IP address is 172.16.107.11.
- SCADA Master2 IP address is 172.17.107.11.
- Configuration of the serial interface validated is 9600-8N1.
- Serial interface validated is Async0/2/0 (corresponds to line 0/2/0).
- SCADA Master reaches the IP IED on IoT Gateway IP on port 2404.
- SCADA Master1 reaches the Serial IED on IoT Gateway IP on port 25000.
- SCADA Master2 reaches the Serial IED on IoT Gateway IP on port 25001.

Configuration Group Name: IR1101_DUAL_CC_IP_and_RawSocket

```
<#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
<#--- Beginning of custom modification for tunnel to secondary control center -->
<#if far.IPSecTunnelDestAddr2?has_content>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
interface Tunnel1
description IPSec tunnel to Secondary Tunnel Destination
ip unnumbered loopback0
ipv6 unnumbered loopback0
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile tunnel source ${wanInterface[0].name}
exit
!
crypto ikev2 client flexvpn FlexVPN_Client_Tunnel1
peer 1 ${far.IPSecTunnelDestAddr2}
client connect Tunnel1 exit
</#if>
<#--- End of custom modification for tunnel to secondary control center -->
!
<#--- Beginning of IR1101_DUAL_CC_IP 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
!
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
ip nat inside source static tcp 192.168.0.2 26000 interface Loopback0 26000
!
<#--- End of IR1101_DUAL_CC_IP Configuration -->
!
<#--- Beginning of IR1101_DUAL_CC_Raw_Socket Configuration -->
interface Async0/2/0
no ip address
encapsulation raw-tcp
!
line 0/2/0
raw-socket tcp client 172.16.107.11 25000
raw-socket tcp client 172.17.107.11 25000
databits 8
stopbits 1
speed 9600
parity none
!
<#--- End of IR1101_DUAL_CC_Raw_Socket Configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

Configuration Group Name: IR1101_DUAL_CC_IP_and_ProtocolTranslation

```
<#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
<#--- Beginning of custom modification for tunnel to secondary control center -->
<#if far.IPSecTunnelDestAddr2?has_content>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
interface Tunnel1
description IPSec tunnel to Secondary Tunnel Destination
ip unnumbered loopback0
ipv6 unnumbered loopback0
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
tunnel source ${wanInterface[0].name}
exit
!
crypto ikev2 client flexvpn FlexVPN_Client_Tunnel1
peer 1 ${far.IPSecTunnelDestAddr2}
client connect Tunnel1
exit
</#if>
<#--- End of custom modification for tunnel to secondary control center -->
!
<#--- Beginning of IR1101_DUAL_CC_IP 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
!
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
ip nat inside source static tcp 192.168.0.2 26000 interface Loopback0 26000
!
<#--- End of IR1101_DUAL_CC_IP Configuration -->
!
<#--- Beginning of IR1101_DUAL_CC_Protocol_Translation Configuration -->
interface Async0/2/0
no ip address
encapsulation scada
!
line 0/2/0
databits 8
stopbits 1
speed 9600
parity none
!
scada-gw protocol t101
channel t101_ch1
link-addr-size two
bind-to-interface Async0/2/0
session t101_session1
attach-to-channel t101_ch1
sector t101_sector1
attach-to-session t101_session1
scada-gw protocol t104
channel t104_ch1
t3-timeout 20
tcp-connection 0 local-port 25000 remote-ip any
tcp-connection 1 local-port 25001 remote-ip any
session t104_session1
attach-to-channel t104_ch1
sector t104_sector1
attach-to-session t104_session1
map-to-sector t101_sector1
!
scada-gw enable
!
<#--- End of IR1101_DUAL_CC_Protocol_Translation Configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

IR807 Platform: Single Control Center Profiles

ICT Enablement for IP-based IED using IR807

The following scenarios were validated using this profile:

- IP-based IED is configured with 192.168.0.2.
- Default gateway for IED is 192.168.0.1, which is the IP address of IR807.
- IED is connected to FastEthernet1 and listening on port 2404.
- SCADA Master IP address is 172.16.107.11.
- SCADA Master reaches the IP IED on IoT Gateway IP on port 2404.

Configuration Group Name: IR807_SINGLE_CC_IP_Only

```
<#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
ip virtual-reassembly in
duplex auto
speed auto
!
interface Tunnel0
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
!
<#-- End of custom addition of configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

ICT Enablement for Serial and/or IP-based IED using IR807

The following scenarios were validated using this profile:

- IP-based IED is configured with 192.168.0.2.
- Default gateway for IED is 192.168.0.1, which is the IP address of IR807.
- IED is connected to FastEthernet1, and listening on port 2404.
- SCADA Master IP address is 172.16.107.11.
- Configuration of the serial interface validated is 9600-8N1.
- Serial interface validated is Async1 (corresponding to line 4).
- SCADA Master reaches the IP IED on IoT Gateway IP on port 2404.
- SCADA Master reaches the Serial IED on IoT Gateway IP on port 25000.

Configuration Group Name: IR807_SINGLE_CC_IP_and_RawSocket

```
<#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
!
<#--- Beginning of custom modification for tunnel to secondary control center -->
<#if far.IPSecTunnelDestAddr2?has_content>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
interface Tunnel1
description IPSec tunnel to Secondary Tunnel Destination
ip unnumbered loopback0
ipv6 unnumbered loopback0
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
tunnel source ${wanInterface[0].name}
exit
!
crypto ikev2 client flexvpn FlexVPN_Client_Tunnel1
peer 1 ${far.IPSecTunnelDestAddr2}
client connect Tunnel1
exit
</#if>
!
<#--- End of custom modification for tunnel to secondary control center -->
!
<#--- Beginning of IR807_SINGLE_CC_IP Configuration -->
!
interface FastEthernet1
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
```

```
speed auto
!
interface Tunnel0
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
!
<#--- End of IR807_SINGLE_CC_IP Configuration -->
!
<#--- Beginning of IR807_SINGLE_CC_RawSocket Configuration -->
!
!
interface Async1
no ip address
encapsulation raw-tcp
!
!
line 4
raw-socket tcp client 172.16.107.11 25000
databits 8
stopbits 1
speed 9600
parity none
!
!
!
<#--- End of IR807_SINGLE_CC_RawSocket Configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

Configuration Group Name: IR807_SINGLE_CC_IP_and_ProtocolTranslation

```
<#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
!
<#--- Beginning of IR807_SINGLE_CC_IP 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
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
!
<#--- End of IR807_SINGLE_CC_IP Configuration -->
!
<#--- Beginning of IR807_SINGLE_CC_Protocol_Translation Configuration -->
!
interface Async1
no ip address
encapsulation scada
```

```
!
line 4
databits 8
stopbits 1
speed 9600 parity none
!
scada-gw protocol t101
channel t101_ch1
link-addr-size two
bind-to-interface Async 0
session t101_session1
attach-to-channel t101_ch1
sector t101_sector1
attach-to-session t101_session1
scada-gw protocol t104
channel t104_ch1
t3-timeout 20
tcp-connection 0 local-port 25000 remote-ip any
session t104_session1
attach-to-channel t104_ch1
sector t104_sector1
attach-to-session t104_session1
map-to-sector t101_sector1
scada-gw enable
!
<#--- End of IR807_SINGLE_CC_Protocol_Translation Configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

IR807 Platform: Dual Control Center Profiles

The following scenarios were validated using this profile:

- IP-based IED is configured with 192.168.0.2
- Default gateway for IED is 192.168.0.1, which is the IP address of IR807.
- IED is connected to FastEthernet1, and listening on port 2404.
- SCADA Master1 IP address is 172.16.107.11.
- SCADA Master2 IP address is 172.17.107.11.
- Configuration of the serial interface validated is 9600-8N1.
- Serial interface validated is Async1 (corresponding to line 4).
- SCADA Master reaches the IP IED on IoT Gateway IP on port 2404.
- SCADA Master1 reaches the Serial IED on IoT Gateway IP on port 25000.
- SCADA Master2 reaches the Serial IED on IoT Gateway IP on port 25001.

ICT Enablement for Serial and/or IP-based IED using IR807

Configuration Group Name: IR807_DUAL_CC_IP_and_RawSocket

```
<#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
!
<#--- Beginning of custom modification for tunnel to secondary control center -->
<#if far.IPSecTunnelDestAddr2?has_content>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
interface Tunnel1
description IPSec tunnel to Secondary Tunnel Destination
ip unnumbered loopback0
ipv6 unnumbered loopback0
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
tunnel source ${wanInterface[0].name}
exit
!
crypto ikev2 client flexvpn FlexVPN_Client_Tunnel1
peer 1 ${far.IPSecTunnelDestAddr2}
client connect Tunnel1
exit
</#if>
!
<#--- End of custom modification for tunnel to secondary control center -->
!
<#--- Beginning of IR807_DUAL_CC_IP Configuration -->
!
interface FastEthernet1
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404  ip nat inside source
static tcp 192.168.0.2 26000 interface Loopback0 26000
!
<#--- End of IR807_DUAL_CC_IP Configuration -->
!
<#--- Beginning of IR807_DUAL_CC_RawSocket Configuration -->
!
interface Async1
no ip address
encapsulation raw-tcp
!
line 4
```

```
raw-socket tcp client 172.16.107.11 25000 25000
raw-socket tcp client 172.17.107.11 25000 25001

databits 8
stopbits 1
speed 9600
parity none
!
<#--- End of IR807_DUAL_CC_RawSocket Configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

Configuration Group Name: IR807_DUAL_CC_IP_and_ProtocolTranslation

```
<#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
!
!
<#--- Beginning of custom modification for tunnel to secondary control center -->
<#if far.IPSecTunnelDestAddr2?has_content>
<#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
interface Tunnel1
description IPSec tunnel to Secondary Tunnel Destination
ip unnumbered loopback0
ipv6 unnumbered loopback0
tunnel destination dynamic
tunnel protection IPSec profile FlexVPN_IPSec_Profile
tunnel source ${wanInterface[0].name}
exit
!
crypto ikev2 client flexvpn FlexVPN_Client_Tunnel1
peer 1 ${far.IPSecTunnelDestAddr2}
client connect Tunnel1 exit
</#if>
<#--- End of custom modification for tunnel to secondary control center -->
!
<#--- Beginning of IR807_DUAL_CC_T101_To_T104_PT Configuration -->
!
interface FastEthernet1
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in duplex auto
speed auto
!
interface Tunnel0
ip nat outside
!
interface Tunnel1
ip nat outside
!
ip nat inside source static tcp 192.168.0.2 2404 interface Loopback0 2404
ip nat inside source static tcp 192.168.0.2 26000 interface Loopback0 26000
!
!
interface Async1
no ip address
encapsulation scada
!
line 4
databits 8
stopbits 1
speed 9600
parity none
!
scada-gw protocol t101

channel t101_ch1
link-addr-size two
bind-to-interface Async1
session t101_session1
attach-to-channel t101_ch1
sector t101_sector1
attach-to-session t101_session1
scada-gw protocol t104
channel t104_ch1
t3-timeout 20
tcp-connection 0 local-port 25000 remote-ip any
tcp-connection 1 local-port 25001 remote-ip any
session t104_session1
attach-to-channel t104_ch1
sector t104_sector1
attach-to-session t104_session1
map-to-sector t101_sector1
scada-gw enable
<#--- End of IR807_DUAL_CC_T101_To_T104_PT Configuration -->
<#else>
${provisioningFailed("FAR is not running IOS")}
</#if>
```

Appendix E: End-to-End Application Use Case Scenarios

DTM Workspace for Volt/VAR

- https://cisco.app.box.com/file/387107724522

DTM Workspace for FLISR

- https://cisco.app.box.com/file/387115037625