Distribution Automation – Secondary Substation
Design Guide

First Published: January 2019
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>1</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Navigator</td>
<td>2</td>
</tr>
<tr>
<td>Audience</td>
<td>2</td>
</tr>
<tr>
<td>Distribution Automation Architecture for Utilities</td>
<td>3</td>
</tr>
<tr>
<td>Distribution Automation Use Cases</td>
<td>5</td>
</tr>
<tr>
<td>Secondary Substation Monitoring and Control</td>
<td>6</td>
</tr>
<tr>
<td>Secondary Substation Role</td>
<td>6</td>
</tr>
<tr>
<td>Secondary Substation Router Functions</td>
<td>7</td>
</tr>
<tr>
<td>Volt/VAR Control</td>
<td>8</td>
</tr>
<tr>
<td>Volt/VAR Control Use Case and Benefits</td>
<td>8</td>
</tr>
<tr>
<td>Volt/VAR Actors</td>
<td>8</td>
</tr>
<tr>
<td>Voltage Regulator and Load Tap Controllers</td>
<td>9</td>
</tr>
<tr>
<td>Volt/VAR Application Flow</td>
<td>9</td>
</tr>
<tr>
<td>Fault, Location, Isolation, Service Restoration</td>
<td>12</td>
</tr>
<tr>
<td>FLISR Use Case and Benefits</td>
<td>12</td>
</tr>
<tr>
<td>How FLISR Works</td>
<td>12</td>
</tr>
<tr>
<td>FLISR Actors</td>
<td>13</td>
</tr>
<tr>
<td>Solution Architecture</td>
<td>16</td>
</tr>
<tr>
<td>Places in the Network</td>
<td>16</td>
</tr>
<tr>
<td>Control Center Block</td>
<td>16</td>
</tr>
<tr>
<td>Secondary Substation Block</td>
<td>17</td>
</tr>
<tr>
<td>Field Area Block</td>
<td>17</td>
</tr>
<tr>
<td>Utility Devices Block</td>
<td>17</td>
</tr>
<tr>
<td>Distribution Automation Solution Architecture</td>
<td>17</td>
</tr>
<tr>
<td>SCADA &lt;----&gt; RTU &lt;----&gt; IEDs</td>
<td>19</td>
</tr>
<tr>
<td>SCADA &lt;----&gt; IEDs</td>
<td>20</td>
</tr>
<tr>
<td>Solution Components</td>
<td>20</td>
</tr>
<tr>
<td>Cisco IoT Field Network Director with Oracle Database</td>
<td>21</td>
</tr>
<tr>
<td>Tunnel Provisioning Server</td>
<td>21</td>
</tr>
<tr>
<td>Headend Routers</td>
<td>21</td>
</tr>
<tr>
<td>Registration Authority</td>
<td>22</td>
</tr>
<tr>
<td>RSA Certificate Authority</td>
<td>22</td>
</tr>
<tr>
<td>Active Directory</td>
<td>22</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>NMS Serviceability</td>
<td>71</td>
</tr>
<tr>
<td>Security, High Availability &amp; Scale</td>
<td>74</td>
</tr>
<tr>
<td>Security</td>
<td>74</td>
</tr>
<tr>
<td>Security Management Overview in the Secondary Substation</td>
<td>74</td>
</tr>
<tr>
<td>Access Control</td>
<td>75</td>
</tr>
<tr>
<td>Authentication, Authorization and Accounting</td>
<td>75</td>
</tr>
<tr>
<td>Certificate-Based Authentication</td>
<td>75</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>76</td>
</tr>
<tr>
<td>Threat Defense and Mitigation</td>
<td>76</td>
</tr>
<tr>
<td>High Availability</td>
<td>78</td>
</tr>
<tr>
<td>HER Level Redundancy</td>
<td>78</td>
</tr>
<tr>
<td>WAN Backhaul Redundancy</td>
<td>79</td>
</tr>
<tr>
<td>Scale</td>
<td>81</td>
</tr>
<tr>
<td>Architecture Summary</td>
<td>82</td>
</tr>
<tr>
<td>Appendix A: Related Documentation</td>
<td>84</td>
</tr>
<tr>
<td>Appendix B: Glossary</td>
<td>85</td>
</tr>
</tbody>
</table>
Preface

This Cisco Distribution Automation - Secondary Substation Design Guide provides a comprehensive explanation of the Cisco Smart Grid FAN solution design for Secondary Substation monitoring use cases, including FLISR and Volt/VAR control.

The document, which includes information about the system’s architecture, possible deployment models, and guidelines for deployment, also recommends best practices and potential issues when deploying the reference architecture.

Executive Summary

Several key business drivers underlie the optimization of the distribution grid enabled by this solution. A pervasive, highly available, and well designed communications network will help enable increased reliability and availability while also reducing OpEx.

Cisco Systems is addressing the networking needs of the utility industry. Specifically, in this Distribution Automation - Secondary Substation Design Guide, the communications solutions that address the utility distribution grid with use cases such as SCADA transport, Fault Location, Isolation, and Service Restoration (FLISR), and line voltage-monitoring enabling applications such as Volt/VAR Control are being highlighted. Field devices like transformers can offer predictive maintenance opportunities that will help eliminate customer outages and expensive unscheduled repairs and truck rolls.

The Cisco Distribution Automation validated solution, which is part of the Cisco portfolio of industry-leading, validated, and secure networking solutions for substation automation, Utility WAN, and Field Area Network Advanced Meter Infrastructure (FAN AMI), provides the following unique capabilities for distributed control and protection operations:

- Cisco Resilient Mesh and cellular networking with FlexVPN technologies that are cost-effectively built to scale for the large number of Distribution Automation devices being enabled in the distribution grid

- An IT-preferred security architecture, including hardware and software certification management, firewall, and malware protection with robust encryption to help ensure secure network communications and edge applications

- Enhanced management and serviceability by Cisco Field Network Director (FND) with Zero Touch Deployment (ZTD) and plug-and-play (PnP) functionality to help enable deployment and enhance operations

- High availability that is designed in the headend and WAN, with redundant control center support

- Edge application capabilities within FND lifecycle-managed Cisco equipment that include deployment, monitoring, upgrading, and troubleshooting

- End-to-end testing and validation, which are completed and documented with various Distribution Automation device vendors and use cases
The recent enhancements to Cisco Resilient Mesh have increased by nearly tenfold the available bandwidth on the 900mhz field area network over the first generation, thus also reducing the latency between hops, helping enable peer-to-peer communication, and equipping the network with enhanced security features. Cisco has transformed a previously low performance wireless mesh network that was designed for smart metering into a network that is suitable for Distribution Automation use cases.

Cellular can be applied to areas or use cases where extremely high performance is needed. Since they are managed under a single highly usable Field Network Director (FND) system, the customer will receive a consistently intuitive management experience.

As a foundational element to any Cisco network, this DA architecture leverages enhanced security from the control center to the edge of the distribution network. The result is a reliable, scalable, and highly available DA network via wired and wireless, and a cellular WAN that supports large-scale DA deployments and secures communications to redundant control centers.

Deployment, ongoing operation, and management is simplified via standards-based protocols and ZTD tools for proven large scale DA network provisioning. This is all addressed in detail as part of this design guide.

This document covers this DA communications solution, which is based on industry-leading innovations in Cisco Resilient Mesh and cellular networking technologies that are built into the Cisco CGR 1240 and CGR 1120 Connected Grid Routers; the Cisco IR510 and IR530 Wi-Sun Mesh Industrial Routers product family; the IR807, IR809, and IR1101 Industrial Router cellular gateways; and the Cisco FND management system.

### Navigator

The following table describes the chapters in this document.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Automation Use Cases, page 5</td>
<td>Overview of the Secondary Substation Monitoring and Control, Volt/VAR Control, and Fault, Location, Isolation, Service Restoration use cases.</td>
</tr>
<tr>
<td>Solution Architecture, page 16</td>
<td>Description of Distribution Automation places in the network, the solution architecture, and solution components.</td>
</tr>
<tr>
<td>Design Considerations, page 27</td>
<td>Design considerations for IP addressing, WAN, backhaul, routing, network encryption, SCADA services, timing services, NAT, QoS Network Management System, and Serviceability.</td>
</tr>
<tr>
<td>Appendix A: Related Documentation, page 84</td>
<td>Acronyms and initialisms used in this document.</td>
</tr>
</tbody>
</table>

### Audience

The audience of this guide comprises, but is not limited to, system architects, network/compute/ systems engineers, field consultants, Cisco Advanced Services specialists, and customers.

Readers should be familiar with networking protocols, Network Address Translation (NAT), and SCADA protocols, and should be exposed to the FAN Solution Architecture.
Cisco Systems has taken a holistic approach to Distribution Automation, and, in this release, the focus will be the Utility Distribution system. The goal of Distribution Automation in the Utility grid is real-time adjustment to changing loads, distributed generation, and failure conditions within the Distribution grid, usually without operator intervention. This requires control of field devices, which implies that information technology (IT) has developed adequately enough that automated decision making exists in the field and critical information can be relayed to the Utility control center. The IT infrastructure includes real-time data acquisition and communication with utility databases and other automated systems. Accurate modeling of distribution operations supports optimal decision making at the control center and in the field. This heavily depends on a highly reliable and high performing communications infrastructure. This document address these communications requirements as an architecture and addresses the key use cases below.

Distribution Automation technologies are commercially available for wide scale utility deployments. The key for the utility is to identify and unlock the value that these solutions provide. Applications that may have the greatest potential are those that directly effect operations and efficiency such as management of peak load via demand response, predictive technologies for advanced maintenance or equipment replacement and secure communications for equipment, and system restoration technologies.

Automated control of devices in distribution systems is the closed-loop control of switching devices, voltage controllers, and capacitors based on recommendations of the distribution optimization algorithms. These closed loop systems often have rigorous communications systems requirements that vary from manufacturer to manufacturer and by application. The communications system must meet the most rigorous standards and do so at scale. Volt/VAR control is one of the key applications to optimize the distribution grid for the utility.

A utilities fault may occur when a short circuit between two phase lines occurs or for other reasons. The fault in any one of the lines can affect a large number of customers. Before the fault on the line can be corrected, it has to be identified and isolated from the large utility network. This identification and isolation is done by placing reclosers in the network. The reclosers are, in turn, connected to the recloser controller. The recloser controller is a connected gateway, which establishes a connection to the control center.

When a fault is identified, the reclosers perform the trip operation and the fault is isolated from the larger network. This trip operation can be automated or can be sent from the control center. Once the fault is corrected, the close operation on the circuit, which is done from the control center, can be executed. This is commonly referred to as Fault, Location, Isolation, and Service Restoration (FLISR), and is also one of the key use cases for a utility in a grid optimization effort.

This Distribution Automation architecture address the utility requirements for Volt/VAR and FLISR via a robust communications infrastructure that addresses the two predominant distribution automation schemes:

- In Europe, portions of South America, and Asia, the distribution scheme is based on a more centralized transformer design and is commonly referred to as the Secondary Substation.
- In North America, portions of South America, and along the Pacific Rim, the distribution scheme is based on a decentralized transformer model and this scheme will be referred to throughout this document as a Feeder Network.

The following architecture leverages the latest technologies and recent enhancements to best address use cases and these topologies with a variety of cell-based gateways for the Secondary Substastion as well as a combination of 900 Mhz mesh and cell gateways at the edge. The architecture addresses the requirements for these edge services and communications, including the edge as Neighborhood Area Network (NAN), the backhaul as Wide Area Network (WAN), and the Operations and Control Centers commonly referred to as the Headend.
The Headend provides aggregation and security for and between the distribution automation applications typically at the Utility control center. This architecture leverages a secure WAN aggregation for scalability since feeder sections may scale to hundreds or more devices with the DA network scaling to thousands of feeder segments and Secondary Substation networks with over 100,000 nodes.

As part of this architecture, the WAN segment is referred to in two modes: On-Net and Off-Net:

- **On-Net** is a high speed communications network owned and operated by the utility; examples include SDH/SONET, Carrier Ethernet, or MPLS as the most common.

- On the other hand, the **Off-Net** network is a service provider-leveraged network that can be based on the same technologies but as a shared service that often includes pre-negotiated service level agreements.

The WAN segment for DA networks is often a cellular backhaul connection because building out a private network in numerous and remote locations, especially in the Secondary Substation model, is frequently cost prohibitive. The NAN Mesh offers opportunities to leverage the On-Net network as backhaul when the radio network gateway can be co-located at a utility-owned facility such as a substation or depot.

The edge or NAN is built on a small form factor gateway or NAN router connected to the edge device such as a Capacitor Bank Controller (CBC) or voltage line monitor based on application or service. The connection to the edge device is often serial, but is rapidly moving to Ethernet. The NAN router can be configured to deliver edge services such as adaptation for serial connections via raw socket encapsulation or translation from serial protocols like IEC-101 to the packet-based IEC-104 protocol. The NAN router also provides security services such as 802.1x port-based authentication, encryption, and routing with possible alternate backhaul options, thus providing a secure connection for the edge device to the control center. The backhaul in the case of Secondary Substations is most often cellular with some satellite or DSL options.
Cisco Resilient Mesh is the latest version of the 900 Mhz Connected Grid Mesh radio with significant performance improvements now applicable for many Distribution Automation applications and use cases. However, it is recognized that Resilient Mesh may not be applicable for all use cases. The Distribution Feeder network will likely be a combination of mesh where the 900 Mhz radio network is feasible and hop count and latency meet application requirements with cellular to augment based on hop count, application performance, or latency requirements.

Distribution Automation Use Cases

Distribution Automation refers to the monitoring and control of devices located on the distribution feeders, such as line reclosers, load break switches, sectionalizers, capacitor banks and line regulators, and devices located in the distribution substation. DA is an overlay network deployed in parallel to the distribution feeder. It enables two-way communication between controllers used in the distribution feeder and the intelligence application that resides in the Utility control center or Secondary Substation for improving grid reliability, availability, and control. Figure 2 depicts a radial distribution feeder.

Figure 2  Radial Distribution Feeder

In Figure 2, the distribution feeder can be observed coming out of the Secondary Substation; various distribution automation controllers (IEDs) in the feeder, such as the recloser controller, voltage regular controller, and capacitor bank controller, are positioned along the distribution feeder. Key functions and operations of Distribution Automation include protecting the distribution system, managing the fault, measuring the energy usage, managing the assets, and controlling and managing system performance. European feeders are largely three-phase and most European countries have a standard secondary voltage of 220, 230, or 240 V.

This design guide discussed the following EMEA region Distribution Automation use cases:

- Secondary Substation Monitoring and Control, page 6
- Volt/VAR Control, page 8
- Fault, Location, Isolation, Service Restoration, page 12

The radial feeder distribution system design is considered for Volt/VAR regulation use cases and the parallel feeder distribution system is considered for FLISR use cases. Cisco DA Gateways are very well suited for other feeder deployments such as mesh and loop distributed feeder designs.
Secondary Substation Monitoring and Control

Secondary Substation Role

Secondary Substations, which are part of the Distribution Automation system, are used to step down the power voltage from medium to low voltage for end consumer needs. It has a bus topology that can split the distribution power off in multiple directions. Secondary Substations host transformers as well as a number of devices called intelligent electronic devices (IEDs), such as circuit breakers, voltage sensors, reclosers, surge protectors, and gateways (Secondary Substation Routers or SSRs).

The fundamental function of the SSR is to provide reliable, two-way, real-time communication between the IED and Remote Terminal Unit (RTU) devices that reside in the Secondary Substation and backend SCADA systems running in the centralized control center of the Distribution System Operator (DSO). See Figure 3.

Figure 3  Role of Secondary Substation

Various operational functions, which will be performed on Secondary Substation IEDs/RTUs by central SCADA applications, are listed below:

1. **Monitoring**—A SCADA application is used to monitor the values of the MV and LV transformers’ voltage and current levels using periodic poll operation. This monitoring data will be important for control, protection, and preventive maintenance functions. IEDs will be configured to send unsolicited reporting to SCADA systems if they exceed certain threshold values or failure conditions.

2. **Control**—Includes remote control operations such as operation of circuit breakers and switches.

3. **Protection**—Performs various protection functions for isolating the Secondary Substation from the transmission grid when there is a failure.
Figure 4 depicts various Secondary Substation components such as RTUs, IEDs, SSR, and meter data concentrator.

Figure 4  Secondary Substation Components

Secondary Substation Router Functions

The Secondary Substation Router aggregates traffic from various IEDs and RTUs and routes traffic to both primary and secondary regional Control Centers hosted by the DSO via public connectivity options such as cellular (LTE) or leased line (Ethernet/Fiber) on an IPV4 or IPV6 backhaul. The SSR encrypts the application traffic using the IPSec tunnel for maintaining confidentiality of application data over the public network. The headend router (HER) in the DSO control center aggregates various secured tunnels from multiple SSRs and decrypts the encrypted traffic; the traffic is routed after decryption to various SCADA application.

The uplink WAN connectivity, routing, backhaul redundancy, QoS, encryption, and NAT features that will be performed on the SSR are discussed in detail in Design Considerations, page 27.

The RTU, having legacy RS232/RS485 interfaces, can be directly connected to the SSR serial interfaces. Raw sockets or protocol translation techniques will be used to transport legacy application traffic such as T101 to the control center. Raw sockets and protocol translation techniques are discussed in detail in Design Considerations, page 27.

IPV4 IEDs can be directly connected to the Ethernet port of the SSR, which can act as a Dynamic Host Configuration Protocol (DHCP) relay agent to provide IP addresses to the IEDs (IEDs need support from DHCP client functionality) and dot1x relay agent functionality (IEDs need to support the dot1x supplicant feature) for performing device-level authentication. If a modern IED supports IPV6 addressing, the SSR can route the IPV6 traffic to IPV6 SCADA applications residing in the control center.

The SSR can aggregate and route meter concentrator data to a metering application residing in the DSO control center. It can also be used to transport IP camera traffic and asset monitoring traffic to DSO control center applications.

For advanced use cases like Distributed Energy Resources (DER), a fiber will be extended from the Secondary Substation to connect various IEDs residing in the consumer premises. This interface is called the extended LAN interface. A future version of this guide will address this use case.

Design Considerations, page 27 will discuss in detail how the SSR can be deployed in secured Zero Touch fashion over a public internet connection and how different configuration profiles as per vertical use cases can be pushed to SSR.
Volt/VAR Control

Volt/VAR Control Use Case and Benefits

This use case addresses automating dynamic and efficient delivery of power. Utilities look at achieving large savings by enhancing the efficiency of their power distribution infrastructure—in other words, improving the effectiveness of the flow of electricity. In order to evaluate the process, it is important to review the differences between what is called real power and reactive power.

- **Real power** is used to run all lights, devices, and production lines. It is the power that "does the work."
- **Reactive power** does not contribute anything to doing work, but it does cause conductors to heat up and it takes up a certain amount of "space" in the wires.

The more reactive power flowing on a line, the less "room" there is for real power, and the less efficient is the distribution system.

Today, in order to eliminate or at least minimize reactive power flows, utilities have deployed on their local distribution systems devices, such as capacitor banks or special transformers that are typically located at substations or on the feeder. These devices work to keep reactive power flows down, making the full capacity of the conductor available for the real power. This process is known as Volt/VAR regulation or control:

- **Power Factor Regulation/VAR Compensation**—Improves efficiency of energy supply by ensuring voltage and current are in phase when supplied to the customer.
- **Conservation Voltage Regulation**—At times of peak load, ensure the minimum required voltage level is supplied to the customer.
- **Volt/VAR Control**—Power factor regulation + Conservation voltage regulation.

Volt/VAR Actors

Figure 5 depicts various actors used in the Volt/VAR use case. The actors used in the Volt/VAR use case are Load Tap Changers, Voltage Regulators, and Capacitor Bank Controllers (CBC).
Voltage Regulator and Load Tap Controllers

Voltage regulation functions are performed using the Voltage Regulator/Load Tap Controller actors. Voltage can be raised or lowered based on load conditions. Voltage Regulators are types of transformers that make small adjustments to voltage levels in response to changes in load. They are installed in substations (where they are called load tap changers) and along distribution feeders to regulate downstream voltage. Voltage Regulators have multiple "raise" and "lower" positions and can automatically adjust according to feeder configurations, loads, and device settings.

Capacitor Bank Controllers

CBCs are used to supply reactive power. Capacitor Bank utilities use capacitors to compensate for reactive power requirements caused by inductive loads from customer equipment, transformers, or overhead lines. Compensating for reactive power reduces the total amount of power that needs to be provided by power plants, resulting in a flatter voltage profile along the feeder and less energy wasted from electrical losses in the feeder. A distribution capacitor bank consists of a group of capacitors connected together. Capacitor banks are mounted on substation structures, distribution poles, or are "pad-mounted" in enclosures.

Volt/VAR Application Flow

In Figure 6, Volt/VAR and SCADA applications are hosted in the DSO control center and RTU and load tap controllers are located in the Secondary Substation. The RTU acts as a outstation device that proxies the poll and/or control command to various field devices like the CBC and end-of-line voltage monitor. This guide covers the use case scenario where the Volt/VAR application flow between IED and SCADA happens via RTU and the distribution feeder type considered is radial. A direct application flow from field devices to the control center for the Volt/VAR use case will be covered in future guides.

Figure 6 Volt/VAR Use Case Block Diagram

![Volt/VAR Use Case Block Diagram](image-url)
The detailed application flow between different actors for power factor regulation is depicted in Figure 7.

Figure 7  Power Factor Regulation

1. Event class data poll to the following devices from RTU:
   - Substation meter, poll measured Value (Short Floating Point) registers (0 to 4)
   - All CBC(s), poll measured Value (Short Floating Point) (0) and double point command(0)
   - End-of-line voltage monitor, poll measured Value (Short Floating Point) register (0)

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 RTU via SCADA to CBCs to close the Capacitor Bank Controller N by writing in a Control Relay Output Block (CROB) command register in T104.

4. Event class data poll to the following devices from the RTU:
   - Substation meter, poll measured Value (Short Floating Point) registers (0 to 4)
   - All CBC(s), poll measured Value (Short Floating Point) (0) and double point command(0)
   - End-of-line voltage monitor, poll measured Value (Short Floating Point) register(0)

5. All of the above steps are repeated on all the CBCs on the feeder line to maintain a Power Factor value close to 1.
Figure 8 depicts the detail call flow involved in conservation voltage regulation:

1. Event class data poll to the below devices from RTU:
   - Substation meter, poll measured Value (Short Floating Point) registers (0 to 4)
   - All CBC(s), poll measured Value (Short Floating Point) (0) and double point command (0)
   - End-of-Line voltage monitor, poll measured Value (Short Floating Point) register (0)

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 RTU via SCADA to the load tap controller to lower/raise LTC by writing in a Control Relay Output Block (CROB) command register in T104.

4. Event class data polls to the following devices from RTU:
   - Substation meter, poll measured Value (Short Floating Point) registers (0 to 4)
   - All CBC(s), poll measured Value (Short Floating Point) (0) and double point command(0)
   - End-of-Line voltage monitor, poll measured Value (Short Floating Point) register (0)

5. The above steps are repeated to maintain a Power Factor value close to 1 along the feeder line.
Fault, Location, Isolation, Service Restoration

FLISR Use Case and Benefits

Fault, Location, Isolation, Service Restoration (FLISR) is the process for dealing with fault conditions on the electrical grid. The following occurs as part of this process:

1. Detects (and locates) faults
2. Isolates the faults to the smallest segment of the grid possible
3. Restores as much service as possible while the fault is isolated

FLISR includes automatic sectionalizing and restoration and automatic circuit reconfiguration. These applications accomplish DA operations by coordinating operation of field devices, software, and dedicated communication networks in order to automatically determine the location of a fault and rapidly reconfigure the flow of electricity so that some or all of the customers can avoid experiencing outages. Because FLISR operations rely on rerouting power, they typically require feeder configurations that contain multiple paths to single or multiple other substations. This creates redundancies in the power supply for customers located downstream or upstream of a downed power line, fault, or other grid disturbance.

The benefits of FLISR include:

- Consumers experience minimal outage.
- Utilities improve the System Average Interruption Duration Index (SAIDI) and the System Average Interruption Frequency Index (SAIFI) numbers and avoid financial penalties being levied by the regulator.

FLISR application control can be implemented in the following modes:

- **Supervised Mode**—In supervised mode of operation, no automatic control, system delivers information to operator. Operator initiates manual control actions. Restoration time will be longer in this approach. Please refer to the *Secondary Substation 1.0 Implementation Guide*, which addresses this use case, at the following URL:
  
  https://salesconnect.cisco.com/#/search/Secondary%2520Substation%2520Implementation%2520Guide/content

- **Semi Automatic Mode**—A mix of automatic and supervised control is followed. The DA system automatically isolates the fault and performs the restoration part of upstream restoration. The upstream section is between the substation and the faulted section. Manual restoration operation is performed on the downstream section, which is between the fault section and the end of feeder. This guide will address this mode of operation. In this mode, communication happens between IEDs in field to the Distribution Management System (DMS) application residing in control center.

- **Fully Automatic Mode**—Isolation and restoration happens automatically without any dispatcher intervention. Communication happens directly between a group of associated IEDs. Restoration is very fast (<1 second), but this mode is a complex approach to deploy.

How FLISR Works

Figure 9 is divided into four parts (A, B, C, and D) to show how FLISR operations typically work.

- In **Part A** of Figure 9, the FLISR system locates the fault, typically using line sensors that monitor the flow of electricity, measures the magnitudes of fault currents, and communicates conditions to other devices and grid operators.

- Once located, FLISR opens switches on both sides of the fault: one immediately upstream and closer to the source of power supply (Example B of Figure 9), and one downstream and further away (Example C of Figure 9).
The fault is now successfully isolated from the rest of the feeder. With the faulted portion of the feeder isolated, FLISR next closes the normally open tie switches to neighboring feeders. This re-energizes the un-faulted portion(s) of the feeder and restores services to all customers served by these un-faulted feeder sections from another substation/feeder (Example D of Figure 9).

**Figure 9   How FLISR Works**

**FLISR Actors**

- **Recloser**—The circuit recloser is a self-contained device with a necessary monitoring circuit to detect and interrupt over-current conditions and automatically reclose the line.

- **Sectionalizing Switch or Remote Control Switch**—Remote Controller Switches can be load break or fault interrupting devices.

- **Remote Fault Indicator**—Used to detect faults.

- **Distribution Management System (DMS)**—The DMS application residing in the DSO control center is an intelligent application, which is the brain of FLISR systems and which performs application circuit reconfiguration logic.
**Figure 10** depicts a parallel feeder distribution system. Two distribution feeders are common out of two different Secondary Substations and each feeder has a recloser associated with it. Remote fault Indicators and remote control switch are distributed across both feeders. RCS3 is, by default, an open switch.
In Figure 11, the application flow can be observed happening directly from feeder devices to the DMS application in the DSO control center. The flow is summarized below:

- Remote Fault Indicator (RFI) 1 reports to the Distribution Management System (DMS) whenever it encounters a fault.
- Recloser2 opens and send a report to DMS when it encounters a temporary fault.
- Recloser2 opens and send a report to DMS when it encounters a permanent fault.
- Remote Control Switch (RCS) 2 reports no voltage status to DMS.
- RCS 2 opens when it encounters faults for second time and send a report to DMS.
- DMS issues a close command to the RCS 3.
- DMS initiates a periodic poll (every minute) for the all feeder devices.
- DMS initiates a solicit periodic poll (every 5 minutes once) for all feeder devices.
Solution Architecture

This chapter covers the DA places in network, the solution architecture for various DA application flows, and details about solution components that make up the DA architecture.

Places in the Network

The DA solution is a subset of the Field Area Network (FAN) solution architecture. It follows similar two-tier places in network. The WAN tier connects the control center block with the Secondary Substation block or field area block. In turn, the field area or Secondary Substation blocks connect to utilities device blocks via different last mile connectivity methods such as Ethernet, Serial, or Wi-Fi.

Figure 12 Distribution Automation Places in the Network

Control Center Block

The control center block acts as a data center for DSOs, which are used to organize these blocks dedicated for each region (called Regional Network Operating Centers or NOCs). Regional NOCs host various SCADA applications that are needed to perform centralized management for various vertical use cases that are discussed in Distribution Automation Use Cases, page 5. The control center blocks house the HER in clustering mode. As per the Cisco DA solution architecture, the ASR 1000 series of routers will deployed as the HER. The role of the HER is to terminate and aggregate IPSec tunnels from various DA Gateways and SSRs. Additional responsibilities include enforcement of QoS and security policies.

The control center block hosts the IoT Field Network Director (FND), which is a network management system for managing the various gateways. Certificate authorities, which support RSA and elliptic-curve cryptography (ECC) encryption and the AAA server, provide authentication, authorization, and accounting. For details on the design of the control center, please refer to Cisco FAN-Headend Deep Dive Implementation and FAN Use Cases at the following URL

Solution Architecture

The control center security design, with respect to IPS/IDS functionality and application load balancing, will be addressed in detail in upcoming releases. For the current version of the security design, refer to the *Cisco Connected Utilities - Field Area Network 2.0 Design and Implementation Guide* at the following URL:


Secondary Substation Block

A key component of the Secondary Substation block is the Secondary Substation Router (SSR). Cisco IR1101, IR807, and CGR1120 series routers will be deployed as SSRs, which connect and aggregate traffic from various IEDs and RTUs present in Secondary Substations to single or dual Control Centers.

Field Area Block

The Field Area block hosts various distribution automation gateways. Cisco IR1101, IR807, and IR809 will be deployed as DA Gateways. Most of the DA Gateways will be installed 1:1 to DA controllers. DA Gateways will connect primarily to cellular or Ethernet backhaul. DA Gateways are managed from the IoT FND Network Management System (NMS) application residing in the control center block. DA Gateways are deployed in zero touch fashion. Zero Touch Deployment (ZTD) of DA Gateways is discussed in detail in *Network Management System, page 59*. DA Gateways will be provisioned based on application use cases and last mile connectivity to the utility control devices.

Utility Devices Block

The Utility Devices Block hosts various DA controllers such as voltage regulator controllers, recloser controllers, RCSs, and CBCs. These controllers are connected to DA Gateways via Ethernet or serial (RS232, RS485) interfaces.

Distribution Automation Solution Architecture

The Distribution Automation Solution Architecture, which is depicted in *Figure 13*, is a centralized architecture where the control center, which plays a key role, hosts communication, security, utility, and network management applications. The DSO organizes this control center as a regional DSO NOC that aggregates ICT traffic from different SSRs and Distribution Automation gateways in that region.

The firewall segregates the control center in three zones: the external, DMZ, and internal zones.

- The DMZ Zone includes:
  - An HER interface, which will be installed in clusters for redundancy and scaling purposes
  - The Registration Authority (RA), which offloads authentication and authorizing functionalities of the CA and leverages the AAA server for authorization
  - The Tunnel Provisioning Server (TPS), which is the proxy for the NMS FND

- The Internal Zone hosts the Network Time Protocol (NTP), Domain Naming Server (DNS), DHCP, NMS, and Edge Application management using FND, Field Network Director Database (FND-DB), PKI elements like CA, Active Directory, and AAA, and DA applications like SCADA and DMS.
The DA application bidirectional flow can be classified as follows:

1. **SCADA <----- RTU <----- IEDs**, page 19

2. **SCADA <----- IEDs**, page 20

3. **IEDs <----- IEDs**

This section addresses the solution architecture and design for the first two flows. The radial feeder distribution system is considered for the ICT architecture.
SCADA ----> RTU ----> IEDs

The application bidirectional traffic flow from field IEDs to SCADA in the control center is via RTU, which is located in the Secondary Substation. Application traffic is depicted by the yellow arrow in Figure 14. The ICT solution design for this application flow is as follows:

- DA Gateways, which are installed 1:1 with the controllers and last mile connectivity, will have Ethernet or serial connectivity.
- DA Gateways will have public WAN connectivity; in most deployment cases, it would be cellular backhaul.
- Application traffic would be encrypted using FlexVPN. In this architecture, tunnels from the DA Gateways are terminated on the SSR.
- The WAN IP address of the Secondary Substation should be a static (fixed IP) address.
- SSRs route traffic from the IEDs to the RTU, which is co-located.
- RTU processes this application traffic as unsolicited reporting or response to poll/control command.
- RTU sends the DA application traffic to the SCADA application in the control center.
- To transport this application, the SSR will have secure encrypted FlexVPN tunnel to the HER which resides in the control center.

For redundancy purposes, two tunnels will be destined to two different regional Control Centers. These tunnels will be designed and deployed active/active tunnels. Separate control traffic will exist from the NMS, i.e., FND to DA Gateways and SSRs. This is depicted by the green arrow in Figure 14. As per this design, DA Gateways will have one FlexVPN tunnel for NMS application traffic and a separate FlexVPN tunnel for application traffic. Similarly, the SSR will have two FlexVPN tunnels to two different regional Control Centers. Application and control traffic can flow through the same FlexVPN tunnel. If required, a third FlexVPN tunnel from SSR to HER can be provisioned for control traffic.
**Solution Architecture**

**SCADA <----> IEDs**

*Figure 15* depicts a solution architecture where IEDs can directly communicate with the centralized SCADA. In this design, DA Gateways and SSRs directly connect to HER in the regional control center via public WAN connectivity. For redundancy design, DA Gateways can have two active/active tunnels to two different regional Control Centers. DA application traffic and NMS control traffic can flow in the same FlexVPN tunnel.

*Figure 15  SCADA-IED Flow DA Design*

**Solution Components**

*Table 1* lists various solution components and their role.

<table>
<thead>
<tr>
<th>Solution Component</th>
<th>Role</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 1000</td>
<td>HER in Control Center</td>
<td>03.17.04.S/156(1)S4</td>
</tr>
<tr>
<td>CSR1000v</td>
<td>Virtual HER in Control Center</td>
<td>03.16.08.S/15.5(3)S8 (or) later</td>
</tr>
<tr>
<td>IR1101</td>
<td>SSR or Distribution Automation Gateway</td>
<td>16.10(1)</td>
</tr>
<tr>
<td>CGR 1120</td>
<td>SSR</td>
<td>15.8.3M0a</td>
</tr>
<tr>
<td>IR807</td>
<td>SSR or Distribution Automation Gateway</td>
<td>15.8.3M0a</td>
</tr>
<tr>
<td>IR809</td>
<td>SSR or Distribution Automation Gateway</td>
<td>15.8.3M0a</td>
</tr>
<tr>
<td>IoT Field Network Director with Database</td>
<td>Network Management System</td>
<td>4.4.0</td>
</tr>
<tr>
<td>ISR 4400</td>
<td>Registration Authority</td>
<td>15.8(3)M0a</td>
</tr>
</tbody>
</table>
Solution Architecture

Table 1  Cisco Components (continued)

<table>
<thead>
<tr>
<th>Solution Component</th>
<th>Role</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESR5921</td>
<td>Registration Authority (Virtual)</td>
<td>15.8(3)M0a</td>
</tr>
<tr>
<td>Tunnel Proxy Server</td>
<td>Proxy for IOTFND</td>
<td>4.4.0</td>
</tr>
<tr>
<td>ASA 4150</td>
<td>Firewall</td>
<td>FXOS 2.4(1)</td>
</tr>
</tbody>
</table>

Table 2 lists third party components of the solution

Table 2  Third Party Components

<table>
<thead>
<tr>
<th>Solution Component</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eximprod ES200</td>
<td>Virtual RTU in Secondary Substation</td>
</tr>
<tr>
<td>Eaton and Beckwith Capacitor bank controller</td>
<td>Field IED for Volt/VAR use cases</td>
</tr>
<tr>
<td>Beckwith Load tap controller</td>
<td>Secondary Substation IED for Volt/VAR use cases</td>
</tr>
<tr>
<td>Beckwith Recloser Controller</td>
<td>Field IED for FLISR use cases</td>
</tr>
<tr>
<td>SCADA simulation Triangular MicroWorks DTM</td>
<td>DSO SCADA</td>
</tr>
<tr>
<td>Microsoft Certificate Authority</td>
<td>RSA CA for PKI</td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td>Active Directory services</td>
</tr>
<tr>
<td>Microsoft Network Policy Server</td>
<td>AAA services</td>
</tr>
</tbody>
</table>

Cisco IoT Field Network Director with Oracle Database

The Cisco IoT Field Network Director (formerly called Connected Grid Network Management System or CG-NMS) is a software platform that manages the infrastructure for smart grid applications. It provides enhanced Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities for highly scalable and distributed systems such as smart metering and Distribution Automation. Additional capabilities of Cisco IoT FND include:

- Network topology visualization and integration with the existing Geological Information System (GIS)
- Simple, consistent, and scalable network layer security policy management and auditing
- Extensive network communication troubleshooting tools
- Northbound APIs are provided for utility applications such as Distribution Management System (DMS), Outage Management System (OMS), and Meter Data Management (MDM)
- Zero Touch Deployment (ZTD) for Field Area Routers

Tunnel Provisioning Server

The TPS acts as a proxy to allow DA Gateways/SSRs to communicate with Cisco IoT FND when they are first deployed in the field. After TPS provisions the tunnels between DA Gateways/SSRs and the HER, the DA Gateways/SSRs can then communicate with Cisco IoT FND directly.

Headend Routers

The primary function of a HER is to aggregate the WAN connections coming from field area routers. HERs terminate the VPN tunnels from the Cisco Connected Grid Routers (CGRs) and may also enforce QoS, profiling (Flexible NetFlow), and security policies. HERs will be deployed in clusters. HER clustering and scale design are discussed in detail in Security, High Availability & Scale, page 74.

The ASR 1000 series of routers will be used as HERs.
Registration Authority

The Registration Authority (RA) acts as a proxy to the CA server in the backend for automated certificate enrollment for the SSR and DA Gateways, which must go through the RA and TPS to establish a secure tunnel with the HER. Before this tunnel is established, the device cannot reach the data center network.

A Cisco IOS router can be configured as a Certificate Server-Simple Certificate Enrollment Protocol (SCEP) in RA mode. The Cisco ISR 4400 series of routers are recommended for high scale deployments although ESR5921 (Virtual Router) or any Cisco ISR 4000 series of routers could be chosen to serve the functionality of RA in low scale deployments.

RSA Certificate Authority

The RSA Certificate Authority (CA) provides certificates to network components such as routers and Cisco IoT FND. This solution makes use of the RSA CA within the control center block. Alternatively, an external utility-owned RSA-based CA can be used.

Active Directory

The Active Directory, which is a part of the utility data center and provides directory services, stores identity information for the SSRs and DA Gateways. It provides authentication of the various gateways in the DA solution.

AAA

The Microsoft Network Policy Server (NPS) provides RADIUS-based AAA services for network admission control of SSRs such as CGR 1120 and IR1101 and DA Gateways such as IR807 and IR809. It supports the certificate-base identity authentication used in this solution.

Network Time Protocol Server

Certain services running on the Distribution Automation require accurate time synchronization between the network elements. Many of these applications process a time-ordered sequence of events, so the events must be time stamped to a level of precision that allows individual events to be distinguished from one another and correctly ordered. A Network Time Protocol (NTP) Version 4 server running over the IPv4 and IPv6 network layer can act as a Stratum 1 timing source for the network.

The NTP might deliver accuracies of 10 to 100 milliseconds over the DA solution, depending on the characteristics of the synchronization source and network paths in the WAN.

SSR and DA Gateways

IR1101 Industrial Integrated Services Router

The IR1101 is modular and ruggedized (IP30 specification) platform designed for the utility and machine-to-machine market segment. As part of the Secondary Substation solution, IR1101 can play the role of both SSR and DA Gateway.

<table>
<thead>
<tr>
<th>SKU ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1101-K9</td>
<td>IR1101 Base Unit</td>
</tr>
</tbody>
</table>
Distribution Automation - Secondary Substation Design Guide

Solution Architecture

Table 4  Cellular Pluggable Module SKUs for Cisco IR1101

<table>
<thead>
<tr>
<th>SKU ID</th>
<th>Description</th>
<th>Modem Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-LTE-VZ</td>
<td>U.S. (Verizon) Single Micro SIM</td>
<td>WP7601-G</td>
</tr>
<tr>
<td>P-LTE-NA</td>
<td>North America (AT&amp;T) Dual Micro SIM</td>
<td>WP7603-G</td>
</tr>
<tr>
<td>P-LTE-GB</td>
<td>Europe Dual Micro SIM</td>
<td>WP7607-G</td>
</tr>
</tbody>
</table>

For more details refer to the *IR1101 Industrial Integrated Services Router Hardware Installation Guide* at the following URL:


As shown in Figure 16, IR1101 is designed as a modular platform for supporting expansion modules and edge compute modules. IR1101 supports a variety of communication interfaces such as four FE ports, one combo WAN port RS232 DTE port, and LTE modules. The cellular modem is pluggable and a dual SIM card and IPV6 LTE data connection are supported. Raw sockets and protocol translation feature are available.

**Figure 16  Cisco IR1101**

Connected Grid Router 1120

The CGR 1120 is designed as an indoor model well suited for Secondary Substation deployment. CGR 1120 has a rich feature set for utilities and energy verticals. CGR 1120, which acts a SSR in the DA solution, integrates applications like Distributed Energy Resources (DERs) and Secondary Substation monitoring and control. For more details, please refer to the Cisco 1120 Connected Grid Router specification guide at following URL:

Distribution Automation - Secondary Substation Design Guide

Solution Architecture

**IR807 Industrial Integrated Services Router**

The IR807 (see Figure 17) is a compact, ruggedized, lower power, and smart-grid compliant router suited for DA and Secondary Substation deployment. IR807 supports a variety of communication interfaces like Ethernet, serial, and in-built cellular modems to support LTE and 3G networks. Dual SIM support is available for high reliability.

**Figure 17  Cisco IR807**

![IR 807](image)

**Table 5  IR807 SKU Information**

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR807G-LTE-GA-K9</td>
<td>Compact Cisco IR807 Ruggedized Secure Multi-Mode 4G LTE Industrial ISR for Europe: Multimode 4G, 3G, and 2G connectivity to cellular networks operating in LTE 800 MHz (band 20), 900 MHz (band 8), 1800 MHz (band 3), 2100 MHz (band 1), and 2600 MHz (band 7) frequencies Backward-compatible with UMTS and HSPA+ 900 MHz (band 8) and 2100 MHz (band 1) and EDGE/GSM/GPRS 900 MHz and 1800 MHz</td>
</tr>
<tr>
<td>IR807G-LTE-NA-K9</td>
<td>Compact Cisco IR807 Ruggedized Secure Multi-Mode 4G LTE Industrial ISR for North America: Multimode 4G and 3G, connectivity to cellular networks operating in LTE 1900 MHz (band 2 PCS), 1700/2100 MHz (band 4 AWS), 850 MHz (band 5), 700 MHz (band 12), 700 MHz (band 17), 1900 MHz (band 25 extended PCS) and 850 MHz (band 26 extended CLR) frequencies Backward-compatible with UMTS and HSPA+ 850 MHz (band 5), 1900 MHz (band 2 PCS), and 1700/2100 MHz (band 4 AWS), and CDMA BC0, BC1 and BC10</td>
</tr>
<tr>
<td>IR807G-LTE-VZ-K9</td>
<td>Compact Cisco IR807 Ruggedized Secure 4G LTE Industrial ISR for Verizon in North America: LTE connectivity to cellular networks operating in LTE 700 MHz (band 13) and 1700/2100 MHz (band 4 AWS)</td>
</tr>
</tbody>
</table>

For more details on IR807, please refer to the *Cisco 807 Industrial Integrated Services Routers Data Sheet* at the following URL:

IR809 Industrial Integrated Services Router

The Cisco IR809 (see Figure 18) is a compact, ruggedized router designed for harsh environments. It will well suited for the Distribution Automation and asset management solution. It plays the role of a DA Gateway and has the edge compute capability, which can be used to host the applications to cater to mission-critical or time-sensitive requirements for fast decision making at the edge of IoT network. For more details on IR809, please refer to the Cisco 809 Industrial Integrated Services Routers Data Sheet at the following URL:


Figure 18  Cisco IR809

Table 6  Cisco IR809 SKU Information

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR809G-LTE-LA-K9</td>
<td>Compact Cisco IR809 Ruggedized Secure Multi-Mode 4G LTE Industrial Integrated Services Router for Australia, Asia (including Japan) and Latin America; LTE FDD bands 1, 3, 5, 7, 8, 18, 19, 21, 28 and TDD LTE band 38, 39, 40, 41 bands with carrier aggregation, UMTS/HSPA+ bands and TD-SCDMA band 39 with ETSI compliance</td>
</tr>
<tr>
<td>IR809G-LTE-GA-K9</td>
<td>Compact Cisco IR809 Ruggedized Secure Multi-Mode 4G LTE Industrial Integrated Services Router for Europe; LTE 800/900/1800/2100/2600 MHz, 850/900/1900/2100 MHz UMTS/HSPA+ bands with ETSI compliance</td>
</tr>
<tr>
<td>IR809G-LTE-NA-K9</td>
<td>Compact Cisco IR809 Ruggedized Secure Multi-Mode 4G LTE Industrial Integrated Services Router for North America; LTE 700 MHz (band 17), 1900 MHz (band 2 PCS), or 1700/2100 MHz (band 4 AWS) networks; backward-compatible with UMTS and HSPA+: 850 MHz (band 5), 900 MHz (band 8), 1900 MHz (band 2 PCS), and 1700/2100 MHz (band 4 AWS) with FCC compliance</td>
</tr>
<tr>
<td>IR809G-LTE-VZ-K9</td>
<td>Compact Cisco IR809 Ruggedized Secure Multi-Mode 4G LTE Industrial Integrated Services Router for Verizon in North America; LTE 700 MHz (band 13), 1700/2100 MHz (band 4 AWS), or 1900 MHz (band 25 extended PCS) networks; backward-compatible with EVDO Rev A/CDMA 1x BC0, BC1, BC10 with FCC compliance</td>
</tr>
</tbody>
</table>
Solution Architecture

Firewall

A high performance, application-aware firewall with IPS/IDS capability should be installed between the WAN and the head-end infrastructure at the DSO control center. The firewall performs inspection of IPv4 and IPv6 traffic from/to the FAN. Its throughput capacity must match the volume of traffic flowing between the application servers and the FANs.

The Cisco Adaptive Security Appliances (ASA) 4150 is recommended. The Cisco ASA 4150 is a high-performance data center security solution. For smaller deployments, low and mid-range firewalls such as the ASA 4110 and the ASA 4120 may be used.

The ASA FirePOWER module may be added for next generation firewall services such as Intrusion Prevention System (IPS), Application Visibility Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

Firewalls can be configured for multiple (virtual) security contexts. For instance, IoT FND servers can be on a different context from infrastructure servers for segmentation. Firewalls are best deployed in pairs to permit failover in case of malfunction.

IEDs

This section describes the following IEDs that were considered during the validation of the Distribution Automation solution:

- Capacitor Bank Controller, page 26
- Recloser Controller, page 26
- Load Tap Controller, page 26
- SCADA and Other IED Simulation, page 27

Capacitor Bank Controller

- Eaton CBC-8000—This Capacitor Bank Controller (CBC) is designed to control capacitor banks installed in distribution feeders. This IED plays a key role in power factor regulation. For details, please refer to the following URL:

- Beckwith M-6280A Digital Capacitor Bank Control—Digital CBC for Remote Capacitor Automation, Monitoring, and Protection. It supports the Classic Automatic mode of operation that is Voltage, optional VAR Control or optional Current Control. For details, please refer to the following URL:
  - http://www.beckwithelectric.com/products/m-6280a/

Recloser Controller

- Beckwith M-7679 R-PAC—Protection, Automation and Control (PAC) System for Recloser, Switch, Sectionalizer, and Advanced Distribution Automation Applications. This is a key component for FLISR use case. For details, please refer to the following URL:
  - http://www.beckwithelectric.com/products/m-7679/

Load Tap Controller

- Beckwith M-2001D Tap Changer Control—Digital Tap Changer Control for Transformers and Regulators. This is a key component for conservation voltage regulation use case. For details, please refer to the following URL:
SCADA and Other IED Simulation

- The Triangular Microwave Dynamic Synchronous Transfer Mode (DTM) tool used for DMS (SCADA) and other IEDs like remote control switch, Line Fault Indicator. Used for automated testing of RTUs, IEDs, gateways, and SCADA systems. For details, please refer to an overview of DTM at the following URL:

RTU

- Eximprod ES 200 is Virtual RTU. This RTU application can be hosted as a docker application on Cisco edge compute platforms like IR809 and IR1101. For more details on ES200, refer to the following URL:
- For Virtual RTU implementation, please refer to the [Connected Utilities Virtual RTU Implementation Guide](https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/FAN/Virtual-RTU/IG/CU-VRTU-IG/CU-VRTU-IG.html) at the following URL:

Design Considerations

This chapter includes the following major topics:

- **IP Address Schema, page 27**
- **Network Services, page 40**
- **SCADA Services, page 44**
- **Network Address Translation, page 52**
- **Quality of Service, page 55**
- **Timing Synchronization, page 58**
- **DHCP Services, page 58**
- **Network Management System, page 59**

IP Address Schema

The IP Address Schema is discussed in a combination of the following multiple options:

- Addressing at various layers of the solution
- Types of network involved (Underlay Network vs Overlay Network):
  - Underlay network—Service provider-assigned addresses used in establishment of tunnel
  - Overlay network—Reachable only after a secure overlay network path is established
- Choice of network layer protocol (IPv4 vs IPv6 vs Dual Stack)
- Mode of address assignment (Static vs Dynamic)

**Note:** SSRs and DA Gateways shall be referred to as IoT Gateways in the abstract context in this document.
**Design Considerations**

**Figure 19** serves as the reference base for the discussion of IP address schema used in this solution.

Various layers include:

1. Utility Private Network
2. Utility Public Network
3. Wide Area Network
4. Secondary Substation
5. Distribution Network

**Overlay versus Underlay Network**

Since the WAN is a highly unsecure network, the communication path between the DA Gateways/SSRs and the HERs have to be secured with FlexVPN tunnels.

- The **Underlay Network** is the name of the underlying public network over which the tunnels are established.
- Once the tunnels are established, any network connectivity established as an overlay on top of the already established tunnel is called an **Overlay Network**.

As an example, with reference to **Figure 20**, the FlexVPN tunnel can be established between the public IP of the DA Gateway (located in the Distribution Network) and the DMZ Virtual IP of the HER Cluster (located in the Utility Public Network). Once the tunnel is established, reachability information of FND and SCADA (located in the Utility Private Network) could be advertised as overlay routes through the tunnel to the DA Gateway.
Figure 20   FlexVPN Tunnels, Underlay vs Overlay Networks

Note: Both IPv4 and IPv6 are supported Overlay/Underlay IP addresses in this solution.

Note: The term IP is used to represent both IPv4 and IPv6 addresses throughout the document unless explicitly called out.

In Figure 20, the public IP of the HER cluster and the DA Gateways are used in establishing the FlexVPN Tunnel. They are Underlay IP addresses.

The following list includes Overlay IP addresses:

- **Advertised by HER Cluster:**
  - IP address of the Loopback interface on HER
  - IP address of the Utility Private Network components (such as SCADA, FND, and application servers)
  - These routes are advertised through the tunnel towards the IoT Gateway

- **Advertised by the IoT Gateway:**
  - IP address of the Loopback interface on the gateway
  - Optionally, locally connected devices on IoT Gateway can be advertised
  - These routes are advertised through the tunnel towards the HER Cluster
**Design Considerations**

Table 7 captures the distinction between the usage of underlay address at different points in the solution.

**Table 7  Underlay IP Addresses (Public IPs) facing Wide Area Network**

<table>
<thead>
<tr>
<th>Underlay Public IP address</th>
<th>HER Cluster</th>
<th>SSR</th>
<th>DA Gateway in Distribution Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode of IP Address</td>
<td>Static IP Address</td>
<td>Static IP address (or)</td>
<td>Dynamically allocated IP address by service provider.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td>Dynamic allocated IP address</td>
<td></td>
</tr>
<tr>
<td>IP modes</td>
<td>IPv4-only (or)</td>
<td>IPv4-only (or)</td>
<td>IPv4-only (or)</td>
</tr>
<tr>
<td></td>
<td>IPv6-only (or)</td>
<td>IPv6-only (or)</td>
<td>IPv6-only (or)</td>
</tr>
<tr>
<td></td>
<td>Dual-Stack</td>
<td>Dual-Stack</td>
<td>Dual-Stack</td>
</tr>
<tr>
<td>Location of the positioned</td>
<td>DMZ Network</td>
<td>Secondary Substation</td>
<td>Distribution Network</td>
</tr>
<tr>
<td>device</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Underlay IP addresses on the HER cluster have to be static IP addresses (IPv4 and/or IPv6).

**Note:** As long as the tunnel is up, overlay routes to Utility Private Network components like FND and SCADA, would be reachable on the SSR or DA Gateway.

**Note:** Overlay IPv4 and IPv6 reachability is agnostic to the underlying network layer. In other words, both IPv4 and IPv6 overlay reachability can be enabled between SCADA masters and outstations over an underlay network, which can be IPv4-only or IPv6-only or Dual-stack.

**Loopback Addressing Design**

With the WAN IP address (Underlay address) allocated dynamically to the IoT Gateway, this address could possibly change every time the device disconnects and reconnects. Therefore, the mechanism for uniquely identifying the IoT Gateway is allocating an Overlay IP address to the gateway’s loopback interface, with a permanent lease from the DHCP server located in the communication headend of the Utility Private Network. Both IPv4 and IPv6 Overlay addresses can be configured on the loopback interface of the IoT Gateway. This configuration is taken care of dynamically by Cisco IoT FND during ZTD.

Considering that the IoT Gateways are aggregated at the HER cluster, the Overlay IP addresses that are to be allocated to the loopback interface of the gateways are chosen from the same IPv4 and IPv6 DHCP pool to which the HER Loopback Interface’s IPv4/IPv6 belongs.

**Note:** Although the gateways and HERs share the same IPv4 and IPv6 subnets while configuring loopback interfaces, the recommendation is to use a subnet mask of /32 for IPv4 and /128 for IPv6 addresses.
Figure 21 captures the loopback addressing design used in this solution.

**Figure 21  IP Address Schema - Loopback Addressing on HER Cluster and IoT Gateways**

For example, if 192.168.150.0/24 and 2001:db8:baba:face::/64 are the subnet chosen for representing the SSRs and DA Gateways:

- Few IP addresses of this subnet are reserved for loopback interface configuration on HERs. These addresses are statically assigned on HERs. For example, the following addresses as shown in Figure 21 can be reserved for HERs:
  - IPv4 addresses 192.168.150.1, 192.168.150.2 and 192.168.150.3

These reserved addresses must be excluded from the DHCP pool meant for Overlay address allocation to SSRs and DA Gateways.

**Note:** These loopback addresses are to be allocated with permanent lease by the DHCP server (IPv4 and IPv6).

The allocated loopback IP addresses (with permanent lease) would serve the purpose of uniquely representing the DA Gateway to Cisco IoT FND, as well as SCADA and other application servers located in the Utility Private Network.

**Note:** The tunnel aggregation point has to have a statically-configured IP address.

**Utility Private Network**

The Utility Private Network aligns with the headend block shown in *Places in the Network, page 16*. Utility Private Networks, which are comprised of the components residing in the protected data center part of the network, have the following sub blocks:

- Private network portion of the communication headend
- Utility control center
- Utility PKI

**Note:** All the components located in the Utility Private Network fall under the overlay network category. FND, SCADA, DHCP Server, Certificate Authority, Active Directory, and AAA server are among the components that are part of this Utility Private Network.
Of all these private network components, the reachability information of only selected components like FND and SCADA need to be advertised as overlay routes to the IoT Gateways. All components need not be advertised to the IoT Gateways.

The Utility Private Network layer interacts with the rest of the layers by interfacing with the Utility Public Network components such as the RA, TPS, and HER Cluster.

Private Network Portion of the Communication Headend

Table 8 captures the list of components located in the Private Network portion of the communication headend, its mode of IP address configuration, the single/dual stack requirement, and the requirement to be advertised as an overlay route to the IoT Gateway.

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-stack</th>
<th>Should it be advertised to the IoT Gateway as overlay route?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Network Director</td>
<td>Static IP address Configuration</td>
<td>Dual Stack</td>
<td>Yes</td>
</tr>
<tr>
<td>FND-Database</td>
<td>Static IP address Configuration</td>
<td>IPv4 would be sufficient, although IPv6 is supported.</td>
<td>No</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Static IP address Configuration</td>
<td>Dual Stack</td>
<td>FND will interact with DHCP server within Utility Private Network. Need not advertise to IoT Gateway.</td>
</tr>
<tr>
<td>NTP</td>
<td>Static IP address Configuration</td>
<td>IPv4 would be sufficient</td>
<td>No</td>
</tr>
<tr>
<td>DNS</td>
<td>Static IP address Configuration</td>
<td>Dual Stack</td>
<td>No</td>
</tr>
</tbody>
</table>

Utility Control Center

Table 9 captures the list of components located in the Utility control center part of the headend, its mode of IP address configuration, the single/dual stack requirement, and the requirement to be advertised as an overlay route to the IoT Gateway.

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-stack</th>
<th>Should it be advertised to the IoT Gateway as overlay route?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA</td>
<td>Static IP address Configuration</td>
<td>Dual Stack</td>
<td>Yes</td>
</tr>
<tr>
<td>Other Application Servers</td>
<td>Static IP address Configuration</td>
<td>According to what the control center Application server supports</td>
<td>Can be advertised if needed</td>
</tr>
</tbody>
</table>
Utility PKI

Table 10 captures the list of components located in the Utility PKI part of the headend, its mode of IP address configuration, the single/dual stack requirement, and the requirement to be advertised as an overlay route to the IoT Gateway.

Table 10 Utility PKI - Part of Headend

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-stack</th>
<th>Should it be advertised to the IoT Gateway as overlay route?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Authority</td>
<td>Static IP address Configuration</td>
<td>IPv4 would be sufficient</td>
<td>No</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Static IP address Configuration</td>
<td>IPv4 would be sufficient</td>
<td>No</td>
</tr>
<tr>
<td>AAA Server</td>
<td>Static IP address Configuration</td>
<td>IPv4 would be sufficient</td>
<td>No</td>
</tr>
</tbody>
</table>

As the IoT Gateway can receive the certificate with the help of the RA, the route for the CA does not need be advertised to the IoT Gateway.

Utility Public Network

The Utility Public Network aligns with the headend block shown in Places in the Network, page 16.

Utility Public Networks are comprised of publicly-exposed network portions of the communication headend and are typically positioned under the DMZ. This network portion of the communication headend handles the communication from IoT Gateways located in the Secondary Substation (or) Distribution Network.

The Utility Public Network has the following sub-block:

- The DMZ Network portion of the Communication headend, which includes:
  - Registration Authority
  - HER Cluster
  - Tunnel Provisioning Server

Both SSRs and DA Gateways should be able to reach the RA, TPS, and HERs.
As Figure 22 shows, Utility Public Networks are comprised of TPS, HER Clustering, and RA, which interact with the (underlay) WAN in the southbound. Utility Public Networks also interact with the Utility control center, PKI, and the communication headend in the northbound.

**Figure 22 Utility Public Network - IP Addressing, Advertised Overlay Addresses**

**Note:** The HER Cluster can serve as the default gateway for all the Utility Private Network components, including Utility control center, Utility PKI, and communication headend private network.

- DMZ IPs 1–6 are underlay public IP addresses, and should already be reachable from IoT Gateways.
- Overlay routes to be advertised, once the FlexVPN Tunnel is established, include:
  - IPv4 and IPv6 addresses of SCADA from the control center
  - IPv4 and IPv6 addresses of FND from the communication headend
  - IPv4 and IPv6 addresses of loopback interfaces of the HER routers in the clusters
  - IP addresses of any other application server that needs to be advertised to the IoT Gateways
  - IP addresses of DHCP server, if there is any requirement of IoT Gateway to act as DHCP relay
Table 11 captures the list of components located in the Utility Public Network of the headend, and its mode of IP address configuration, the single/dual stack requirement, and requirement to be advertised as an overlay route to the IoT Gateway.

**Table 11  Utility Public Network of Headend Matrix**

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-Stack</th>
<th>Should it be advertised to the IoT Gateway as overlay route?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Authority</td>
<td>Static IP</td>
<td>Northbound Network with CA: IPv4 would be sufficient</td>
<td>N/A. It’s an underlay public IP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Southbound Network facing WAN: Can be enabled for IPv4/IPv6/Dual-Stack according to network capability and requirement.</td>
<td></td>
</tr>
<tr>
<td>Tunnel Provisioning Server</td>
<td>Static IP</td>
<td>Northbound Network with FND: IPv4 would be sufficient. Dual-Stack is recommended.</td>
<td>N/A. It’s an underlay public IP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Southbound Network facing WAN: Can be enabled for IPv4/IPv6/Dual-Stack according to network capability and requirement.</td>
<td></td>
</tr>
<tr>
<td>HER Cluster</td>
<td>Static IP</td>
<td>Northbound Network with Utility control center (hosting SCADA, and other application servers): Dual-Stack is recommended.</td>
<td>Yes, SCADA Master needs to be advertised.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Northbound Network with Utility PKI: IPv4 would be sufficient.</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Northbound Network with Utility Private Communication Headend: Dual-Stack is recommended.</td>
<td>Yes, FND needs to be advertised.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>East West Networks with Registration Authority: IPv4 would be sufficient.</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>East West Networks with Tunnel Provisioning Server: IPv4 would be sufficient. Dual-Stack is recommended.</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Southbound Networks facing WAN: Can be enabled for IPv4/IPv6/Dual-stack according to WAN (underlay) network capability.</td>
<td>N/A. It’s an underlay public IP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loopback Interface representing HER: Dual-Stack recommended.</td>
<td>Yes. Both IPv4 and IPv6 addresses need to be advertised to IoT Gateway.</td>
</tr>
</tbody>
</table>
**Wide Area Network**

DA Cellular leverages the Wide Area Network (WAN) for connecting the headend block with the substation (or) DA blocks. The solution uses WAN as an underlay network. IP backhaul categories can be IPv4-only or IPv6-only or dual-stack serving both IPv4 and IPv6 at the same time.

**Secondary Substation**

IP addressing of the SSR would be very similar to IP addressing on the DA Gateway. The difference comes only if a utility requirement exists for aggregating the communication from multiple DA Gateways at the SSR, instead of aggregating directly at the DSO headend.

**Note:** If the SSR needs to aggregate tunnels from multiple DA Gateways, then static WAN IP addresses are recommended on the SSRs.

As shown in [Figure 23](#), the SSR could serve RTU, IPv4 IED, and IPv6 IED.

**Figure 23** IP Addressing in SSR - Dynamic Public IP Address

WAN IP could be a dynamically-allocated public IP, which could change every time the SSR disconnects and reconnects to the network. The SSR is uniquely represented by its IPv4 and IPv6 loopback addresses. The loopback addresses are configured on the SSR by Cisco IoT FND during ZTD. Static WAN IP also would work perfectly fine in this scenario.

The IPv4 and IPv6 devices can be advertised to the DSO headend using its configured IP addresses or could be Network Address Translated (NAT’d) to the IP address of the SSR to keep a simple and consistent routing information. More about this is discussed under [Network Address Translation, page 52](#).
Any legacy (serial interface based) Secondary Substation device could also be enabled for communication with the DSO headend with the use of raw sockets (or) protocol translation services, provided by the SSR.

Table 12  IP Addresses on SSR – Dynamic WAN IP Scenario

<table>
<thead>
<tr>
<th>IP address</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-stack</th>
<th>Should it be advertised to the DSO headend (as overlay route)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN IP</td>
<td>Dynamically allocated IP address</td>
<td>Could be IPv4–only (or) IPv6–only (or) Dual–stack</td>
<td>N/A (it’s an underlay IP)</td>
</tr>
<tr>
<td>Loopback IP</td>
<td>Dynamically configured by FND during ZTD</td>
<td>Dual–stack recommended</td>
<td>Yes</td>
</tr>
<tr>
<td>Addresses of the IPv4 and IPv6 IEDs</td>
<td>SSR have the capability to allocate IP addresses to the IEDs through DHCP, if IED is capable of DHCP</td>
<td>Could be IPv4–only (or) IPv6–only (or) Dual–stack</td>
<td>It depends. Not required if the IED IP addresses are NAT’d by the SSR’s IP address.</td>
</tr>
</tbody>
</table>

Figure 24 portrays the scenario where the DA Gateways are aggregated at the SSR. In this case, the SSR must have a STATIC Public IP to handle the termination of tunnels from the DA Gateways. The loopback address configuration and enabling access to IPv4 and IPv6 IEDs are similar to the previous section.

Figure 24  IP Addressing in SSR – Static Public IP Address
In addition to advertising the routes to the DSO headend, the SSR could choose to selectively advertise a subset of the routes in the southbound direction to the DA Gateways.

### Table 13  IP Addresses on SSR - Static WAN IP Scenario

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-stack</th>
<th>Should it be advertised to the DSO headend and DA Gateways (as overlay route)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN IP</td>
<td>Statically configured IP addresses</td>
<td>Could be IPv4-only (or) IPv6-only (or) Dual-stack</td>
<td>N/A (it’s an underlay IP)</td>
</tr>
<tr>
<td>Loopback IP</td>
<td>Dynamically configured by FND during ZTD</td>
<td>Dual-stack recommended</td>
<td>Yes</td>
</tr>
<tr>
<td>Addresses of the IPv4 and IPv6 IEDs</td>
<td>Static/DHCP – both supported</td>
<td>Could be IPv4-only (or) IPv6-only (or) Dual-stack</td>
<td>It depends. Not required if the IED IP addresses are NAT’d by the SSR’s IP address.</td>
</tr>
</tbody>
</table>

### Distribution Network

DA Gateways in the field would receive their WAN IP addresses (IPv4 and/or IPv6) dynamically from the service provider. This is an underlay IP address, which is used for forming the FlexVPN Tunnel.

As Figure 25 shows, the DA Gateway could serve IPv4 IED, IPv6 IED, and also serial devices, and enable overlay communication with the DSO headend components such as FND and SCADA.

![Figure 25 IP Addressing in DA Gateway](image)

The IPv4 and IPv6 IEDs can be advertised to the DSO headend, using the IED’s configured IP addresses (or) could be NAT’d to the IP address of the DA Gateway to keep a simple and consistent routing information. More about this is discussed in Network Address Translation, page 52.
The DA Gateway is uniquely represented by its IPv4 and IPv6 loopback addresses. The loopback addresses are configured on the DA Gateway by Cisco IoT FND as part of ZTD.

Figure 25 on the previous page shows the FlexVPN Tunnel established between the DA Gateway and the HER Cluster of the DSO headend. If the utility requires aggregating multiple DA Gateways at the substation level, the DA Gateway could establish an additional tunnel with the SSR.

### Table 14  IP Addresses on DA Gateway - Dynamic WAN IP Scenario

<table>
<thead>
<tr>
<th>IP address</th>
<th>Mode of IP Address Configuration</th>
<th>IPv4/IPv6/Dual-stack</th>
<th>Should it be advertised to the DSO headend (as overlay route)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN IP</td>
<td>Dynamically allocated IP address</td>
<td>Could be IPv4-only (or) IPv6-only (or) Dual-stack.</td>
<td>N/A (it’s an underlay IP)</td>
</tr>
<tr>
<td>Loopback IP</td>
<td>Dynamically configured by FND during ZTD</td>
<td>Dual-stack recommended</td>
<td>Yes</td>
</tr>
<tr>
<td>Addresses of the IPv4 and IPv6 IEDs</td>
<td>Static/DHCP – both supported</td>
<td>Could be IPv4-only (or) IPv6-only (or) Dual-stack.</td>
<td>Not required if the IED IP addresses are NAT’ed with the DA Gateway’s IP address.</td>
</tr>
</tbody>
</table>

### Summary of IP Address Allocation Methods

Table 15 captures the summary of the various IP addressing components, the location in which the component exists, and the method of address allocation.

### Table 15  Address Allocation Methods to Components

<table>
<thead>
<tr>
<th>Components Category</th>
<th>Location</th>
<th>Type of IP Assignment</th>
<th>Sample subnet (or) IP description.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Components in Data/control center like CA, SCADA, FND/NMS, and so on</td>
<td>Utility Private Network (Trusted Area)</td>
<td>Static IP address assignment</td>
<td>Utility control center: 172.16.107.0/24  2001:db8:16:107::/64  Communication Private Network: 172.16.103.0/24  2001:db8:16:103::/64  Utility PKI Network: 172.16.102.0/24</td>
</tr>
<tr>
<td>Components in public part of Head end like RA, TPS, HER1, HER2 and HER3</td>
<td>Utility Public Network (DMZ Area)</td>
<td>Static IP address assignment</td>
<td>DMZ IP-X (IPv4 and/or IPv6)</td>
</tr>
<tr>
<td>IoT Gateways positioned as SSR, aggregating multiple DA Gateways</td>
<td>Secondary Substation</td>
<td>Static IP address assignment</td>
<td>Public WAN IP statically configured. Should be reachable from DA Gateways across the Distribution Network.</td>
</tr>
<tr>
<td>IoT Gateways positioned as SSR, not aggregating any DA Gateway</td>
<td>Secondary Substation</td>
<td>Dynamically allocated</td>
<td>Public WAN IP allocated dynamically by service provider over Cellular/Ethernet networks.</td>
</tr>
<tr>
<td>IoT Gateways positioned as DA Gateway</td>
<td>Across Distribution network</td>
<td>Dynamically allocated</td>
<td>Public WAN IP dynamically allocated by service provider over Cellular/Ethernet networks.</td>
</tr>
</tbody>
</table>
Design Considerations

Loopback addresses of HER1, HER2, and HER3 are one-time manual configurations on the Utility Public Network.

Loopback addresses of SSRs as well as DA Gateways are dynamically configured by Cisco IoT FND during the ZTD. The DHCP (IPv4 and IPv6) pool chosen for this address allocation is the pool to which the HER loopback addresses belongs.

Network Services

WAN

The WAN tier connects the Field Area and Secondary Substation blocks with the control center. The following are some considerations while choosing the technology for the WAN backhaul and its routing protocols:

- Scalability evaluation: The WAN must cater to the aggregation routers located in the control center and the SSRs/DA Gateways in the DA, and to support the multitude of IP tunnels between them. Dual tunnel configuration should be accounted for in order to support resiliency

- Redundancy and high availability as per SLAs

- Dual stack routing protocols supported by Cisco IOS, such as MP-BGP, OSPFv3, RIPv2/RIPng, EIGRP, static routes, and IKEv2 prefix injection from FlexVPN

- Leverage existing WAN infrastructure connecting to the Control Centers

- Topology considerations such as hub-and-spoke configurations

- Static versus dynamic routing

- Ease of configuration

- Convergence time when loosing connectivity with the HER or the SSR

- Latency and bandwidth requirements depending on traffic flow patterns

- Minimize the control traffic over WAN


Cellular Backhaul

Cellular backhaul will be the most prevalent deployment backhaul and Cisco IR1101 is the correct choice for deploying as a SSR and as a DA Gateway. However, Cisco IR807 could be deployed in cases where lower cost and lower power consumption are the primary requirements.

Cisco IR1101 supports a 4G LTE module to support cellular backhaul deployment. Most European carriers will be operating in FDD Bands 3, 7, and 20. These bands are well supported by the Cisco IR1101 LTE modem. For more details about other supported TDD LTE, UMTS, HSPA+ and HSPA bands, please refer to Cisco IR100 product specification document.

Other important features supported by IR1101 LTE modules include:

- Dual SIM, which allows SIM to be active in either slot; failover to the alternative SIM slot if the active SIM loses connectivity to the network

- Auto SIM mode, which will automatically select the right carrier after a SIM slot switching and automatically reset the modem

- SIM Online Insertion and Removal (OIR)

- Assisted GPS (A-GPS)
Design Considerations

- Short Message Service (SMS)
- Modem Firmware Upgrade
- SIM lock and unlock capabilities
- IPV6 protocol is supported on the cellular interface to enable LTE IPV6 data connection

IP Tunnels

If Distribution Automation traffic traverses any kind of public WAN, data should be encrypted with standards-based IPSec. This approach is advisable even if the WAN backhaul is a private network. A site-to-site IPSec VPN can be built between the DA Gateway/SSR and the HER in the control center. The Cisco Distribution Automation solution implements a sophisticated key generation and exchange mechanism for both link-layer and network-layer encryption. This significantly simplifies cryptographic key management and ensures that the hub-and-spoke encryption domain not only scales across thousands of field area routers, but also across thousands of DA Gateways and SSRs.

IP tunnels are a key capability for all DA use cases forwarding various traffic types over the backhaul WAN infrastructure. Various tunneling techniques may be used, but it is important to evaluate the individual technique's OS support, performance, and scalability for the DA Gateway/SSR and HER platforms.

The following are tunneling considerations:

- **IPSec Tunnel**—To protect the data integrity of all traffic over the unsecure WAN. The IPSec GRE tunnel could be established over the IPv4-only WAN infrastructure or Native IPv6/Dual-Stack WAN infrastructure.

- Communication with IPv6 IEDs could be securely transported as an overlay traffic through the IPv4 or IPv6 GRE Tunnel, secured with IPSec.

In Figure 26, the underlay IPSec Tunnel could be established over an IPv4-only/IPv6-only/Dual-stack WAN infrastructure. It could carry communication to both IPv4 and IPv6 IEDs in a secure manner.

**Figure 26  Tunnel between the DA Gateway/SS Router and the HER**

FlexVPN

FlexVPN is a flexible and scalable VPN solution based on IPSec and IKEv2. To secure DA data communication with the headend across the WAN, FlexVPN is recommended. The IoT FND establishes FlexVPN tunnels between the HERs and the DA Gateways as a part of the ZTD process.

FlexVPN, which integrates various topologies and VPN functions under one framework, simplifies the deployment of VPNs by providing a unified VPN framework that is compatible with legacy VPN technologies.

FlexVPN has some of the following benefits:

- Allows use of a single tunnel for both IPv4 and IPv6, when the medium supports it.
Design Considerations

- Supports NAT/PAT traversal.
- Supports QoS in both directions: hub-to-spoke and spoke-to-hub.
- Supports Virtual Routing and Forwarding (VRF).
- Reduces control plane traffic for costly links with support for tuning of parameters.

**Note:** In this solution, IPSec is configured in the tunnel mode.

- IKEv2 has fewer round trips in a negotiation than IKEv1: two round trips versus five for IKEv1 for a basic exchange.
- Built-in dead peer detection (DPD).
- Built-in configuration payload and user authentication mode.
- Built-in NAT traversal (NAT-T). IKEv2 uses ports 500 and 4500 for NAT-T.
- Improved re-keying and collision handling.
- A single Security Association (SA) can protect multiple subnets, which improves scalability. Support for Multi-SA Dynamic Virtual Tunnel Interfaces (DVTI) support on the hub.
- Asymmetric authentication in site-to-site VPNs, where each side of a tunnel can have different pre-shared keys, different certificates, or on one side a key and the other side a certificate.

In the FlexVPN model, the HER acts as the FlexVPN hub and the DA Gateways act as the FlexVPN spokes. The tunnel interfaces on the DA Gateways acquire their IP addresses from address pools configured during ZTD. These addresses only have local significance between the HER and the DA Gateways. Since the DA Gateway’s tunnel addresses are both dynamic and private to the HER, NMS must address the DA Gateways by their loopback interface in this network architecture. Conversely, the DA Gateway sources its traffic using its loopback interface.

Before the FlexVPN tunnel is established, the DA Gateway can only communicate to the HER in the headend network. This is done over the WAN backhaul via a low priority default route. During FlexVPN handshake, route information is exchanged between the HER and the DA Gateway. The DA Gateway learns the headend routes (IPv4 and IPv6) through FlexVPN.

**Figure 27** FlexVPN Hub-and-Spoke

In this release, only the FlexVPN hub-and-spoke design is discussed. Spoke-to-spoke ICT design will be needed for IED-to-IED application traffic flow deployment scenarios.
FlexVPN versus DMVPN Selection Criteria

FlexVPN has advantages over DMVPN primarily when the cost of the WAN links is based on volume of data flowing between the hub and the spokes. The reasons for this include:

- Dynamic routing is not necessary, as the Internet Key Exchange v2 (IKEV2) prefix injection for IPv4 and IPv6 is supported.
- IPv6 is available and this reduces control plane traffic, while dynamic IPv4 and IPv6 routing cannot be avoided in DMVPN. Note that with FlexVPN, prefixes are only injected when the tunnel is being established.
- Next Hop Resolution Protocol (NHRP) is not used between the hub and the spoke, reducing control plane traffic, while in DMVPN, NHRP is required between the hub and the spoke.
- Specific QoS rules can be dedicated to each side of the channels, while in DMVPN, the same QoS rules applied to all channels in the downstream (hub and spokes) direction.
- NAT/PAT can be configured on both sides of the hub and the spoke.
- Clustering of the hubs can be done in different ways, allowing various redundancy scenarios.
- IKEV2 tunnel allows switching tunnel across physical interfaces.

IKEV2 supports snapshot-based routing, which can be used in the case of the mesh network at the southbound traffic.

If the connectivity between the hub and the SSR is over cellular, then these protocols will consume data from a service provider. If no data limit exists, these protocols are suitable and can be used without any problem. But if there is a limit (such as 1GB/month) on the service provider-provided data, then the exchange packets between the protocol processes on the routers will exceed the limit and might incur an additional cost (depending on the service provider).

With FlexVPN, these protocols are not necessary. Prefix-based injection and snapshot-based routing are more preferred with FlexVPN. No control packet exchanges occur between the hub and the SSR. With this design, the service provider’s monthly or the daily limit is sufficient, and the customer can expect a lower overhead cost than the cost incurred when DMVPN is implemented with the above-mentioned dynamic routing protocols.

Therefore, FlexVPN-based implementation is preferred over DMVPN-based implementation. DMVPN can also be considered if the service provider does not have a limit on data consumption.

IP Routing

For most deployment in the European region, cellular backhaul will be considered as the primary backhaul. FlexVPN IKEV2-based prefix injection is the recommended design for IP routing. This approach will ensure minimization of control traffic over the WAN (by saving approximately 100 MB or more of control traffic every month), and, in turn, the saved data is available for application traffic.

The “value add” in this type of routing is the total cost of ownership (TCO) control achieved. As soon as the tunnel is provisioned between the DA Gateway or SSR and the HER is provisioned as part of Zero Touch Provisioning using IoT FND, IED prefixes from the field area/Secondary Substation block will be advertised to HER and SCADA prefixes will be advertised to the DA Gateways/SSRs after tunnel establishment. This is depicted in Figure 28.
Design Considerations

Figure 28 Routing via IKEv2 Prefix Injection

Send IED prefixes to HER via IKEv2 prefix injection

Send SCADA application prefix to SS router via IKEv2

DA Gateway/Secondary Substation Router

SCADA Services

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.

A new or upgraded SCADA system will not only provide better monitoring and control, it can extend the life of substations and related equipment by providing current data for troubleshooting small problems before they escalate. Furthermore, the ample historical data provided by SCADA systems can improve preventive maintenance scheduling and cut associated costs.

SCADA Service Models

Three SCADA Service Models will be supported within this release, as shown in Table 16:

<table>
<thead>
<tr>
<th>Service</th>
<th>Connectivity</th>
<th>Service Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy SCADA (DNP3, Modbus, T101)</td>
<td>Point-to-Point (Master Slave)</td>
<td>Raw-Socket over FlexVPN</td>
</tr>
<tr>
<td>Legacy SCADA (DNP3, Modbus, T101)</td>
<td>P2MP Multi drop</td>
<td>Raw-Socket over FlexVPN</td>
</tr>
<tr>
<td>SCADA Gateway (DNP3, T101) to IP Conversion (DN3-IP, T104)</td>
<td>Point-to-Point (Master Slave)</td>
<td>Protocol translation over FlexVPN</td>
</tr>
<tr>
<td>SCADA Gateway (DNP3, T101) to IP Conversion (DN3-IP, T104)</td>
<td>Multi Master</td>
<td>Protocol translation over FlexVPN</td>
</tr>
<tr>
<td>SCADA (DNP3-IP, Modbus-TCP, T104)</td>
<td>Point-to-Point (Master Slave)</td>
<td>FlexVPN</td>
</tr>
</tbody>
</table>
Figure 29 depicts multiple technologies for transporting SCADA traffic. Raw Sockets and Protocol Translation are discussed in detail starting in Raw Sockets, page 46. Regular IP routing design will take care of transporting IEC 60870-5-14, DNP3 IP, and Modbus application traffic between IEDs in Secondary Substations and feeders to the SCADA application in the DSO control center.

SCADA Components and Protocols

Monitoring and controlling electrical distribution systems, which involve many remote applications and sites, has often been difficult. To solve this problem, utilities began installing remote terminal/telemetry units (RTUs) at substations. IEDs are a more recent technology development, and these devices are now installed at most substations to some extent.

Remote Terminal Units

An RTU provides intelligent I/O collection and processing such as reading inputs from switches, sensors, and transmitters, and then arranging the representative data into a format that the SCADA system can understand. The RTU also converts output values provided by the SCADA system from their digital form into that which can be understood by field-controllable devices such as discrete (relay) and analog outputs (current or voltage).

Intelligent Electronic Devices

IEDs, which are now installed at most substations to some extent, generally communicate with the substation RTU.

Control Center

The SCADA system consists of a master control station with one or more PC-based human machine interfaces (HMIs). The SCADA system may also contain other secondary control stations with HMIs, and large substations may also have local HMIs.
Operators view information on the HMIs to monitor and control substation operations and related equipment. Modern SCADA systems are extremely adept at handling the large amounts of data necessary to monitor the electrical state of all power lines, cables, and equipment.

SCADA Protocols

Legacy SCADA protocols, which are supported over legacy asynchronous interfaces, include:

- Modbus
- DNP3
- IEC 60870-5-101

Newer SCADA protocols can be transported over Ethernet interfaces.

1. IP-based protocols:
   - Modbus-IP
   - DNP3-IP
   - IEC 60870-5-104
   - IEC 61850 MMS

2. Layer 2-based protocols:
   - IEC 61850 GOOSE
   - IEC 61850 SV

Many other SCADA protocols exist, but in the utility space only those listed above are discussed.

Raw Sockets

Raw sockets are a means for transporting streams of characters from one serial asynchronous interface to another over the IP network for utility application. Serial communications have been the mainstay for utilities communications for more than a decade using RS232 and RS485 as the physical layer. The industry is currently starting to migrate to Ethernet. However, retrofitting Ethernet and newer IEDs into existing communications systems requires supporting a hybrid network of both Ethernet and serial devices. Raw sockets transport SCADA data from RTUs, support point-to-point and point-to-multipoint connections over an asynchronous serial line, and have a built-in auto Transmission Control Protocol (TCP) connection retry mechanism. Packetization of serial packets that will be triggered will be based on specific packet length or special character or timer. Sub-options are available with the raw rockets feature. The end user can choose these options according to their deployment needs. Monitoring and control (SCADA) data will be routed from the substation to the control center. SCADA communications have latencies ranging from ~500 milliseconds to ~5 seconds.

Raw Socket TCP Transport

TCP raw socket transport uses a client-server model. At most, one server and multiple clients can be configured on a single asynchronous serial line. A raw socket client receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The raw socket client initiates a TCP connection with the raw socket server and sends the packetized data across the IP network to the raw socket server, which retrieves the serial data from the packets and sends it to the serial interface, and onto the utility management.
Figure 30 depicts three different deployment scenarios for point-to-point raw socket service:

Figure 30  Raw Socket TCP Transport

- **Scenario A**—Raw socket between SSRs/DA Gateways and SCADA Router in headend; no change on SCADA server; communications through COM ports.

- **Scenario B**—Raw socket between IR1101 and SCADA Server; no SCADA application change on server but IP/Serial Redirector software maps COM port to IPv4 address +TCP port, running over the Ethernet interface.

- **Scenario C**—Raw socket between IR1101 and SCADA Server; SCADA application knows how to directly communicate over a raw socket (IPv4 address + TCP port) & Ethernet interface.

**Note:** Scenario A is not scalable. Scenario B or Scenario C are highly recommended for raw socket deployments.

**Raw Socket UDP Transport**

User Datagram Protocol (UDP) transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line. The raw socket UDP peer receives streams of serial data from the RTUs and accumulates this data in its buffer, and then places the data into packets based on user-specified packetization criteria. Raw socket UDP peer sends the packetized data across the IP network to the raw socket peer at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.
Raw Socket Dual Control Center Multi-Drop Bridging

A Raw Socket on the DA Gateway or SSR can replicate its packets to different Control Centers. In Figure 31, two geographically-separated (primary and secondary) DSO Control Centers can be observed, each of them hosting SCADA applications. DA Gateways are configured as a TCP raw socket client with two different sockets, one per control center.

Figure 31  SCADA Multi-Drop Poll

IP routing is key for successful establishment of sockets across the control center. This design serves as a key for disaster recovery and application-level redundancy. The SCADA server in the control center polls RTU periodically. The poll will be addressed to a specific RTU. The HER is configured for replicating application traffic to Raw Socket destinations.

Only the RTU that is addressed by SCADA application replies to poll. The SCADA reply is replicated to all SCADA destinations.
Design Considerations

The SCADA reply from the RTU must not be fragmented. The SCADA reply is depicted in Figure 32. In order to prevent fragmentation of the SCADA reply at the TCP layer, the client supports configuration options such as special-char, packet-length, and packet-timer to ensure that the reply is packed correctly into a single TCP packet.

**Figure 32** SCADA Multi-Drop Response

From the control center, both simultaneous SCADA application poll and device control operations will be performed. If an RTU wants to send unsolicited reporting, Raw Sockets will replicate application traffic across two different Control Centers.

**Protocol Translation**

As the utility industry begins the transition from legacy-based SCADA protocols to IP-based protocols, a migration strategy is needed in order to enable both legacy and newer IP-based protocols to interoperate. The protocol translation (otherwise known as the SCADA Gateway feature on the IR1101, IR807, and CGR 1120) provides this capability.

The Cisco IOS SCADA protocol translation function allows translations between:

- IEC-60870-5-101 and IEC-60870-5-104
- DNP3 Serial and DNP3 IP

More protocol translation capability could be added with the help of IOx applications leveraging the Edge Compute capability of the platform. For more details, please refer to *Cisco IoT Connected Utilities Virtual RTU Implementation Guide*, at the following URL:


The following software stacks are implemented in the Cisco SSRs or DA Gateways:

- IEC-101 and DNP3 serial Protocol Stack
- IEC-104 and DNP3 IP Protocol Stack
- Translation Module to translate between:
  - IEC-101 and IEC-104
--- DNP3 Serial and DNP3 IP

In Figure 33, IR1101 IR1101 can be observed as deployed as a SCADA Gateway. SCADA Gateway will host both T101 Master and T104 Slave functionalities. One RTU per serial interface will be connected. The DA Gateway/SSR will act as the T101 Master for the T101 Slave RTU. In turn, the DA Gateway/SSR will acts as the T104 Slave to the SCADA T104 Master residing in the control center. This scenario depicts the point-to-point protocol translation scenario.

**Figure 33 Raw Sockets Point to Point**

T101/T104 Protocol translation features:
- T101/T104 refers to the IEC 60870-5-101 and IEC 60870-5-104 standard, respectively.
- T101 supports the point-to-point and multi-drop links over serial communications.
- T104 uses TCP/IP transport and network protocols to carry the application data (ASDU), which was specified in T101.
- Allows **balanced** and **unbalanced** communication types:
  - Balanced mode is limited to point-to-point links where either station can initiate transaction (similar to DNP3 unsolicited response).
  - Unbalanced mode is suitable for multi-drop links where only the master station can send primary frames.

DNP3/ DNP3 IP Protocol translations features:
- Serial Stack:
  - Poll all data from RTU every 90 seconds.
  - Provide local time to RTU every 90 seconds.
  - Support file transfer to and from RTU.
Design Considerations

- Enable/disable of unsolicited response on RTU.

**IP Stack:**

- Respond to control center request with local data.
- Trigger counter interrogation to RTU when receive such request from control center.
- Trigger control transaction to RTU when received such request from the control center.
- Support file transfer to and from control center.
- Enable/disable of sending unsolicited response to control center.

**Multi Master Scenario**

Figure 34 depicts multi-master scenario protocol translation scenario where the SCADA Gateway router establishes two different TCP connections with the SCADA master in the primary and secondary control center. Both SCADA masters will be able to do the poll and control of RTU. If RTU needs to send an unsolicited report, SCADA Gateway will replicate the report to both SCADA masters.

**Figure 34  Protocol Translation Multi-Master Scenario**
Network Address Translation

The IoT Gateway has the capability to support the NAT as well as Port Address Translation (PAT). Figure 35 captures a couple of deployment scenarios, one involving NAT-PAT and the second scenario without any NAT-PAT.

**Figure 35  IoT Gateway’s NAT Capabilities vs non-NAT Capabilities**
### Table 17  NAT Scenario versus Non-NAT Scenario

<table>
<thead>
<tr>
<th>Non-NAT Scenario</th>
<th>NAT Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA communicates with IED’s IP on application port number.</td>
<td>SCADA communicates with IoT Gateway’s Loopback IP address and on Application/Custom port number.                                                                -----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>For example, in Figure 35, the SCADA communication is sent to 10.16.21.2 port 2404 directly (yellow line).</td>
<td>IoT Gateway translates the communication and is sent to the IED on Application/Custom port number. For example, in Figure 35, the SCADA communication is sent to Loopback IP of Gateway (192.168.150.21) on port 2404, which, after reaching the IoT Gateway, consultation is made with the NAT Table, is translated to 192.168.0.2 port 2404, and then sent to IED.</td>
</tr>
<tr>
<td>All ports of that IED’s IP address are open for communication. This could be a possible security risk.</td>
<td>Only desired application ports are opened up at the IoT Gateway for communication with IED. This adds up to the security of the IED.</td>
</tr>
<tr>
<td>For example, when the IED is supposed to receive T104 traffic, the IoT Gateway could be remotely provisioned (from FND) to open up the default port 2404 of T104 (or) any custom port as utility customer desires.</td>
<td></td>
</tr>
<tr>
<td>Each and every IED must be configured with utility scope routable IP address, along with configuring on the IoT Gateway’s interface. This method might consume twice the utility scope routable IP address for each IED.</td>
<td>All IEDs can be configured with the same IP address (for example, 192.168.0.2). The overhead in configuring hundreds of thousands of IEDs with unique and correct utility scope routable IP address has been drastically reduced.</td>
</tr>
<tr>
<td>Configuring hundreds of thousands of IEDs could be a huge overhead, especially for configuring <strong>unique</strong> Utility scope routable IP address on the IED.</td>
<td>To make the IED deployment even easier, the IP address of 192.168.0.2 could be allocated to the IED, if the IED is capable of sending the DHCP request.</td>
</tr>
</tbody>
</table>
| Every IoT Gateway has to advertise the IP address of the IED, in addition to advertising its loopback address. | Provisioning IoT Gateway is made easy and remotely doable with the power of FND:  
  - IoT Gateway port serving the IED can be provisioned with 192.168.0.1.  
  - DHCP server functionality can be provisioned on the IoT Gateway to serve IEDs with IP address dynamically.                                                                                                                                                                                                                       |
| IEDs to be allocated with routable addresses within the utility network scope, which could be an overhead for scaled number of deployments. | The IoT Gateway need not advertise the IP address of the IED and only advertises its loopback address, which uniquely represents the IoT Gateway.                                                                                                                                                                                                                                      |
| Network reachability information of each of the IEDs connected to their respective IoT Gateways has to be available in the HER’s routing table, thus consuming more memory space. More resource consumption would have its impact on scalability of HER. | No overhead associated, as IED IP is not advertised. Very much scalable as it’s almost like PNP for IED, if IED is configured for DHCP.                                                                                                                                                                                                                       |
| Migration from one subnet to another subnet requires IED to be reconfigured.      | IED can be reached over IoT Gateway’s loopback address itself.  
  Network reachability information of IED is masked by the IoT Gateway.  
  Frees up lots of memory resource on the HER, which could enhance the scaling on HER.                                                                                                                                                                                                                                                                                     |
|                                                                                                                                 | No reconfiguration required on IED. Any configuration changes could be handled at the IoT Gateway layer itself with the help of FND.                                                                                                                                                                                                                      |
**Table 17  NAT Scenario versus Non-NAT Scenario (continued)**

<table>
<thead>
<tr>
<th>Non-NAT Scenario</th>
<th>NAT Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Since the IP address of the IED itself is advertised, all the port numbers on</td>
<td><strong>This is a security advantage.</strong> Only the application ports that the IED serves</td>
</tr>
<tr>
<td>the IED are exposed to communication requests/denial of service attacks.</td>
<td>(for example, port 2404 while serving IEC 60870–5–104) are opened up at the IoT Gateway.</td>
</tr>
<tr>
<td></td>
<td>Any communication attempt on another port number will be cut off at the IoT Gateway itself.</td>
</tr>
<tr>
<td></td>
<td>This certainly frees up lots of CPU cycles of IED, allowing IED to process one and only</td>
</tr>
<tr>
<td></td>
<td>interesting traffic.</td>
</tr>
<tr>
<td>Once the IED is configured to listen on certain port number (for example,</td>
<td>Since the IED is network and port translated at the IoT Gateway, the SCADA could communicate</td>
</tr>
<tr>
<td>2404) and deployed on the field, if the SCADA server wants to establish</td>
<td>with the IoT Gateway on any custom port number, and the IoT Gateway could translate the</td>
</tr>
<tr>
<td>communication on a custom port number other than 2404, a reconfiguration is</td>
<td>communication to 192.168.0.2 on port 2404 (for which the IED is configured to receive).</td>
</tr>
<tr>
<td>needed on IED.</td>
<td></td>
</tr>
<tr>
<td>Since the IP address of the IED is exposed, there is a prevailing risk of</td>
<td>With only the secure Flex-VPN Tunnel interface configured to receive NAT</td>
</tr>
<tr>
<td>attacks on IED.</td>
<td>inbound traffic from the DSO headend (read: 'ip nat outside' enabled on Tunnel interface), the</td>
</tr>
<tr>
<td>Could be mitigated with ACLs on the cellular interface. Thus, permitting the</td>
<td>only way to establish a communication with the IED is</td>
</tr>
<tr>
<td>communication to IED only from the DSO headend through the Flex-VPN Tunnel.</td>
<td>incoming through the secure tunnel from the DSO control center.</td>
</tr>
<tr>
<td></td>
<td>Incoming traffic on any interface other than secure tunnel interface would get dropped, as the</td>
</tr>
<tr>
<td></td>
<td>translation works only for NAT (outside) enabled ports (which is tunnel interface only).</td>
</tr>
<tr>
<td></td>
<td>As the 'ip nat outside' is not enabled on the cellular interface, even if there is an attack on</td>
</tr>
<tr>
<td></td>
<td>the IED would be smoothly communicating with the SCADA headend on port 2404.</td>
</tr>
<tr>
<td></td>
<td>While at the same time, the IED would be smoothly communicating with the SCADA headend on port 2404.</td>
</tr>
<tr>
<td></td>
<td>This case, the attack is canceled by the IoT Gateway.</td>
</tr>
<tr>
<td></td>
<td>No one on the Internet would be able to NAT/PAT connect to IED, unless they come through the</td>
</tr>
<tr>
<td></td>
<td>secure tunnel from the DSO headend.</td>
</tr>
<tr>
<td>IP address of the IED is reachable to DSO headend only after secure FlexVPN</td>
<td>IP address of the IED is not exposed. Only the IP address of the loopback interface is exposed,</td>
</tr>
<tr>
<td>tunnel is established.</td>
<td>which is reachable to DSO headend only after secure FlexVPN tunnel is established.</td>
</tr>
<tr>
<td></td>
<td>SCADA could reach the IED via the IoT Gateway’s loopback address, on application port numbers</td>
</tr>
<tr>
<td></td>
<td>(port number 20000 for DNP3, 2404 for IEC 60870–5–104, or any custom port), as per the</td>
</tr>
<tr>
<td></td>
<td>configuration provisioned remotely from Cisco IoT FND.</td>
</tr>
<tr>
<td></td>
<td>Additional ports could be opened up on IoT Gateway for IED at any point in time, as the IoT</td>
</tr>
<tr>
<td></td>
<td>Gateway could be remotely re-provisioned from FND, whenever needed.</td>
</tr>
<tr>
<td></td>
<td>Would be slightly faster.</td>
</tr>
<tr>
<td></td>
<td>Would be slightly slow (relative to not having NAT), as NAT consumes extra CPU cycles on the IoT</td>
</tr>
<tr>
<td></td>
<td>Gateway. However, the IoT Gateway is powerful enough to handle this with ease.</td>
</tr>
<tr>
<td></td>
<td>End-to-end IP reachability exists.</td>
</tr>
<tr>
<td></td>
<td>End-to-end communication is not permitted by design. Only the needed application ports are</td>
</tr>
<tr>
<td></td>
<td>opened up.</td>
</tr>
<tr>
<td>Ping test from SCADA is responded by IED.</td>
<td>Ping test from SCADA is responded by the IoT Gateway, as the communication point is the Loopback IP of the IoT Gateway, not IED.</td>
</tr>
</tbody>
</table>
While Table 17 summarizes the advantages of NAT/PAT, if the customer intends to deploy a non-NAT scenario, that too could be secured with ACLs on the cellular port, denying the access to the IED IP. At the same time, the SCADA communication from the DSO headend to IED could be honored, as it arrives over the encrypted tunnel, and therefore should be able to reach the IED.

**Note:** Use of the NAT scenario is recommended; this can help in easy deployment and scalability unless the end-to-end traceability requirement is mandatory.

## Quality of Service

Quality of Service (QoS) and Class of Services (CoS) refer 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 a multi-services Distribution Automation solution since differentiation and prioritization must occur between traffic from AMI, Distribution Automation, Remote Workforce, and network management use cases. 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, IEC 61850 traffic bridged over WAN links between substations
Design Considerations

Figure 36 lists different priorities among Distribution Automation traffic. IP-based protocols can be classified using DSCP. Ethernet Layer 2-based protocols like GOOSE could be classified using CoS.

Figure 36  DA Traffic Priority Chart

<table>
<thead>
<tr>
<th>FLISR</th>
<th>GOOSE</th>
<th>High Priority LLQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volt/VAR</td>
<td>SCADA</td>
<td>Medium Priority CBWFQ 1</td>
</tr>
<tr>
<td>NMS</td>
<td></td>
<td>Medium Priority CBWFQ 2</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>Normal Priority Default Queue</td>
</tr>
</tbody>
</table>

Following the IETF DiffServ model, the Distribution Automation solution will deliver a particular kind of service 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. QoS specification can be used to classify, mark, shape, and police traffic, and to perform intelligent queuing.

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

1. Classification
2. Marking
3. Queuing

Upstream QoS: From Distribution Automation IED to SCADA
DA IEDs perform the marking functionality. If IED does not have the 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 Manufacturing Message Specification (MMS) will be assigned in Class-Based Weighted Fair Queue 1 and IoT FND Network Management traffic will be assigned in Class-Based Weighted Fair Queue 2. The rest of the traffic will be treated with normal priority and will be assigned to the default queue. All QoS is done based on DSCP marking.

Note: It is recommended to define queuing bandwidth as remaining percentage instead of values so that the same policy can be applied across Cellular or Ethernet backhaul interfaces.

If RTU is connected to DA Gateway via R232 async serial interface and, if the raw socket feature is enabled, marking will be enabled on the serial line.

HER-ASR 1000 supports the rich QoS feature set from Cisco IOS. For further details, please refer to Cisco ASR 1000 Series Aggregation Services Routers: QoS Architecture and Solutions at the following URL:


The ASR 1000 provides DoS protection for applications like FND and SCADA.
Downstream QoS: From SCADA to IED

Applications like SCADA and FND generate DSCP markings based on message priority. The HER ASR 1000 provides egress shaping/policing based on DSCP marking. This achieve DoS protection and traffic prioritization. The DA Gateway queues the packets based on DSCP Marking.

Downstream QoS: From SCADA to IED

If SS router is connected to multiple IEDs, it can perform queuing functionality toward IED.
Note: QoS behavior is always on a per-hop basis. Even though the high priority traffic is prioritized at the IoT Gateway, once the traffic enters the service provider’s network, the packets are subjected to the QoS treatment as defined by the service provider. In some scenarios, the service provider could even remark all the incoming packet’s priority to default priority. It is recommended to ensure a SLA if the QoS marking done at the gateway needs to be honored by the service provider (or) at least treated as per the SLA.

Timing Synchronization

The DA Secondary Substation solution supports a multiple arrays of applications. Many of these applications process a time-ordered sequence of events; therefore, the events must be time stamped to a level of precision where individual events can be distinguished from one another and correctly ordered. Timing synchronization can be achieved by using various protocols that depend upon time accuracy and the time sources. Table 18 shows the time accuracy that might be required by different DA use cases.

<table>
<thead>
<tr>
<th>Description</th>
<th>Required Time Synchronization Accuracy</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA FLISR</td>
<td>10 to 100 ms</td>
<td>Real-time fault location and isolation</td>
</tr>
<tr>
<td>DA FLISR</td>
<td>1000ms</td>
<td>Isolation and restoration, assuming protection action happening locally</td>
</tr>
<tr>
<td>DA Volt/VAR</td>
<td>10ms</td>
<td>Integrated Volt/VAR</td>
</tr>
<tr>
<td>DA Volt/VAR</td>
<td>1000ms</td>
<td>SCADA based Volt/VAR</td>
</tr>
</tbody>
</table>

The time synchronization mechanisms available for DA solution include:

1. **NTP**—The NTP delivers accuracies of 10 to 100ms, depending upon the characteristics of synchronization sources and network paths. NTP version 4 is used and the NTP server is placed in the control center. The DA Gateways and the SSR act as a NTP client.

2. **GPS**—In the Cisco IR 800 series platform, GPS can be configured as a clock source (Cisco IOS software release 15.8.3M0a onwards).

DHCP Services

The two DHCP services used include:

- **Staging Phase of ZTD, page 58**
- **Tunnel Provisioning Phase of ZTD, page 59**

Staging Phase of ZTD

One of the four PnP server discovery mechanisms (DHCP server-assisted PnP Provisioning) uses the DHCP server to derive the PnP server details. As part of staging, while the DHCP server advertises the IP address to the IoT Gateway, PnP server details are also advertised as part of Vendor Specific Options.

For more details on this DHCP server usage, please refer to the following URL:

Tunnel Provisioning Phase of ZTD

During the tunnel provisioning phase of the ZTD, Cisco IoT FND sends out a DHCP relay request for IPv4 and IPv6 addresses on behalf of the IoT Gateway attempting ZTD. The DHCP server should be configured to allocate an IPv4 and IPv6 address for the gateway. Once Cisco IoT FND receives the IPv4 and IPv6 addresses from the DHCP server, Cisco IoT FND compiles the tunnel provisioning configuration and pushes it onto the IoT Gateway with the help of intermediate TPS. The IPv4 and IPv6 addresses configured on the IoT Gateway help Cisco IoT FND and SCADA application to uniquely identify the IoT Gateway.

Network Management System

The Network Management System (NMS) resides as part of the communication headend. The NMS of this solution is referred to as Field Network Director (FND), which is a software platform that manages the multi-service network and security infrastructure for IoT applications in this Distribution Automation solution.

Zero Touch Deployment

Zero Touch Deployment (ZTD) is a powerful process available to onboard hundreds of thousands of the SSRs and DA Gateways onto the network. These devices can be deployed on the field and be brought to a fully operational state with no manual intervention.

Note: The field technician just has to mount the devices in the desired location and power it up. The remainder is left to the ZTD process. Considering the flexibility offered by ZTD, it’s a much-needed capability particularly during scaled deployments.

ZTD happens in two stages:

- Staging of the IoT Gateway
- Deployment of the IoT Gateway

IoT Gateway, by default, comes with a factory default configuration.

As part of staging, the IoT Gateway is provisioned with the minimal configuration needed for ZTD to kick in. This is a dynamic procedure leveraging the PnP architecture. This procedure can also be referred as PnP staging.

Note: Staging could also be referred as bootstrapping.

The IoT Gateway once deployed, goes through the following procedure:

1. Receives its WAN IP address dynamically from the provider.
2. Receives Utility PKI-signed certificate dynamically through SCEP.
3. Gets a secure tunnel provisioned to the DSO headend by contacting TPS.
4. Receives the “Application traffic enabling” configuration and other device configurations while registering with FND.
5. Keeps Cisco IoT FND updated about its status through periodic updates.
For a high-level overview of the ZTD, please refer to the following URL:


For more detailed interactions between various components involved in ZTD, please refer to Cisco FAN - Headend Deep Dive Implementation and FAN Use Cases at the following URL:

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

Plug-and-Play Staging

Staging refers to the process of provisioning the minimal configuration on the Cisco IOS routers so that the router is ready for ZTD. This minimal configuration is also referred as Day 0 configuration (or) express-configuration.

Cisco IOS routers leverage the PnP agent available on the latest IOS releases to have it provisioned dynamically, with no manual intervention on the router.

Staging Location

The Cisco IoT Gateways could be unpacked, and could be bootstrapped through PnP dynamically, from either of two different locations and approaches:

- **Staging Premise**—Place dedicated for the purpose of bootstrapping the IoT Gateways. The Cisco IoT Gateways could be unpacked and bootstrapped dynamically at the staging premise, and then transported and deployed finally at the deployment location (either at the Secondary Substation or Distribution Network or at other desired places in the network).
**Deployment Location**—Actual location where the device is meant to be deployed. The Cisco IoT Gateways could be unpacked and deployed directly at the desired deployment location, altogether skipping the staging premise. Bootstrapping happens from the deployed location itself instead of from the staging premise.

**Table 19  Actors in Plug ‘n Play Staging**

<table>
<thead>
<tr>
<th>PnP Actors</th>
<th>Custom PnP Profile</th>
</tr>
</thead>
</table>
| PnP Agent    | Comes embedded in Cisco devices in the latest IOS releases. Acquires the IP address of the PnP server through DHCP or DNS or using Cisco Cloud redirection service or custom PnP profile configuration. After a PnP server is found, the agent communicates with the PnP server to perform the bootstrapping operation. PnP agent kicks in only if the startup configuration is not present on the device (router). PnP agent on the IoT Gateway must support the following PnP services:  
  - Certificate Install Service:  
    - Needed for FND to manage trust points and certificate related operations on the IoT Gateway.  
  - File Transfer Service:  
    - Needed for FND to push the configuration and ODM files to the IoT Gateway.  
  - CLI - Exec Service:  
    - Needed for FND to run show commands on the IoT Gateway.  
  - CLI - Configuration Service:  
    - Needed for FND to configure on the IoT Gateway. |
| PnP Proxy (TPS) | TPS is a stateless extension of Cisco IoT FND that is meant for processing requests from an unsecure part of the network. Typically, it is positioned in the DMZ.  
  TPS acts as a PnP proxy (behaves as server for the PnP agent) and then proxies the received PnP communication to the actual PnP server (which is FND).  
  This is an optional, but highly recommended, component. In the absence of TPS, Cisco IoT FND component has to be exposed to the unsecure part of the network, which is not recommended.  
  Listens on the following network ports for communication:  
  - Port 9125 to process the initial communication over http.  
  - Port 9120 to process the further communication over https (for communication over https to work on port 9120, the device must have certificate and a common trustpoint). |
| PnP Server (FND) | FND acts as a PnP server and resides in the secure part of the network. Typically, they are positioned in the secure data center area.  
  PnP server processes the communication from the PnP Proxy. The PnP server communicates with the PnP agent on the device using PnP protocol.  
  PnP server is responsible for provisioning the Day 0 configuration on the IoT Gateway. The required Day 0 configuration could be created as a Template under the Bootstrapping Template section of Cisco IoT FND. |
Table 19   Actors in Plug ‘n Play Staging (continued)

<table>
<thead>
<tr>
<th>PnP Actors</th>
<th>Custom PnP Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Mandatory and main actor, if the chosen staging method is <strong>DHCP server-assisted PnP provisioning</strong>.</td>
</tr>
<tr>
<td></td>
<td>Mandatory and supporting actor, if the chosen staging method is <strong>DNS server-assisted PnP provisioning</strong>.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, optional.</td>
</tr>
<tr>
<td></td>
<td>Helps the Cisco device discover the PnP server by advertising the server-related information as part of the DHCP options. If TPS is used, the TPS (instead of FND) address should be advertised as the PnP server address.</td>
</tr>
<tr>
<td></td>
<td>For bootstrapping device over IPv4 backhaul:</td>
</tr>
<tr>
<td></td>
<td>• DHCP server should advertise DHCP vendor-specific option 43, delivering the ASCII string.</td>
</tr>
<tr>
<td></td>
<td>• Sample ASCII String format: <strong>5A;K4;B1;ltps-san.ipg.cisco.com;J9125</strong></td>
</tr>
<tr>
<td></td>
<td>For bootstrapping device over IPv6 backhaul:</td>
</tr>
<tr>
<td></td>
<td>• DHCP server should advertise DHCP vendor-specific option 9, along with the following sub-options:</td>
</tr>
<tr>
<td></td>
<td>• sub-option 16 for ciscopnp</td>
</tr>
<tr>
<td></td>
<td>• sub-option 17 for the ASCII string</td>
</tr>
<tr>
<td></td>
<td>• Sample ASCII string format: <strong>5A1N;K4;B1;ltps-san.ipg.cisco.com;J9125</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This DHCP server is only from the bootstrapping context. This DHCP server could be the same as / different from the DHCP server that allocates the WAN IP address during deployment on the Secondary Substation (or) Distribution Network.</td>
</tr>
<tr>
<td></td>
<td>This option might not be applicable for the cellular network, if the IP address allocation mechanism used is IP Control Protocol (IPCP).</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Mandatory actor if the chosen staging method is <strong>DNS server-assisted PnP provisioning</strong>.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, optional.</td>
</tr>
<tr>
<td></td>
<td>In sequence, DHCP server would advertise the IP address along with DNS server IP and domain name (for example, domain.com).</td>
</tr>
<tr>
<td></td>
<td>Gateway will send out a DNS resolution request for <strong>pnpserver.domain.com</strong>.</td>
</tr>
<tr>
<td></td>
<td>DNS server helps resolve the FQDN <strong>pnpserver.domain.com</strong> to IP address of the PnP server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>pnpserver.domain.com</strong> should resolve to PnP Proxy’s IP address, when design involving TPS is chosen.</td>
</tr>
<tr>
<td></td>
<td>• <strong>pnpserver.domain.com</strong> should resolve to PnP Server’s IP address, when design involving only FND (without TPS) is chosen.</td>
</tr>
<tr>
<td></td>
<td>DNS: A record should be created if the staging network uses IPv4.</td>
</tr>
<tr>
<td></td>
<td>DNS: AAAA record should be created if the staging network uses IPv6.</td>
</tr>
<tr>
<td>Cisco Cloud Redirection Server</td>
<td>Mandatory actor if the chosen staging method is <strong>Cisco PnP Cloud Redirection Service-assisted provisioning</strong>.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, optional.</td>
</tr>
</tbody>
</table>
**Four Methods for PnP Server Discovery:**
The IoT Gateway discovers the IP address of PnP server with four different methods:

- DHCP server-assisted PnP provisioning
- DNS server-assisted PnP provisioning
- Cisco PnP Cloud Redirection Service-assisted provisioning
- Custom PnP profile for PnP server

**Note:** The Cisco IoT Gateway shouldn’t be require any startup configuration for the PnP server discovery to kick in.

**Note:** In the PnP architecture, any key press on the console of the Cisco IoT Gateway could possibly terminate the PnP server discovery procedure, as it’s a manual intervention on the router.

**Figure 40 PnP Server Discovery Flow**

Note: In environments using TPS as PnP Proxy, PnP Proxy IP/FQDN must be advertised in place of PnP server IP/FQDN.

The PnP agent on the Cisco router would attempt the DHCP server-assisted provisioning first; if that succeeds, the PnP discovery should complete and the router should reach out to the received PnP server for bootstrapping. The IP/FQDN address of the PnP server is obtained through vendor specific options from the DHCP server.

- Vendor Specific Option 43 is used to advertise PnP proxy/server in the IPv4 network.
- Vendor Specific Option 9 is used to advertise PnP proxy/server over the IPv6 network.

If the PnP server (Vendor Specific Option) detail is not found in the DHCP response, then the DNS server-assisted provisioning will be tried out. If this succeeds, the PnP discovery should complete, and the router should reach out to the received PnP server IP/FQDN for bootstrapping. The IP address of the PnP server is obtained through the DNS name resolution of `pnpserver.domain.com`.

If the PnP server detail is not found while trying to resolve `pnpserver.domain.com`, then the Cisco Cloud Redirection service would be tried out.

**Note:** After discovery of PnP server using DHCP, DNS, or Cloud redirection services, a PnP server profile is dynamically created on the IoT Gateway.
While the above options are completely automated ways of obtaining the IP address of the PnP server, a manual CLI approach also exists. Network administrators may use the CLI configuration mode to initiate the PnP agent process at any time. By configuring a PnP profile through CLI, a network administrator can start and stop the PnP agent on a device. When the PnP profile is configured with CLI, the device starts the PnP agent process which, in turn, initiates a connection with the PnP server using the IP address in the PnP profile.

More details about the PnP server discovery process, along with useful graphics, can be found under the “Plug-n-Play Agent Discovery Process” section of the Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E at the following URL:


Role of PnP Actors in Each PnP Server Discovery Method - Summary Matrix

Table 20 summarizes the various components required for PnP staging for each of the staging option chosen.

Table 20  Plug ‘n Play Actors in Various PnP Server Discovery Methods

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server assisted PnP Provisioning</td>
<td>Yes</td>
<td>Preferred</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Vendor Specific Options advertises PnP server details</td>
<td>Might be needed if the DHCP VSO advertises an FQDN instead of an IP address</td>
</tr>
<tr>
<td>DNS server assisted PnP Provisioning</td>
<td>Yes</td>
<td>Preferred</td>
<td>Mandatory</td>
<td>Advertises: IP address + domain name + DNS server</td>
<td>PnP server information not provided by DHCP</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Cisco Cloud Redirection service assisted PnP provisioning</td>
<td>Yes</td>
<td>Preferred</td>
<td>Mandatory</td>
<td>PnP server information not provided by DHCP</td>
<td>To resolve the Cisco Cloud redirection server</td>
<td>PnP server information not provided by DNS</td>
</tr>
<tr>
<td>Custom Profile Configuration assisted PnP provisioning</td>
<td>Yes</td>
<td>Preferred</td>
<td>Mandatory</td>
<td>Optional</td>
<td>Advertises IP address along with DNS server details</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Role of TPS PnP Proxy

TPS is a stateless extension of FND that is meant for handling requests from the untrusted part of the network. Typically, TPS, which is positioned in DMZ, is needed in scenarios where FND cannot be exposed. TPS receives the communication from the untrusted part of network and proxies it to FND located in a trusted part of the network.

Note: In the absence of TPS, FND components have to be exposed to the untrusted part of the network, which is not recommended.

In the case of PnP Bootstrapping, TPS could act as the PnP Proxy for the PnP Server (FND). During PnP Bootstrapping, if the incoming bootstrapping request uses a custom port (instead of the default port of 9125), then TPS could be configured to listen on the custom port, and, in turn, the TPS could communicate with FND on port 9125.

TPS (PnP Proxy), acting as the server for the PnP agent on the IoT Gateway, receives the communication from the PnP agent and then proxies the same to actual PnP Server (FND).
**Note:** TPS (as a PnP Proxy) is a highly recommended component for all bootstrapping scenarios crossing the WAN/Internet to reach PnP server.

**Note:** TPS (as a Tunnel proxy server) is highly recommended for all ZTD scenarios.

However, in a controlled staging environment running the private local network, FND could be connected to the local network, and made available directly for IoT Gateways to bootstrap. TPS Proxy could be made optional in such PnP Bootstrapping scenarios.

TPS Proxy serves in two different stages of ZTD:
- As PnP Proxy for Day0 configuration provisioning (also called as bootstrapping).
- As Tunnel Proxy Server for Tunnel provisioning in ZTD.

### Table 21 Use of PnP Proxy in Various Bootstrapping Methods

<table>
<thead>
<tr>
<th>Platform</th>
<th>PnP Proxy</th>
<th>Is PnP Proxy Mandatory?</th>
<th>Can ZTD TPS be the same as PnP Proxy TPS?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrapping in local staging network</td>
<td>Optional component</td>
<td>Not mandatory if the local staging network is a controlled private network</td>
<td>Probably not as the staging environment is local, ZTD TPS is reachable over Internet/WAN</td>
</tr>
<tr>
<td></td>
<td>If used, scope of the PnP Proxy could be limited to local staging network</td>
<td>PnP Server (FND) could be used directly for bootstrapping, without using TPS PnP Proxy</td>
<td>However, TPS Proxy is optional in private local staging network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exposing FND should be acceptable in controlled private local networks</td>
<td></td>
</tr>
<tr>
<td>Bootstrapping in distributed staging network</td>
<td>PnP Proxy to reside in DMZ</td>
<td>Mandatory</td>
<td>Yes, could be the same TPS/FND located in DSO control center could be used for both:</td>
</tr>
<tr>
<td></td>
<td>Faces untrusted WAN on southbound</td>
<td>PnP proxy could cater to Bootstrapping requests from the IoT Gateways located in local staging network as well as from multiple distributed staging sites</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faces trusted network on northbound connecting to PnP server (FND)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bootstrapping straight out of deployment location</td>
<td>PnP Proxy to reside in DMZ</td>
<td>Mandatory</td>
<td>Yes, could be the same Same TPS/FND located in DSO Control center could be used for both Bootstrapping as well as for Tunnel Provisioning</td>
</tr>
<tr>
<td></td>
<td>Faces untrusted WAN on southbound</td>
<td>PnP proxy could cater to Bootstrapping requests from IoT Gateways reachable from anywhere over the WAN/Internet</td>
<td></td>
</tr>
</tbody>
</table>
Two Approaches: Bootstrapping versus Deployment of IoT Gateway

Bootstrapping and deployment could exist at two separate locations or at the same location. This differentiation, which is primarily based on the location from where the device is bootstrapped, is discussed in this section.

Approach 1: IoT Gateway Bootstrapped in Staging Location but Deployed in a Different Location

In this approach, bootstrapping of the IoT Gateways are done at the dedicated staging location. Once the devices are bootstrapped successfully, they are powered off and transported to the final deployment locations.

More than one staging premise could exist. The PnP proxy/server could either be located locally in the staging premise or could be located in some central premise securely connected over WAN, thus catering to distributed staging premises.

In Figure 41, the local staging premise hosts PnP Proxy/Server locally within the premise. This could be an entirely private connection. Internet connection may not be needed.

On the left, "N" number of distributed staging premises are connected to the centrally hosted PnP Proxy over a WAN network. The common bootstrap template could be maintained at one central PnP server, with many distributed sites catering to the staging of the IoT Gateway.

**Figure 41  Bootstrapping of IoT Gateway at the Staging Premises (Local vs Distributed)**

*Note:* Bootstrapping could be done over IPv4 Network or IPv6 Network.

*Note:* IR1101 also supports bootstrapping over Native IPv6 Network.
As shown in Figure 42, staged IoT Gateways are deployed on the Secondary Substation and the Distribution Network and are powered up. The PnP bootstrapped IoT Gateway activates the ZTD procedure and then proceeds with:

1. Certificate enrollment to receive the certificate for the Gateway from the Utility PKI.
2. Provisioning a secure communication with the DSO control center.
3. Establishing a secure communication path between IoT Gateway and the DSO control center.
4. Enabling Utility Application Traffic as “READY TO GO” traffic to flow through the provisioned secure path.
5. Periodic updates to Cisco IoT FND by the IoT Gateway, via the provisioned secure path.

Note: IR1101 supports also ZTD over the Native IPv6 network.
Approach 2: IoT Gateway Bootstrapped Straight Out of the Deployed Location

In this approach, the IoT Gateways are bootstrapped directly out of the deployed location itself. The staging premise is not needed for this approach.

**Figure 43  IoT Gateway Bootstrapped Straight out of the Deployed Location + ZTD**

Note: Devices could be unboxed and deployed directly at the desired deployment location. The deployed device wouldn’t have gone through Bootstrapping yet.

Note: With TPS in place, the PnP proxy would represent itself as the PnP server to the IoT Gateways. All the PnP server discovery methods should be advertising the TPS details in place of the PnP server.

Unlike Approach 1: IoT Gateway Bootstrapped in Staging Location but Deployed in a Different Location, page 67, the deployed IoT Gateway will not need Day 0 configuration for the activation of ZTD process. To receive this Day 0 configuration:

1. The gateway attempts the PnP server discovery methods to discover the PnP server.
2. The IoT Gateway reaches out to the advertised PnP server for performing the bootstrapping operation.
3. As part of PnP bootstrapping, the IoT Gateway could talk to the PnP RA to obtain public certificate of the CA server (trustpoint for TPS and FND).
4. As part of the bootstrapping, the ZTD script in the IoT Gateway could be activated.
5. The PnP bootstrapped IoT Gateway, which is activated for ZTD, proceeds with further steps like Certificate Enrollment, Tunnel Provisioning, "READY to GO" provisioning of Utility application traffic, gateway monitoring, and serviceability functionality.

**Figure 43** above logically captures the two different functionalities of TPS and FND:

1. PnP functionality to bootstrap the IoT Gateway:
   - FND hosting bootstrapping template, acting as PnP server.
   - TPS acting as PnP Proxy.
Design Considerations

2. ZTD functionality to provision the secure tunnel connecting IoT Gateway with the DSO control center:
   - FND hosting the Tunnel provisioning template.
   - TPS acts as Proxy for FND. Helps provision tunnels on gateways.

Note: PnP and ZTD functionalities could both be served by the same pair of TPS/FNDs, although it is possible to host the first pair of TPS/FND exclusively for PnP Bootstrapping, and the second pair of TPS/FND exclusively for ZTD functionality.

Although Figure 43 portrays two logically separate TPS/FNDs, the TPS/FND server residing in the DSO control center could also be used to serve the purpose of PnP Proxy/Server functionality.

Certificate Considerations for PnP and ZTD

Table 22 captures the sample certificate parameter requirements of the certificate that are to be installed on the TPS/FND server.

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Common Name Requirement</th>
<th>Subject Alternate Name requirement (FQDN) - Mandatory</th>
<th>Subject Alternate Name requirement (IP) - Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>PnP TPS</td>
<td>tps.ipg.cisco.com</td>
<td>tps.ipg.cisco.com</td>
<td>IP address of the TPS</td>
</tr>
<tr>
<td>PnP FND</td>
<td>fnd.ipg.cisco.com</td>
<td>fnd.ipg.cisco.com</td>
<td>Not Required</td>
</tr>
<tr>
<td>ZTD TPS</td>
<td>tps.ipg.cisco.com</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>ZTD FND</td>
<td>fnd.ipg.cisco.com</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
</tbody>
</table>

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

ZTD, TPS, and FND must have Common Name entries match the hostname FQDN used in the URL during https communication from the IoT Gateways.

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

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

After successful Zero Touch Deployment, the IoT Gateway would:

1. Be securely connected to FND (NMS).
2. Enable communication for SCADA and other application traffic.
3. Be periodically updating FND.

Once the IoT Gateway is registered with Cisco IoT FND, the following sections describe some important serviceability aspects of FND:

- IoT Gateway Monitoring, page 71
- IoT Gateway Management, page 72
- Facilitating IoT Gateway Interfacing to handle Utility Controller Device Upgrades, page 72
- IoT Gateway Edge Compute Application Life Cycle Management, page 72
- IoT Gateway Troubleshooting, page 73
- North Bound APIs, page 73

IoT Gateway Monitoring

The IoT Gateway could be remotely monitored from Cisco IoT FND located in the control center. Summarized below are some of the monitoring aspects that could be performed from Cisco IoT FND:

- Cellular RSSI (signal strength) monitoring
- Cellular Link Traffic monitoring
- Event and Issues Monitoring, Alerts
- Router states over time: Summary status of "N" number of IoT Gateways over period of time
- Portrays high level picture of number of gateways that are Up, Down, Unheard, and so on
- Inventory details of each IoT Gateway:
  - Details about each IoT Gateway
  - Health of the Router (uptime of the router)
  - Cellular Link Settings and Active/Inactive Status
  - Cellular Link Metrics, including RSRP, RSRQ, and SNR metrics
  - Ethernet Link Metrics
  - Ethernet/Serial interface status that connects to IED/RTU
  - Ethernet/Cellular interface status that serves WAN backhaul
  - Tunnel interface status
  - Operational status, addresses assigned, traffic speed, and drops
- Location Tracking
Design Considerations

IoT Gateway Management

The IoT Gateway could be remotely managed from Cisco IoT FND located in the control center. Summarized below are some of the management aspects that could be performed from Cisco IoT FND:

- Deploy Now, Manage it Remotely
- Handling upgrading of controllers from Serial to IP with ease, by remotely handling the interfacing on the IoT Gateway
- Ability to upgrade firmware for group of IoT Gateways in one go
- Ability to remotely reconfigure one/group of device(s) to serve different application traffic. For example:
  - Enabling/disabling raw-socket remotely
  - Enabling/disabling protocol translation remotely
  - Enabling IPv4/IPv6 IED communication remotely
  - Enabling/disabling connectivity to second control center
  - Switching from raw-socket to protocol translation remotely, and vice versa
  - Remotely tweaking Traffic prioritization (QoS) to cater to application requirement
- Remotely enabling the IoT Gateway to offer DHCP service to the IED for address configuration
- Remotely enabling the IoT Gateway to offer NAT/PAT service to the IED
- Re-provisioning of backhaul from Ethernet Primary to Cellular Primary, and vice versa
- Re-provisioning of backhaul from Cellular Provider1 primary to Cellular Provider2 Primary
- Enabling/disabling the Secondary Backhaul on the IoT Gateway from FND

Facilitating IoT Gateway Interfacing to handle Utility Controller Device Upgrades

The controller device connected to the IoT Gateway, when replaced or upgraded, might require modification handling at the IoT Gateway, which could include:

- Migrating from Serial interface or Ethernet interface, or vice versa
- Migrating from IPv4 IED to IPv6 IED, or vice versa
- Migration from one Application protocol to another protocol, or vice versa
- Moving from a Serial Application protocol to an IP-aware Application protocol

Any technological upgrade to controller devices might also need any of above migrations. For such technological upgrades to the Controller devices, the compatible interfacing on the IoT Gateway could be handled remotely from the Control center using FND.

IoT Gateway Edge Compute Application Life Cycle Management

Certain IoT Gateways supports Edge Compute capabilities. Utility Customers could leverage this Edge Compute infrastructure to host custom applications to serve their custom requirements. Custom applications could be written and installed onto IoT Gateway’s Edge compute infrastructure, remotely using the IoT FND located in the control center. FND could take care of the lifecycle management of edge compute applications on the IoT Gateway’s Edge Compute platform.
Design Considerations

IoT Gateway Troubleshooting

FND provides a set of troubleshooting and recovery tools that could be used remotely from the control center. These tools include:

- Ping, trace route to verify network reachability to the IoT Gateway
- Refresh Metrics—a solicited way to retrieve latest metrics from the IoT Gateway
- Reboot—a way to remotely reload the IoT Gateway, from the control center

If the problem is not remotely resolvable, a work order could be created from the IoT FND for a particular device so that Field Technicians could be deployed for device inspection.

For more details on creating work order, please refer to the “Creating Work Orders” section of the Cisco IoT Field Network Director User Guide, Release 4.1.x at the following URL:


The IoT Device Manager (DM) is the tool (Windows-based application, installed on a laptop) that the field technicians use to download all the work orders in the Assigned state. Field Technicians could use the IoT DM to connect to the particular problematic device and resolve it locally (from the field). Field Technicians could update the work order status in the IoT DM and the status is then sent to the IoT FND.

Note: The IoT DM Field laptops are to be pre-installed with necessary certificates before downloading the work orders from the IoT FND.

For more details on Work Orders, Importing Certificates, Setting up the IoT FND connection, Synchronizing with IoT-FND, Updating Work Order status, and so on, please refer to the Cisco IoT Device Manager Installation and User Guide, Release 5.x at the following URL:


North Bound APIs

The IoT FND typically resides in the utility control center along with other utility headend operational systems. IoT FND supports the North Bound (NB) API for transparent integration with utility headend and operational systems, and manager of manager systems.

The IoT FND maintains a database of inventory information about network devices, groups, properties, metrics, and events. NB API can be used to retrieve network statistics and properties for deployed networked devices. The database could be accessed using the IoT FND NB API.

The IoT FND NB API is a Simple Object Access Protocol (SOAP) API that provides methods for:

- Read-only access to the IoT FND database
- Push-based event reporting

The NB API can send events using HTTPS. NB API clients must subscribe to IoT FND by providing a valid HTTPS URL to send events. IoT FND accepts all SSL and handshake certificates published by the NB API client (the event consumer) while making the secure connection.

For more information about Cisco IoT FND North Bound API for your IoT FND installation, see the North Bound API User Guide for the Cisco IoT Field Network Director, Release 3.0 at the following URL:

Security, High Availability & Scale

This chapter includes the following major topics:

- Security, page 74
- High Availability, page 78
- Scale, page 81

Security

To properly secure the Cisco IR/CGR routers, please refer to the following Cisco documents:

- *Cisco Guide to Harden Cisco IOS Devices* at the following URL:

For the selection of crypto configuration, it is recommended to refer to the following white paper:

- *Cisco Next-Generation Cryptography: Enable Secure Communications and Collaboration* at the following URL:

Security Management Overview in the Secondary Substation

Security across the layers is a critical aspect of the Distribution Automation solution architecture. Cisco DA solutions provide critical infrastructure-grade security for controlling access to critical utility assets, monitoring the network, mitigating threats, and protecting grid facilities. The solutions enhance overall network functionality while simultaneously making security easier and less costly to manage.
Security principles governing the architecture include the following:

- Preventing unauthorized users and devices from accessing the head-end systems
- Protecting the SSRs/DA Gateways from cyber-attacks
- Identifying and addressing relevant security threats
- Meeting relevant regulatory requirements
- Maximizing visibility into the network environment, devices, and events
- The DA solution is dual stack and thus security policies must apply to both IPv4 and IPv6
- Preventing intruders from gaining access to field area router configuration or tampering with data
- Containing malware from proliferation that can impair the solution
- Segregating network traffic so that mission-critical data in a multi-services DA solution is not compromised
- Assuring QoS for critical data flow, whereas possible DoS attack traffic is policed
- Real-time monitoring of the DA solution for immediate response to threats
- Provisioning of network security services, which allows utilities to efficiently deploy and manage DA Gateways

Access Control

Utility facilities, assets, and data should be secured with user authentication and access control. The fundamental element of access control is to have strong identity mechanisms for all grid elements: users, devices, and applications. It is equally important to perform mutual authentication of both nodes involved in the communications for it to be considered secure.

Authentication, Authorization and Accounting

In order to perform the AAA tasks, the DSO control center infrastructure must host a scalable, high-performance policy system for authentication, user access, and administrator access. The solution must support RADIUS, a fully open protocol that is the de facto standard for implementing centralized AAA by multiple vendors.

In the context of device access control, TACACS+ may be used to support command authorization on DA Gateways and SSRs.

Certificate-Based Authentication

The CGR1120, IR8xx, and IR1101 series are manufactured with an X.509-based digital certificate (IdevID) that can be used to bootstrap the device and subsequently install a utility’s own digital certificate (LdevID) by means of SCEP. Such an identity then forms the basis of AAA services performed by the router with other entities such as meters, aggregation routers, network management system, and authentication servers.

For remote workforce automation, the Cisco 1000 Series CGR comes equipped with a Wi-Fi interface that can be accessed by field technicians for configuration. In order to gain access to the device, the technician will need to be authenticated and authorized by the authentication server in the headend. For such role-based access control (RBAC), the technician’s credentials could be a username and password or a X.509 digital certificate. The credentials may be stored in the utility’s enterprise Active Directory.

To summarize, RSA algorithm is used for authentication of DA Gateways and SSRs. It is recommended to install certificates with a lifetime of five years.
Table 4 illustrates the DA Gateways that support RSA.

<table>
<thead>
<tr>
<th>Device/Application</th>
<th>Supports RSA Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGR 1120</td>
<td>Yes</td>
</tr>
<tr>
<td>HER</td>
<td>Yes</td>
</tr>
<tr>
<td>FND</td>
<td>Yes</td>
</tr>
<tr>
<td>TPS</td>
<td>Yes</td>
</tr>
<tr>
<td>IR 1101</td>
<td>Yes</td>
</tr>
<tr>
<td>IR807</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Confidentiality

Confidentiality of DA application traffic is achieved using network level encryption between the HER and the DA Gateways/SSRs. Cisco FlexVPN technology is used for network level encryption. FlexVPN is discussed in detail in Design Considerations, page 27.

Threat Defense and Mitigation

Data Segmentation

Logically separating different functional elements that should never be communicating with each other is a simple but powerful network security technique. For example, in the distribution grid, smart meters should not be communicating with Distribution Automation devices and vice versa. Similarly, traffic originating from field technicians should be logically separated from AMI and DA traffic. The Cisco Connected Grid security architecture supports tools such as VLANs and Generic Routing Encapsulation (GRE) to achieve network segmentation. To build on top of that, access lists and firewall features can be configured on field area routers to filter and control access in the distribution and substation part of the grid.

VLAN Segmentation

Design and guidance for VLAN segmentation is discussed in detail in IP Address Schema, page 27.

Firewall

All traffic originating from the SSRs and DA Gateways are aggregated at the control center tier and needs to be passed through a high performance firewall, especially if it has traversed through a public network. This firewall should implement zone-based policies to detect and mitigate threats. The Cisco ASA with FirePOWER Services, which brings threat-focused, next-generation security services to the Cisco ASA 45xx firewall products, is recommended for the solution. It provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks.
The firewall must be configured in transparent mode. The interface connecting to the HER must be configured as the inside interface and the interface connecting to the WAN link must be configured as outside, as shown in Figure 45.

**Figure 45  Firewall**

Firewalls are best deployed in pairs to avoid a single point of failure in the network. The guidelines for configuring the firewall are as follows:

- DA to headend and vice versa: ACLs should be configured to permit traffic between the DA Gateways and the HER at the ASA.

- Security levels are defined as follows:
  - NAN-facing interface-outside: 0
  - Headend-facing interface-inside: 100

Based on **Table 24**, ACLs may be configured on the firewall.

**Table 24  Firewall Ports to be Enabled for AMI**

<table>
<thead>
<tr>
<th>Application/Device</th>
<th>Protocol</th>
<th>Port</th>
<th>Port Status</th>
<th>Service</th>
<th>Exposed</th>
<th>Interface on the ASA</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPS</td>
<td>TCP</td>
<td>9120</td>
<td>Listening</td>
<td>CGR tunnel provisioning HTTPS</td>
<td>FAN</td>
<td>Outside</td>
</tr>
<tr>
<td>Registration Authority</td>
<td>TCP</td>
<td>80</td>
<td>Used</td>
<td>HTTP for SCEP</td>
<td>FAN</td>
<td>Outside</td>
</tr>
<tr>
<td>HER</td>
<td>UDP</td>
<td>123</td>
<td>Used</td>
<td>NTP</td>
<td>FAN</td>
<td>Outside</td>
</tr>
<tr>
<td>HER</td>
<td>ESP</td>
<td>-</td>
<td>Used</td>
<td>IP protocol 50</td>
<td>FAN</td>
<td>Outside</td>
</tr>
<tr>
<td>-</td>
<td>UDP</td>
<td>500</td>
<td>Used</td>
<td>IKE</td>
<td>Both</td>
<td>Outside/Inside</td>
</tr>
<tr>
<td>-</td>
<td>UDP</td>
<td>4500</td>
<td>Used</td>
<td>NAT traversal (if any)</td>
<td>Both</td>
<td>Outside/Inside</td>
</tr>
</tbody>
</table>
High Availability

High availability is achieved by designing redundancy at multiple levels in the Distribution Automation solution as listed below:

- HER Level Redundancy, page 78
- WAN Backhaul Redundancy, page 79
- Control center level; that is, dual control center and application level redundancy, which are explained in SCADA Services, page 44.

In order to meet customer’s redundancy expectations while ensuring a successful deployment, the following scenarios are evaluated in this document. For all scenarios, the assumptions are:

- The ZTD process is fully operational. The initial traffic sent during the ZTD process assumes that a CGR/IR1101/IR807 can reach the following servers via a primary backhaul network: RA, NTP, DNS, and TPS.
- Data traffic, DA IPv4 traffic to SCADA server, IPv6 MAPT traffic to MAPT Border router, and NMS traffic to IoT FND are sent encrypted over a FlexVPN tunnel.
- Network services, such as DHCP, NTP, and AAA, must be fully operational.
- When a FlexPN tunnel failover from a high speed to low speed links designed QoS policy should work seamlessly.
- Policies regarding routing, network services, and QoS can be pushed to the DA Gateways through IoT FND.

HER Level Redundancy

This scenario primarily addresses a potential failure of an aggregation HER:

- IR1101, IR807, and CGR11120, acting as FlexVPN spokes and deployed with a single or dual backhaul interface, connect to ASR 1000 aggregation routers in a multi-hub scenario.
- Backhaul interface may be any supported Cisco IOS interface’s type: cellular and/or Ethernet.
- Two ASR 1000s or more (multi hub) in the same Layer 2 domain can terminate the FlexVPN tunnel setup with a spoke.
- A single FlexVPN tunnel is configured to reach one of the ASR 1000s.
- A FlexVPN tunnel configured for both IPv4 and IPv6 traffic, including IPv6 multicast for the WPAN use cases.
- Routing over the FlexVPN tunnel can be IKEv2 prefix injection through IPv4/IPv6 ACL (preferred) or dynamic routing, such as Multi-Protocol BGP (MPB-BGP).

This scenario may also be applicable to the dual SIM case on cellular interface.
HER redundancy is achieved using the FlexVPN load balancer. Failover between HERs will be automatically managed by the FlexVPN load balancer function. The FlexVPN load balancer feature provides a Cluster Load Balancing (CLB) solution.

ASR 1000s act as a FlexVPN server. Remote spokes (IR1100, CGR1Ks, and IR807) act as FlexVPN clients. The FlexVPN server redirects the requests from the remote spokes to the Lease Loaded Gateway (LLG) in the HSRP cluster. An HSRP cluster is a group of FlexVPN servers in a Layer 3 domain. The CLB solution works with the Internet Key Exchange Version 2 (IKEv2) redirect mechanism defined in RFC 5685 by redirecting requests to the LLG in the HSRP cluster.

For the ASR 1000 configuration, the HSRP and FlexVPN server (IKEv2 profile) must be configured. For the spoke configuration, the FlexVPN client must be configured. The IoT FND NMS must be able to configure HSRP on the ASR 1000 in addition to the FlexVPN server feature set. In case of any HER failure, tunnels are redirected to other active HER. If the Master fails, one of the Slaves resume the role of Master.

**WAN Backhaul Redundancy**

This scenario addresses the potential failure of a WAN backhaul path.

- SSRs/DA Gateway are deployed with dual backhaul interfaces that connect different aggregation routers.
- The backhaul interface may be a combination of any Cisco IOS-supported interface’s type: Cellular or Ethernet.
- **WAN Backhaul Redundancy** can be designed with multiple options:
  - Option 1: Single Tunnel FlexVPN tunnel pivot dual backhaul interfaces (dual ISP)
  - Option 2: Double Tunnel (Active/Active) and dual ISP
Single Tunnel FlexVPN Tunnel Pivot

The single FlexVPN tunnel approach may leverage the IKEv2 Tunnel Pivot feature when configuring the FlexVPN client on the DA Gateway or SSR. Both backhaul interfaces are configured as “up,” but traffic is only forwarded over a single backhaul interface at a time. Each backhaul interface can be associated with a different ISP. A “primary” backhaul interface is identified for initializing the ZTD communications. WAN monitoring based on IP SLA can be used to detect a physical interface or path failure and activate the redundancy.

For more details on WAN monitoring features, refer to the *Cisco IR800 Integrated Services Router Software Configuration Guide* at the following URL:


**Figure 47 FlexVPN Tunnel Pivot**

Double FlexVPN Tunnel

This design is ideal for active/active deployments. Two active FlexVPN tunnels via two different backhaul interfaces connect via different ISP (one tunnel per ISP) terminating on two different HERs. This FlexVPN multi-WAN resiliency enables dual backhaul interface redundancy as well as dual WAN or ISP failover. FlexVPN provides the capability to configure two active FlexVPN tunnels between the DA Gateways and the HERs.

This design will work for DSO control center redundancy. Creating and maintaining two tunnels may add complexity to the ZTD process and configuration while a single tunnel approach can also leverage the IKEv2 Load Balancer function to select the appropriate ASR 1000 per WAN path and ensure ASR 1000 redundancy.
Scale

The following scaling parameters have been factored in for the Distribution Automation HER design and implementation:

**Control Plane**
- ASR 1000 HER can support 10k tunnels and 10k IKEv2(IPV4) prefixes.
- Hardware combination to achieve this control plane scaling are ASR 1004 RSP2 ESP40 or ASR 1002-X.

**Data Plane**
- ASR1004 ESP40 can support 7.4 Gbps of data plane throughput.
- ASR1002-X can support 4 Gbps of data plane throughput.

**FlexVPN Load Balancer Feature Scaling**
- FlexVPN load balancer feature scale was validated up to 30k IKEv2 sessions.

**HER Scale Guidance**
- HERs needs to deployed a cluster running FlexVPN load balancer feature.
- Per cluster can handle 30k sessions from spokes and the assumption is one session/tunnel per spoke to the hub cluster.
- As each ASR 1000 can support 10k tunnels, to handle 30k tunnels, at a minimum, three ASR 1000s per cluster are needed. Considering n+1, four ASR 1000s will be used per cluster (one master, three slaves).
- Total number of such clusters needed for 100k scale = 100k/30k = Four.
- Therefore, using IKEv2 CLB, a scale of 100k tunnels with four regional clusters having four ASR 1000 per cluster (effectively 16 hub routers) can be achieved.
- Each cluster, if deployed with ASR 1004 and RSP2 ESP40 hardware combination, can aggregate 3*7.4 Gbps = 22.2 Gbps of throughput traffic from SSRs and DA Gateways.
Each cluster can aggregate approximately 22 Gbps of traffic for more throughput ESP 100 or ESP 200 forwarding engine on ASR 1000 needs to be selected.

DSO used to organize their operations by splitting into multiple Regional NOCs, which aggregate the traffic multiple Secondary Substation and DA Gateways in that region. Regional NOCs connectivity design is beyond the scope of this document.

The DA solution recommendation would be to install four ASR 1000s with hardware combination ESP40 and RSP2 to run as cluster using the FlexVPN load balancer in each Regional NOCs, as depicted in Figure 49.

**Figure 49  HER Scale Design**

Note: IoT FND currently provisions and manages 10000 DA Gateways or SSRs. 30000 scale support is in the solution roadmap.

### Architecture Summary

- The Cisco DA Solution provides multi-service, secured, and converged architecture for various Distribution Automation use cases.
- Cisco’s DA Gateway or SSR plays a crucial role in the Distribution Automation solution architecture.
- Choosing the correct DA Gateway model, according to requirements of the Distribution Automation use cases, will be key.

Please refer to Table 25 for details..

### Table 25  Selection Criteria for DA Gateway/SSR

<table>
<thead>
<tr>
<th></th>
<th>CGR 1120</th>
<th>IR 1101</th>
<th>IR807</th>
<th>IR809</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Substation Router</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DA Gateway</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Modularity</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Edge Compute</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
<td>Yes</td>
</tr>
<tr>
<td>Dual LTE</td>
<td>Yes</td>
<td>Upcoming</td>
<td>NA</td>
<td>Yes</td>
</tr>
<tr>
<td>Dual SIM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cisco DA Gateway or SSR provides various interfaces for connecting modern IEDs and legacy RTUs with centralized SCADA applications in the control center.

The Cisco DA solution provides secure way of provisioning of DA Gateways using the ZTD process and PnP-based staging.

Cisco DA Gateways can be provisioned for IED-to-SCADA or IED-to-SCADA via RTU application flows.

Cisco DA Gateways can replicate or route DA application traffic to dual Control Centers to provide application-level redundancy.

Cisco DA Gateways have multiple backhaul options like Cellular and Ethernet. Backhaul redundancy with WAN monitoring feature for detecting failure between backhauls can be provisioned.

Cisco DA Gateways provide SCADA Gateway service to convert legacy serial traffic to IP or it can transport serial traffic to control center using the raw sockets feature.

Cisco DA Gateway provides value-added services like network level encryption, NAT, NTP, DHCP, Edge compute, and QoS.

Cisco Headend blocks provide firewall and PKI services.

HER routes application traffic to various SCADA applications and can provide VRF services to segregate different applications.

---

<table>
<thead>
<tr>
<th></th>
<th>CGR 1120</th>
<th>IR 1101</th>
<th>IR807</th>
<th>IR809</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Supply</strong></td>
<td>Integrated AC/DC</td>
<td>9.6 - 60V DC</td>
<td>Minimum and maximum</td>
<td>Nominal voltage:</td>
</tr>
<tr>
<td></td>
<td>power supply: 3-phase AC</td>
<td></td>
<td>voltage: 9.6 to 60V DC</td>
<td>12-48V DC</td>
</tr>
<tr>
<td></td>
<td>power supply: 100-240 VAC</td>
<td></td>
<td>Maximum and</td>
<td>Min/max voltage: 9.6</td>
</tr>
<tr>
<td></td>
<td>10.6-52 VDC (nominal),</td>
<td></td>
<td>minimum current:</td>
<td>- 60V DC input Max,</td>
</tr>
<tr>
<td></td>
<td>9-60 VDC (maximum)</td>
<td></td>
<td>1.04A (9.6V DC) and</td>
<td>Min current: 3A, 0.5A</td>
</tr>
<tr>
<td><strong>Serial</strong></td>
<td>Two</td>
<td>One RS232 DTE port</td>
<td>Two RS-232 ports</td>
<td>2 x RJ45 (1xRS-232</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>and 1xRS232/RS-485)</td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
<td>Two Gigabit Ethernet</td>
<td>One Gigabit copper or</td>
<td>Two 10/100BASE-T</td>
<td>Two x RJ45</td>
</tr>
<tr>
<td></td>
<td>Combination Ports (10/100</td>
<td>SFP combination port</td>
<td>fast Ethernet ports</td>
<td>10/100/1000Mbs</td>
</tr>
<tr>
<td></td>
<td>Copper, 100/1000 SFP)</td>
<td>4 10/100 Fast Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Six 10/100 Fast</td>
<td>Copper Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethernet Copper</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>16-23 Watts</td>
<td>10/13 Watts</td>
<td>Typical: 6.7W</td>
<td>Maximum 19 Watts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum: 10W</td>
<td></td>
</tr>
<tr>
<td><strong>Din rail</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Vertical mount</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>IP Rating</strong></td>
<td>IP30</td>
<td>IP30</td>
<td>IP30</td>
<td>IP30 (vertical)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IP31 (horizontal)</td>
</tr>
</tbody>
</table>

---

Table 25 Selection Criteria for DA Gateway/SSR (continued)
Appendix A: Related Documentation

- The Cisco DA solution architecture provides HER clustering as a scalable approach for aggregating application traffic from DA Gateways and SSRs.

- Cisco NMS IoT FND can manage various DA Gateways and edge applications.

In short, the Cisco DA solution enables the DSO to seamless migrate existing legacy applications and enables advanced applications like Integrated Volt/VAR and fully automatic FLISR and new DA applications like Distributed Energy Resources and microgrids.

Appendix A: Related Documentation

- Field Area Networks on Cisco.com at the following URL:

- Cisco IoT Field Network Director User Guide, Release 4.1.x at the following URL:

- Cisco FAN - Headend Deep Dive Implementation and FAN Use Cases at the following URL:

- Connected Utilities - Field Area Network 2.0 Design and Implementation Guide at the following URL:

- Connected Utilities Virtual RTU Implementation Guide at the following URL:

- Cisco Next-Generation Cryptography: Enable Secure Communications and Collaboration White Paper at the following URL:

- Cisco Guide to Harden Cisco IOS Devices at the following URL:

- Cisco 1000 Series Connected Grid Routers Data Sheet at the following URL:

- Cisco 807 Industrial Integrated Services Routers Data Sheet at the following URL:

- Cisco 809 Industrial Integrated Services Routers Data Sheet at the following URL:

- IR1101 Industrial Integrated Services Router Hardware Installation Guide at the following URL:
## Appendix B: Glossary

The following table lists acronyms and initialisms used in this document:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>AD - Active Directory</td>
</tr>
<tr>
<td></td>
<td>AMI - Advanced Meter Infrastructure</td>
</tr>
<tr>
<td></td>
<td>AMP - Advanced Malware Protection</td>
</tr>
<tr>
<td></td>
<td>ASA - Cisco Adaptive Security Appliances</td>
</tr>
<tr>
<td></td>
<td>AVC - Application Visibility Control</td>
</tr>
<tr>
<td>C</td>
<td>CA - Certificate Authority</td>
</tr>
<tr>
<td></td>
<td>CBC - Capacitor Bank Controller</td>
</tr>
<tr>
<td></td>
<td>CGRs - Cisco Connected Grid Routers</td>
</tr>
<tr>
<td></td>
<td>CLB - Cluster Load Balancing</td>
</tr>
<tr>
<td></td>
<td>CROB - Control Relay Output Block</td>
</tr>
<tr>
<td>D</td>
<td>DA - Distribution Automation</td>
</tr>
<tr>
<td></td>
<td>DER - Distributed Energy Resources</td>
</tr>
<tr>
<td></td>
<td>DHCP - Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td></td>
<td>DM - IoT Device Manager</td>
</tr>
<tr>
<td></td>
<td>DMS - Distribution Management System</td>
</tr>
<tr>
<td></td>
<td>DMVPN - Dynamic Multipoint Virtual Private Network</td>
</tr>
<tr>
<td></td>
<td>DNS - Domain Naming Server</td>
</tr>
<tr>
<td></td>
<td>DPD - Dead Peer Detection</td>
</tr>
<tr>
<td></td>
<td>DSO - Distribution System Operator</td>
</tr>
<tr>
<td></td>
<td>DTM - Dynamic Synchronous Transfer Mode</td>
</tr>
<tr>
<td></td>
<td>DVTI - Dynamic Virtual Tunnel Interfaces</td>
</tr>
<tr>
<td>E</td>
<td>ECC - Elliptic-curve cryptography</td>
</tr>
<tr>
<td>F</td>
<td>FAN - Field Area Network</td>
</tr>
<tr>
<td></td>
<td>FCAPS - Fault, Configuration, Accounting Performance, and Security</td>
</tr>
<tr>
<td></td>
<td>FLISR - Fault Location Isolation and Service Restoration</td>
</tr>
<tr>
<td></td>
<td>FND - Field Network Director</td>
</tr>
<tr>
<td></td>
<td>FND-DB - Field Network Director Database</td>
</tr>
<tr>
<td>G</td>
<td>GIS - Geological Information System</td>
</tr>
<tr>
<td></td>
<td>GOOSE - Generic Object Orient State Event</td>
</tr>
<tr>
<td></td>
<td>GRE - Generic Routing Encapsulation</td>
</tr>
</tbody>
</table>
## Appendix B: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H</strong></td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>HMI</td>
<td>Hot Standby Router Protocol</td>
</tr>
<tr>
<td>I</td>
<td>Intelligent electronic device</td>
</tr>
<tr>
<td>IED</td>
<td>Internet Key Exchange v2</td>
</tr>
<tr>
<td>IKEV2</td>
<td>IP Control Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td><strong>L</strong></td>
<td>Least Loaded Gateway</td>
</tr>
<tr>
<td>LLG</td>
<td>Meter Data Management</td>
</tr>
<tr>
<td>MDM</td>
<td>Manufacturing Message Specification</td>
</tr>
<tr>
<td><strong>N</strong></td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NAT</td>
<td>Next Hop Resolution Protocol</td>
</tr>
<tr>
<td>NHRP</td>
<td>Network Management System</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Operating Center</td>
</tr>
<tr>
<td>NOC</td>
<td>NPS Microsoft Network Policy Server</td>
</tr>
<tr>
<td>NPS</td>
<td>NTP Network Time Protocol</td>
</tr>
<tr>
<td>O</td>
<td>Outage Management System</td>
</tr>
<tr>
<td>OMS</td>
<td>PAC Protection, Automation and Control</td>
</tr>
<tr>
<td>PAT</td>
<td>PAC Protection, Automation and Control</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>R</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RA</td>
<td>Remote Control Switch</td>
</tr>
<tr>
<td>RCS</td>
<td>Remote Fault Indicator</td>
</tr>
<tr>
<td>RFI</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>RTU</td>
<td>Secondary Substation Routers</td>
</tr>
<tr>
<td>S</td>
<td>SAIDI System Average Interruption Duration Index</td>
</tr>
<tr>
<td>SAIFI</td>
<td>System Average Interruption Frequency Index</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCEP</td>
<td>Simple Certificate Enrollment Protocol</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SSR</td>
<td>Secondary Substation Routers</td>
</tr>
</tbody>
</table>
## Appendix B: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TPS</td>
<td>Tunnel Provisioning Server</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Routing and Forwarding</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>ZTD</td>
<td>Zero Touch Deployment</td>
</tr>
</tbody>
</table>