Connected Utilities Virtual RTU Implementation Guide

This implementation guide includes the following major sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction, page 1</td>
<td>Introduction to the Virtual RTU application and SCADA protocol matrix supported by Virtual RTU.</td>
</tr>
<tr>
<td>System Overview and Components, page 9</td>
<td>Overview of system topology and description of the hardware and software components used in the Virtual RTU system.</td>
</tr>
<tr>
<td>Lifecycle Management Implementation, page 11</td>
<td>Implementation details of the Lifecycle Management with reference to Virtual RTU and IR809.</td>
</tr>
<tr>
<td>SCADA Protocol Translation Use Case using Virtual RTU, page 27</td>
<td>Implementation details of Virtual RTU protocol translation use cases.</td>
</tr>
<tr>
<td>Limitations, page 60</td>
<td>Description of Virtual RTU system limitations.</td>
</tr>
<tr>
<td>References, page 60</td>
<td>List of references that are relevant to Virtual RTU.</td>
</tr>
<tr>
<td>Glossary, page 61</td>
<td>Acronyms and initialisms used in this document.</td>
</tr>
</tbody>
</table>

Introduction

This section includes the following topics

- Overview, page 1
- Audience and Scope, page 2
- Implementation Workflow, page 3

Overview

This document captures implementation details of the Virtual Remote Terminal Unit (Virtual RTU) application on the Cisco IR809 router, which can be deployed as a secondary substation router in the Europe region or as a distribution automation gateway in the North America region. The Virtual RTU application's lifecycle is managed using the Cisco Fog Director. Eximprod, which provides our Supervisory Control and Data Acquisition (SCADA), is a Cisco Solution partner. The ES 200 is Eximprod's Virtual RTU application. When we use Virtual RTU terminology in this document, we are referring to the only software we have validated—the ES 200.

Use cases that have been addressed in this guide are SCADA visibility and monitoring of secondary substation IEDs, SCADA protocol translations, and lifecycle management of Virtual RTU. Later, this document will be expanded to include distribution automation use cases such as Fault Location Identification and Service Restoration (FLISR) and Volt/VAR. Finally, this information will be integrated into the Secondary Substation CVD planned efforts that are under the umbrella of the Cisco Field Area Network (FAN) Solution.
Protocol translation supported matrix support by Virtual RTU is shown in Table 1.

Table 1  Virtual RTU SCADA Protocol Translation Matrix

<table>
<thead>
<tr>
<th>Communication Protocol</th>
<th>Type</th>
<th>Communication Mode</th>
<th>Communication Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Serial RS232/RS485</td>
<td>Ethernet TCP/IP</td>
</tr>
<tr>
<td>Modbus</td>
<td>Master/Client</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Slave/Server</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DNP3</td>
<td>Master/Client</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Slave/Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC 608750–5-104</td>
<td>Master/Client</td>
<td>NA</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Slave/Server</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>IEC 61850</td>
<td>Client</td>
<td>NA</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Virtual RTU ES 200 will work as the Modbus/DNP3/T104 master to Southbound SCADA clients in the secondary substation (or distribution feeder controller) and, in turn, can act as the Modbus/DNP3 Slave to Northbound Distribution System Operator (DSO) SCADA systems. Southbound of Virtual RTU can be Ethernet or RS232 and Northbound is Ethernet TCP/IP communication.

For more details about Virtual RTU, please refer to the following URLs:


Audience and Scope

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

This guide describes how to deploy edge compute applications. Readers should be familiar with networking protocols, Network Address Translation (NAT), and SCADA protocols, and have exposure to Edge computing and Field Area Network Solution Architecture.
Implementation Workflow

**Figure 1** provides the high-level implementation flow for deploying Virtual RTU use cases.

**Figure 1   Virtual RTU Implementation Workflow**
System Use Cases

This section, which describes secondary substation monitoring, distribution automation, and SCADA Protocol translation use cases and how the use of Virtual RTU will benefit DSOs, includes the following major topics:

- Secondary Substation Monitoring, page 4
- Distribution (Feeder) Automation, page 5
- Virtual RTU and Protocol Translation, page 6

Secondary Substation Monitoring

Secondary substations are used to step down the power voltage from medium (1kv – 40 kV) to low voltage (110/220 V). A secondary substation hosts transformers and a number of devices called intelligent end devices (IEDs) such as circuit breakers, voltage sensors, reclosers, and surge protectors. IEDs are currently managed by a centralized application located at the DSO's Control Center called the SCADA. IEDs are connected to RTUs in the secondary substation. DSO SCADA software will be communicated to Remote RTUs to poll for the current register value associated with IEDs or to issue control command.

A secondary substation may also host a smart meter concentrator that collects data from the meters and performs local processing to report information back to the Control Center. Information and Communication Technology networks play a key role in connecting secondary substation RTUs to centralized SCADA systems.

In Figure 2, two different physical components are depicted: RTUs and the substation router. In the Virtual RTU use case, we are combining two different functionalities into one physical component: the Virtual RTU Eximprod ES 200 application, which will be hosted on the CISCO IR809 secondary substation router as a docker container.
System Use Cases

Distribution (Feeder) Automation

Distribution Automation (DA) refers to the monitoring and control of devices located out on the feeders themselves such as line reclosers, load break switches, sectionalizers, capacitor banks, and line regulators.

Distribution Automation is the overlay network deployed in parallel to the Distribution Feeder to enable the two-way communication between controllers used in the Distribution Feeder and Intelligence Application that is residing in the utility Control Center or substation for improving grid reliability, availability, and control.

Figure 3 depicts a typical DA system.

Two important use cases for Distribution Automation are:

- FLISR
- DA Volt/VAR regulation

DA Volt/VAR Regulation and FLISR use cases will deployed globally around the world. Cisco DA gateways such as CISCO IR809 and IR807 will be deployed 1:1 with DA controllers, including the recloser controller and capacitor bank controllers.

FLISR Use Case

Fault Location Isolation and 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 to automatically determine the location of a fault, and then 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 power supply for customers located downstream or upstream of a downed power line, fault, or other grid disturbance.

Benefits of FLISR include:

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

Volt/VAR Use Case

This use case address 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 what we use 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 takes up a certain amount of space in the wires. The more reactive power flowing on a line, the less room exists 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 a 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.

- **VAR Compensation**—Improves efficiency of energy supply by ensuring voltage and current are in phase when supplied to the customer.
- **Conservation Voltage Regulation**—During peak load, ensures the minimum required voltage level is supplied to the customer.

Most existing deployments have a centralized approach of controlling DA controllers from the DSO Control Center using SCADA applications. Utilities are moving towards distributed control approach where decisions can be made more quickly at the distribution feeder level by running customer business logic at the DA Gateway level. Cisco IR809 plays a perfect role for these deployment scenarios since we can host Virtual RTU software that allows utilities to implement customer business logic according to their requirements and needs.

Virtual RTU and Protocol Translation

Virtual RTU

Eximprod ES 200 over the Cisco IR809 series, as shown in Figure 4, is a fourth-generation (Internet of Things or IoT) SCADA RTU gateway for control, measurement, and supervision in power distribution systems. ES 200 is designed to efficiently operate secondary distribution substations, feeders, and electrical substations using modern and secure communication and automation standards.

Virtual RTU can integrate existing multi-vendor equipment and runs SCADA software without dedicated hardware. Since it is software based, RTU time to deploy and add new features can be done more quickly than with legacy hardware RTU. Security features and customer business logic can be implemented based on customer requirements.
SCADA Protocol Translation

SCADA protocol translations are needed when DSO is running different (or advance) SCADA protocols as compared to field devices in secondary substation IEDs or distribution feeder controllers. Another scenario for protocol translations is when the last mile (such as between DA gateway and field devices) is connected via a legacy RS232 connection, but the DSO connections are migrated to Ethernet TCP/IP.

Figure 5 depicts a SCADA protocol translation scenario where the DSO SCADA uses the Modbus TCP Protocol, but sensors and actuators in the secondary substation are using Distributed Network Protocol 3 (DNP3).
The SCADA protocol translation matrix supported by Virtual RTU is explained in Introduction, page 1. SCADA Protocol Translation Use Case using Virtual RTU, page 27 will discuss in detail the various SCADA protocol translation implementations.

**Note:** The protocol translations are not related to the implementation of Cisco IOS.
System Overview and Components

The solution is comprised of the Utilities Distrusted System Operator Control Center block (the green cloud in the solution topology in Figure 6), the Wide Area Network (WAN) block, and the Secondary Substation block.

The Cisco Fog Director and SCADA software are installed on the DSO. The Cisco ASR 1000 series router is acting as the Headend Router (HER/Control Center router), which terminates the encrypted tunnels from different secondary substation routers. Encrypted tunnels carry SCADA traffic. HER decrypts and routes SCADA traffic to DSO SCADA systems. The Cisco Fog Director is used for lifecycle management of the Virtual RTU application.

For more information about Cisco ASR 1000, please refer to Cisco ASR 1000 Series Aggregation Services Routers at the following URL:


Backhaul to the DSO Control Center can be Ethernet or cellular. Backhaul can be fully secured through Cisco’s VPN technologies such as Cisco Dynamic Multipoint Virtual Private Network (DMVPN) and Cisco FlexVPN.

In the topology in Figure 6, the Virtual RTU ES 200 software is installed on the Cisco IR809, which is acting as a secondary substation router. Sensors and actuators are simulated using a PC running the Triangle MicroWorks (TMW) Protocol Test Harness application. A PC running TMW is connected to the Cisco IR809 using Ethernet and serial (RS232) interfaces. This guide will be later enhanced to include Distribution Automation use cases.
Table 2 lists the hardware and software combination used in solution validation.

### Table 2 Hardware and Software Matrix

<table>
<thead>
<tr>
<th>Device</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IR809</td>
<td>Refer to the following URL: <a href="https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M2-Release-Notes.html">https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M2-Release-Notes.html</a></td>
</tr>
<tr>
<td>Cisco Fog Director</td>
<td>1.3.0</td>
</tr>
<tr>
<td>Eximprod ES 200</td>
<td>container name: inovium/es200 tag: 2.1</td>
</tr>
<tr>
<td>Distributed Test Manager (DSO Center SCADA simulator)</td>
<td>1.1.0.19</td>
</tr>
<tr>
<td>Protocol Test Harness (Southbound IED simulator)</td>
<td>3.17.3.0</td>
</tr>
</tbody>
</table>
Lifecycle Management Implementation

This section includes the following major topics:

- Cisco IR809 Prerequisite, page 11
- Cisco Fog Director, page 14
- ES 200 Lifecycle Management, page 23

Cisco IR809 Prerequisite

Image and Upgrade Details

Note: Cisco IR809 should be running with a minimum 15.6 version to support the Docker container application. For details, please refer to the release notes at the following URL:


1. Download and copy the Cisco IR809 bundle image to the Cisco IR809 flash drive.

2. Stop guest OS:

   ```
guest-os 1 stop
   ```

3. Upgrade guest OS using the following command. After upgrading, restart the router.

   ```
bundle install flash:<bundle_image_name>
   ```

4. Verify the upgrade using the following command:

   ```
   DEMO1-89-250#show platform guest-os
   Guest OS status:
   Installation: Cisco-GOS,version-1.3.2.3
   State: RUNNING
   
   DEMO1-89-250#show iox host list
   Host Name        IPV4 Address     IPV6 Address     IOX Client
   Version
   DEMO1-89-250-GOS-1   192.168.1.250    fe80::1ff:fe90:8b05                          0.4
   ```

5. Make sure you have the correct licenses:

   License UDI:

   ```
   Device#   PID                   SN
   *1        IR809G-LTE-GA-K9      JMX1941X00B
   ```

   Suite License Information for Module:'ir800'

   ```
   Suite       Suite Current     Type       Suite Next reboot
   ```

   Technology Package License Information for Module:'ir800'

   ```
   ```
Lifecycle Management Implementation

<table>
<thead>
<tr>
<th>Technology</th>
<th>Technology-package</th>
<th>Type</th>
<th>Technology-package</th>
<th>Next reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipbase</td>
<td>ipbasek9</td>
<td>Permanent</td>
<td>ipbasek9</td>
<td></td>
</tr>
<tr>
<td>security</td>
<td>securityk9</td>
<td>Permanent</td>
<td>securityk9</td>
<td></td>
</tr>
<tr>
<td>data</td>
<td>datak9</td>
<td>Permanent</td>
<td>datak9</td>
<td></td>
</tr>
</tbody>
</table>

6. **WAN interface configuration for Northbound communication towards DSO Control Center:**

   ```
   interface GigabitEthernet0
   description to WAN Backhaul
   ip address 10.10.70.89 255.255.255.0
   ip nat outside
   ip virtual-reassembly in
   duplex auto
   speed auto
   ```

7. **Internal interface to IOX:**

   ```
   interface GigabitEthernet2
   description IOX
   ip address 192.168.1.1 255.255.255.0
   ipv6 address autoconfig
   ipv6 enable
   ip nat inside
   ip virtual-reassembly in
   duplex auto
   speed auto
   iox client enable interface GigabitEthernet2
   ```

8. **Serial Interface connecting to serial devices in the substation (Southbound):**

   ```
   interface Async0
   no ip address
   encapsulation relay-line
   media-type rs232
   async mode dedicated
   ```

**Note:** Validation was done using RS232 based on the configuration above. Async0 can work in RS232 DCE mode and RS485 DCE Mode. Async1 can only work in RS232 DTE mode.

9. **Serial relay configuration:**

   ```
   line 1
   exec-timeout 0 0
   no exec
   transport preferred none
   transport input all
   transport output none
   stopbits 1
   ```

**Note:** Async0 and Async1 reserve line 1/5 and 1/6, respectively, to relay serial data to the corresponding GuestOS /dev/ttyS1 and /dev/ttyS2.

**Serial Relay Line allows Serial ports to pass traffic directly to the Guest OS**

   ```
   relay line 1 1/5 propagation
   relay line 2 1/6 propagation
   ```

**Note:** Propagation options allow the baudrate, databits, stopbits, and parity propagation from Guest OS. If propagation is present, the control parameters will be passed from the Guest OS to the IOS physical port.
10. IOS NAT:

Static NAT or Interface overload needs to be configured

```
ip nat inside source static 192.168.1.250 10.10.70.250
```

In this example, 192.168.1.250 is Guest OS IP address. We are doing Static NAT to convert into public routable IP address. Fog Director uses this public IP address to identify the device.

To preserve public IP address interface overload can be used.

A sample configuration is shown below.

```
ip access-list standard NAT_ACL
permit 192.168.0.0 0.0.255.255
ip nat inside source list NAT_ACL interface gigabitEthernet0 overload
```
11. IOX NAT:

The app obtains the IP address from a DHCP server within IOx and IOx assigns the outside port numbers if the application is deployed in NAT mode.

IOX should be configured in NAT mode for docker container applications.

The port required by application should be specified in YAML file. For the ES 200 Virtual RTU application, the Port 1731 needs to opened up.

12. LTE Backhaul and Network Layer Encryption:

Please refer to *Cisco IR800 Integrated Services Router Software Configuration Guide* at the following URL:


Cisco Fog Director

How to Install Cisco Fog Director

To install the Cisco Fog Director, please refer to the *Cisco Fog Director Reference Guide, Release 1.3* at the following URL:


The recommended version is 1.3 and above.

**Figure 9  Cisco Fog Director Version**
Adding Cisco IR809 Secondary Substation Router into Fog Director

1. From Devices, click **ADD**, as shown in **Figure 10**, and then enter the relevant details for devices such as IP address and port.

![Figure 10 Adding Cisco IR809 in Fog Director](image)

2. Once the device is added successfully, you can verify the last heard status using the option shown in **Figure 11**.

![Figure 11 Device Status](image)
Adding Docker Container ES 200 Application

The Virtual RTU Docker package.yaml will be provided by Eximprod. Refer to the following configuration for a sample file. This file needs to be loaded on your laptop/client machine running the Cisco Fog Director client application.

Edit necessary network ports. For example, specify the Northbound ports needed by the Fog Director and device parameters (such as serial interface parameters). Port 1731 will be used by the Virtual RTU. Port 2401 is be used for Northbound communication from the Virtual RTU to Control Center communication.

```yaml
Package.yaml file
descriptor-schema-version: "2.2"
info:
  name: es200_inovium_CC_DNP3_10
  description: "IOX Docker es200 v0.9"
  version: "1.0.9"
  author-link: "http://www.inovium.ro"
  author-name: "Inovium Digital Vision"

app:
cpuarch: "x86_64"
type: docker
resources:
  profile: c1.small
devices:
  -
      device-id: serial
      label: HOST_DEV0
      type: serial
      usage: "Serial Adapter"

network:
  -
      interface-name: eth0
      ports:
        tcp:
        - 1731 --------- ES200 application port
        - 2401 --------- Modbus TCP
        - 20000--------- DNP3 IP Port
        - 2404 -------- T104 port

# Specify runtime and startup
startup:
  rootfs: rootfs.tar
  target: ["/opt/es200/initProcess.sh"]
```
Adding a New Application

Click **Add New App** under the App tab in the Fog Director, as shown in Figure 12:

![Figure 12 Add New App](image)

Click the **Create from Docker image** option listed, as shown in Figure 13.

![Figure 13 Docker Image Option](image)

Fill in the required credentials in order to download the image from the repository and then choose the application's corresponding valid configuration file (*package.yaml*).

Click **SUBMIT** and wait for a successful application download.
Publishing a Newly Added Application

After successful application download, the application is ready to be published, as shown in Figure 15.

After successful publication, the application is ready for installation, as shown in Figure 16.
Installing a Newly Published App

The application can be installed on devices of interest. As part of the installation process, those devices are chosen and the networking parameters and interfaces of the device are configured, as shown in Figure 17 and Figure 18.
After clicking **ADD SELECTED DEVICES**, click **NEXT**. Modify the **Resource Profile** if needed, as shown in Figure 19.
Networking should be set to *nat-0*, as shown in **Figure 20**.

By default, Serial Device would point to *async1*, but you should change it to *async0* since the Southbound IED is connected to the async0 serial port, as shown in **Figure 21**.
A successful installation of the application will be reflected on the Cisco Fog Director portal. More details of the application will also be shown on the Cisco Fog Directory portal, as shown in Figure 22.

**Figure 22  App Installation Success**
ES 200 Lifecycle Management

Stopping ES 200 Docker Container Application from Fog Director

Click Devices to see the App running status and then click the square Stop App button to stop the application, as shown in Figure 23.

Figure 23  Stopping App
Restarting the ES 200 Docker Container Application from the Fog Director

Click **Start App** to restart the stopped application from the Fog Director, as shown in **Figure 24**.

**Figure 24  Restarting App**
Editing Parameters from the Fog Director

Stop the App. Edit **App Settings** (Network and Serial parameters) and then click **RECONFIGURE SETTINGS**, as shown in **Figure 25**. Then, re-start the App.

**Figure 25  Editing App Parameters**
Uninstalling ES 200 Docker Container Application from the Fog Director

Stop the App. Then click **Remove App** to remove the App, as shown in **Figure 26**.

**Figure 26  Removing App**
SCADA Protocol Translation Use Case using Virtual RTU

This section provides details implementation details for the following SCADA protocol translation scenarios:

- DNP3 Serial (Southbound) to DNP3 IP (Northbound) Translation Use Case, page 27
- DNP3 IP (Southbound) to Modbus TCP (Northbound) Translation Use Case, page 38
- DNP3 IP (Southbound) to T104 (Northbound) Translation Use Case, page 48

For more details on SCADA, please refer to the Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide at the following URL:


Virtual RTU acts as a master to Southbound IEDs and, in turn, acts as a slave to the DSO SCADA master.

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

DNP3

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

Reading Data (Inputs)

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

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

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

Control Operations (Output)

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

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

Cisco IR809 is connected to an actuator or sensor in the Southbound via Ethernet and uses DNP3 as the SCADA communication protocol. Virtual RTU software does the Northbound translation to DNP3 IP since the Control Center software is running the DNP3 IP SCADA application. The Southbound DNP3 actuator is simulated using the TMW Test Harness application. The Northbound DNP3 IP SCADA software is simulated using the TMW Distributed Test Manager (DTM) application.

Southbound DNP3 TMW Configuration

Channel Configuration

The Southbound serial IED is simulated using TMW software. In this example, as shown in Figure 27 and Figure 28, the serial port COM62 with Baud Rate 19200 is connected to Async0 of Cisco IR809.

Figure 27  DNP3 Channel Configuration

Async0 (line 1) has the same baud rate as the serial RTU simulator and 1/5 serial relay connecting to the Guest OS /dev/ttyS1 where the Eximprod Southbound DNP3 master application is running.
Make sure Parity is set to None, port is configured in DTR mode, StopBits is 1, and DataBits is 8.

Session-related Configuration

The DNP3 Southbound serial RTU simulator is configured as slave and the source and destination layers are configured as 1 and 1. The DNP3 Master will be running on ES 200. Link layer addresses needs to be communicated to the Eximprod team accordingly; they will configure the Virtual RTU database. See Figure 29.
Northbound DNP3 IP TMW Configuration

DNP3 IP Channel Configuration

The TMW DTM software is configured in the DNP3 IP. Master mode is used to simulate Control Center SCADA software. Port 2401 is used to communicate between the DNP3 master and slave running in ES 200. This port needs to be opened in IOX NAT mode, which will be defined in the package.yaml file. See Figure 30.

![Figure 30  DNP3 IP Channel Configuration](image)

DNP3 IP Session-related Configuration

Configure the DNP3 IP Link layer address based on Virtual RTU ES 200 database settings. See Figure 31.

![Figure 31  DNP3 IP Session Configuration](image)
DNP3 IP Advanced Settings

AutoTimeSyncIn and AutoEnabledUsnol are advance DNP3 IP settings, which need to be enabled; AutoIntegrityOnline and AutoIntegrityRestart settings need to be disabled. Please refer to Figure 32 for details.

Figure 32  DNP3 Advance IP Session Configuration
Integrity Poll Use Case

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

The integrity poll retrieves all events (Class 1, 2, and 3) and static (Class 0) data from the device. It is typically sent after device restart, loss of communication, or on a periodic basis to ensure all data is accurate. This integrity poll is executed in our case from the Northbound DTM application depicted in Figure 33 and Figure 34.

Click **Apply** and then click **OK** to initiate a poll.
Poll results for the Northbound DTM application are shown in Figure 35. Click the Show Point List option under the DNP3 IP Session.

**Figure 35  DNP3 IP Point List**

In the poll results on the Northbound simulator that are shown above, we received four register values (0, 1, 2, and 3) of binary inputs. In the Southbound IED simulator, these are mapped to register values (6, 7, 8, and 9).

Virtual RTU does the mapping of these registers, which matches the Southbound TMW application register values. Therefore, we conclude that the integrity poll is successful. See Figure 36.

**Figure 36  DNP3 IP Input Registers**

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

**Unsolicited Reporting**

DNP3 supports unsolicited reporting, which means slave devices can send updates as values change without having to wait for a poll from the master.

In our earlier Integrity polling case, we observed that Southbound Input Register # 7 is off. Southbound Register #1 is mapped as Register #7 in the Northbound. If we change the state of the Southbound register, the Northbound register state will change automatically.

After checking the state check of Input Register #1 value @ Northbound DTM application; in this case, it is **OFF**. See Figure 37.
Now change the register # 7 value to **ON** (right click and toggle) on the Southbound application, as shown in Figure 38.

Unsolicited reporting is observed on the Northbound application for Input register value #1. The current value is **ON**, as shown in Figure 39.
Control Command

In DNP3, binary output statuses registers will be used for control write operations. We will try to issue a CROB command from the Northbound DTM application to Register value #1, which will then write on Register # 7 in our case. Register Value #1 on the Northbound application is mapped to Register Value #7 in the Southbound application. If we make changes on Register value #1 on the Northbound application, which is depicted in Figure 40, we will see changes reflected in the Southbound application Register value #7.

The status check on the Southbound TMW application binary output statuses Register #7 before issuing a control command from the Northbound. We can see the binary output register #7 status is OFF in Figure 40.
Now we will issue a command from the Northbound simulator to change the state of the register to **ON**.

**Figure 41  DNP3 IP Northbound Control Command**

![DNP3 IP Northbound Control Command](image)
Command LatchOn is executed on Point Number 1 in Figure 42 above. Mode is direct. Control Code is LatchOn. Click **Apply** and then click **OK** to execute the command from the Northbound DTM application.
Binary Output Statuses Register # 7 value on the Southbound TMW application are changed from **OFF** to **ON**; this is depicted in **Figure 43**.

**Figure 43  DNP3 Southbound Register Value Changed to ON**

---

**DNP3 IP (Southbound) to Modbus TCP (Northbound) Translation Use Case**

Cisco IR809 is connected to an actuator or sensor in the Southbound via Ethernet and DNP3 IP is the SCADA communication protocol. Virtual RTU software does the Northbound translation to Modbus IP since the Control Center software is running the Modbus IP SCADA application.

- The Southbound DNP3 IP actuator is simulated using the TMW Test Harness application.
- The Northbound Modbus IP SCADA software is simulated using the TMW DTM application.

**Southbound DNP3 IP TMW Configuration**

**Channel Configuration**

The Southbound Ethernet IED is simulated using the TMW Test Harness software. In this example, port 20000 is used for communication between the Southbound IED and the Virtual RTU ES 200. See **Figure 44**.

**Session Configuration**

The DNP3 Southbound Ethernet simulator is configured as the slave and source and destination layers are configured as **1** and **1**. The DNP3 Master will be running on ES 200. The Link Layer addresses needs to be communicated to the Eximprod team and the Virtual RTU database will be configured accordingly. See **Figure 45**.
Figure 44  DNP3 Southbound DNP3 IP Configuration 1

Figure 45  DNP3 Southbound DNP3 IP Configuration 2
Northbound Modbus TCP TMW Configuration

Channel Configuration

The Northbound Ethernet SCADA Control Center is simulated using DTM software. In this example, port 2401 is used for communication between the Northbound Control Center and Virtual RTU ES 200. See Figure 46.

Figure 46 Northbound Modbus TCP Configuration

Virtual RTU ES 200

Use the following command to ensure that the corresponding applications are running.

```
DEMO1-89-250-GOS-1:~# ps -aux | grep es200
root      1188  0.1  0.5  35348  5472 ?        Ss   Sep27   1:01 /opt/es200/Watchdog -d
root      1232  1.1  0.6  38416  5956 ?        Ss   Sep27  10:53 /opt/es200/ModbusSlave -c 3 -s
/opt/es200/db/racdb.db -L0 -d -l1
root      1253  0.0  0.6  40916  6060 ?        Ss   Sep27   0:00 /opt/es200/ESRemote -s
/opt/es200/db/racdb.db -L2 -d -l1
root      1262  0.8  0.5  34712  5324 ?        Ss   Sep27   8:37 /opt/es200/MultiDataMaster -s
/opt/es200/db/racdb.db -L2 -d -l1 -i
root      1305  1.3  0.6  36876  6260 ?        Ss   Sep27  13:31 /opt/es200/ModbusMaster -c 1 -s
/opt/es200/db/racdb.db -L0 -d -l1 -i
root      2924  0.5  0.6  36520  5956 ?        Ss   Sep27   5:45 /opt/es200/DNP3Master -c 2 -s
/opt/es200/db/racdb.db -L0 -d -l1 -i
root     25540  0.0  0.0   4428   844 pts/0    S+   05:12   0:00 grep es200
DEMO1-89-250-GOS-1:~#
```
Modbus TCP (Control Center) to DNP3 IP (IED) Register Mapping

ES 200 Virtual RTU software maps and translates different registers in the DNP3 IP-aware Southbound device to the Modbus TCP protocol-aware Northbound Control Center. The sample register mappings in use by the current version of ES 200 application evaluated in the Connected Utilities Solutions lab are as shown in Figure 47.

**Figure 47 Northbound Modbus TCP Configuration**

<table>
<thead>
<tr>
<th>MODBUS IP (NorthBound)</th>
<th>DNP3 IP (SouthBound)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiscreteInputRegister</td>
<td>BinaryInput</td>
</tr>
<tr>
<td>(Register 3 &amp; 4)</td>
<td>(Register 1 &amp; 2)</td>
</tr>
<tr>
<td>InputRegister</td>
<td>AnalogInput</td>
</tr>
<tr>
<td>(Register 3 &amp; 4)</td>
<td>(Register 1 &amp; 2)</td>
</tr>
<tr>
<td>Coil</td>
<td>BinaryOutputStatuses</td>
</tr>
<tr>
<td>(Register 3 &amp; 4)</td>
<td>(Register 1 &amp; 2)</td>
</tr>
<tr>
<td>HoldingRegister</td>
<td>16bit AnalogOutputBlock</td>
</tr>
<tr>
<td>(Register 1 &amp; 2)</td>
<td>(Register 1 &amp; 2)</td>
</tr>
</tbody>
</table>
As the register mapping depicts the InputRegister in the Northbound, the Modbus Control Center is mapped to the AnalogInput Registers in the DNP3 Southbound device. The InputRegister in the Control Center should read the corresponding AnalogInputRegister values set in the DNP3 Southbound device. See Figure 48 and Figure 49.

The Southbound DNP3 IP IED AnalogInput 1 & 2 register values are translated to Modbus TCP. We could observe that register values are matching in the Northbound Control Center application.
Unsolicited Reporting

The DNP3 protocol supports unsolicited reporting. Slave devices send updates as values change, without having to wait for a poll from the master.

In Figure 50 and Figure 51, we are changing the BinaryInput Register #1 & #2 in the Southbound application and checking that the state of DiscreteInputRegister #3 & #4 values at Northbound DTM application are dynamically updated.

Figures 50 Present Value at Southbound

![Figure 50 Present Value at Southbound](image)

Figures 51 Present Value at Northbound

![Figure 51 Present Value at Northbound](image)

Changing Southbound Values

Choose BinaryInputRegister #1, right-click, and then toggle the value to ON, as shown in Figure 52. The earlier value was set to OFF.

Figure 52 Change Value at Southbound

![Figure 52 Change Value at Southbound](image)
Dynamically Updated Northbound Values

See Figure 53.

**Figure 53  Register Value Changes at Northbound**

Control Command

A status check on the Southbound TMW application Binary Output Statuses Register #1 and #2 before issuing control command from the Northbound shows that the values are set to **OFF**.

Binary output register # 1 & #2 status is OFF, as shown in Figure 54.

**Figure 54  Register Value Changes Status at Southbound**

In the example shown in Figure 55, we tried to toggle the Southbound DNP3 values from the Northbound Control Center using Modbus. As per the register mapping, we toggled Coil Register #3 and checked the corresponding register value in the Southbound device. Present Coil Register #3 value is **OFF**.

**Figure 55  Present Coil Register#3 Value**
Changing Coil Register #3 value to **ON**, as shown in *Figure 56*. The Modbus TCP Command is issued on the Control Center.

*Figure 56  Command to Toggle Coil Register#3 Value*

Check Southbound BinaryOutputStatuses Register#1 value. As stated earlier, the Southbound has a different SCADA Protocol DNP3 IP and different register Binary Output Statuses register #1. See *Figure 57*.

*Figure 57  Command to Toggle Coil Register#1*

Since DNP3 supports unsolicited reporting, the Modbus command center also reflects updated data for the Coils Register#3. See *Figure 58*.

*Figure 58  Unsolicited Reporting at Control Center*
Present Analog Output Block Register #2 Value at Southbound

On a similar exercise to the previous one, you can try changing the DNP3 Southbound 16 bit Analog Output Block Register #1 & #2 statuses by changing the Modbus Northbound Holding Register #1 & #2. See Figure 59.

Figure 59  Analog Output Register Present Value

Present HoldingRegister #2 Value at Northbound

See Figure 60.

Figure 60  Holding Register Present Value
Changing Holding Register #2 Value

See Figure 61.

Figure 61  Command to Change Holding Register Value

Changes reflected in the Southbound Binary Output Statuses Register 2 are shown in Figure 62.

Figure 62  Changes Reflected at Southbound Output Register
Unsolicited reporting in the Modbus Control Center is shown in Figure 63.

**Figure 63 Unsolicited Reporting at Modbus Control Center**

DNP3 IP (Southbound) to T104 (Northbound) Translation Use Case

Cisco IR809 is connected to the actuator or sensor in the Southbound via Ethernet and DNP3 IP is the SCADA communication protocol. Virtual RTU software does the Northbound translation to T104 since the Control Center software is running T104 SCADA application.

- Southbound DNP3 IP Actuator is simulated using TMW Test Harness application.
- Northbound T104 SCADA Software is simulated using TMW DTM Application.

Southbound DNP3 IP TMW Configuration

Channel Configuration

Southbound Ethernet IED is simulated using the TMW Test Harness software. In this example, port 20000 is used for communication between the Southbound IED and Virtual RTU ES 200.

Session Configuration

The DNP3 Southbound Ethernet simulator is configured as slave and the source and destination layer is configured as 1 and 1, as shown in Figure 64. The DNP3 Master will be running on ES 200. Link layer addresses needs to be communicated to the Eximprod Team and the Virtual RTU database will be configured accordingly.
Figure 64  DNP3 Southbound DNP3 IP Configuration

Figure 65  DNP3 Southbound DNP3 Session Configuration
Northbound T104 TMW Configuration

Channel Configuration

The Northbound Ethernet SCADA Control Center is simulated using DTM software. In this example, port 2404 is used for communication between the Northbound Control Center and the Virtual RTU ES 200. See Figure 66.

Figure 66  Northbound T104 Configuration
T104 (Control Center) to DNP3 IP (IED) Register Mapping

The ES 200 Virtual RTU software maps and translates different registers in the DNP3 IP-aware Southbound device to the T104 protocol-aware Northbound Control Center. The sample register mappings in use by the current version of the ES 200 application evaluated in Connected Utilities Solutions lab are as shown in Figure 67.

Figure 67 Northbound Modbus TCP Configuration

<table>
<thead>
<tr>
<th>T104 (NorthBound)</th>
<th>DNP3 IP (SouthBound)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-point Information (Register 3 &amp; 4)</td>
<td>Mapped to</td>
</tr>
<tr>
<td>Normalized (Register 3 &amp; 4)</td>
<td>Mapped to</td>
</tr>
<tr>
<td>Single-point Commands (Register 3 &amp; 4)</td>
<td>Mapped to</td>
</tr>
<tr>
<td>Normalized Commands (Register 1 &amp; 2)</td>
<td>Mapped to</td>
</tr>
</tbody>
</table>
Reading DNP3 Southbound Data from Northbound T104 Control Center

As the register mapping depicts Single Point Information in the Northbound T104 Control Center is mapped to the BinaryInput registers in the DNP3 Southbound device. Single Point Information in the Control Center should show the corresponding BinaryInput values set in the DNP3 Southbound device.

Northbound Control Center Single Point Information 3 & 4

See Figure 68 and Figure 69.

Figure 68  Reading Single Point Information

![Figure 68](image)

Figure 69  Southbound Binary Input Registers

![Figure 69](image)

The Southbound DNP3 IP IED BinaryInput 1 & 2 register values are translated to T104 and we could observe register values are matching in the Northbound Control Center application.
Unsolicited Reporting

DNP3 supports unsolicited reporting. Slave devices send updates as values change without having to wait for a poll from the master.

In the example shown in Figure 70 and Figure 71, we are changing the AnalogInput Register #1 & #2 in the Southbound application and checking that the state of normalized #3 & #4 values in the Northbound DTM application are dynamically updated.

**Figure 70  Present Value at Southbound**

![Figure 70](image)

**Figure 71  Present Value at Northbound**

![Figure 71](image)
Changing Southbound Values

Choose AnalogInput Register #1, right-click, and then change the value of the register, as shown in Figure 72. The earlier value was set to 0.

Figure 72  Change Value at Southbound

Dynamically Updated Northbound Values

See Figure 73.

Figure 73  Register Value Changes at Northbound
Control Command

The status check on the Southbound TMW application Binary Output Statuses Register #1 and #2 before issuing a control command from the Northbound shows that the values are set to OFF. Binary output register #1 & #2 status is OFF, as shown in Figure 74.

**Figure 74  Register Value Changes Status at Southbound**

![Data Window - "Default" View](image)

**Figure 75 shows that we tried to toggle Southbound DNP3 values from the Northbound Control Center using T104. As per the register mapping, we would toggle Single Point Commands Register #3 and check the corresponding register value in the Southbound device. The present Single-point Command Register#3 value is OFF.**

**Figure 75  Present Single Point Command Register#3 Value**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[0] Coils</td>
<td>3</td>
<td>Off</td>
<td>N/A</td>
<td>9/28/2017 11:44:52 AM</td>
</tr>
<tr>
<td>[0] Coils</td>
<td>4</td>
<td>Off</td>
<td>N/A</td>
<td>9/28/2017 11:44:52 AM</td>
</tr>
</tbody>
</table>
Changing Single Point Command Register #3 value to ON, as shown in Figure 76. T104 Command is issued on the Control Center.

Figure 76  Command to Toggle Single Point Command Register#3 Value

Figure 76 captures the control command from the Northbound application, which is configured to work in the T104 SCADA protocol. The Southbound application is configured to work in the DNP3 IP SCADA protocol. The intermediate Virtual RTU converts the T104 command into the DNP3 IP command. In this example, the Northbound register value #3 is mapped to the Southbound register value # 1. We are issuing a control command to toggle the value of register from OFF to ON, which is depicted in Figure 77.

Figure 77  Command to Toggle Single Point Command Register#1
Since DNP3 supports unsolicited reporting, the T104 command center also reflects updated data for the Single Point Command Register#3. See Figure 78.

**Figure 78  Unsolicited Reporting at Control Center**

Present Analog Output Block Register #2 Value at Southbound

On a similar exercise, one can try changing the DNP3 Southbound 16 bit Analog Output Block Register #1 & #2 statuses by changing the T104 Northbound Normalized Commands Register #1 & #2. See Figure 79.

**Figure 79  Analog Output Register Present Value**
Present Normalized Commands Register#2 Value at Northbound

See Figure 80.

Figure 80  Normalized Commands Register Present Value

Changing Normalized Commands Register #2 Value

See Figure 81.

Figure 81  Command to Change Normalized Commands Register Value ImageID: 5055
Changes Reflecting in Southbound Binary Output Statuses Register 2

See Figure 82.

Figure 82 Changes Reflected at Southbound Output Register

Unsolicited Reporting in T104 Control Center

See Figure 83.

Figure 83 Unsolicited Reporting at Control Center
Limitations

This section covers the list of open limitations in the system.

Virtual RTU ES 200 database changes based on different protocol translations need to be done manually by logging into the App console or the container needs to be pre-built with fixed database settings. Eximprod is working with the Cisco Fog Director Team to bring in support for editing the ES 200 database from Fog Director.

References

This section, which lists the documentation used in this implementation guide, includes the following major topics:

- Cisco Documentation, page 60
- Eximprod Documentation, page 60
- General Documentation, page 60

Cisco Documentation

Cisco IR809: Cisco 809 Industrial Integrated Services Routers Data Sheet at the following URL:


Cisco ASR 1000: Cisco ASR 1000 Series Aggregation Services Routers at the following URL:


Cisco Fog Director at the following URL:


Cisco IOx Data Sheet at the following URL:


Eximprod Documentation

ES 200 Data Sheet (ES 200 Supervision, Control and Communication RTU Gateway) at the following URL:


Eximprod SCADA at the following URL:


General Documentation

EuroElectric Power Distribution in Europe Facts & Figures at the following URL:

# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR</td>
<td>Cisco Aggregation Services Routers</td>
</tr>
<tr>
<td>CROB</td>
<td>Control Relay Output Block</td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
</tr>
<tr>
<td>DA</td>
<td>Distribution Automation</td>
</tr>
<tr>
<td>DMVPN</td>
<td>Dynamic Multipoint Virtual Private Network</td>
</tr>
<tr>
<td>DNP</td>
<td>Distributed Network Protocol</td>
</tr>
<tr>
<td>DSO</td>
<td>Distribution System Operator</td>
</tr>
<tr>
<td>DTM</td>
<td>TMW Distributed Test Manager</td>
</tr>
<tr>
<td>FAN</td>
<td>Field Area Network</td>
</tr>
<tr>
<td>FLISR</td>
<td>Fault Location Identification and Service Restoration</td>
</tr>
<tr>
<td>HER</td>
<td>Headend Router</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent End Devices</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>I Pv4</td>
<td>Internet Protocol Version 4</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>RBE</td>
<td>Report by Exception</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SAIDI</td>
<td>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>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TMW</td>
<td>Triangular MicroWorks</td>
</tr>
</tbody>
</table>